

# Configure Active Directory Guest Authentication on WAP571 or WAP571E

## Objective

The objective of this article is to guide you in configuring Active Directory authentication using the WAP571 and WAP571E devices. Active Directory is a Microsoft identity directory for authenticating via domain controller users as a service. To put it simply – its a way to verify that a person joining the network is an expected user.

## Requirements

- WAP571
- WAP571E
- A running Active Directory server [[Link to setting up Active Directory on Microsoft Server 2016](#) ]

## Getting Started – Enabling Captive Portal

Step 1. Click the **Captive Portal** option in the left-hand menu bar. The page will default to the Global Configuration section.



Step 2. Click the **Enable** toggle button.

## Global Configuration

Captive Portal Mode:  Enable

Authentication Timeout: 3600

Additional HTTP Port: 0

Additional HTTPS Port: 0

Step 3. Click the **Save** button at the bottom of this page.

## Wireless-AC/N Premium Dual P

## Global Configuration

Captive Portal Mode:  Enable

Authentication Timeout: 3600

Additional HTTP Port: 0

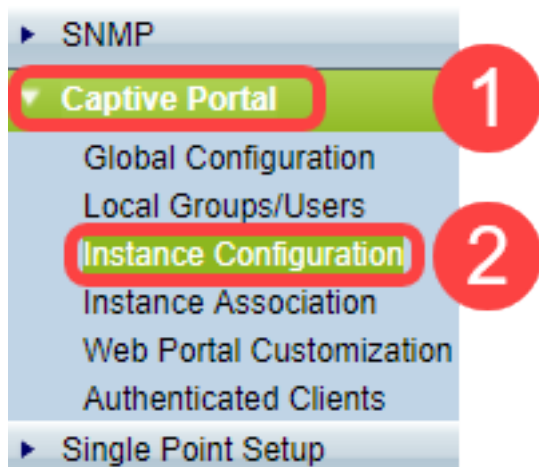
Additional HTTPS Port: 0

### Captive Portal Configuration Counters

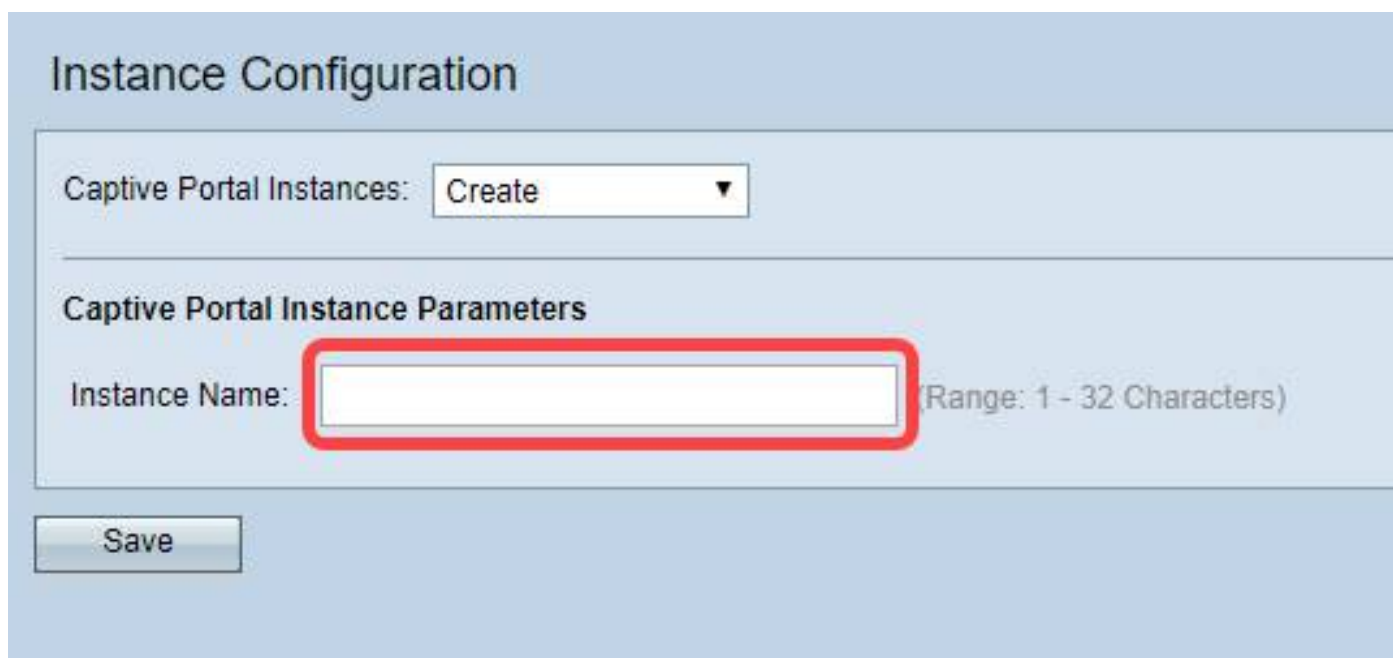
Instance Count: 2

## Configuring the Instance

Step 1. Now click **Instance Configuration** from the Captive Portal sub-menu on the left-hand side of the screen.



Step 2. **Title** the Active Directory Instance in the name field.

A screenshot of the 'Instance Configuration' form. The form has a title 'Instance Configuration' at the top. Below the title, there is a section for 'Captive Portal Instances' with a dropdown menu set to 'Create'. Below that is a section titled 'Captive Portal Instance Parameters'. In this section, the 'Instance Name' field is highlighted with a red box. To the right of the text input field, there is a note: '(Range: 1 - 32 Characters)'. At the bottom left of the form, there is a 'Save' button.

**Note:** We have named our Instance CP\_Test\_Instance.

Step 3. Click **Save**.

## Instance Configuration

Captive Portal Instances:

### Captive Portal Instance Parameters

Instance Name:  (Range: 1 - 32 Characters)

This will open the Instance Configuration page and contains many details. Example below:

## Instance Configuration

Captive Portal Instances: CP\_Test\_Instance ▼

### Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode:  Enable

Protocol: HTTP ▼

Verification: Guest ▼

www.msftconnecttest.com,

Walled Garden Range:

Redirect:  Enable

Redirect URL:  (Range: 0 - 256 Characters)

Away Timeout: 60  (Range: 0 - 1440 Min, Default: 60)

Session Timeout: 0  (Range: 0 - 1440 Min, Default: 0)

Maximum Bandwidth Upstream: 0  (Range: 0 - 1300 Mbps, Default: 0)

Maximum Bandwidth Downstream: 0  (Range: 0 - 1300 Mbps, Default: 0)

User Group Name: Default ▼

RADIUS IP Network: IPv4 ▼

Global RADIUS:  Enable

RADIUS Accounting:  Enable

Server IP Address-1:  (xxx.xxx.xxx.xxx)

Server IP Address-2:  (xxx.xxx.xxx.xxx)

Step 4. Click the **Protocol** dropdown box and select **HTTPS**.

## Instance Configuration

Captive Portal Instances: CP\_Test\_Instance ▾

### Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode:  Enable

Protocol: HTTP ▾

Verification: HTTP ▾

1

2

Step 5. Click the **Verification** dropdown box and select **Active Directory Server**. Selecting this option opens new input fields which expect the IP address(es) of the Active directory servers.

## Instance Configuration

Captive Portal Instances: CP\_Test\_Instance ▾

### Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode:  Enable

Protocol: HTTPS ▾

Verification: Guest ▾

Walled Garden Range:

Guest

Local

RADIUS

Active Directory Server

3rd Party Credentials

1

2

Step 6. Enter the **IP address** of the Active Directory Server, or servers.

## Instance Configuration

Captive Portal Instances: CP\_Test\_Instance ▾

### Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode:  Enable

Protocol: HTTPS ▾

Verification: Active Directory Server ▾

Active Directory Server Host-1: 10.2.0.2 Port: 3268

Active Directory Server Host-2: Port: 3268

Active Directory Server Host-3: Port: 3268

**Note:** The LAN address of the active directory server on our lab is located at 10.2.0.2. Your IP address will of course be dependent on your network topology.

