Configure Active Directory Guest Authentication on WAP125 or WAP581

Objective

Active Directory (AD) guest authentication allows a client to configure a captive portal infrastructure to use their internal Windows Directory Service for authentication. Captive Portal is a feature that allows an administrator to block clients connecting to the Wireless Access Point (WAP) network until they are granted access onto the network. Clients are directed to a web page for authentication and conditions of access before they are able to connect to the network. Captive Portal verification is for both guests and authenticated users of the network. This feature makes use of the web browser and turns it into an authentication device.

Captive portal instances are a defined set of configurations used to authenticate clients on the WAP network. Instances can be configured to respond in different ways to users as they attempt to access the associated virtual access points. Captive portals are often employed at Wi-Fi hotspot locations to ensure users agree to terms and conditions as well as provide security credentials prior to gaining access to the Internet.

To support AD Authentication the WAP will need to communicate with one to three Windows Domain Controllers to provide authentication. It can support multiple domains for authentication by choosing domain controllers from different AD domains.

The objective of this document is to show you how to configure the AD guest authentication on the WAP125 or WAP581.

Applicable Devices

- WAP125
- WAP581

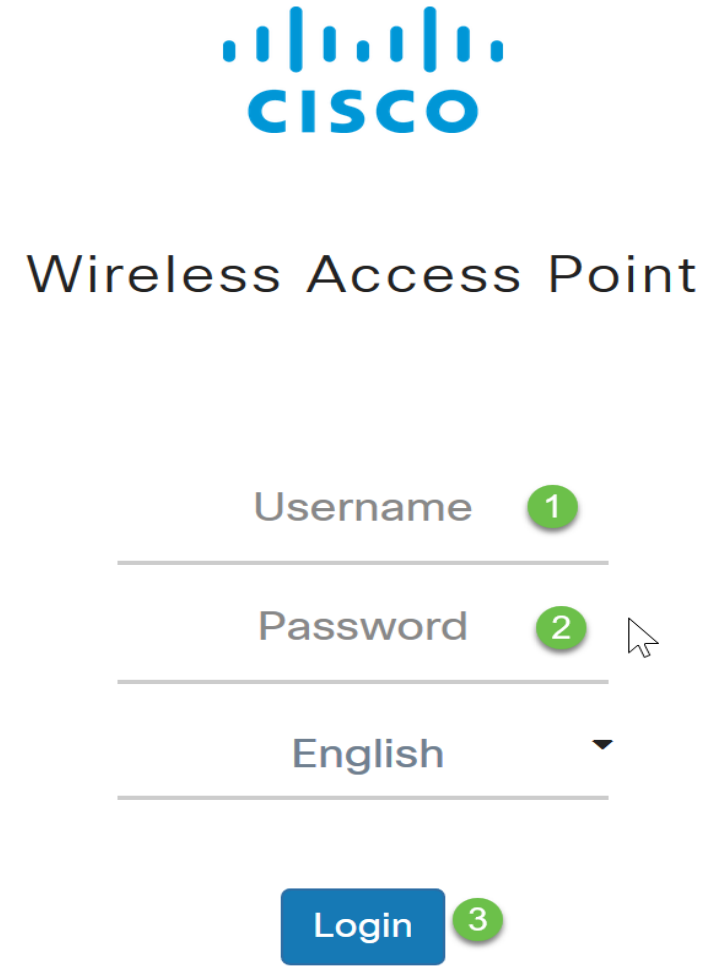
Software Version

- 1.0.1

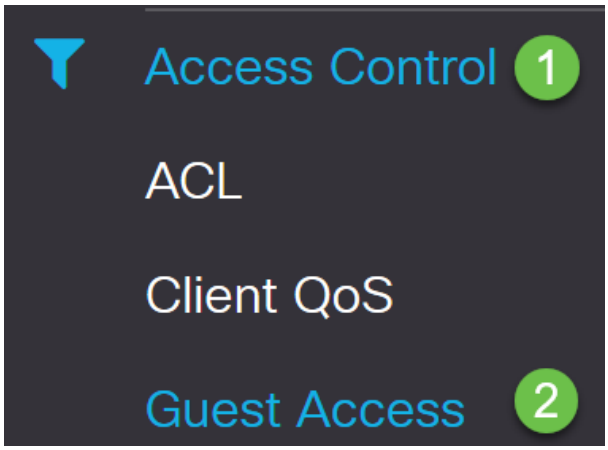
Configure Active Directory Guest Authentication

