

Campus B-02 Wireless Lab Guide

WiFi Guest Access and WIPS



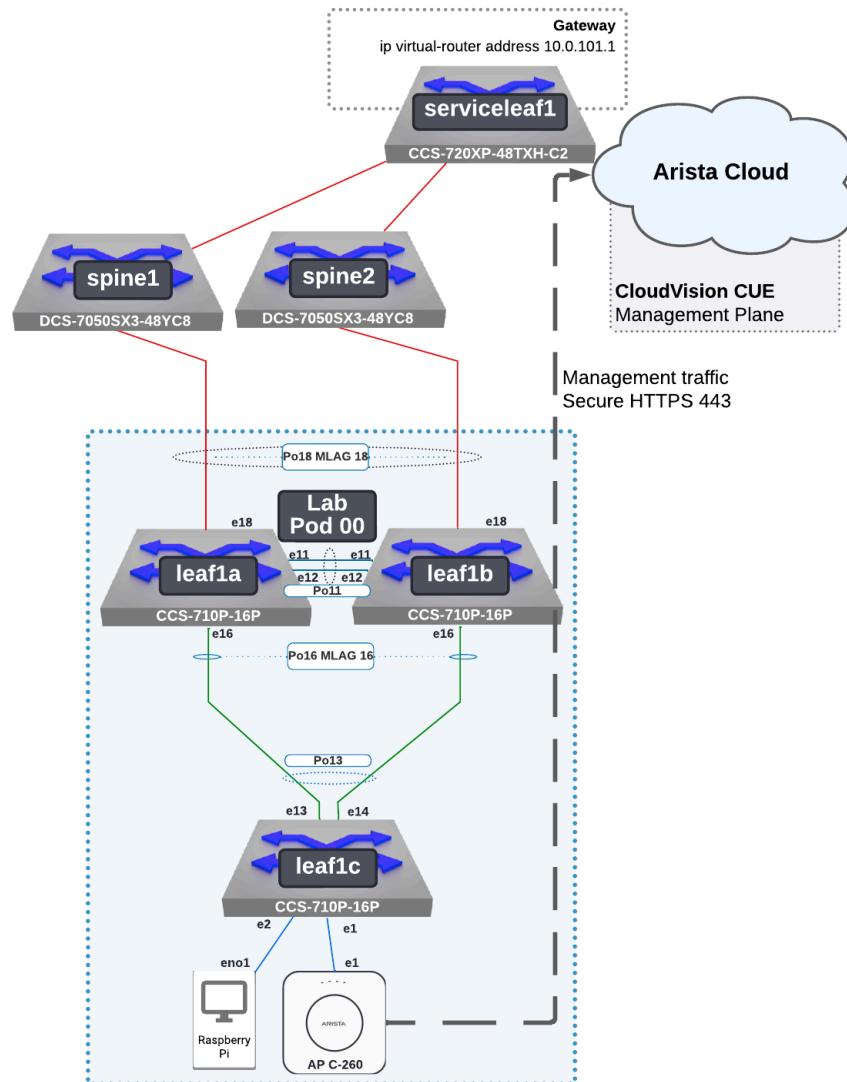
Links:

1. This Lab Guide:
 - a. <https://github.com/arista-rockies/Workshops/tree/main/Campus>
2. Lab Floor Plan Download:
 - a. <https://tinyurl.com/wififloorplan> [Arista-rockies Github]

Table of Contents

| | |
|--|-----------|
| Arista WiFi Solution Diagram..... | 2 |
| 1. Log in to CV-CUE CloudVision Cognitive Unified Edge..... | 3 |
| 2. Creating a Guest Captive Portal..... | 5 |
| 3. WIPS Wireless Intrusion Prevention System..... | 14 |
| WIPS - Classify and Prevent client..... | 20 |

