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.

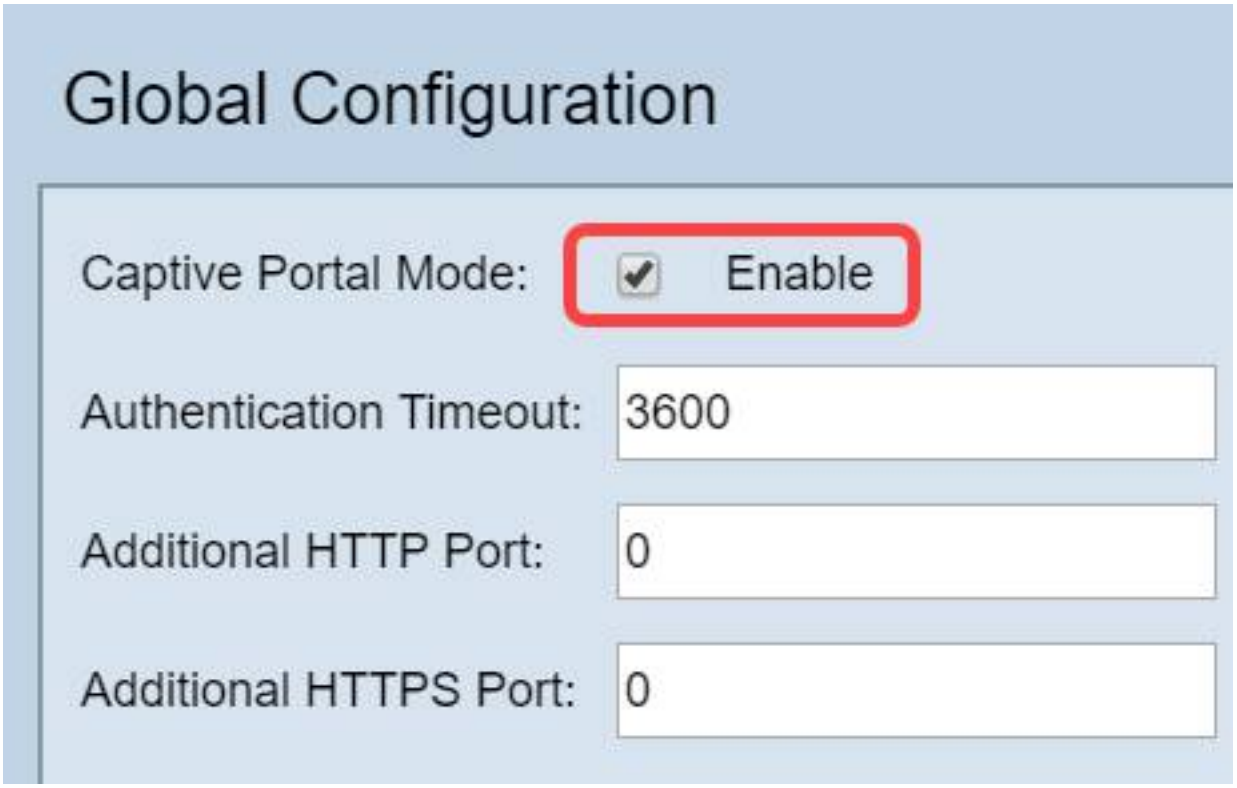
Requirements

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

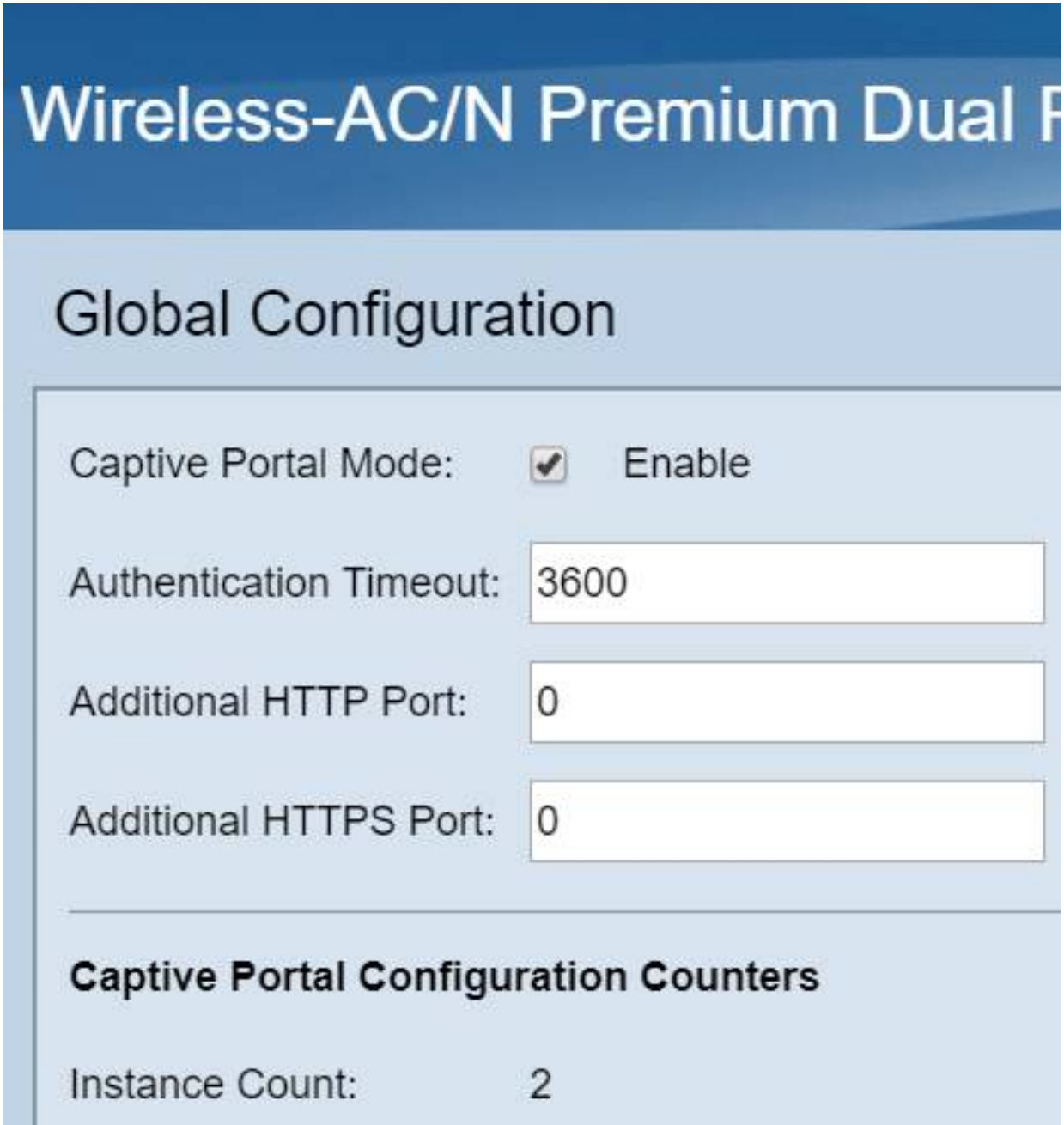
Getting Started – Enabling Captive Portal

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.

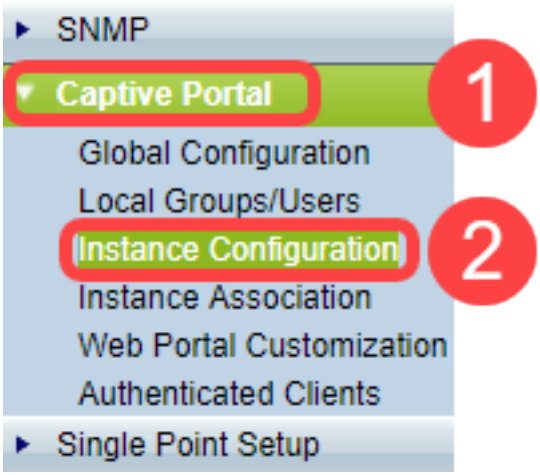


Step 3. Click the **Save** button at the bottom of this page.