Step 7. *(Optional)* To test the status of the connection to the Active Directory server click the **Test** button to the right of the IP address entered in the previous step.

## Instance Configuration

Captive Portal Instances: CP\_Test\_Instance ▾

### Captive Portal Instance Parameters

Instance ID: 2

Administrative Mode:  Enable

Protocol: HTTPS ▾

Verification: Active Directory Server ▾

Active Directory Server Host-1: 10.2.0.2 Port: 3268

Active Directory Server Host-2: Port: 3268

Active Directory Server Host-3: Port: 3268

Step 8. *(Optional)* Enter your **Username**, **Password** and click **Start**.

**Test connectivity to Active Directory server at 10.2.0.2**

Username:

Password:

When the test is successful, you will receive text notification in the window.

**Test connectivity to Active Directory server at 10.2.0.2**

Username:

Password:

**Test success.**

Step 9. Click the **Save** button at the bottom of the page.

Key-3:  (Range: 1 - 63 Characters)

Key-4:  (Range: 1 - 63 Characters)

Locale Count: 0

Delete Instance:

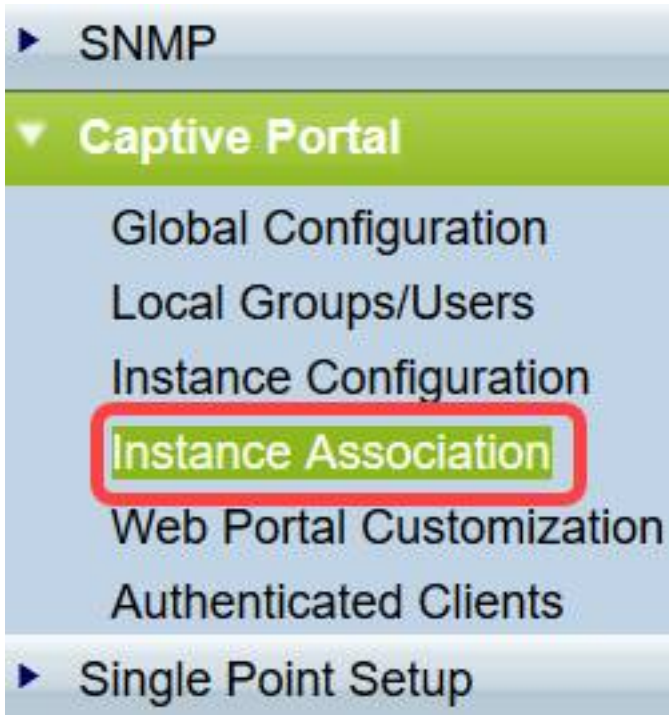
Inc. All rights reserved.



## Wrapping up - Instance Association

Now that we have an instance created, it will need to be associated with a virtual access point (VAP). A virtual access point is somewhat like a copy/pasted version of the access point that behaves the same but is named differently. In our case, the name is VAP 0.

Step 1. Click **Instance Association** while the Captive Portal menu option is active.



Step 2. The Instance Association page counts VAPs up to 16 different VAPs. In this step, we have selected the instance titled "CP\_Test\_Instance". Choose a VAP and click the **Instance Name** drop-down box.

# Wireless-AC/N Premium Dual Radio

## Instance Association

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

### Instance Association

| Network Interface              | Instance Name        |
|--------------------------------|----------------------|
| VAP 0 (WAP571E)                | <input type="text"/> |
| VAP 1 (Virtual Access Point 2) | CP_Test_Instance     |
| VAP 2 (Virtual Access Point 3) | <input type="text"/> |
| VAP 3 (Virtual Access Point 4) | <input type="text"/> |

1

2

Step 3. Repeat this step for the 2.4 GHz radio as well. Begin by clicking the **Radio 2 (2.4GHz)** and then repeating step 2 of the current section.

# Wireless-AC/N Premium

## Instance Association

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

## Conclusion

You should now be setup have users join via active directory authentication. If you would like to continue learning about related topics, see the links below:

- [Configuring Social Media Authentication on WAP571 and WAP571E Devices](#)
- [Umbrella Integration Guide WAP571 and WAP571E](#)