Table of Contents

About the Wireless Plugin ............................................................................ 4
  Wireless Network Access Device Terminology ...........................................5
  How It Works ...............................................................................................6
    About WLAN Controller/Lightweight Access Points .........................6
  Supported Wireless Vendors ......................................................................7
  What to Do .................................................................................................8

Hardware and Software Requirements .......................................................... 8
  CounterACT Requirements ....................................................................8
  Networking Requirements .....................................................................8
  WLAN Device – Read/Write Settings ..................................................9

Plugin Installation and Configuration ........................................................... 9
  Installation ..............................................................................................10
  Configuration ........................................................................................10
    General Configuration .......................................................................11
    SNMP Configuration .........................................................................12
    Permissions Configuration ...............................................................15
    Write Configuration ..........................................................................16
    Command Line Configuration ...........................................................17
    802.1X Integration ...........................................................................17
    Control Plugin Query about Lightweight Access Points ...................20
  Plugin Testing ........................................................................................22
  Troubleshooting ...................................................................................23
  Duplicate a Configuration ....................................................................23
  Import and Export Configurations .......................................................24
  Scheduled Component Backup of Wireless Plugin Configuration ...........25
  Change Connecting Appliance of WLAN Device .....................................26
  Centralized Web Authentication with Cisco Wireless LAN Controllers ......26

Display Wireless Detection Information at the Console ............................... 27

Create Policies that Manage Wireless Clients ............................................. 29
  Wireless Client Properties ...................................................................29
  Wireless SNMP Trap Criteria ................................................................31
  WLAN Device Properties ...................................................................32
  WLAN Actions .....................................................................................33
    WLAN Block Action .........................................................................33
    WLAN Role Action ..........................................................................34
Sample Policies ............................................................................................................ 39
  Wireless User Notification – Company Security and Privacy Policy...................... 39
  Block Wireless Clients Exhibiting Malicious Intent ............................................. 42
  Prevent Wireless Client Access to Organizational Server Farm.......................... 46

Displaying Wireless Inventory Information.................................................................. 49

Additional CounterACT Documentation .................................................................. 50
  Documentation Portal ........................................................................................... 50
  Customer Support Portal ...................................................................................... 51
  CounterACT Console Online Help Tools .............................................................. 51
About the Wireless Plugin

The CounterACT Wireless Plugin is designed to provide CounterACT network access control (NAC) capabilities for 802.11 WLAN controllers and autonomous access points.

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

The NAC capabilities provided by the Wireless Plugin include:

- The plugin manages Cisco WLAN controllers and access points deployed in a network. The plugin can resolve host properties that classify the various types of Cisco WLAN devices in the network – controllers, autonomous access points and lightweight access points.
- The plugin detects Cisco lightweight access points that are managed by a plugin-managed Cisco WLAN controller. Information about detected lightweight access points is reported in the Console.
- Viewing 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.
- Preventing wireless clients from connecting to the organizational network.

### Wireless Network Access Device Terminology

The following table describes several 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><strong>Autonomous Access Point</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autonomic 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><strong>Light Weight Access Point</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lightweight 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.</td>
</tr>
<tr>
<td></td>
<td>LAP</td>
<td></td>
</tr>
<tr>
<td><strong>Wireless LAN Controller</strong></td>
<td></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><strong>Wireless Client</strong></td>
<td>Wireless client</td>
<td>An endpoint that attempts to connect, or is currently connected, to a WLAN.</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.

CounterACT can instruct the WLAN device to carry out a Block MAC command, for example when wireless clients are not compliant with CounterACT 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 either a single wireless local area network (WLAN) or multiple WLANs. Each WLAN is
identified by a unique Service Set Identifier (SSID). The SSID identifies a specific wireless WLAN that can be accessed by a wireless client.