Arista WiFi Solution Diagram

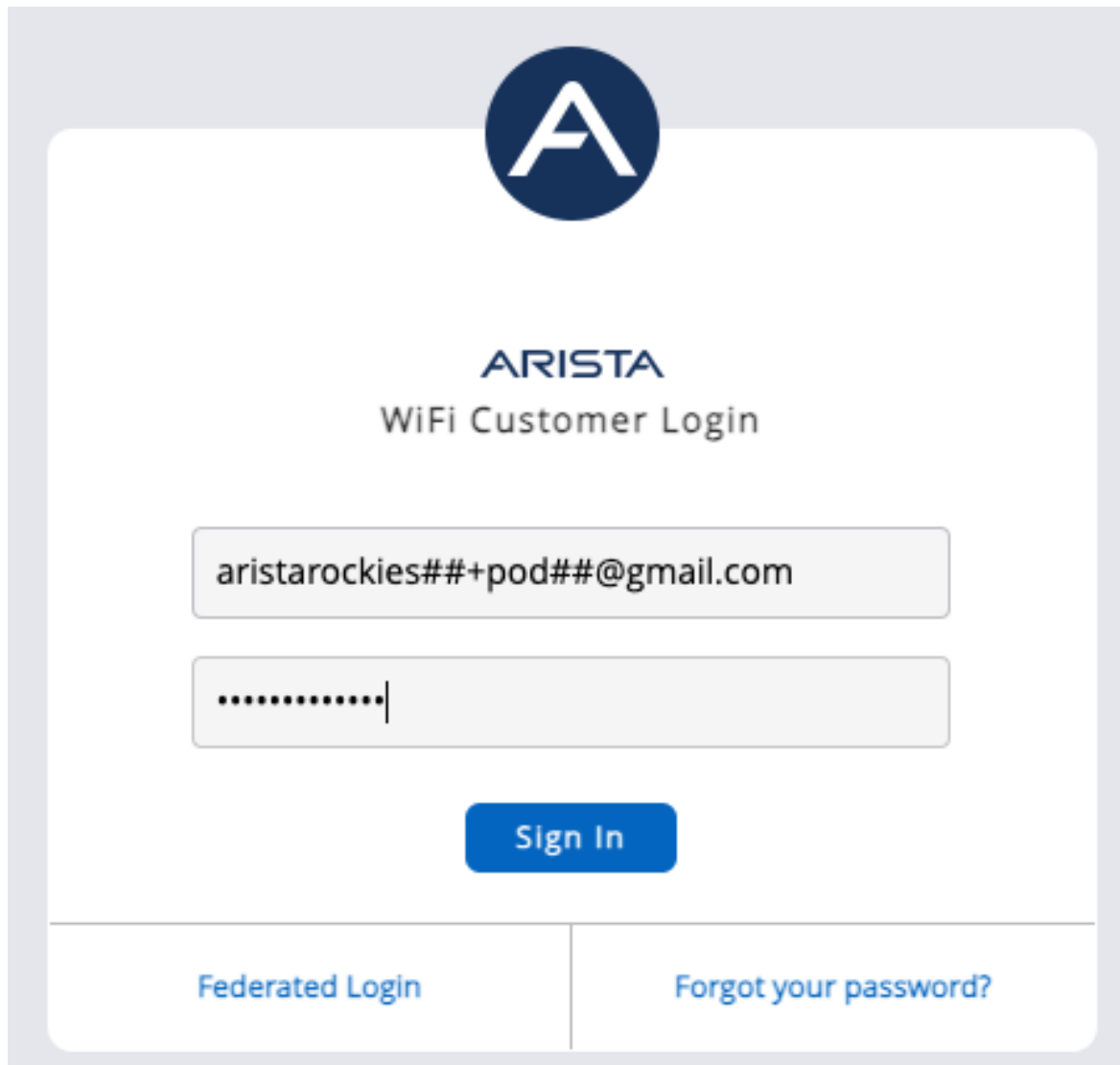



1. Log in to CV-CUE CloudVision Cognitive Unified Edge

Go to the Arista GUI via: <https://launchpad.wifi.arista.com/>

User Login is: *[Provided by event staff]*

User Passwords are: *[Provided by event staff]*

The image shows a login interface for Arista WiFi. At the top is the Arista logo, a dark blue circle with a white 'A'. Below it, the text 'ARISTA' is in a bold, dark blue font, and 'WiFi Customer Login' is in a smaller, grey font. There are two input fields: the first contains the email 'aristarockies##+pod##@gmail.com' and the second contains a masked password '.....|'. Below the password field is a blue 'Sign In' button. At the bottom, there are two links: 'Federated Login' and 'Forgot your password?'.



ARISTA
WiFi Customer Login

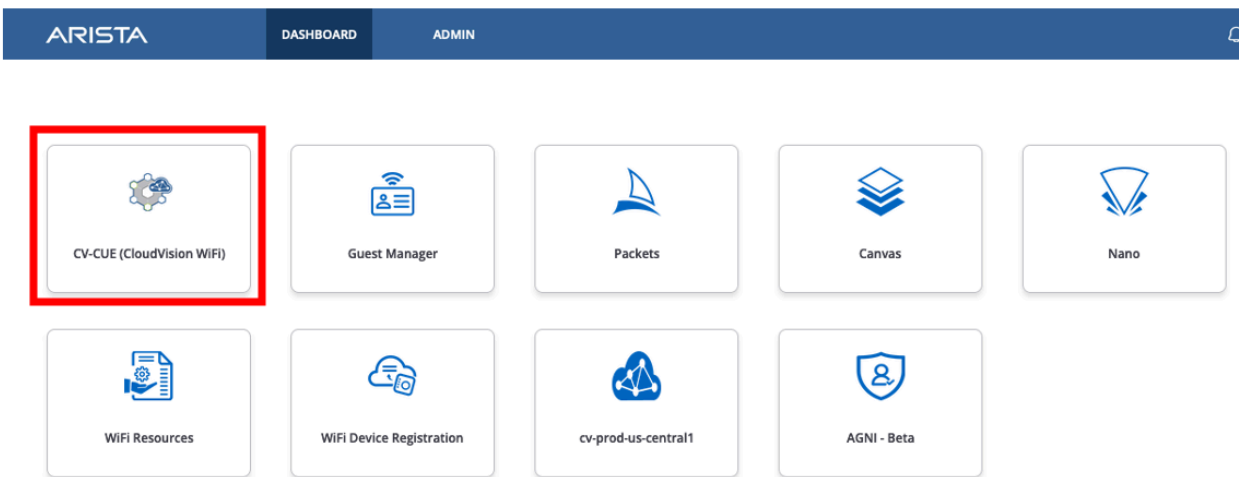
Sign In

[Federated Login](#) | [Forgot your password?](#)

Click **Sign In**

Within the Launchpad Dashboard tab:

Select CV-CUE (CloudVision WiFi). This is the WiFi management and monitoring application.



2. Creating a Guest Captive Portal

CloudVision CUE allows captive portal authentication using public cloud identity providers, social media, or your organizations own directory through SAML integration.

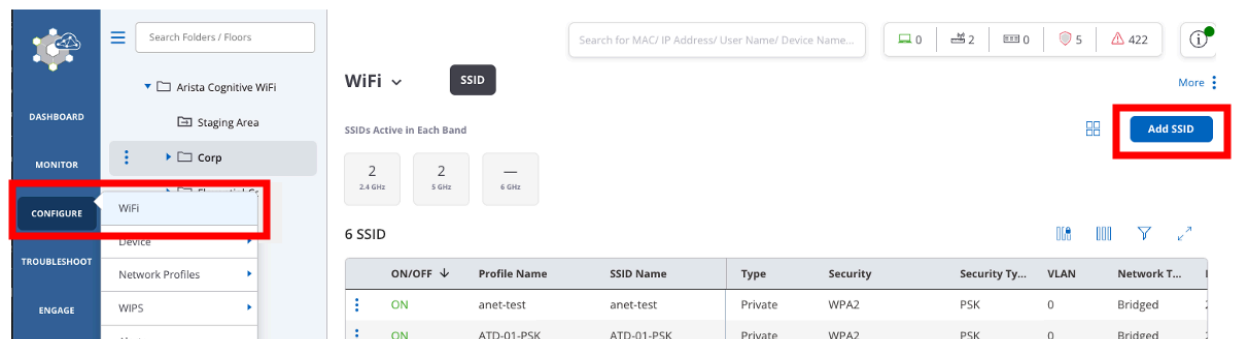
For more information about integration of a SAML identity provider reference this link:

<https://wifihelp.arista.com/post/saml-integration-with-captive-portal>

Let's now create another SSID for guest access with captive portal page.