Step 1. Log in to the web configuration utility of the WAP by entering the username, and password. The default username and password is cisco/cisco. If you have configured a new username or password, enter the credentials instead. Click **Login.**

NOTE: In this article, the WAP125 is used to demonstrate the configuration of AD guest authentication. Menu options may slightly vary depending on the model of your device.



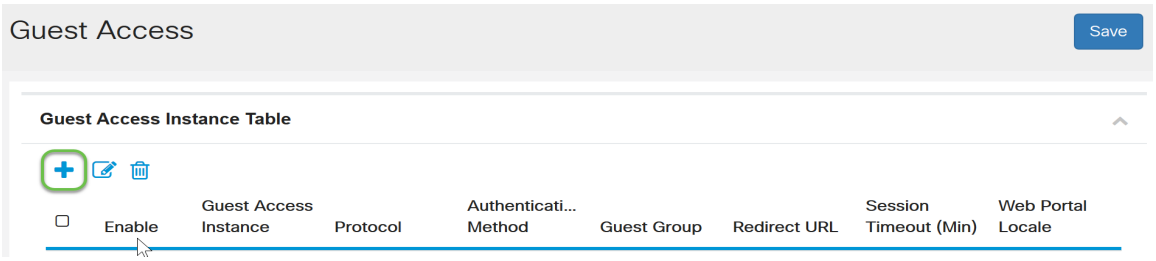
Step 2. Choose **Access Control > Guest Access**.



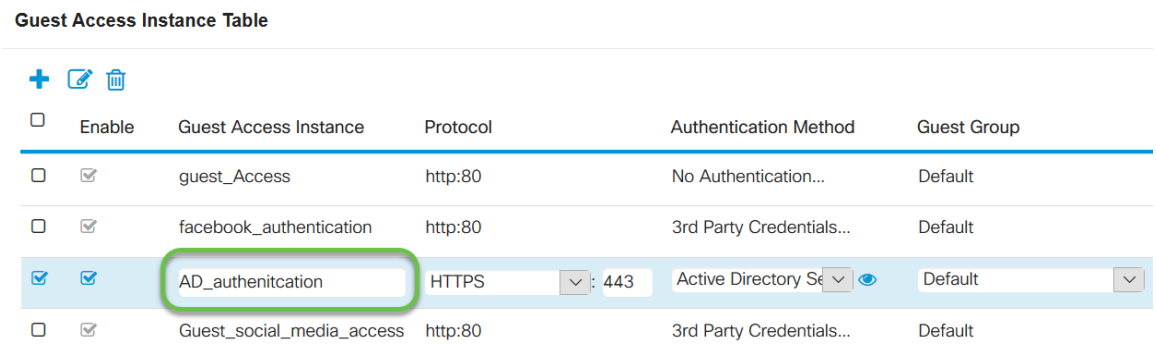
Step 3. In the *Guest Access Instance Table*, you can either add a new *Guest Access Instance* or edit an existing one. The Guest Access feature of the WAP125 or WAP581 access point provides wireless connectivity to temporary wireless clients within the range of the device. It works by having the access point broadcast two different Service Set Identifiers (SSIDs): one for the main network, and the other for the guest network. Guests are then redirected to a Captive Portal where they are required to enter their credentials. In effect, this keeps the main network secure while still giving guests access to the Internet.