**Supported Wireless Vendors**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerohive</td>
<td>Access Points running HiveManager version 5.1</td>
</tr>
<tr>
<td>Aruba Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Aruba 200 Controllers</strong></td>
</tr>
<tr>
<td></td>
<td>- Controllers running Aruba OS version 5.x</td>
</tr>
<tr>
<td></td>
<td><strong>Aruba 620 Controllers</strong></td>
</tr>
<tr>
<td></td>
<td>- Controllers running Aruba OS version 6.1.3.x</td>
</tr>
<tr>
<td></td>
<td><strong>Aruba Instant</strong></td>
</tr>
<tr>
<td></td>
<td>- Access Points running Aruba OS 6.1.3.1-3.0.0.x</td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Controllers</strong></td>
</tr>
<tr>
<td></td>
<td>- Controllers running software version 5.0.148.0</td>
</tr>
<tr>
<td></td>
<td>- Controllers running the IOS-XE operating system, version 3.7.2E</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Aironet Access Point</strong></td>
</tr>
<tr>
<td></td>
<td>- Access Points with software version 12.4(10b)</td>
</tr>
<tr>
<td>Meru Networks</td>
<td>Software version 3.4-109</td>
</tr>
<tr>
<td>Motorola</td>
<td>WiNG software versions 5.4 and 5.8</td>
</tr>
<tr>
<td>Xirrus</td>
<td>Software version 4.0.8</td>
</tr>
</tbody>
</table>

In addition to configuring the plugin to work with these vendors, supported vendor devices must be properly configured to work with CounterACT. This typically includes controller-side configuration to support SNMP traps. For more information about these configurations, refer to the following documents:

- AeroHive: [CounterACT Wireless Plugin Integration with AeroHive Access Points Configuration Guide](#)
- Aruba Networks: [CounterACT Wireless Plugin Integration with Aruba Controllers Configuration Guide](#)
- Cisco: [CounterACT Wireless Plugin Integration with Cisco Controllers Configuration Guide](#)
- Meru Networks: [CounterACT Wireless Plugin Integration with Meru Wireless Controllers Configuration Guide](#)
- Motorola: [CounterACT Wireless Plugin Integration with Motorola Controllers Configuration Guide](#)
- Xirrus: [CounterACT Wireless Plugin Integration with Xirrus Wireless Controllers Configuration Guide](#)
What to Do

To successfully use the Wireless Plugin perform all the following tasks.

1. Verify that you have met hardware and software requirements. See Hardware and Software Requirements.
2. Install and configure the plugin. See Plugin Installation and Configuration.
3. Set up your controller to communicate with CounterACT. See WLAN Device – Read/Write Settings.
4. Test the plugin. See Plugin Testing.
5. Set up CounterACT to view wireless client detections. See Display Wireless Detection Information at the Console.
6. Create CounterACT policies that manage wireless clients. See Create Policies that Manage Wireless Clients.

Hardware and Software Requirements

This section describes software and hardware requirements.

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

CounterACT Requirements

- CounterACT version 6.3.4.0 or above is required.
- CounterACT version 7.0.0 is required for the following feature functionality:
  - In order for the Wireless Plugin to communicate using SNMPv3.
  - In order for the Wireless Plugin to work with CounterACT’s component backup feature, CounterACT 7.0.0 with Hotfix 1.7.1 or above is required.
- In order for the Wireless Plugin to work with SNMP notification traps when your Appliances run a CounterACT version that is below version 7.0.0, Switch Plugin version 8.5.2 or above is required.
- In order for the Network Function property to be resolved and reported in the Console’s NAC Detections pane for plugin-managed, WLAN devices and for detected lightweight access points, the HPS Inspection Engine Plugin is required to be running on your Appliances.

Networking Requirements

Network connectivity between the CounterACT Appliance and the controller is required.
WLAN Device – Read/Write Settings

The following WLAN device read/write settings are required. In addition, controller-side configuration is typically necessary to support SNMP traps reporting to CounterACT.

<table>
<thead>
<tr>
<th>Device</th>
<th>Integration requires:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerohive</td>
<td>Integration requires: SNMP read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>- SSH or Telnet management (write) access to apply the <strong>WLAN Block</strong> action on wireless clients</td>
</tr>
<tr>
<td>Aruba Networks Controller</td>
<td>Integration requires: Either 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 (<strong>WLAN Block</strong> and <strong>WLAN Role</strong>) on wireless clients</td>
</tr>
<tr>
<td>Cisco Controller</td>
<td>Integration requires: SNMP read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>- For Cisco controllers that run the IOS-XE operating system:</td>
</tr>
<tr>
<td></td>
<td>- CLI (SSH or Telnet) privilege mode write access to apply the <strong>WLAN Block</strong> action on wireless clients.</td>
</tr>
<tr>
<td></td>
<td>- For all other Cisco controllers:</td>
</tr>
<tr>
<td></td>
<td>- SNMP write access to apply the WLAN management actions (<strong>WLAN Block</strong> and <strong>WLAN Role</strong>) on wireless clients</td>
</tr>
<tr>
<td>Cisco Aironet Access Point</td>
<td>Integration requires: Either 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 <strong>WLAN Block</strong> action on wireless clients</td>
</tr>
<tr>
<td>Meru Networks Controller</td>
<td>Integration requires: SNMP read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>- SSH or Telnet management (write) access to apply the <strong>WLAN Block</strong> action on wireless clients</td>
</tr>
<tr>
<td>Motorola Controller</td>
<td>Integration requires: Either 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 <strong>WLAN Block</strong> action on wireless clients</td>
</tr>
<tr>
<td>Xirrus Controller</td>
<td>Integration requires: SNMP read access to perform queries</td>
</tr>
<tr>
<td></td>
<td>- SNMP write access to apply the <strong>WLAN Block</strong> action on wireless clients</td>
</tr>
</tbody>
</table>