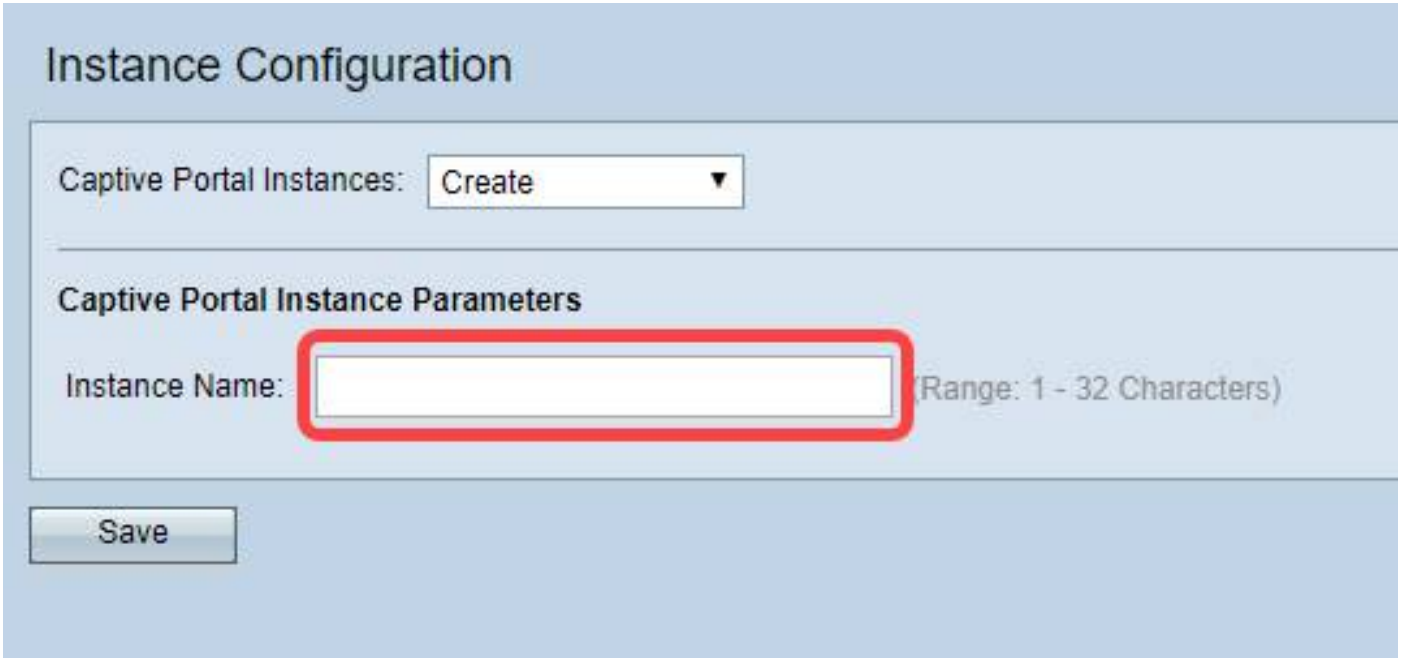


Configuring the Instance

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

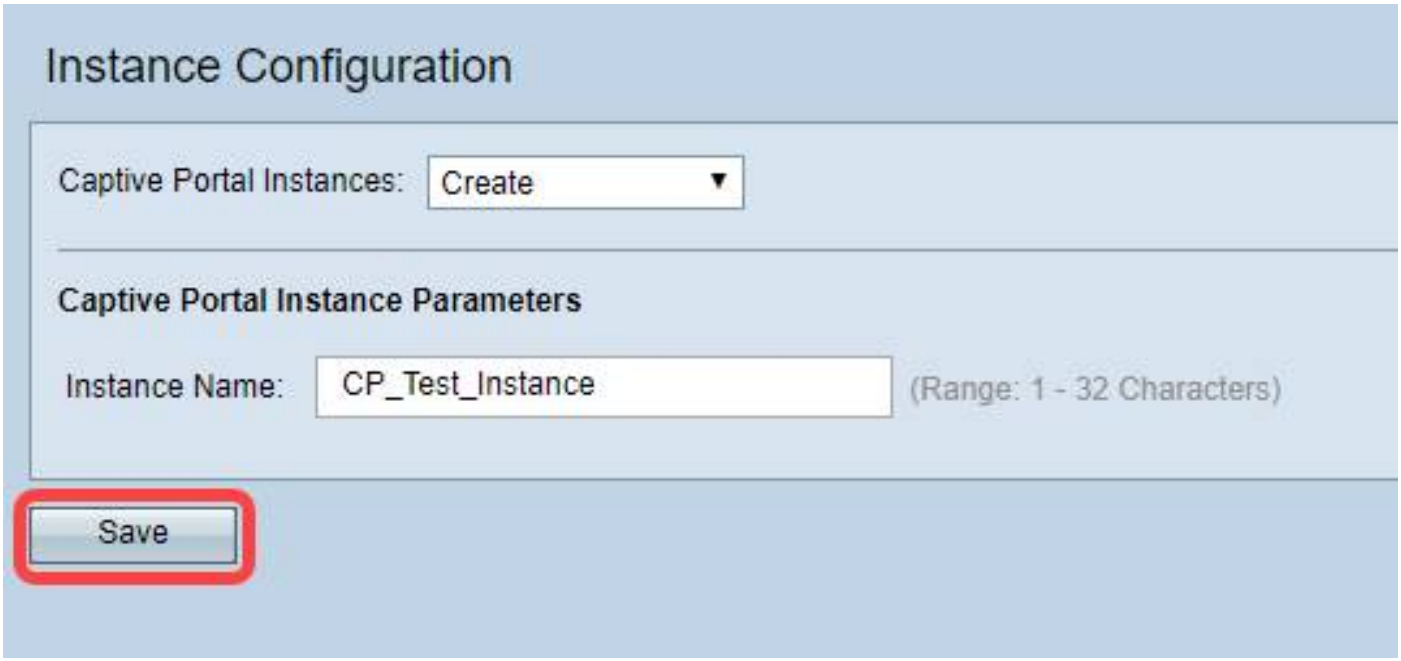


Step 2. **Title** the Active Directory Instance in the name field.