The settings of the Captive Portal are configured at the Guest Access Instance Table of the web-based utility of the WAP. The Guest Access feature is particularly useful in hotel and office lobbies, restaurants, and malls.

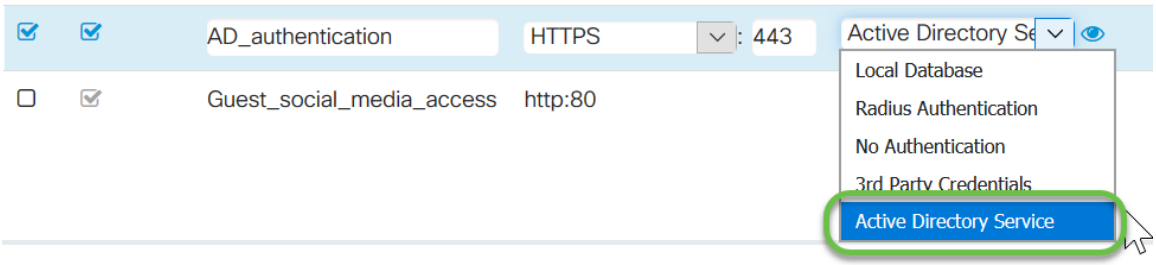
In this example, a new *Guest Access instance* is added by clicking on the **plus icon**.



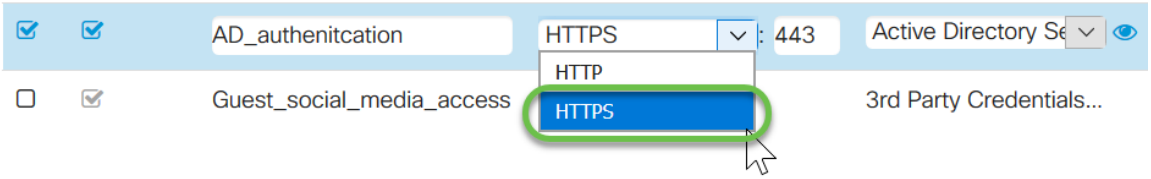
Step 4. Name the *Guest Access Instance*. In this example, it is called **AD_authentication**.



Step 5. Choose the *Authentication Method* as **Active Directory Service**.

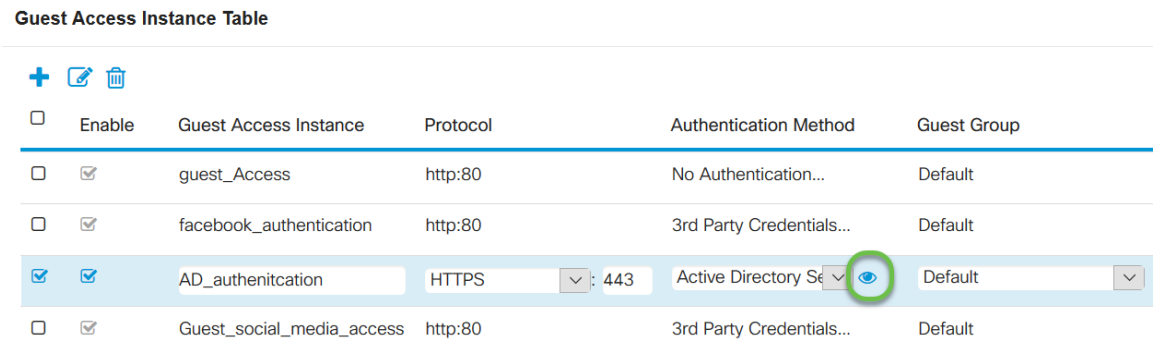


Step 6. Once you choose Active Directory Service as the *Authentication Method*, the Protocol changes from Hyper Text Transfer Protocol (HTTP) to Hyper Text Transfer Protocol Secure (HTTPS).