Ensure the Corp folder is selected, then add a Guest SSID at this level using:

Configure / WiFi / Add SSID



Create a Guest SSID: **LAB-##-GUEST** (where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod) Select SSID Type: **Guest**

WiFi ▾ **SSID**

← LAB-00-GUEST

WLAN ▾ Basic Security Network Access Control Captive Portal ⋮

Name

SSID Name *

Profile Name *

Select SSID Type

☐ Private ☒ Guest

Within Security Tab, Leave the default to Open
Security - Open

WLAN ▾ Basic Security Network

Select Security Level for Associations

Open ▾

Network Tab:
VLAN ID: **0**
Network Mode: **Bridged**

WLAN ▾ Basic Security **Network** Captive Portal ⋮

VLAN *

☒ VLAN ID ☐ VLAN Name

[0 - 4094]

Network Mode

☒ Bridged ☐ NAT ☐ L2 Tunnel ☐ L3 Tunnel

Access Control - Select Client Isolation

WiFi ▾ **SSID**

← LAB-00-GUEST

WLAN ▾ Basic Security Network **Access Control** Captive Portal ⋮

▸ Firewall

☐ Client Authentication

☐ Role Based Control This setting is not editable because of certain other settings. [Change S](#)

☐ DHCP Fingerprinting based Access Control

☐ Bonjour Gateway

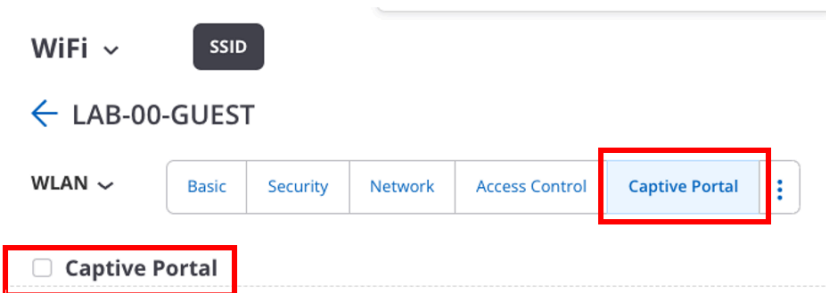
☐ Redirection

☐ WiFi Clients in Allow List or Deny List

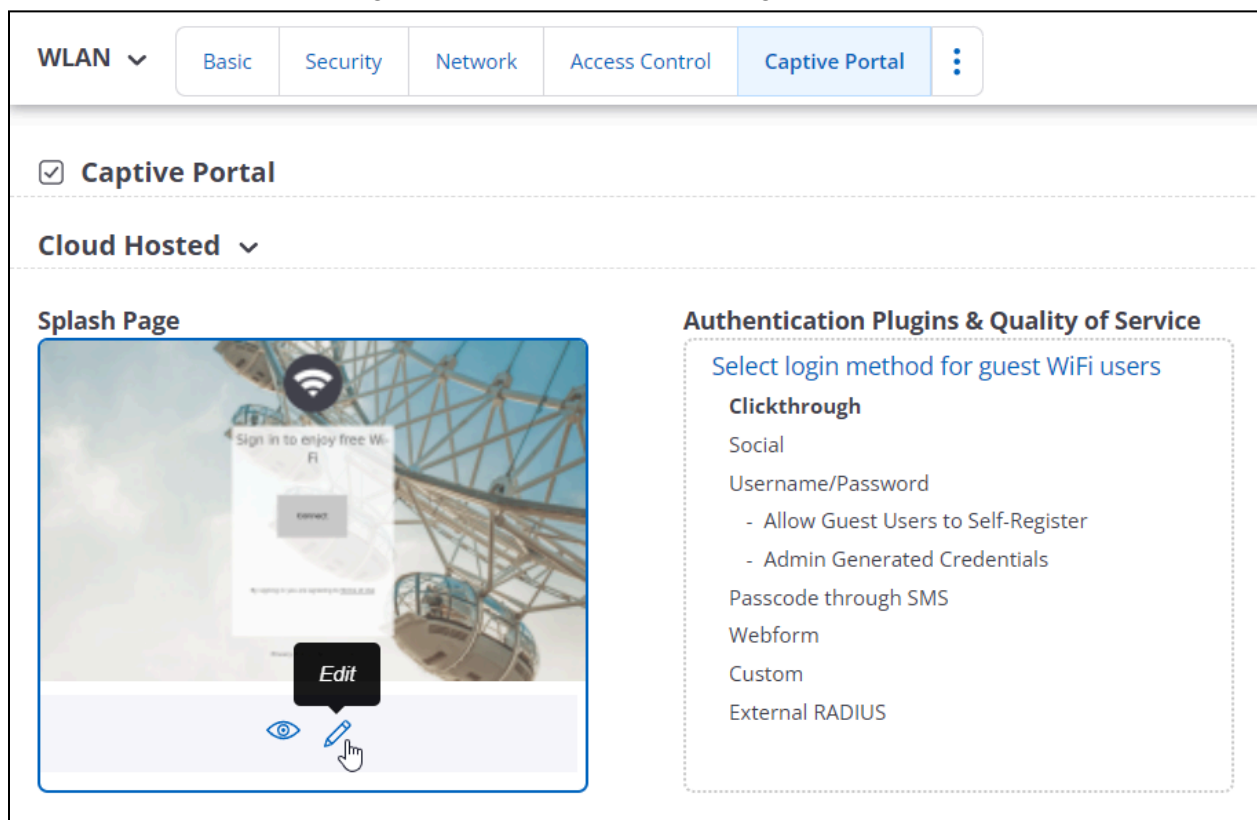
☒ **Client Isolation**

Client Isolation - Additional Info

Next, select **Captive Portal**

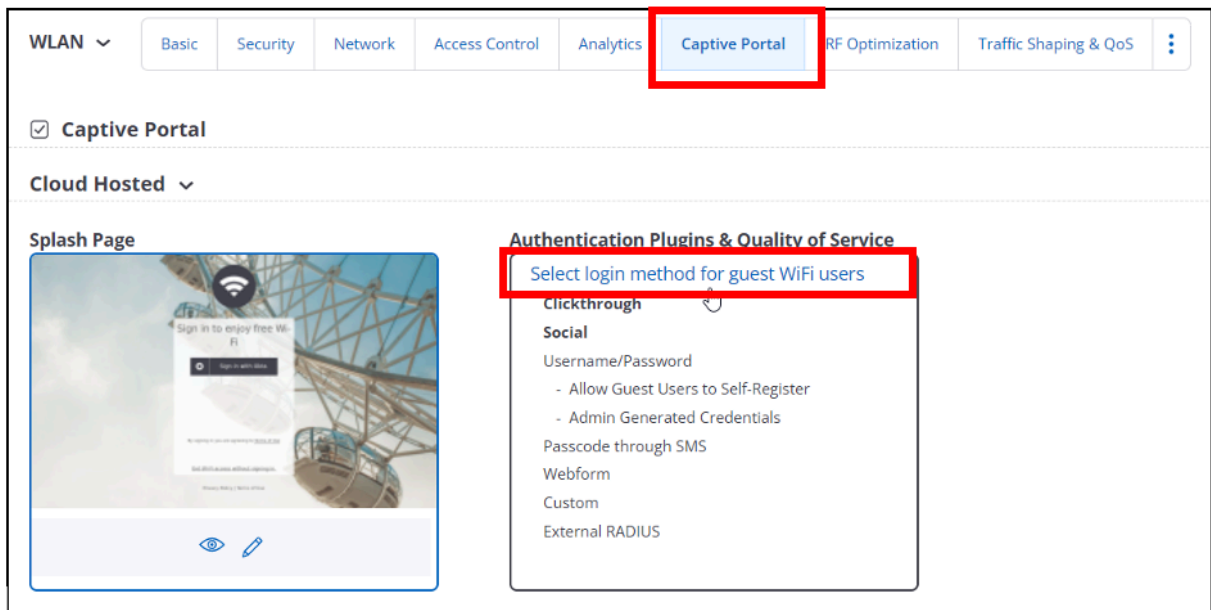


Next, let's edit the splash page. Hover over the Splash page and select **Edit**.



You can customize the Splash Page with the Pencil Edit icon. We will keep the defaults for this lab.

Next, click **Select login Method for Guest WiFi Users**



Let's create a way to allow users to create their own username and password as well as an option to create a bulk import of users.


Select **Username/Password** and then **Allow Guest Users to Self-Register** then **Save** within the Plugins & QoS Menu.

IP Address/ User Name/ Device Name




Plugins & QoS

☐ Clickthrough


☐ Social

☒ Username/Password 

☒ Allow Guest Users to Self-Register [View Users](#)

☒ Free WiFi ☐ Paid WiFi ☐ Free & Paid WiFi



☐ Host Approval

☐ Admin Generated Credentials

[Email/SMS Account Settings](#)

☐ Passcode through SMS

☐ Webform

[Cancel](#) [Save](#)

Save at the bottom within the Plugins & QoS Menu.



You have now staged all the configuration for a simple guest portal.

CloudVision CUE allows the administrator to add users for guest wireless access through a number of secure identity provider options, such as Social, custom webform, and Admin Generated Credentials.

We will explore centralized network access control for secure and guest user access as a focus during the AGNI Lab sections.