Plugin Installation and Configuration

This section describes how to install and configure the plugin. The configuration lets you connect WLAN devices to CounterACT Appliances and assign read/write permissions used to query and block wireless clients.
**Installation**

This section describes how to install the Wireless Plugin.

**To install the plugin:**

1. Acquire a copy of the plugin in either one of the following ways, as relevant:
   a. If you are installing a Beta release of this plugin, acquire the plugin from your ForeScout representative or contact beta@forescout.com.
   b. Otherwise, navigate to the Customer Support Plugins page and download the plugin.
2. Select and save the plugin .fpi file.
3. Select Options from the Console Tools menu.
4. Navigate to and select the Plugins folder. The Plugins pane opens.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.

**Configuration**

This section describes how to configure the Wireless Plugin. Configure the Wireless Plugin to manage autonomous access points and WLAN controllers. The configured Wireless Plugin running on CounterACT Appliances is then able to execute the following plugin activities:

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

**To configure the plugin:**

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

![Wireless pane](image1.png)


![Add Wireless Device](image2.png)

**General Configuration**

1. In the **Address** field, type the IP address of the WLAN device that you are adding.

2. From the **Connecting Appliance** drop-down list, select a CounterACT device. If your CounterACT solution includes multiple Appliances connected to an Enterprise Manager, it is recommended to select an Appliance that is physically close to the controller.

3. From the **Product** drop-down list, select a WLAN device vendor.

4. (Optional) Enter comments about this controller or the configuration.
5. If you selected in the **Product** field either Aruba Controller, Motorola Controller or Cisco Aironet Access Point, the following extra fields display:
   
a. In the **Read Connection Method** section, specify how to connect to the controller.

b. In the **Write Permission** section, if you want to disable the application of plugin-provided WLAN management actions, then clear the **Enable WLAN management actions using Command Line** option. If the option is disabled, CounterACT does not apply the **WLAN Block** and **WLAN Role** actions on wireless clients that are connected to the managed controller. See [Create Policies that Manage Wireless Clients](#) for more information about blocking wireless clients.

![Add Wireless Device](image)

6. If you selected in the **Product** field Cisco Controller, then in the **Write Permission** section, the **Enable WLAN management actions** option displays. Select this option to enable the plugin to apply its WLAN management actions, the **WLAN Block** action and the **WLAN Role** action, on wireless clients that are connected to the managed controller.

7. Select **Next**.
   
a. For Aruba, Cisco, Motorola and Xirrus controllers and the Cisco Aironet access point, the SNMP page opens.

b. For Aerohive and Meru controllers, the Read page opens.

**SNMP Configuration**

The information defined in both the SNMP page and the Read page is used by the plugin to retrieve information about wireless clients connected to the WLAN device, for example, the wireless network to which the wireless client is connected.
1. For Aerohive, Aruba, Cisco, and Motorola controllers, specify whether to enable support for notification traps.

The Wireless Plugin includes SNMP support for notification traps from several controllers. This means that notification of newly connected wireless clients is received from these WLAN devices in near real-time.

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

When your Appliances are running a CounterACT version that is below version 7.0.0, working with SNMP notification traps requires CounterACT Switch Plugin version 8.5.2 or above.
2. Specify the WLAN device query interval.
   a. For Aerohive, Aruba, Cisco and Motorola controllers, the default value is 10 minutes because they support SNMP traps.
   b. For all other WLAN devices, the default value is 1 minute.
3. Configure the SNMP parameters: select an SNMP version from the **SNMP version** drop-down list.
   