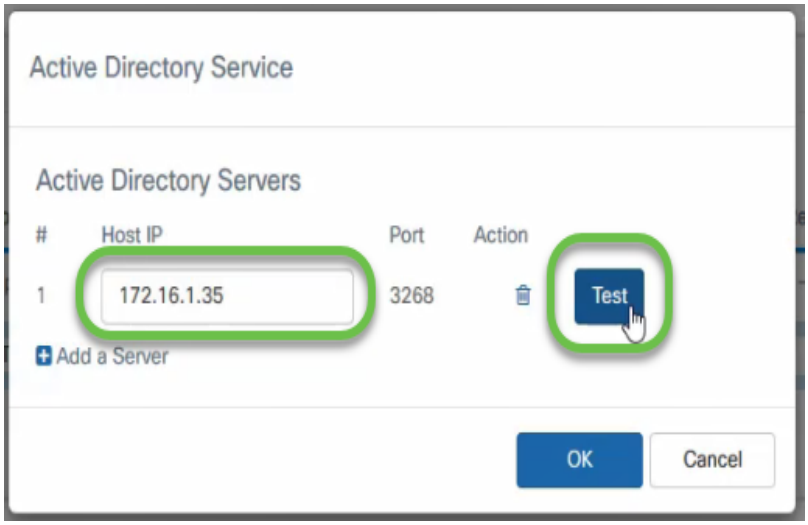


NOTE: It is very important that a client should configure the captive portal page to use HTTPS and not HTTP as the former is more secure. If a client chooses HTTP, they can inadvertently expose usernames and passwords by transmitting them in unencrypted clear text. It is best practice to use a HTTPS captive portal page.

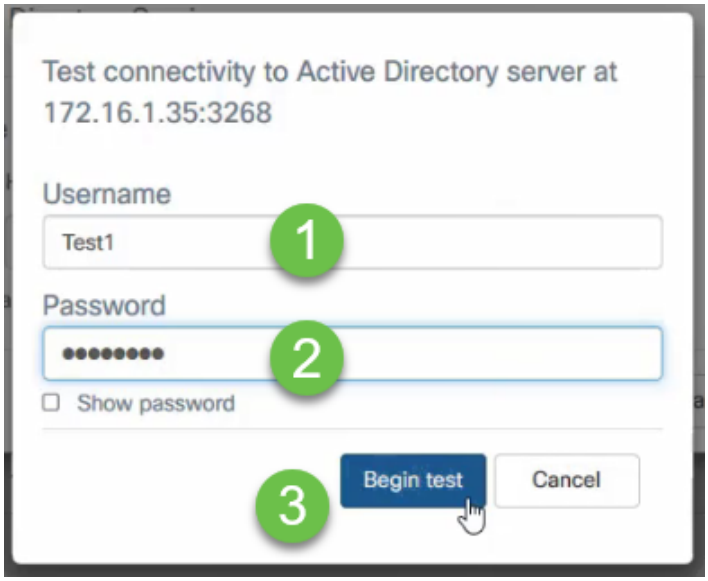
Step 7. Configure the IP address of the AD server by clicking the **blue eye icon** next to the Active Directory Service in the *Authentication Method* column.



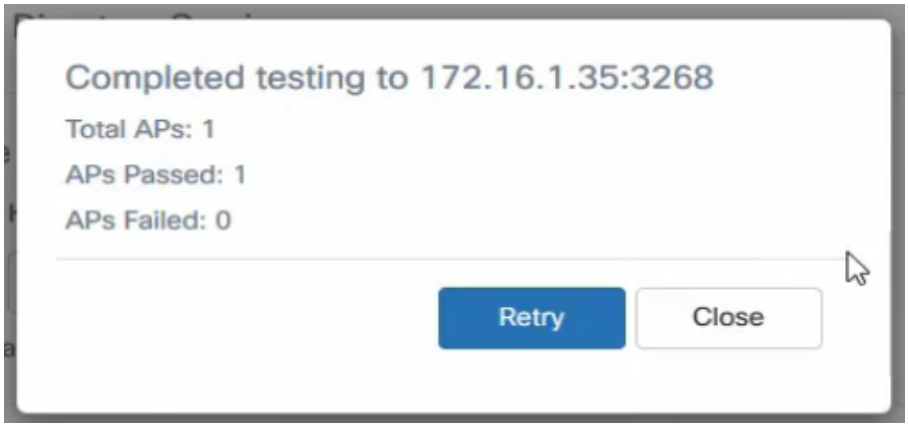
Step 8. A new window will open up. Enter the IP address for the AD server. In this example, the Host IP address used is **172.16.1.35**. As an optional step, you can click on **Test** to verify that it is valid.