For more information here is the [Guest Manager User Guide - PDF](#)

For now Save the changes only, we will explore how to turn on the Guest SSID through another screen:

WiFi ▾ **SSID** More

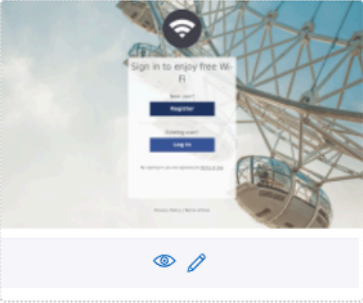
← LAB-00-GUEST

WLAN ▾ Basic Security Network Access Control **Captive Portal** ⋮

☒ **Captive Portal**

Cloud Hosted ▾

Splash Page



☐ Skip Splash Page

☒ Sign Out Popup

☐ HTTPS Redirection

Authentication Plugins & Quality of Service

Select login method for guest WiFi users

Clickthrough

Social

Username/Password

- Allow Guest Users to Self-Register
- Admin Generated Credentials

Passcode through SMS

Webform

Custom

External RADIUS

Websites that users can access before login.

Cancel **Save** Save & Turn SSID On

Finally, let's see how to enable this guest SSID among the existing ones already configured:

Go to **Configure, WiFi** (ensure you have selected the Corp folder in the hierarchy)
Find the Guest SSID in the list and select the **3-dots menu** to "Turn SSID On"

Arista Cognitive V... F... Corp

Search for MAC/ IP Address/ User Name/ Device Name..

WiFi **SSID**

SSIDs Active in Each Band

2 2 —
2.4 GHz 5 GHz 6 GHz

7 SSID

| ON/OFF ↓ | Profile Name | SSID Name | Type | Security | |
|----------|--------------|--------------|---------|----------|--------|
| ON | anet-test | anet-test | Private | WPA2 | |
| ON | ATD-01-PSK | ATD-01-PSK | Private | WPA2 | |
| OFF | | | Private | WPA/WP | |
| OFF | | | Fi | Private | WPA/WP |
| OFF | | | Guest | Open | |
| OFF | | | Private | WPA2 | |
| OFF | LAB-00-GUEST | LAB-00-GUEST | Guest | Open | |

Turn SSID On
Rename SSID
Edit
Create a Copy
Delete

When presented with the Turn SSID On dialog, **Uncheck 2.4 GHz** to disable that frequency. And click **Turn SSID On**.

Turn SSID On - LAB-00-GUEST



Select the frequency bands for this SSID



2.4 GHz



5 GHz



6 GHz

Cancel

Turn SSID On

After a few moments, your guest SSID should become available. You can test connecting the guest wireless network and should see the default splash screen to self register or log in.

Join "LAB-00-GUEST"

Sign in to enjoy free Wi-Fi

New user?

Register

Existing user?

Log In

By signing in you are agreeing to [Terms of Use](#)

< >

agm11001-c4.srv.wifi.arista.com

Cancel

Lab section complete.

3. WIPS Wireless Intrusion Prevention System

Arista Wireless Intrusion Prevention System (WIPS) leverages RF broadcast and protocol properties including packet formats like probe requests and beacons common to all 802.11 standards(including 802.11ac and 802.11ax) to detect and prevent unauthorized access.

