Features in the 1.0.1 Release for the WAP125 and WAP581

Objective

The purpose of this article is to highlight and give an overview of the newest features in this firmware update for the Wireless Access Points (WAP).

Applicable Devices

- WAP125
- WAP581

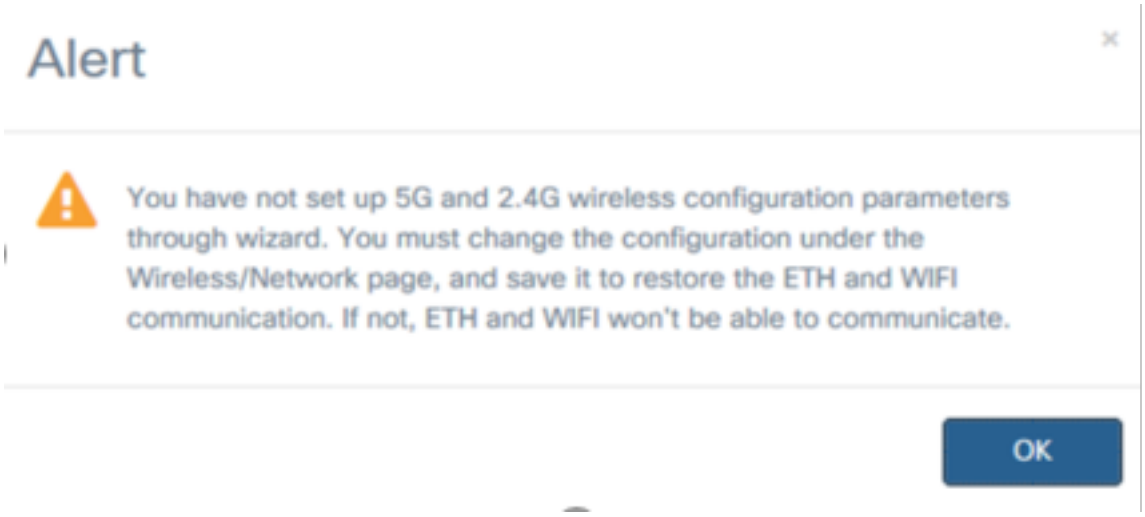
Software Version

- 1.0.1

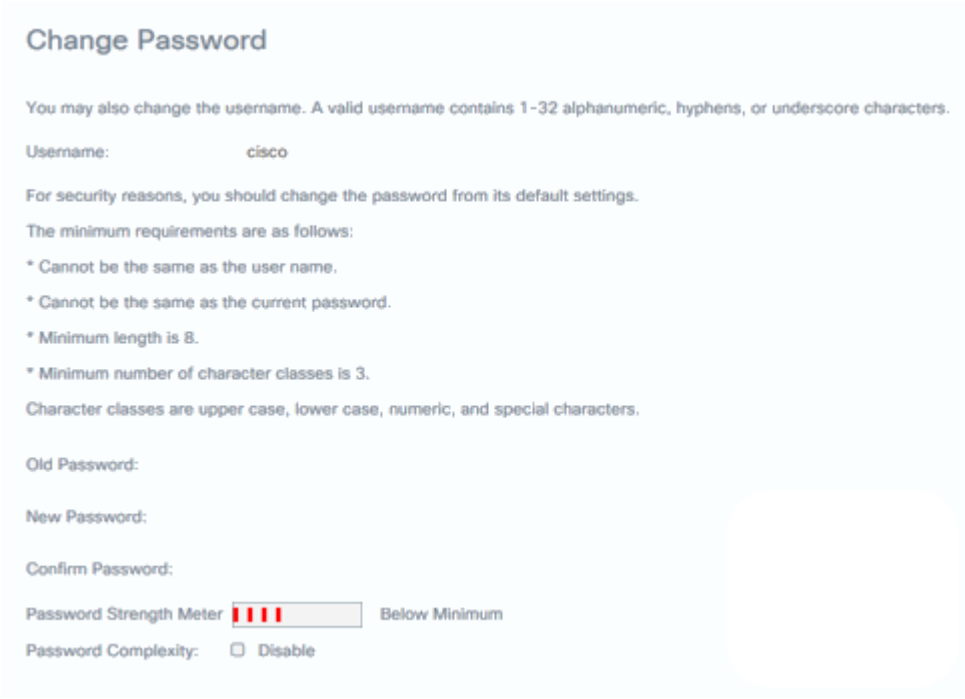
Setup Wizard

In previous versions of the WAP125 and WAP581, if you canceled the Setup Wizard you would be logged out of the WAP.