Step 9. (Optional) Once you click on **Test** in the previous step, another pop-up window will open and you can enter the *Username* and *Password* of the user in AD and click on **Begin test**.

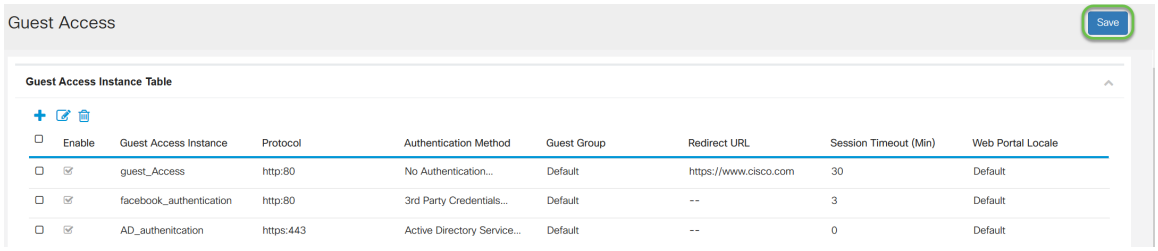


If it is valid, it will pass the test and the following screen will appear. This confirms that you can connect to the domain controller and authenticate.

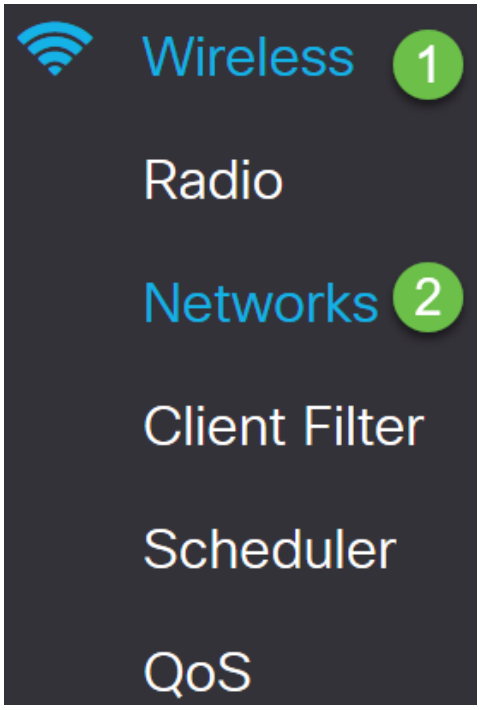


NOTE: You can add up to 3 AD servers.

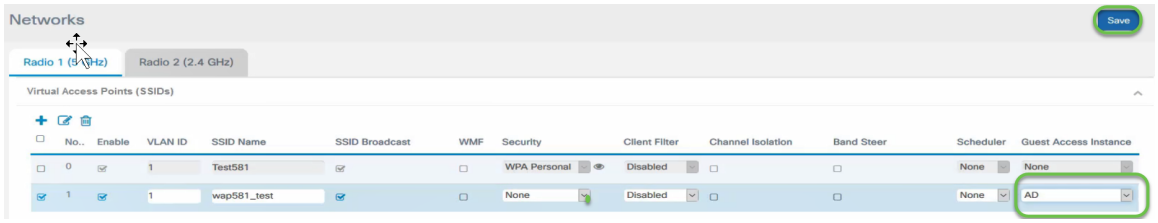
Step 10. Save the changes.