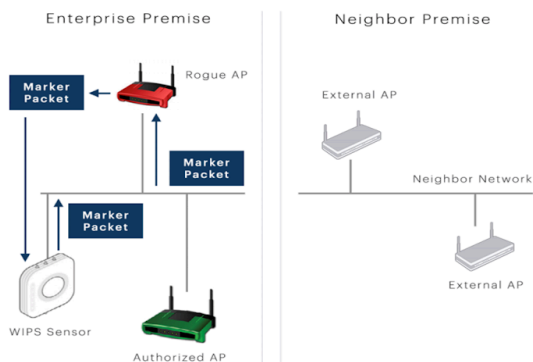
For more information about how Arista's WIPS feature works, refer to this whitepaper:
<https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Marker-Packet-Whitepaper.pdf>

Wi-Fi threats include an ever changing landscape of vulnerabilities, such as:

- Rogue APs
- Unauthorized BYOD Client
- Misconfigured APs
- Client misassociation
- Unauthorized association
- Ad-hoc connections
- Honeypot AP or evil twin "Pineapple"
- AP MAC spoofing
- DoS attack
- Bridging client

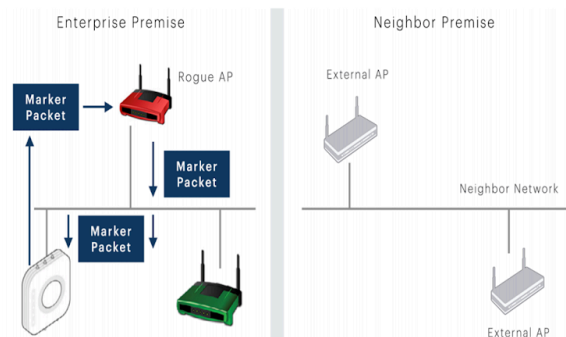
ARP Request Marker Packet

Sensor sends ARP requests with signatures on the wire and detects if any get forwarded onto the wireless side

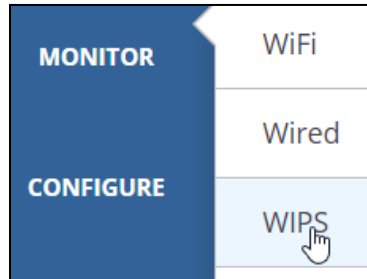


UDP Reverse Marker Packet

Sensor sends UDP packets with signatures in the air and server detects if any get forwarded onto the wire



In the menu on the left hand side of the screen, hover your cursor over “**Monitor**” and then click “**WIPS**”. Now click on “**Access Points**” and “**Clients**” in the menu at the top of the screen and explore if any Rogue APs or Clients are connected to other APs in the area.




WIPS ▾ Managed WiFi Devices **Access Points** Clients Networks

A Authorized R Rogue E External U Uncategorized

70 Access Points

| Classificatio... | | Status | ▲ | Name | Auto Prevention Status |
|-------------------------------------|---|--------------------------|---|-------------------|------------------------|
| E | ⋮ | <input type="checkbox"/> | | BelkinIn_AE:40:1F | Enabled |
| R | ⋮ | <input type="checkbox"/> | | ASUSTekC_B7:3... | Enabled |

Access points that have been detected by WIPS but are not managed within Arista CV-CUE, they are designated as Rogue or External Access Points.

WIPS 

Managed WiFi Devices

Access Points

Clients

Networks


A Authorized


G Guest

R Rogue







E External

U Uncategorized

102 WLAN Clients 



Client Explorer

| Classificatio... | | Status... | Name | User Name |
|------------------|---|--------------------------|---|-----------|
| <div>R</div> |  | <input type="checkbox"/> |   ***** | ***** |
| <div>E</div> |  | <input type="checkbox"/> |   ***** | ***** |

Now, in the left hand side menu, hover your cursor over “**Configure**”, then hover over “**WIPS**”. Explore the menu options available.

WIPS ▸

Alerts

Access Point Auto-classification

Client Auto-classification

Automatic Intrusion Prevention

Authorized WiFi Policy

CONFIGURE

TROUBLESHOOT

ENGAGE

FLOOR PLANS

REPORTS

WiFi

Device ▸

Network Profiles ▸

WIPS ▸

Alerts

☐ Non Compliant Authoriz

☐ Potentially Rogue Access

ention

Access Point Auto-classification

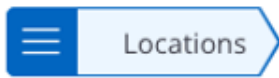
Client Auto-classification

Automatic Intrusion Prevention

Authorized WiFi Policy

Select “**Automatic Intrusion Prevention**”

Toggle the **WIPS** setting from OFF to ON



WIPS ▾

Automatic Intrusion Prevention

OFF ▾

Automatic Intrusion Prevention Level

Current Intrusion Prevention Level **Disrupt** ▾

When you click on the “OFF” toggle, a new dialog box will open allowing you to Activate Automatic Intrusion Prevention. Select the Activate button to turn this function on.

Activate Automatic Intrusion Prevention

Before you activate Automatic Intrusion Prevention, please ensure that:

- *You are done making all network configuration and deployment changes.*
- *Your authorized Access Points are correctly categorized as Authorized under **Monitor > WIPS > Access Points***
(Please check this every time you add new Access Point to the network).

☐ *Apply recursively to subfolders*

Activate

Activate the Automatic Intrusion Prevention by selecting “**Activate**”

Note the default settings prevent authorized clients from connecting to Honeypot Access Points

Prevent the following threats:

Honeypot/Evil Twin Access Points

- ☒ Authorized client connecting to Honeypot/Evil Twin Access Points

Here is some more information on Wireless Intrusion Prevention:

- Tech Field Day - [Arista - Dependable Wireless IPS](#)

Next, let's explore the information we can gather about the wireless environment using Arista's WIPS.

Select **Monitor**, **WIPS**:

The screenshot shows the Arista WIPS interface. The left sidebar has a navigation menu with 'MONITOR' highlighted. The main area shows the 'WIPS' section with a dropdown menu open, highlighting 'WIPS'. Below this, it shows '1 Managed Devices' and a table with one device: 'Arista_52:57:7' with a red update icon and MAC address 'E4:D1:24:52:57:'. A 'Managed Devices Explorer' button is also present.

In the simple lab environment, only your pod's single AP is part of your managed wireless infrastructure. All of the other access points and clients on the network are like crowded neighbors or businesses in a shared office work space.