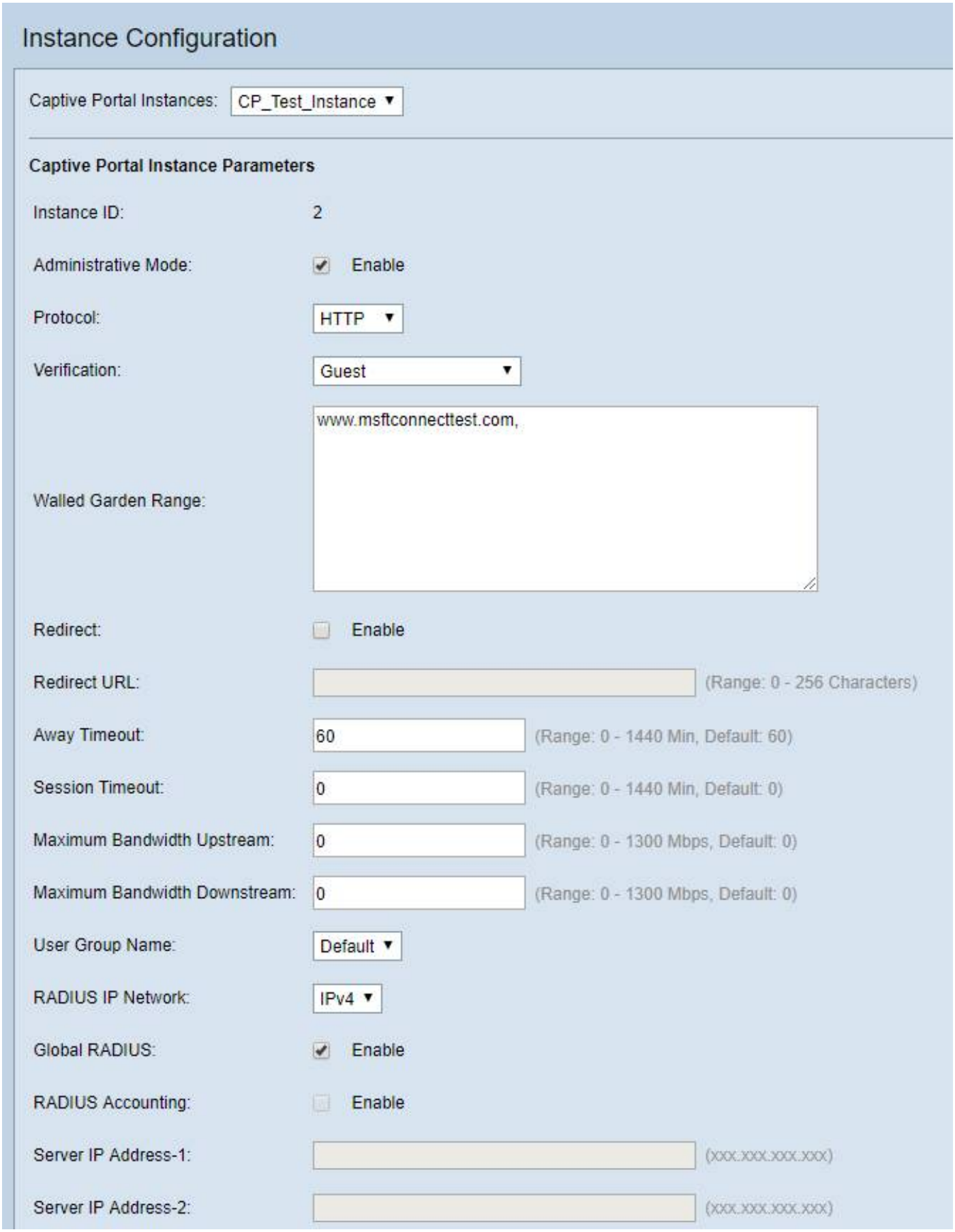


Note: We have named our Instance CP_Test_Instance.

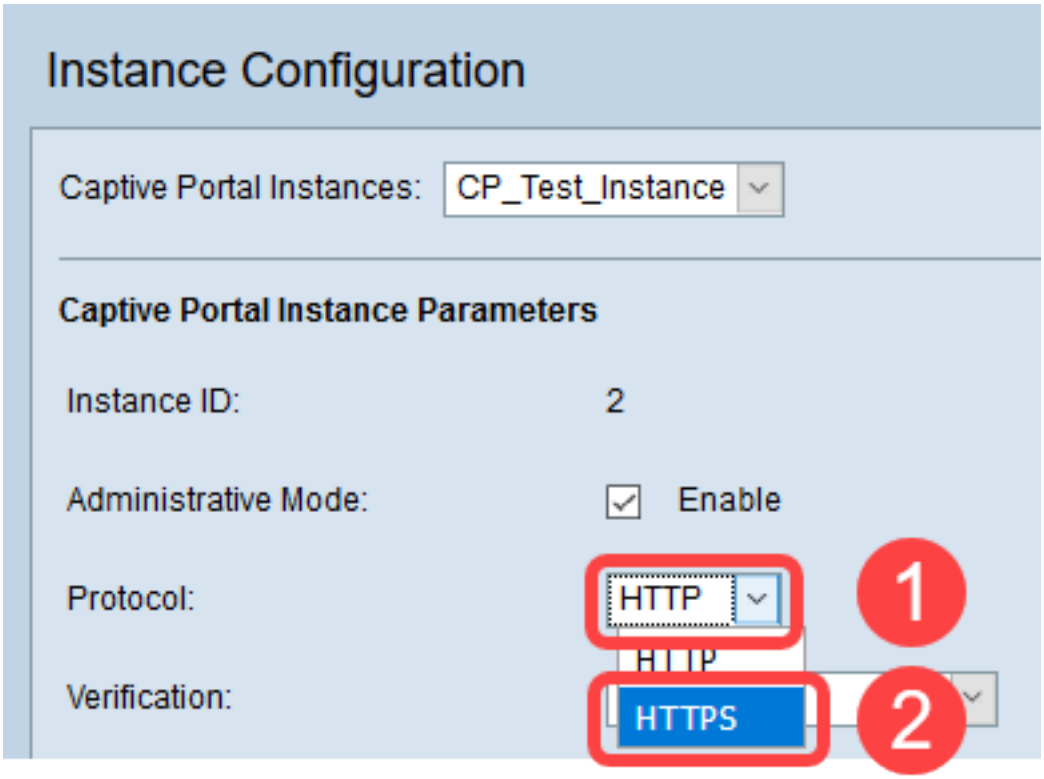
Step 3. Click **Save**.