Step 11. Go to the Menu and choose **Wireless > Networks**

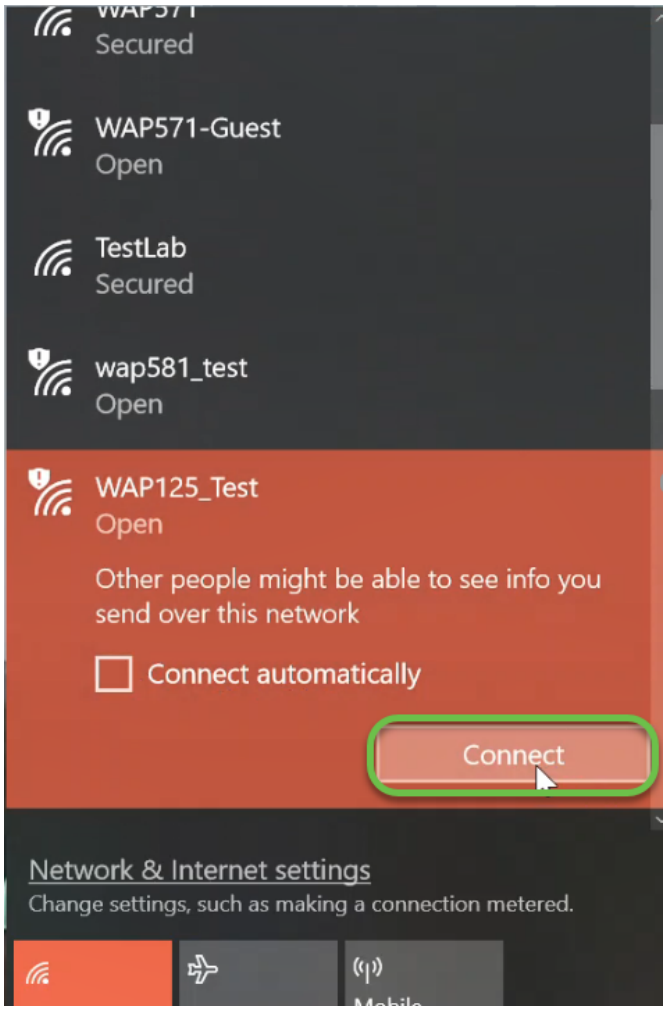


Step 12. Choose the network and specify that it will choose **AD** as the *Guest Access Instance* for authentication. Click **Save.**