   For Aruba and Motorola controllers and the Cisco Aironet access point, if you selected **Command Line** in the **Read Connection Method** section, the SNMP parameters are disabled.
   
   a. For SNMPv1 or SNMPv2c, in the **Community** field, enter a community relevant to the SNMP version that you selected.
   b. For SNMPv3, the following parameters appear:
      
      *SNMPv3 is supported by CounterACT 7.0.0 only.*

   ![SNMP Parameters](image)

   Enter a user name, and enable authentication and privacy options as required. These configuration settings must match SNMP configurations on the controller.
   
   Supported Authentication Protocols: HMAC-MD5 and HMAC-SHA
   
   Supported Encryption Protocols: DES and AES

4. In SNMP v3 communication, the Engine ID uniquely identifies each SNMP agent for queries and trap handling.
   
   a. When wireless controllers in the network use default engine IDs, the plug-in automatically discovers the engine ID value. In this case, clear the **Use Explicit Engine ID** option.
b. When wireless controllers use operator-assigned engine ID values, auto-
discovery of engine IDs may not succeed. To explicitly specify an engine
ID value, select the **Use Explicit Engine ID** option and specify the
**Engine ID Value**. For example, an explicit engine ID must be specified to
define CounterACT as a Trap Receiver in Aruba 620 controllers.

5. Select **Next**.

The next page of the wizard opens:

- Permissions page (Xirrus controller)
- Write page (Aerohive and Meru controllers)
- Command Line page (Aruba, Motorola and Cisco controllers and the Cisco
  Aironet access point)

**Permissions Configuration**

The information defined in the Permissions page is used by the plugin to request
wireless client blocking via the controller. Blocking is based on the wireless client’s
MAC address. Detected MAC addresses are blocked on all WLAN devices that are
configured to communicate with the plugin. See **WLAN Device – Read/Write Settings**
for details.

1. (Optional) When configuring the plugin to manage a Xirrus controller, select **Enable host block** to enable CounterACT to apply the **WLAN Block** action on
wireless clients that are connected to the managed controller. See **Create
Policies that Manage Wireless Clients** for more information about blocking
wireless clients.

2. Do one of the following:

   a. If the CounterACT 802.1X Plugin is not installed, select **Finish**.
   b. If the CounterACT 802.1X Plugin is installed, select **Next** and continue
      with the section **802.1X Integration**.
Write Configuration

1. (Optional) When configuring the plugin to manage an Aerohive or a Meru controller, select **Enable host block** to enable CounterACT to apply the *WLAN Block* action on wireless clients that are connected to the managed controller. See [Create Policies that Manage Wireless Clients](#) for more information about blocking wireless clients.

2. If **Enable host block** is selected, then, in the **Login Parameters** section, enter controller login credentials. These credentials are used to log in using SSH or Telnet.

3. For Meru controllers, if **Enable host block** is selected and a privileged password is required to log in to the controller, select **Enable privilege** and define the privileged password to use.
4. Do one of the following:
   a. If the CounterACT 802.1X Plugin is not installed, select Finish.
   b. If the CounterACT 802.1X Plugin is installed, select Next and continue with the section 802.1X Integration.

Command Line Configuration

A Command Line page for configuring the plugin to manage the following WLAN devices:

- Command Line for Managing the Aruba Controller
- Command Line for Managing the Motorola Controller
- Command Line for Managing the Cisco Controller
- Command Line for Managing the Cisco Aironet Access Point

Command Line for Managing the Aruba Controller

If, in the General page of the wizard, the Read Connection Method is SNMP and you cleared the Enable WLAN management actions using Command Line option, all the fields in this page are disabled.

1. In the Login Parameters section, enter controller login credentials. These credentials are used to log in using SSH or Telnet.
2. In the Miscellaneous section, specify whether CounterACT sends wireless client MAC addresses to each Aruba device with or without colons. Colons are used by default.
3. Do one of the following:
   a. If the CounterACT 802.1X Plugin is not installed, select Finish.
   b. If the CounterACT 802.1X Plugin is installed, select Next and continue with the section 802.1X Integration.

Command Line for Managing the Motorola Controller

1. In the Login Parameters section, enter controller login credentials. These credentials are used to log in using SSH or Telnet.

2. Do one of the following:
   a. If the CounterACT 802.1X Plugin is not installed, select Finish.
   b. If the CounterACT 802.1X Plugin is installed, select Next and continue with the section 802.1X Integration.