Under **Monitor, WIPS, Access Points** you can see all of the detected Rogue Access points. From this screen you can reclassify, set auto-prevention, add to ban list, name or move the AP.

| Classif... | Status | Name | MAC Address | Auto Prevention St... | Prevention St... | Is Network... | Network | Active/Inactive Since | First Detected | Location | RSSI (d... | Channel | No. of Associa... | SSID |
|---------------|---------|-------------------|------------------|-----------------------|------------------|---------------|-----------------|-----------------------|----------------|------------------------|------------|---------|-------------------|---------|
| Authorized | Enabled | ap-M3 | 88:B1:E1AE:7... | Enabled | -- | No | -- | ↑ 1:51 PM | Aug 28, 2023 | //Arista Cognitive ... | -26 | 149 | 0 | anet-t |
| Authorized | Enabled | POD-01-FL1 | 30:86:2D:0D:0... | Enabled | -- | Yes | 192.168.1.0/... | ↑ 1:51 PM | Sep 27, 2023 | */Corp/1st Floor | 0 | 36,6 | 0 | MULT |
| Rogue | Enabled | DA13-99:7C:D5:8F | DA:13:99:7C:D... | Enabled | -- | No | -- | ↓ 10:39 AM | Jul 22 | //Arista Cognitive ... | -- | -- | 0 | DIREC |
| Rogue | Enabled | CC28-AA:2A:04:9C | CC:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/... | ↑ 1:51 PM | Jul 21 | */Corp/1st Floor | -44 | 161 | 0 | wirele |
| Rogue | Enabled | CC28-AA:2A:04:98 | CC:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/... | ↑ 1:51 PM | Jul 21 | */Corp/1st Floor | -28 | 3 | 0 | wirele |
| Rogue | Enabled | 72:28-AA:2A:04:9D | 72:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/... | ↑ 1:51 PM | Jul 21 | */Corp/1st Floor | -44 | 161 | 0 | wirele |
| Rogue | Enabled | 8A:28-AA:2A:04:99 | 8A:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/... | ↑ 1:51 PM | Jul 21 | */Corp/1st Floor | -27 | 3 | 0 | wirele |
| Uncategorized | Enabled | Motorola_F6:95:72 | DC:BF:E9:F6:9... | Enabled | -- | No | -- | ↑ 1:58 PM | 1:58 PM | */Corp/1st Floor | -87 | 1 | 1 | FBI-SI |
| Authorized | Enabled | C6:50:9C:45:E2:5A | C6:50:9C:45:E... | Enabled | -- | No | -- | ↑ 1:51 PM | 1:51 PM | */Corp/1st Floor | -77 | 1 | 0 | |
| Authorized | Enabled | Zyxel_DA:4E:9C | 5C:E2:8C:D4:4... | Enabled | -- | No | -- | ↑ 2:26 PM | 2:26 PM | */Corp/1st Floor | -89 | 6 | 0 | Centu |
| Authorized | Enabled | 96:04:E3:01:DF:7B | 96:04:E3:01:D... | Enabled | -- | No | -- | ↑ 1:51 PM | 1:51 PM | */Corp/1st Floor | -86 | 157 | 0 | |
| Authorized | Enabled | CA:6C:6D:43:E9:D1 | CA:6C:6D:43:E... | Enabled | -- | No | -- | ↑ 1:51 PM | 1:51 PM | */Corp/1st Floor | -90 | 157 | 0 | xfinity |
| Authorized | Enabled | 96:04:E3:01:DF:7B | 96:04:E3:01:D... | Enabled | -- | No | -- | ↑ 1:51 PM | 1:51 PM | */Corp/1st Floor | -87 | 157 | 2 | RUSTY |
| Authorized | Enabled | C6:50:9C:4C:E2:5E | C6:50:9C:4C:E... | Enabled | -- | No | -- | ↑ 1:51 PM | 1:51 PM | */Corp/1st Floor | -91 | 157 | 0 | xfinity |
| Authorized | Enabled | 3E:2D:9E:C9:57:C6 | 3E:2D:9E:C9:5... | Enabled | -- | No | -- | ↑ 1:52 PM | 1:52 PM | */Corp/1st Floor | -92 | 157 | 0 | xfinity |

Additional information about WIPS AP classification can be found here:

<https://www.arista.com/en/ug-cv-cue/cv-cue-wireless-intrusion-prevention-techniques>

Authorized APs

Access Points (APs) that are wired to the corporate network and are compliant with the Authorized Wireless LAN (WLAN) configuration defined by the Administrator in CV-CUE are classified as Authorized APs. Typically, these will be Arista APs, but the administrator can configure the Authorized WiFi policies for any AP vendors.

Rogue Access Point

APs that are wired to the corporate network and do not follow the Authorized WiFi configuration defined in CV-CUE are classified as Rogue APs.

Even if this AP is disconnected from the network, it will continue to be classified as a Rogue. These APs are a potential threat to the corporate environment and can be used for intrusion into the corporate network over Wi-Fi. It is recommended to enable Intrusion Prevention for Rogue APs so that Wi-Fi communication with these APs is always disrupted. Using the Location Tracking ability of Arista WIPS, Rogue APs should be tracked down and physically removed from the network.

Rogue APs are displayed in Red rows on the console.