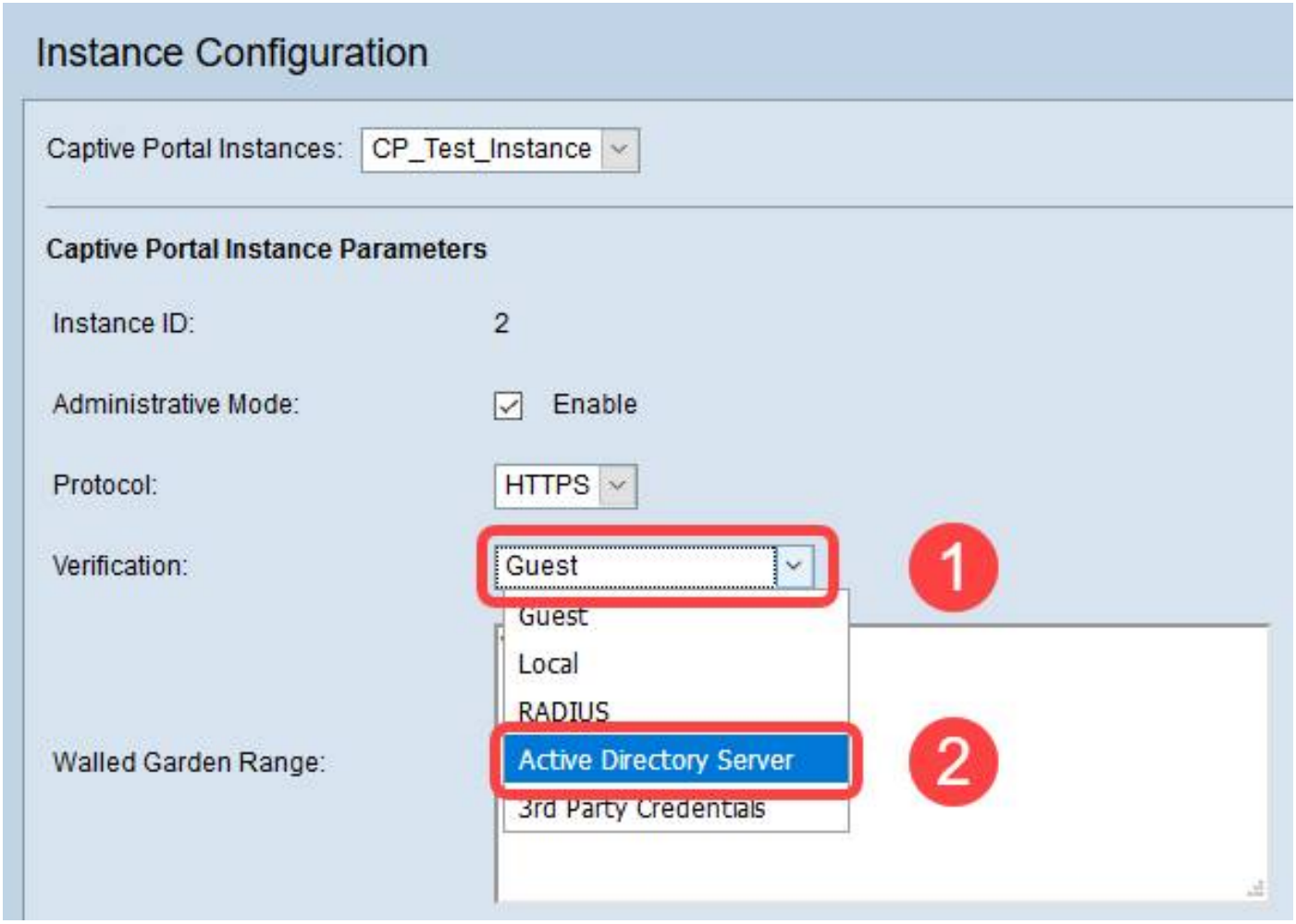
This will open the Instance Configuration page and contains many details. Example below:



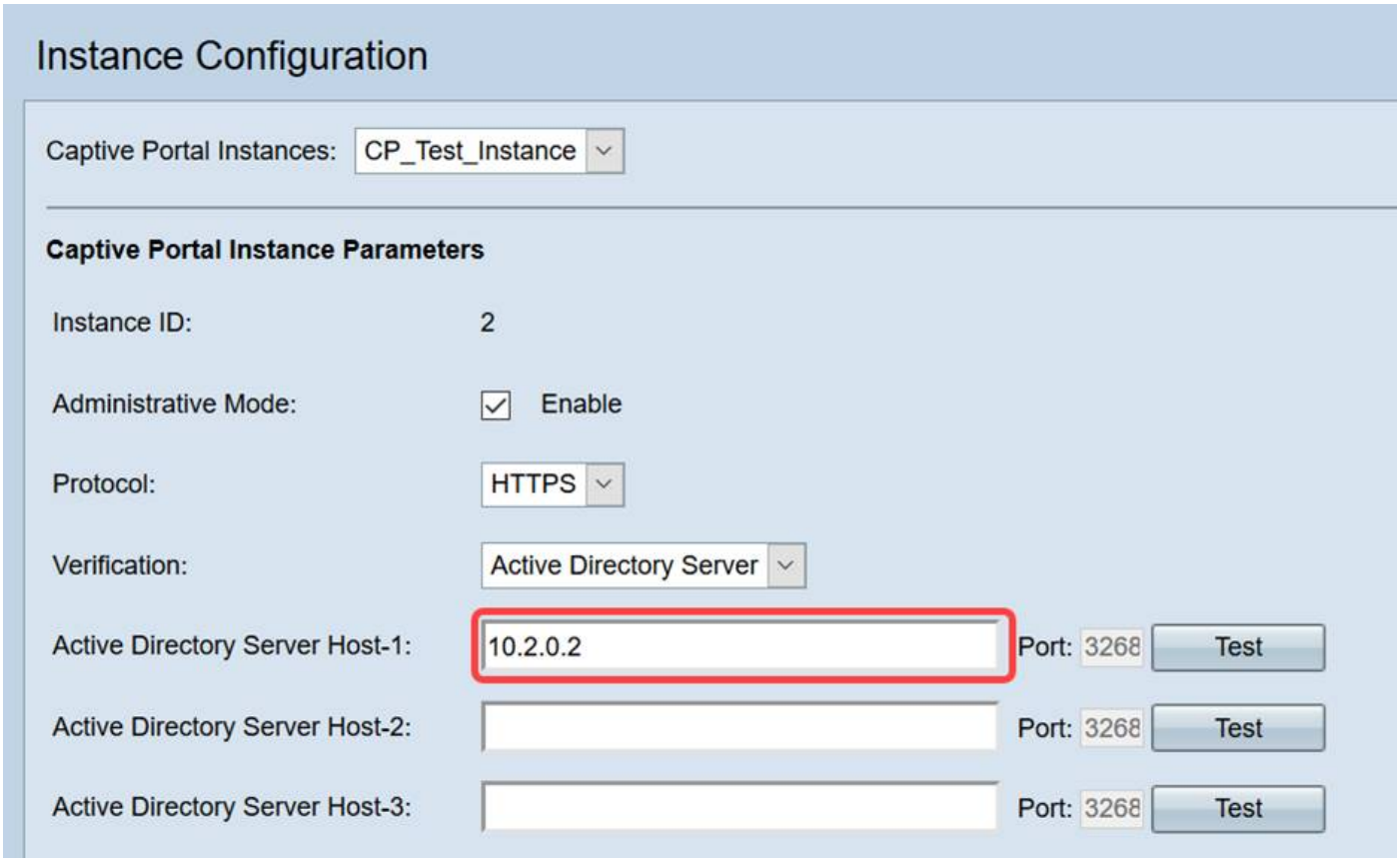
Step 4. Click the **Protocol** dropdown box and select **HTTPS**.



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.