Command Line for Managing the Cisco Controller

You are only required to complete this page when configuring the plugin to manage a Cisco controller that runs the IOS-XE operating system and you want to use the WLAN Block action (the Enable WLAN management actions option is enabled in the General page). For Cisco controllers running the IOS-XE operating system, the plugin uses CLI to apply the WLAN Block action on wireless clients that are connected to such a managed controller.
1. Enable the **Use Command Line** option.

2. In the **Login Parameters** section, select from the **Connection method** drop-down, either SSH or Telnet.

3. In the **Login Parameters** section, enter the credentials that the plugin uses to log in to the controller.

4. The IOS-XE operating system requires the plugin to use CLI privilege mode write access for applying the **WLAN Block** action on wireless clients that are connected to the managed controller.

5. If the provided login credentials are not of the privilege mode type, you must select the **Enable privilege** option and then enter a privilege mode password in the **Privileged password** field.

6. Do one of the following:
   - **a.** If the CounterACT 802.1X Plugin is not installed, select **Finish**.
   - **b.** If the CounterACT 802.1X Plugin is installed, select **Next** and continue with the section **802.1X 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
Command Line for Managing the Cisco Aironet Access Point

1. In the **Login Parameters** section, enter controller login credentials. These credentials are used to log in using SSH or Telnet.

2. Do one of the following:
   - a. If the CounterACT 802.1X Plugin is not installed, select **Finish**.
   - b. If the CounterACT 802.1X Plugin is installed, select **Next** and continue with the section **802.1X Integration**.

**802.1X Integration**

If you are working with 802.1X authentication and authorization and you have installed the 802.1X Plugin on the CounterACT device, the Add Wireless Device wizard presents the 802.1X page. Options here let you:

- Ensure communication between the WLAN device and the CounterACT RADIUS server in 802.1X environments.

You should review information about 802.1X and wireless integration before working with these options.
To review 802.1X Plugin information:

1. Select Options for the Tools menu.
2. Select the Plugins folder
3. Select t **802.1X** from the Plugins pane.
4. Select Help.

---

**Control Plugin Query about Lightweight Access Points**

In order for the Wireless Plugin to detect and resolve property information about Cisco Lightweight Access Points, the Wireless Plugin queries the Cisco WLAN controller about the Cisco Lightweight Access Points that the controller manages.

The following CounterACT local property controls the frequency with which the Wireless Plugin queries a Cisco WLAN controller about the Cisco Lightweight Access Points that the controller manages:

- **conf.cisco_query_aps_internal.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.cisco_query_aps_interval.value <number of seconds>**
Plugin Testing

The Wireless Plugin test verifies the following:

- Connectivity between CounterACT 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.
- Host Query: Identifies how many wireless clients are connected to the configured WLAN device.
- SNMP Traps: This test is performed for Aruba, Aerohive, Cisco and Motorola controllers. If Enable Notification Traps is selected, this test verifies that trap configuration is enabled on the plugin configuration and that, if necessary, the required version of the switch plugin is running.

Test the plugin configuration for managing:

- A WLAN device
- Multiple WLAN devices

To run a test:

1. Select Options from the Tools menu. The Options pane opens.
2. Open the Plugins 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 CounterACT 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.

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, enter the IP address of the new controller in the **Duplicate to Single Address** field.
   b. To create multiple new instances of the selected controller, select **Duplicate to Multiple Addresses**, and select **Add** to create a list of IP addresses. You can select **Import** to import a CSV file of IP addresses.

5. Select **OK**. CounterACT 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 addresses and other device-specific fields.
3. Import the new definitions to another device. CounterACT creates new configurations based on imported data.

CounterACT 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.
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**.
   CounterACT creates wireless device configurations based on the xml file.

**Scheduled Component Backup of Wireless Plugin Configuration**

Wireless Plugin information is included as part of CounterACT’s component backup processing (see **CounterACT 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 X can only be canceled by that plugin/CounterACT device X.

**To change the Connecting Appliance of a managed WLAN device:**

1. In the Console Plugins 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 CounterACT centralized web authentication with Cisco WLCs, reference the CounterACT Centralized Web Authentication How-to Guide.
Display Wireless Detection Information at the Console

Information learned by the Wireless Plugin can be viewed in the Console Detections pane, including:

- Wireless client IP and MAC 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.