The 1.0.1 firmware allows you to cancel the Setup Wizard. You will be sent an alert.



After you acknowledge the alert, you are able to set the local password for the WAP.



You can manually configure all settings at another time.

Mobile Optimized Setup Wizard

The WAP125 and WAP581 devices now include management pages, Captive Portal pages, and Setup Wizards optimized for mobile devices.

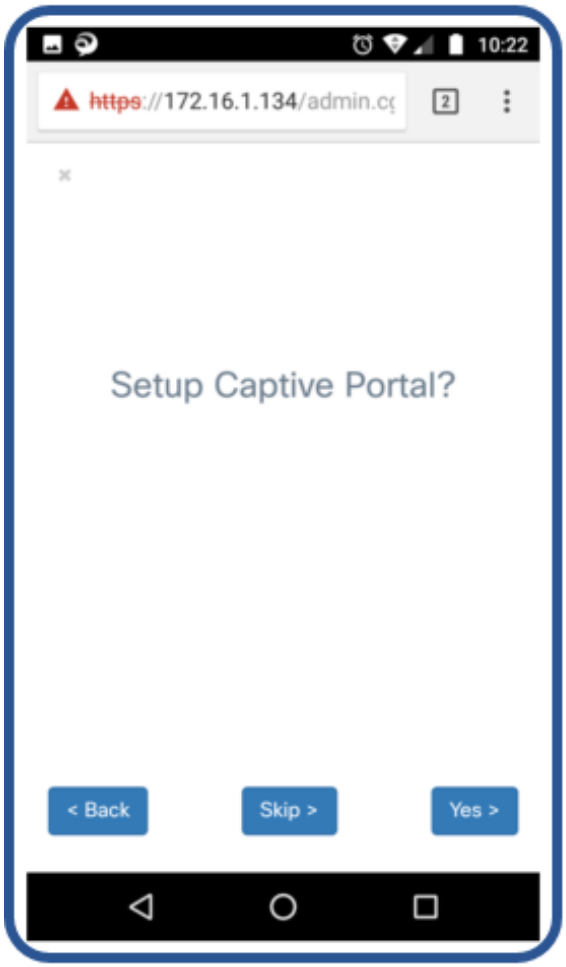
You have the ability to configure a WAP by running the Setup Wizard through a mobile device using the new mobile optimized setup page.

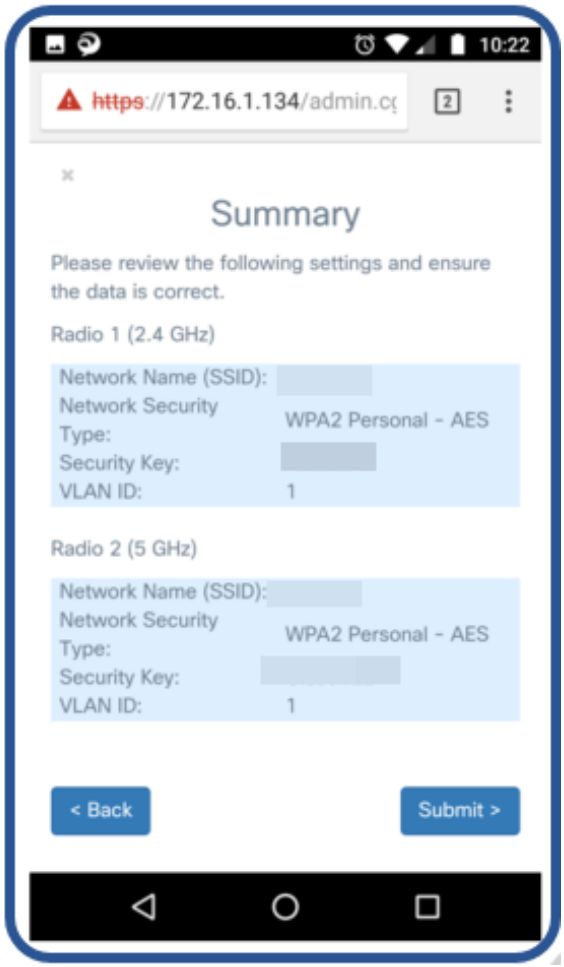
Connect to the ciscoSB-Setup SSID and go to either the IP address of the WAP or the default IP of 192.168.1.245 to configure the device.