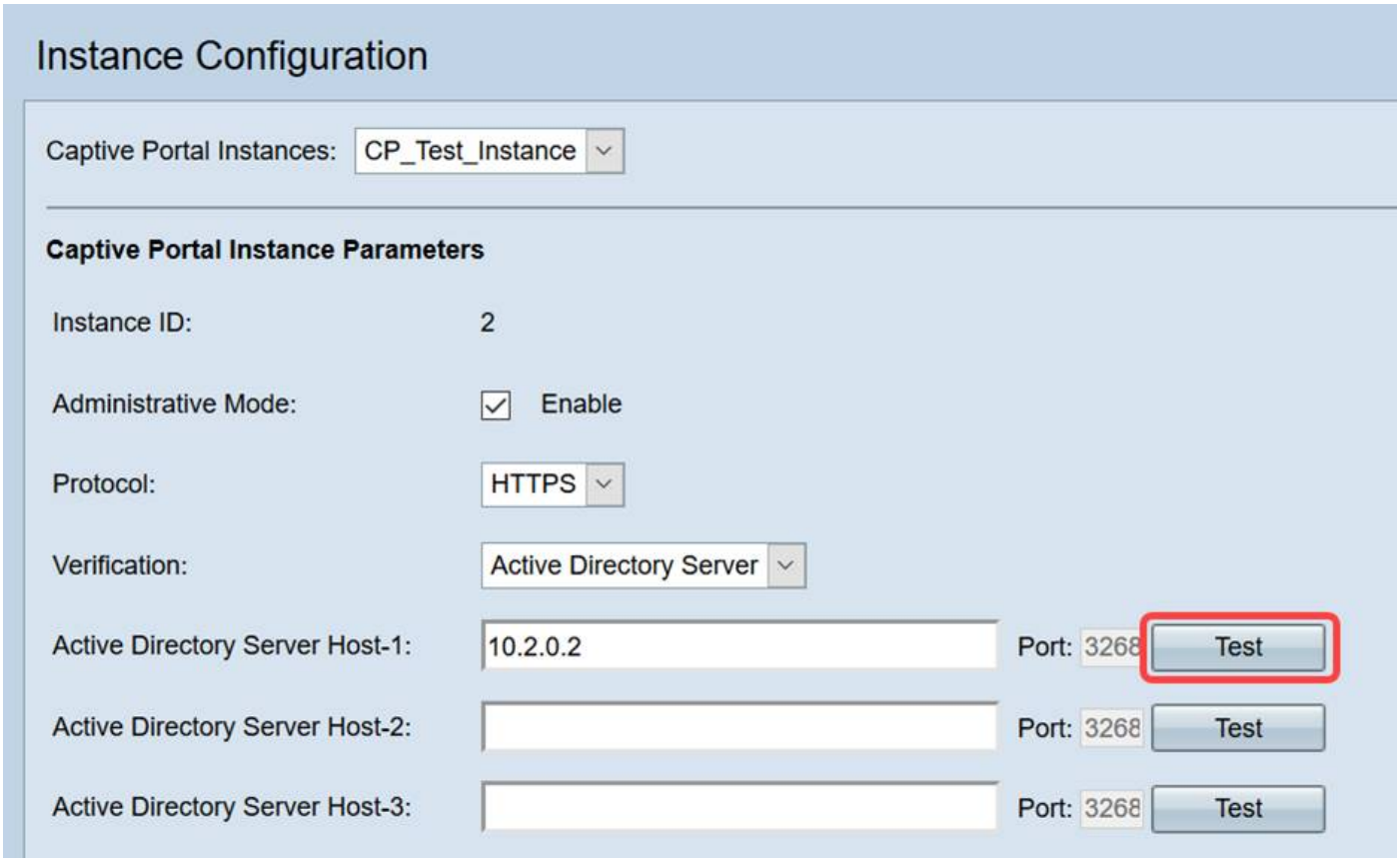


Step 6. Enter the **IP address** of the Active Directory Server, or servers.



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.

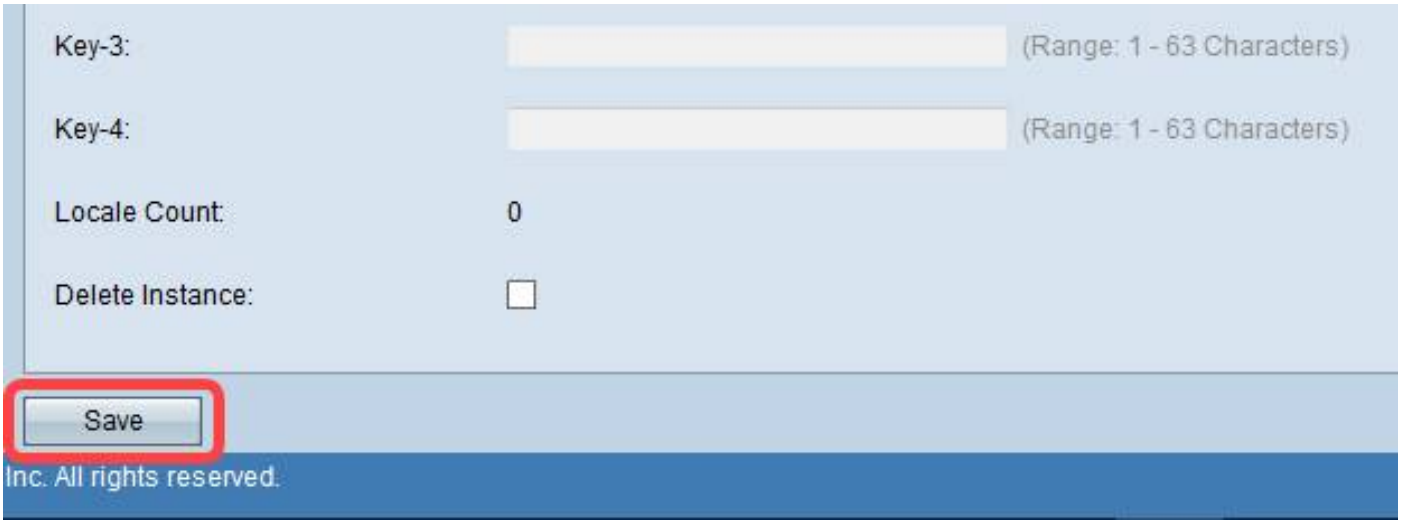
Step 7. *(Optional)* To test the status of the connection to the Active Directory server