- The IP address of detected lightweight access point(s) that are managed by a plugin-managed WLAN controller.

To display/remove the display of wireless information:

1. In the Detections 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 expanded Properties folder, click the Wireless folder to expand it and display its content.
5. To add wireless information to the Detections pane table 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 remove wireless information from the Detections pane table display:
   a. In the Selected Columns pane, select from among the wireless information columns currently selected for display.
   b. Select Remove. The removed information columns display in the Available Columns pane.

7. In the Add/Remove Columns window, select Apply and then select OK.

To promptly remove the display of wireless information:
1. In the Detections pane, right-click a wireless information column heading.

2. Select Remove Column. The column is immediately removed from the Detections pane table display.
Create Policies that Manage Wireless Clients

You can use CounterACT’s policy tools to detect, evaluate and manage 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.

Wireless Client Properties

The plugin provides the following wireless clients 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>
<tr>
<td>WLAN Association Status</td>
<td>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.</td>
</tr>
<tr>
<td>WLAN Association Status Change</td>
<td>Identifies that a change in value occurred in the WLAN Association Status property.</td>
</tr>
<tr>
<td>WLAN Authentication Method</td>
<td>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.</td>
</tr>
<tr>
<td>WLAN Authentication Method Change</td>
<td>Identifies that a change in value occurred in the WLAN Authentication Method property.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WLAN BSSID*</td>
<td>Property only supported for Aruba and Cisco controllers. Identifies the BSSID of the access point to which the wireless client is connected.</td>
</tr>
<tr>
<td>WLAN BSSID Change</td>
<td>Identifies that a change in value occurred in the WLAN BSSID property.</td>
</tr>
<tr>
<td>WLAN Client Role*</td>
<td>Property only supported for Aruba and Cisco controllers. Identifies the role assigned by the access point to the wireless client.</td>
</tr>
<tr>
<td>WLAN Client Role Change</td>
<td>Identifies that a change in value occurred in the WLAN Client Role property.</td>
</tr>
<tr>
<td>WLAN Client User Agent*</td>
<td>Property only supported for Aruba mobility controllers running ArubaOS version 6.0.1 or later. Identifies the user agent running on the wireless client.</td>
</tr>
<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 CTP IP</td>
<td>Identifies the IP address of the WLAN device that is managing the wireless client.</td>
</tr>
<tr>
<td>WLAN CTP IP Change</td>
<td>Identifies that a change in value occurred in the WLAN CTP IP property.</td>
</tr>
<tr>
<td>WLAN CTP Vendor</td>
<td>Identifies the vendor of the WLAN device that manages the wireless client. This information is obtained from the Product field defined in the plugin's configuration for the relevant WLAN device (in the Console, see Options &gt; Wireless &gt; Add/Edit Wireless Device &gt; General pane/tab &gt; Product field).</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>
</tbody>
</table>
Property | Description
--- | ---
WLAN Detected Client Type Change | Identifies that a change in value occurred in the WLAN Detected Client Type property.
WLAN SSID | Identifies the SSID (service set identifier) to which the wireless client is connected.
WLAN SSID Change | Identifies that a change in value occurred in the WLAN SSID property.

* 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.

To use these properties:
1. Create or edit a policy.
2. In the Main/Sub rule dialog box, select Add from the Condition section. The Condition dialog box opens.
3. Expand the Wireless folder 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 options to apply actions to wireless clients based on SNMP traps related to wireless devices. For example, apply actions to wireless clients when CounterACT 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>WLAN Network Function*</td>
<td>Property is only supported for Cisco wireless products.</td>
</tr>
<tr>
<td></td>
<td>The plugin resolves this property with any of the following values:</td>
</tr>
<tr>
<td></td>
<td>▪ Controller - the plugin-managed WLAN device is determined to be a WLAN controller</td>
</tr>
<tr>
<td></td>
<td>▪ Autonomous AP - the plugin-managed WLAN device is determined to be an autonomous access point.</td>
</tr>
<tr>
<td></td>
<td>▪ Lightweight AP - the device is determined to be a lightweight access point that is associated with (managed by) a plugin-managed WLAN controller</td>
</tr>
<tr>
<td></td>
<td>▪ Other - the device is determined to be none of the above. This includes all wireless clients and all other supported wireless vendors.</td>
</tr>
<tr>
<td>WLAN Managing Controller</td>
<td>Property is only supported for Cisco wireless products.</td>
</tr>
<tr>
<td></td>
<td>Identifies the IP address of the WLAN controller managing the lightweight AP.</td>
</tr>
<tr>
<td>WLAN Managing Controller Change</td>
<td>Identifies that a change in value occurred in the WLAN Managing Controller property.</td>
</tr>
</tbody>
</table>