The Setup Wizard is the same on the mobile optimized page as on the standard page.


10:21
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 2 (5 GHz)
< Back
Next >


10:22
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 1 (2.4 GHz)
< Back
Next >


10:22
https://172.16.1.134/admin.cg
Setup Captive Portal?
< Back
Skip >
Yes >


10:22
https://172.16.1.134/admin.cg
Summary
Please review the following settings and ensure the data is correct.
Radio 1 (2.4 GHz)
Network Name (SSID):
Network Security Type:
WPA2 Personal - AES
Security Key:
VLAN ID:
1
Radio 2 (5 GHz)
Network Name (SSID):
Network Security Type:
WPA2 Personal - AES
Security Key:
VLAN ID:
1
< Back
Submit >

Third Party Guest Authentication

Third party guest authentication allows you to configure a guest network using Facebook or Google authentication, a secure authentication validated by a third party. The WAP125 allows for one Guest Access Instance, while the WAP581 allows for multiple instances.

Requirements:

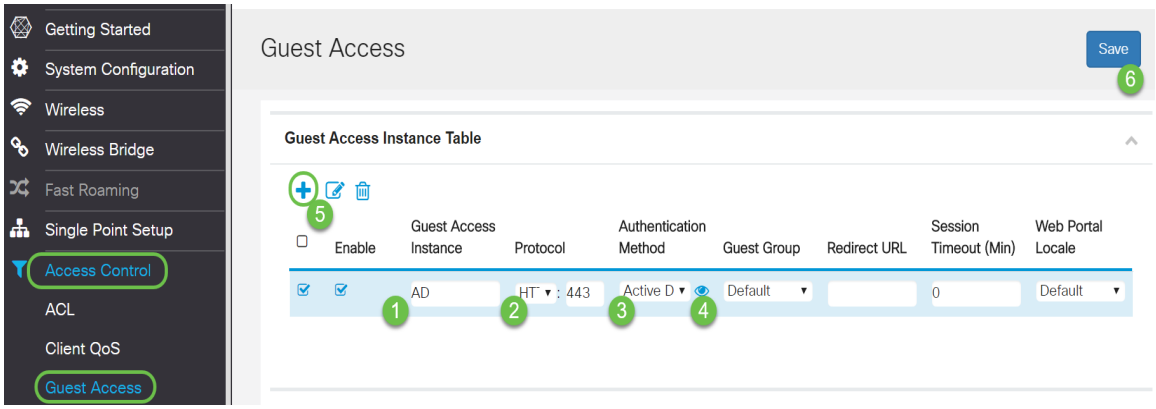
- Internet connectivity to Facebook or Google
- Users must have or create a Facebook or Google account and wireless access to their public profile
- Facebook or Google must be accessible before the authentication is complete so an end user can sign in to validate their credentials.

A business may also choose to have other sites, such as their business web site, available prior to authentication.

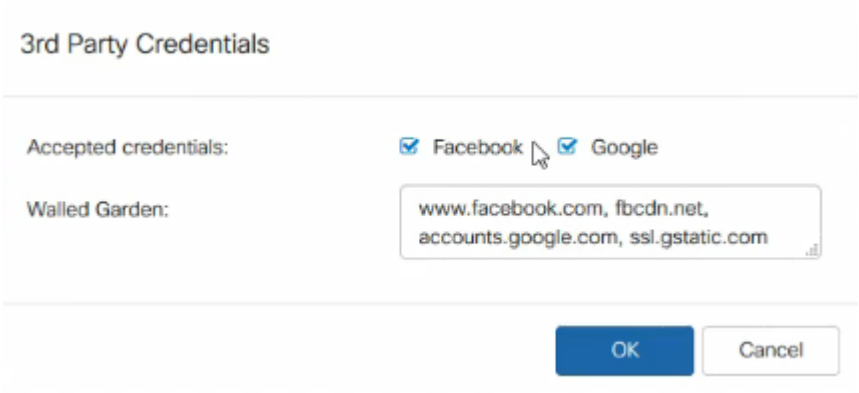
Click **Access Control > Guest Access** and click on the *plus* sign.