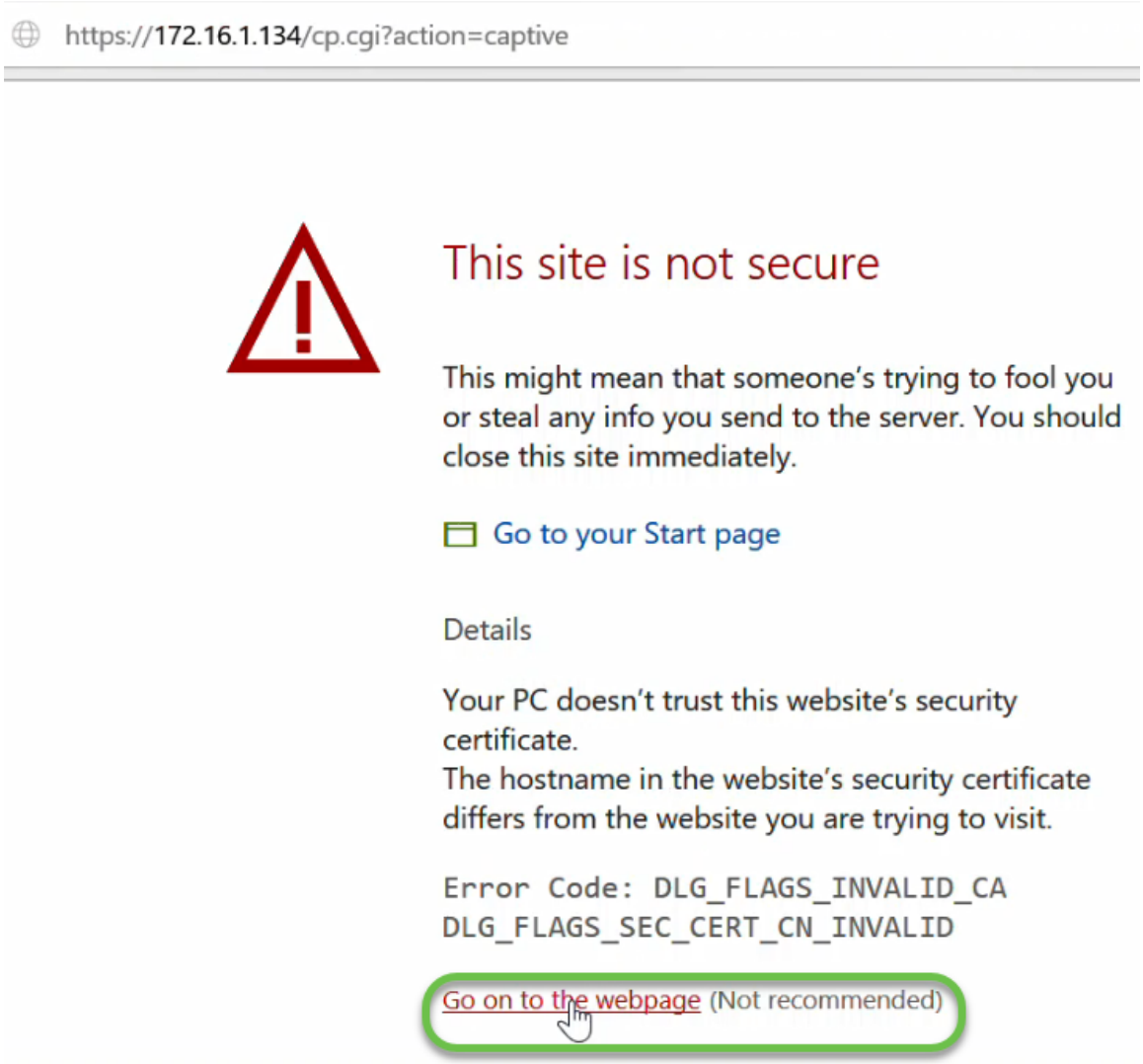


Step 13. To connect to the guest wireless network using AD authentication, go the wireless

option on your personal computer (PC) and select the network that has been configured for AD authentication and click **Connect.**