The HPS Inspection Engine Plugin resolves the **Network Function** property. Beginning with Wireless Plugin version 1.5.0, the HPS Inspection Engine Plugin resolves the **Network Function** property as follows for plugin-managed, WLAN devices:

- For a Cisco Aironet Access Point, with the value *Cisco Autonomous AP Wireless*. 
For a Cisco WLAN Controller, with the value *Cisco Controller Wireless*. For detected Cisco Lightweight Access Points that are managed by a plugin-managed WLAN controller:

- The HPS Inspection Engine Plugin resolves the **Network Function** property, with the value *Cisco Lightweight AP Wireless*.
- Running a policy that was created using the Asset Classification policy template classifies these devices in the **Network Device** group.

### WLAN Actions

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

- **WLAN Block Action**
- **WLAN Role Action**

#### 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.

- For Cisco controllers running the IOS-XE operating system, the plugin uses CLI to apply the *WLAN Block* action.
- 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. 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

The different vendors each use a different name for these roles:

- 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, CounterACT cancels the action and the relevant wireless device, once again, determines the role that is assigned to the wireless client.

Specify the following fields and options when you use the action:

<table>
<thead>
<tr>
<th>Role Name</th>
<th>The name of the role, as defined on the wireless termination point.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For Aruba controllers, this is the name of a User Role.</td>
</tr>
<tr>
<td></td>
<td>For Cisco controllers, this is the name of an Interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role Description</th>
<th>(Optional) A description of the role, or the situation that prompted role assignment. This comment is stored in the controller’s log.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Force re-authentication after role change</th>
<th>When this option is selected, existing wireless client WLAN sessions are disconnected after role assignment. This generates Disconnect and Reconnect traps when the wireless client reconnects. CounterACT authenticates the wireless client with its new role.</th>
</tr>
</thead>
<tbody>
<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 CounterACT 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 CTP IP
- Current Role
- Connectivity Status

See the following sections for vendor-specific deployment considerations:

- Using the WLAN Role Action with Aruba Controllers
- Use 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 you add Aruba controllers:

- This action requires command line interface (CLI) communication with the controller. Specify command line credentials and select CLI as the Read Connection Method
- Check the Enable WLAN management actions using Command Line option.

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.
Use 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 CounterACT 802.1X 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 you add Cisco controllers:

- This action requires SNMP communication with the controller. Specify SNMP credentials and select SNMP as the Read Connection Method.

- Select the Enable WLAN management actions option.

**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 notAuthenticated, CounterACT 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 CounterACT 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 CounterACT. 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 CounterACT 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 policy creation for commonly used policies.

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.
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 the range of IP addresses to be inspected for this policy (for example, the network production range).
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 Host 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.

4.  Enter a policy name and description.

5.  Select Next. The Scope page opens.

6.  Use the IP Address Range dialog box to define the range of IP addresses to be inspected for this policy. For example, the Building 4 network range.

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 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**.

![Image of Action dialog box with WLAN Block selected](image)

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.

![Image of Policy Wizard]

7. Use the IP Address Range dialog box to define the range of IP addresses to be inspected for this policy. For example, the production network range.
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 Connectivity Status**.
11. Verify that **Meets the following criteria** is selected.

![Image of Wireless Connectivity Status]

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.
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 CounterACT Inventory to view a real-time display of wireless device network activity at multiple levels.

The 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 **Inventory** tab from the Console toolbar.
2. Navigate to the Wireless entries. The plugin provides an Inventory view based on each of the wireless client properties supported by the plugin.
Refer to Working at the Console > Working with Inventory Detections in the CounterACT Console User's Manual or the Console, Online Help for information about how to work with the CounterACT Inventory.

Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features and functionality and integrations.
To access the Documentation Portal:

2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:

2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

Console User Manual

1. Select CounterACT Help from the Help menu.

Plugin Help files

1. After the plugin is installed, select Options from the Tools menu and then select Plugins.
2. Select the plugin and then select Help.

Documentation Portal

1. Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2016. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2016-11-02 14:18