A brief explanation of each of the numbers below:

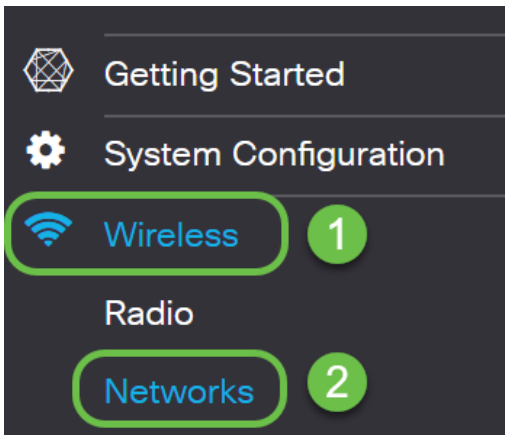
1. Add the name for the Active Directory
2. You should configure the Captive Portal page to use **HTTPS**, not HTTP. If you choose HTTP, you can inadvertently expose usernames and passwords by transmitting them in unencrypted clear text through the air. Secure HTTPS Captive Portal page is recommended.
3. Choose **3rd Party Credentials**.
4. Click on the graphic of the **eye** to select accepted credentials and the correct websites.
5. This is where you would click if you choose to add another Guest Access Instance.
6. Be sure to **Save**.



This example shows Facebook and Google selected. The websites are listed for the Walled Garden.



You then will need to navigate to **Wireless > Networks** on the navigation pane to add or change the Guest Access Instance to the name of the Active Directory.

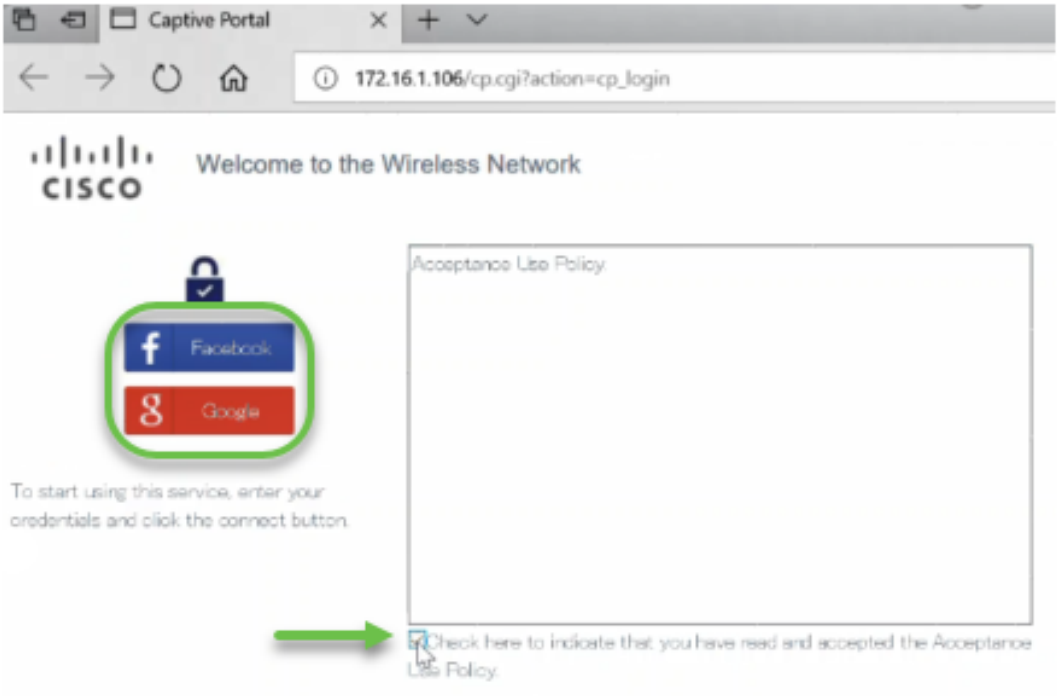


Note: The WAP125 allows you one Guest Access Instance so you must decide if you want to configure for Third Party Authentication or Active Directory Authentication. The WAP581 allows multiple means of authentication.