click the **Test** button to the right of the IP address entered in the previous step.



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

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

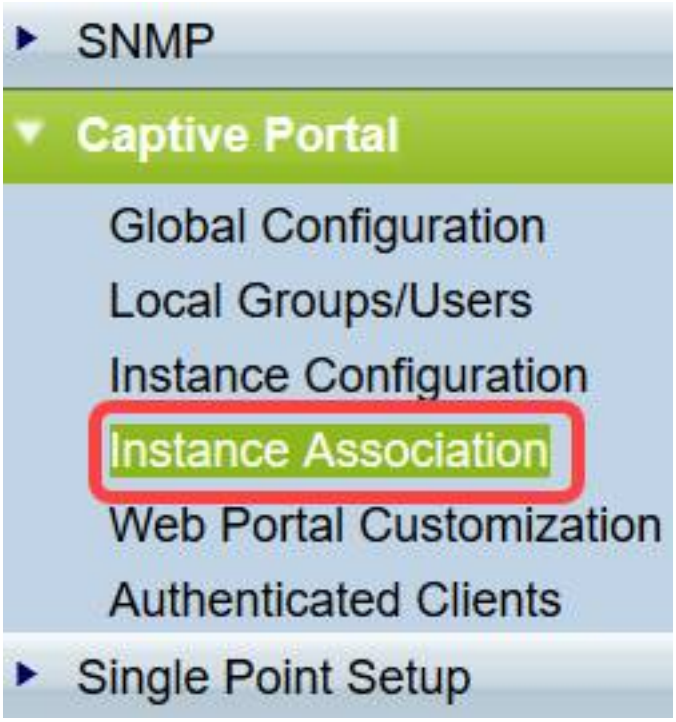
Step 9. Click the **Save** button at the bottom of the page.