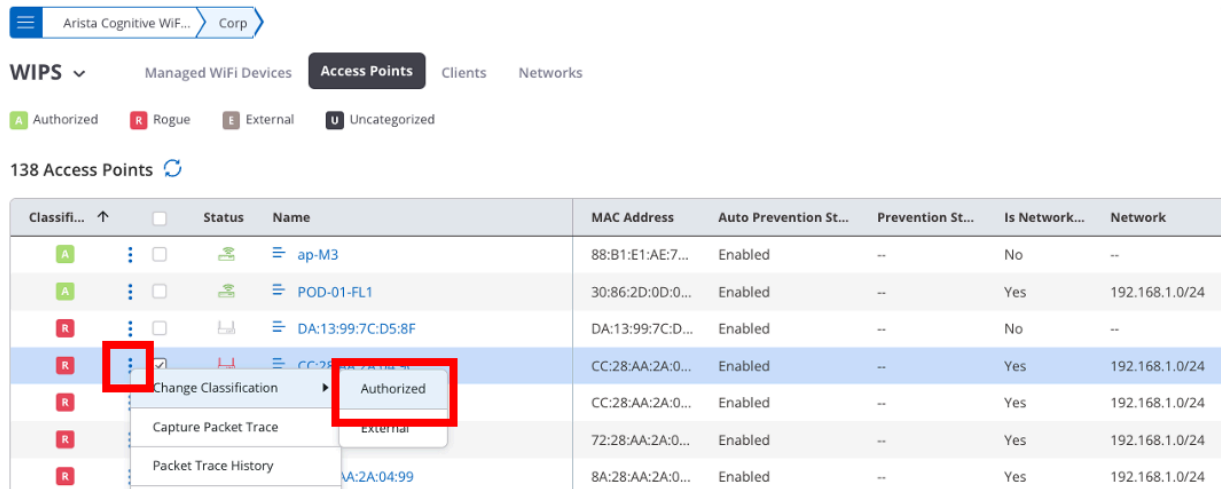
External Access Point

APs that are not wired to your corporate network are classified as External APs.

Through the connectivity tests performed by the WIPS Sensors, Wireless Manager is able to determine that these APs are not connected to the wired network. These are neighboring APs that share the same spectrum as the Authorized APs and may cause interference with your Authorized WLAN. A site survey and channel optimization should be performed to reduce radio interference from the External APs. These APs are not always a threat and hence they should

not be quarantined/prevented by default, as it would disrupt neighboring Wi-Fi activity. Intrusion Prevention policies can be configured to prevent Authorized clients from connecting to External APs.

A Rogue Access point can be reclassified, moved or named from the 3-dots menu for each detected AP.



The screenshot shows the WIPS interface with the 'Access Points' tab selected. A table lists 138 Access Points. The table has columns: Classification, Status, Name, MAC Address, Auto Prevention Status, Prevention Status, Is Network..., and Network. The table is filtered to show only 'Rogue' (R) access points. A context menu is open for one of the Rogue APs, showing options: 'Change Classification', 'Capture Packet Trace', and 'Packet Trace History'. The 'Change Classification' option is highlighted with a red box, and the 'Authorized' option in the dropdown menu is also highlighted with a red box.

| Classifi... | ↑ | Status | Name | MAC Address | Auto Prevention St... | Prevention St... | Is Network... | Network |
|-------------|---|--------|-------------------|------------------|-----------------------|------------------|---------------|----------------|
| A | | | ap-M3 | 88:B1:E1:AE:7... | Enabled | -- | No | -- |
| A | | | POD-01-FL1 | 30:86:2D:0D:0... | Enabled | -- | Yes | 192.168.1.0/24 |
| R | | | DA:13:99:7C:D5:8F | DA:13:99:7C:D... | Enabled | -- | No | -- |
| R | | | CC:28:AA:2A:0... | CC:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/24 |
| R | | | CC:28:AA:2A:0... | CC:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/24 |
| R | | | 72:28:AA:2A:0... | 72:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/24 |
| R | | | 8A:2A:04:99 | 8A:28:AA:2A:0... | Enabled | -- | Yes | 192.168.1.0/24 |

Within an existing campus WiFi environment or one with a mix of wireless solutions, these discovered APs can be explicitly allowed to show the most accurate security profile.

For this lab you do not need to authorize any APs.

WIPS - Classify and Prevent client

Next, let's use the WIPS system to identify and prevent an example problematic client from connecting to your network.

Within **WIPS**, **Clients** Menu.

Find your smartphone device connected to the previous Lab PSK. Reconnect it now to the PSK SSID, if it has been disconnected.

WIPS ▾ Managed WiFi Devices Access Points **Clients** networks

Authorized Guest Rogue External Uncategorized

28 WLAN Clients ▾ Client Explorer

| Classifi... | Sta... | Name | User Name | MAC Address | Locally Ad... | IPv4 Address | IPv6 Addresses | OS | Associated Access ... | Associated SSID | Security | Authentica... | Frequency Band | Capability |
|-------------|--------|----------------------|-----------|-------------------|---------------|--------------|----------------------|--------------------|-----------------------|-----------------|------------|---------------|----------------|------------|
| A | | iwashi | -- | 1C91:80:C0:AD:C0 | No | 192.168.1... | -- | Mac OS | -- | -- | -- | -- | 2.4 + 5 GHz | WiFi 6 |
| A | | DE:46:8E:89:25:D | -- | DE:46:8E:89:25:DA | Yes | 192.168.1... | fe80::18f7:2233:183c | Apple iOS / iPadOS | POD-01-FL1 | ATD-01-PSK | WPA2 | PSK | 5 GHz | WiFi 6 |
| A | | 4A91:0E:7E:FB:C4 | -- | 4A91:0E:7E:FB:C4 | Yes | 192.168.1... | -- | Apple iOS / iPadOS | -- | -- | -- | -- | 5 GHz | WiFi 6 |
| E | | Rename | -- | A4:11:62:87:34:60 | No | -- | -- | -- | ArisTech_24AA/C4 | ARLD_VMB_719' | WPA2 | PSK | 2.4 GHz | Legacy |
| E | | Capture Packet Trace | -- | B4BB:69:03:8C:5C | No | -- | -- | -- | 96:04:E3:01:DF:78 | RUSTY | WPA3, WPA2 | SAE, PSK | 5 GHz | Legacy |

Since this client is associated with the correct PSK for the SSID, it is automatically classified as Authorized.

Next, click the **3-dots menu** for the device, **Change Classification**, **Rogue**

WIPS ▾ Managed WiFi Devices Access Points **Clients**

A Authorized G Guest R Rogue E External U Uncategorized

28 WLAN Clients ▾ Client Explorer

| Classifi... | Sta... | Name | User Name |
|-------------|--------|------------------|-----------|
| A | | iwashi | -- |
| A | | DE:46:8E:89:25:D | -- |
| A | | | |
| E | | | |
| E | | | |

Change Classification Authorized

Rename External

Capture Packet Trace Rogue

Now, **sort the clients menu by Classification column (left)** and find the red marked Rogue device.