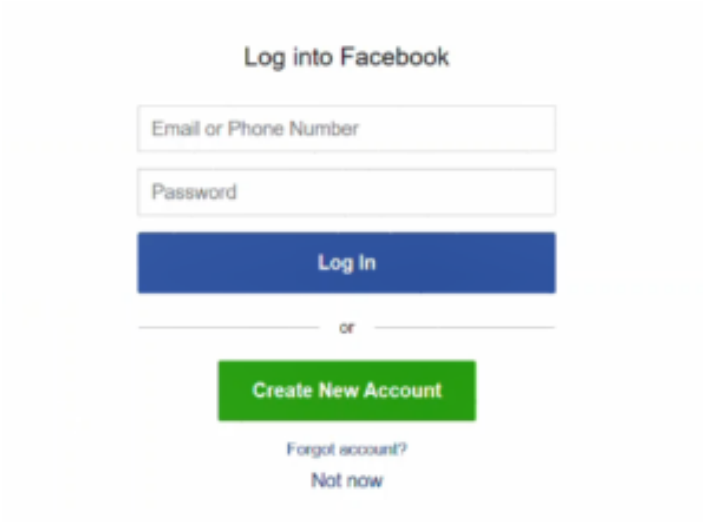
Third Party Client Authentication

When a client clicks to join a wireless connection, the Captive Portal will open. In this example, Facebook and Google are options. The customer needs to check the box to indicate that they have read and accepted the *Acceptance Use Policy*, and then either the **Facebook** or **Google** option to log in.

Note: The first time logging in the client will receive a question asking if they want to use Captive Portal. They need to select *yes.*



The client can then enter credentials. In this example, Facebook was used.



The client is now able to use the internet.

Active Directory Guest Authentication

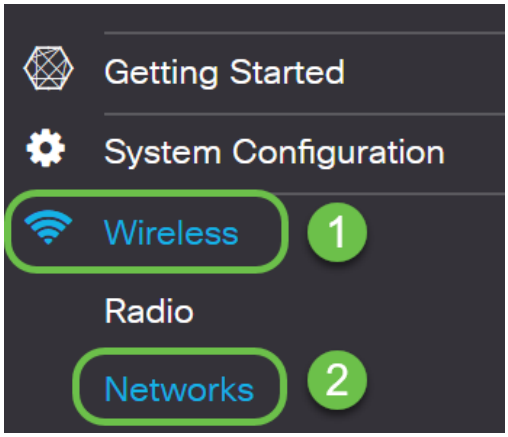
To support Active Directory Authentication, the WAP will need to communicate with a Windows Domain Controller to provide authentication. As an administrator, you have the ability to have up to three Windows Domain Controllers set up to communicate on the WAP581.

Click **Access Control > Guest Access** and click on the **plus** sign.

A brief explanation of each of the numbers below:

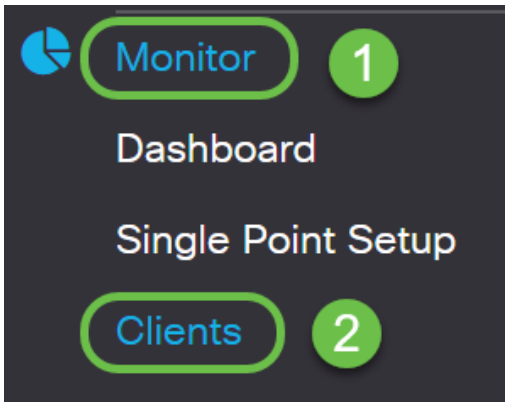
1. Add the name for the Active Directory
2. You should configure the Captive Portal page to use **HTTPS**, not HTTP. If you choose HTTP, you can inadvertently expose usernames and passwords by transmitting them in unencrypted clear text through the air. Secure HTTPS Captive Portal page is recommended.
3. Choose **Active Directory Service**
4. Click on the graphic of the **eye** to add the IP address. You can do a test from there to check for connectivity.
5. This is where you would click if you choose to add another Guest Access Instance.
6. Be sure to Save.

You then will need to navigate to **Wireless > Networks** on the navigation pane to add or change the Guest Access Instance to the name of the Active Directory.



To see clients on the network, click **Monitor > Clients** on the navigation pane.

1. *Monitor* shows the number of connected clients
2. *Clients* shows the details of the client. You can export these if you want to keep a record of the people that connected.