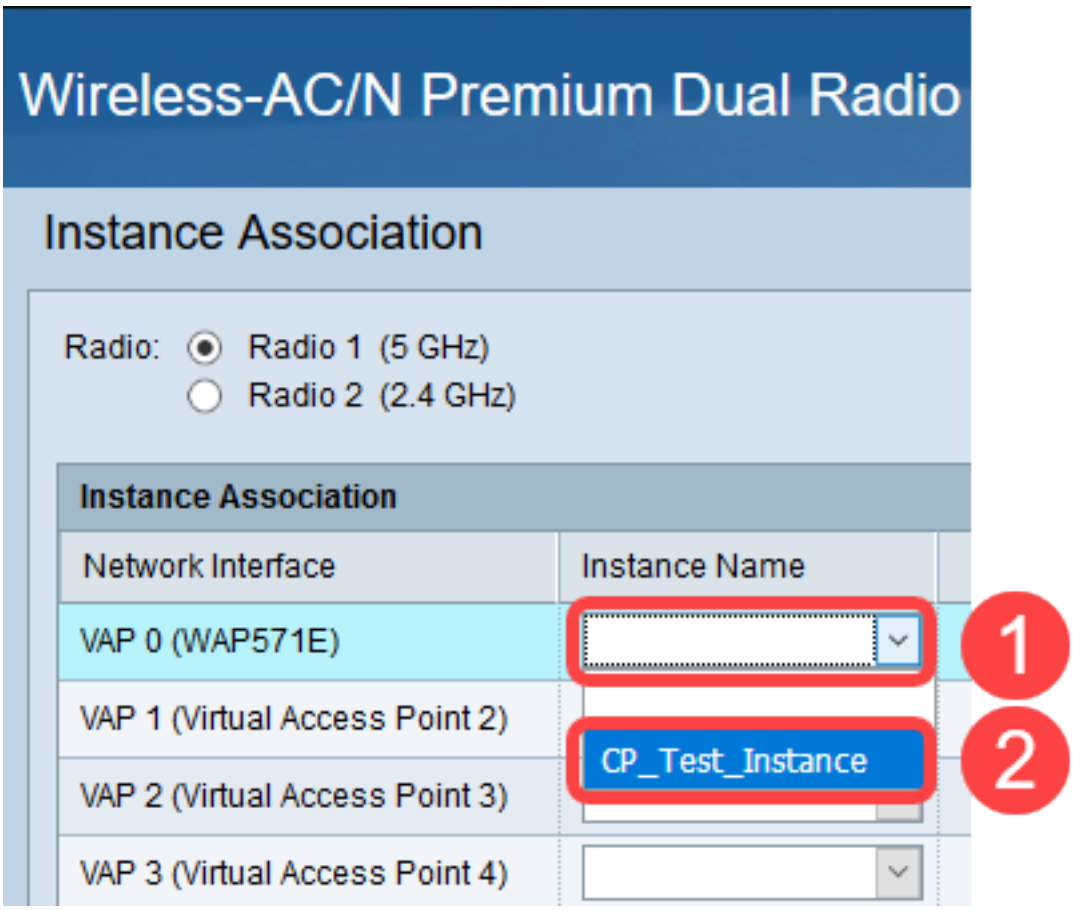
Wrapping up - Instance Association

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.

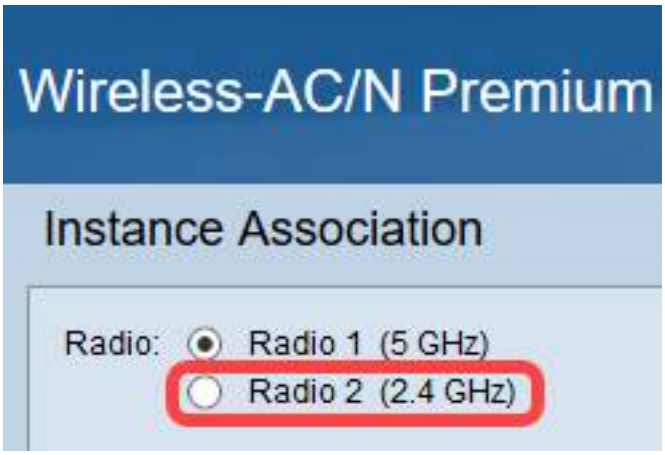
Step 1. Click **Instance Association** while the Captive Portal menu option is active.



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.



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.



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