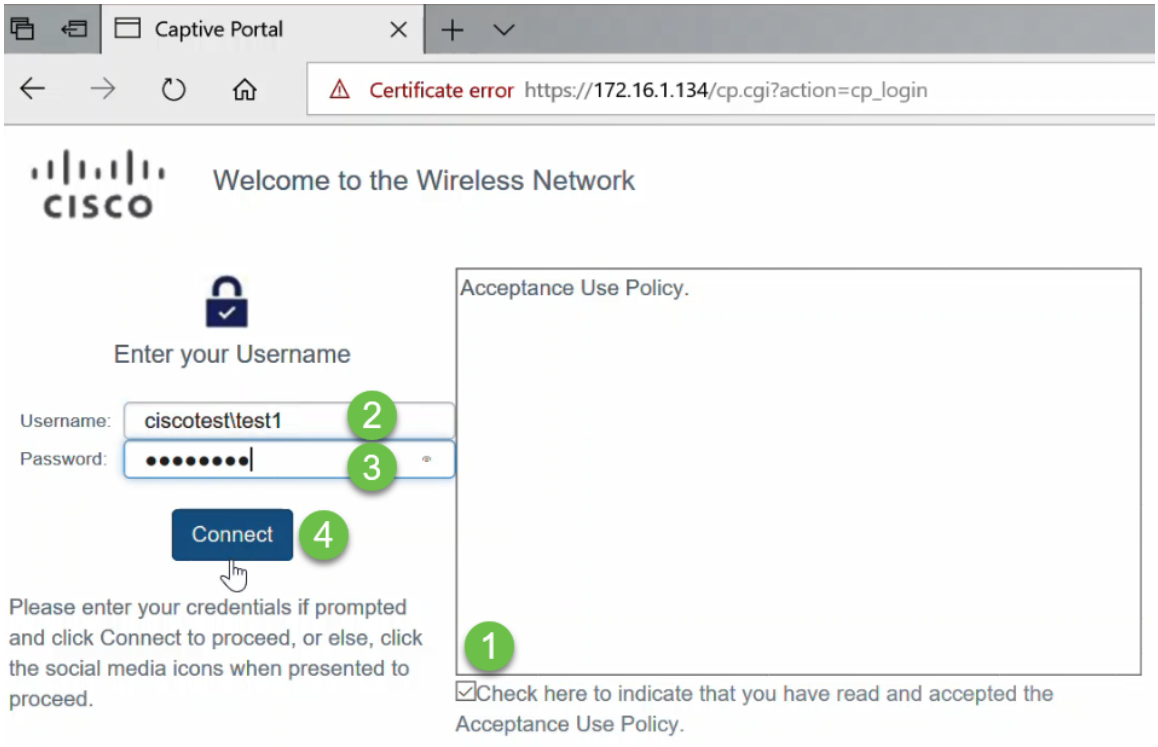


Step 14. Once connected, a web browser window will open up with the standard security certificate warning. Click on **Go on to the webpage**.



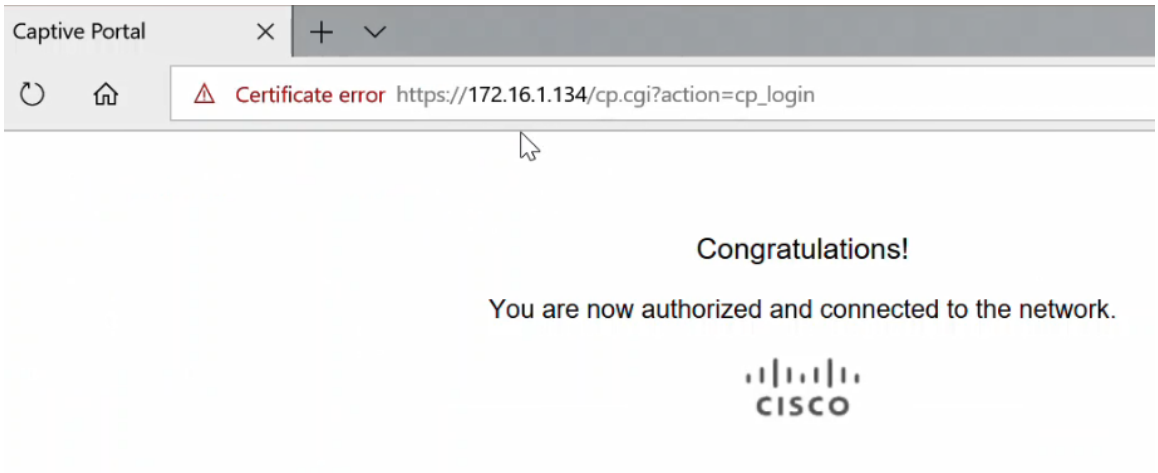
NOTE: The screen may appear differently based on the browser you are using.

Step 15. The *Captive Portal* page is launched. Check the Acceptance Use Policy box to accept the policy and enter the *Username* and *Password* of the user in AD. Click **Connect** to connect to the network.



NOTE: If there are multiple domains, then the username will include the domain name\username. In this example, it is ciscotest\test1.

Step 16. You are now authenticated and have internet access.



Conclusion

You should now have successfully configured the active directory guest authentication on WAP125 or WAP581 and verified its functionality.