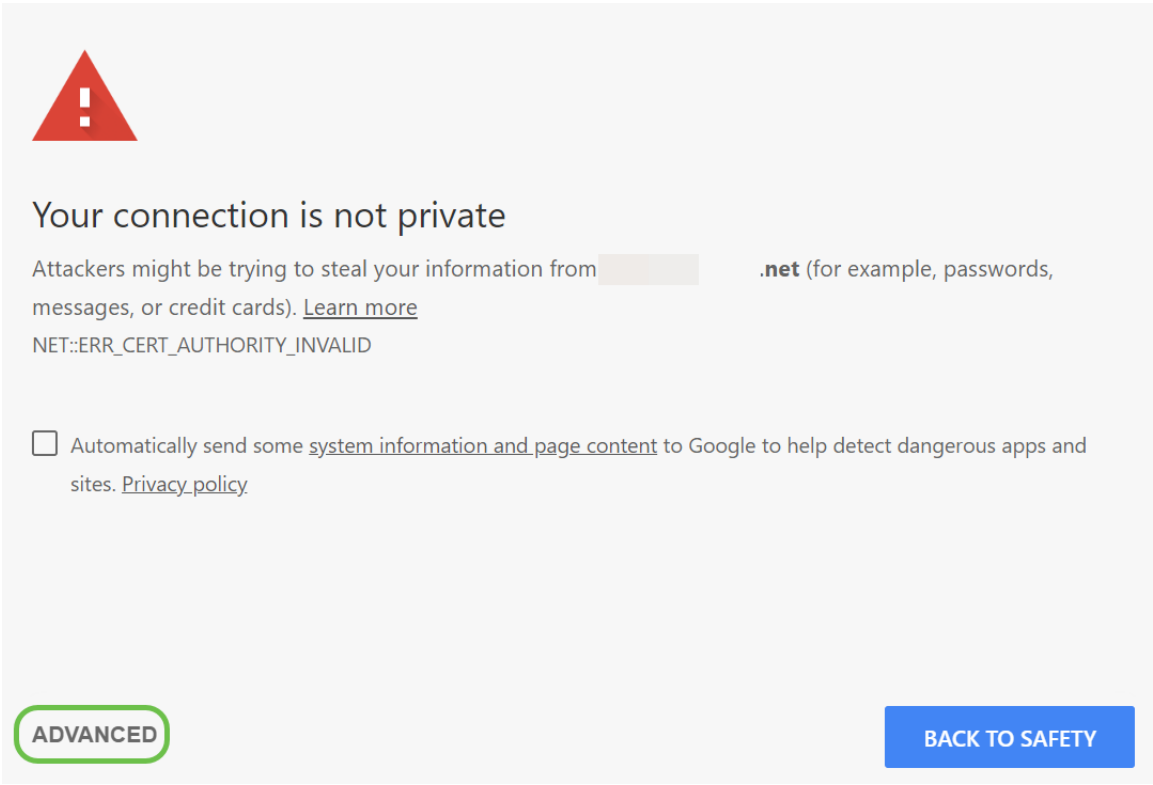


For more information about how to monitor guests, click here.

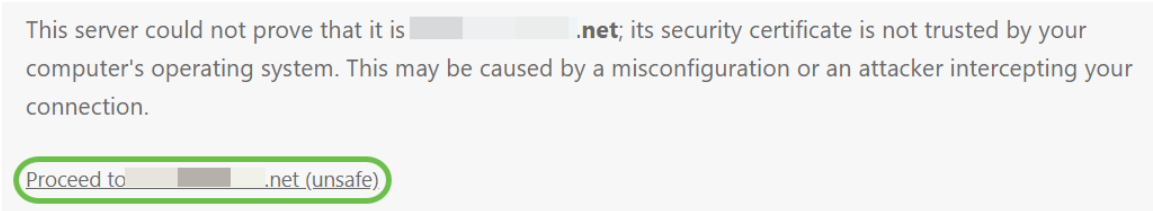
Active Directory Client Authentication

When a client is in the Active Directory, they have the ability to log in to the WAP to access the internet. When they choose the wireless access point, they may receive a warning message similar to this, dependent on the web browser they use. The warning occurs if

there isn't a certificate assigned to the page by a trusted Certificate Authority. The client needs to click on **ADVANCED**.



The client might then receive a warning message similar to the following:



A portal page has been launched. On this page they should enter their credentials and check the box to indicate that they have read and accepted the *Acceptance Use Policy*.

They will receive a welcome message and will be able to safely use the internet.

You are now familiar with some of the latest features that come with the latest WAP125 and WAP581 update.

For more detailed information about these and other new features, click the companion article links below.

Using the Setup Wizard on the WAP125 or WAP581

Using the Setup Wizard on a Mobile Device for the WAP125 or WAP581

How To: Cisco Umbrella Integration

How To: Cisco CloudShark Integration

How To: Configure 3rd party authentication Settings on the WAP125 or WAP581

How To: Microsoft Active Directory Guest Authentication

How To: Umbrella - Registering a new device if you lost your API key secret

To Customize the Appearance of your Captive Portal

View a video related to this article...

Click here to view other Tech Talks from Cisco