Next, Select the **3-dots menu** for the Rogue client and click **“Prevent This Device”**

Arista Cognitive WiFi Corp

WIPS Managed WiFi Devices Access Points **Clients** Networks

Authorized Guest Rogue External Uncategorized

31 WLAN Clients Client Explorer

| Classifi... | Sta... | Name | User Name | MAC Address | Locally Ad... | IPv4 Address | IPv6 Addresses | OS | Associated Access ... | Associated SSID |
|-------------|--------|-----------------------------|-----------|-------------------|---------------|--------------|----------------------|--------------------|-----------------------|-----------------|
| | | DE:46:8E:89:25:D7 | | DE:46:8E:89:25:DA | Yes | 192.168.1... | fe80::18f7:2233:183c | Apple iOS / iPadOS | POD-01-FL1 | ATD-01-PSK |
| | | 7B:8A... | | 3E:BA:EA:F0:7B:8A | Yes | -- | -- | -- | -- | -- |
| | | Rename | | 54:2A:1B:85:0A:20 | No | -- | -- | -- | -- | -- |
| | | Capture Packet Trace | | 70:77:81:B2:E2:65 | No | -- | -- | -- | -- | -- |
| | | Packet Trace History | | AC:63:8E:62:9B:5A | No | -- | -- | -- | -- | -- |
| | | Start Live Client Debugging | | 5C:47:5E:74:F3:EE | No | -- | -- | -- | -- | -- |
| | | Update Device Tag | | 1A:BA:19:4B:3D:AD | Yes | -- | -- | -- | -- | -- |
| | | Locate | | D0:3F:27:41:8E:7A | No | -- | -- | -- | -- | -- |
| | | Move | | 48:A2:E6:04:63:7C | No | -- | -- | -- | ARRISGro_43:E9:D0 | TrashDay |
| | | Prevent This Device | | 02:A6:78:65:2A:26 | Yes | -- | -- | -- | ARRISGro_43:E9:D0 | TrashDay |
| | | | | 6A:67:09:CC:07:EB | No | -- | -- | -- | -- | -- |

Prevent This Device



This will prevent all wireless communication for this client. Are you sure you want to continue?

Cancel

Prevent

Click Prevent to start the WIPS prevention mechanism to disrupt the selected client from sending and receiving traffic.

Try to connect to a public website with your test client device with the prevention setting enabled versus disabled (be sure to disable backup wireless/LTE radios).

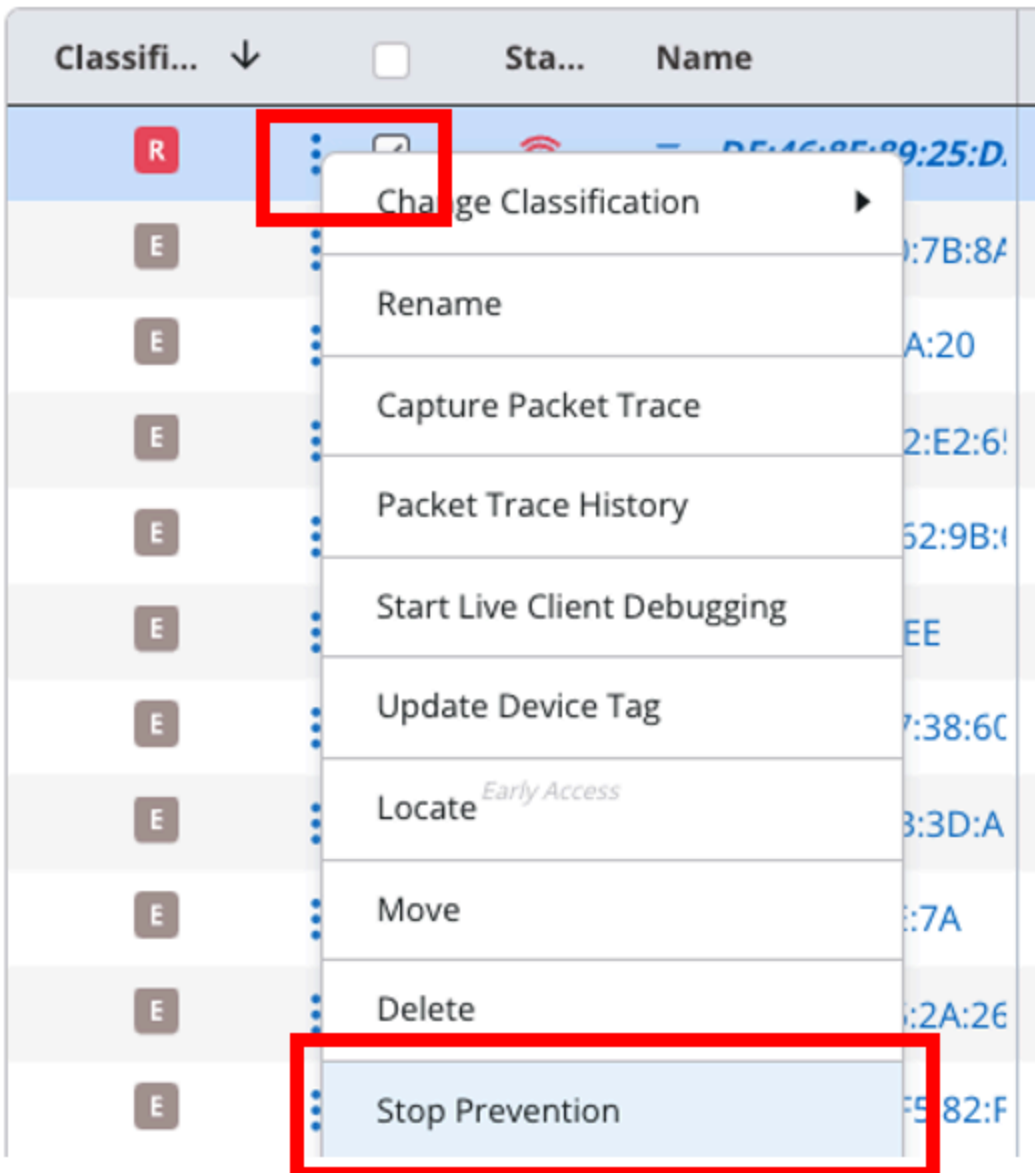
The test device should fail to connect to other devices through the protected WiFi network when prevention is active.

When you are finished, **STOP the client prevention**

28 WLAN Clients ▾



Client Explorer



– When you are finished, **STOP the client prevention** so that you can use this test device in upcoming labs, optionally.



Lab guide complete