Konfigurieren der Active Directory-Gastauthentifizierung auf WAP125 oder WAP581

Ziel

Mithilfe der Active Directory-Gastauthentifizierung (AD) kann ein Client eine Captive Portal-Infrastruktur konfigurieren, um den internen Windows Directory-Dienst für die Authentifizierung zu verwenden. Captive Portal ist eine Funktion, mit der ein Administrator Clients, die eine Verbindung zum Wireless Access Point (WAP)-Netzwerk herstellen, blockieren kann, bis ihnen der Zugriff auf das Netzwerk gewährt wird. Clients werden auf eine Webseite zur Authentifizierung und zu Zugriffsbedingungen geleitet, bevor sie eine Verbindung zum Netzwerk herstellen können. Die Überprüfung des Captive Portals richtet sich sowohl an Gäste als auch an authentifizierte Benutzer des Netzwerks. Diese Funktion nutzt den Webbrowser und verwandelt ihn in ein Authentifizierungsgerät.

Captive Portal-Instanzen sind ein definierter Satz von Konfigurationen zur Authentifizierung von Clients im WAP-Netzwerk. Instanzen können so konfiguriert werden, dass sie auf verschiedene Arten auf Benutzer reagieren, wenn sie versuchen, auf die zugehörigen virtuellen Access Points zuzugreifen. Captive Portale werden häufig an Wi-Fi-Hotspots eingesetzt, um sicherzustellen, dass die Benutzer die Nutzungsbedingungen akzeptieren und Sicherheitszertifikate vorlegen, bevor sie Zugang zum Internet erhalten.

Zur Unterstützung der AD-Authentifizierung muss der WAP mit einem bis drei Windows-Domänencontrollern kommunizieren, um die Authentifizierung bereitzustellen. Es kann mehrere Domänen für die Authentifizierung unterstützen, indem Domänen-Controller aus verschiedenen AD-Domänen ausgewählt werden.

In diesem Dokument wird erläutert, wie Sie die AD-Gastauthentifizierung auf dem WAP125 oder WAP581 konfigurieren.

Anwendbare Geräte

- WAP125
- WAP581

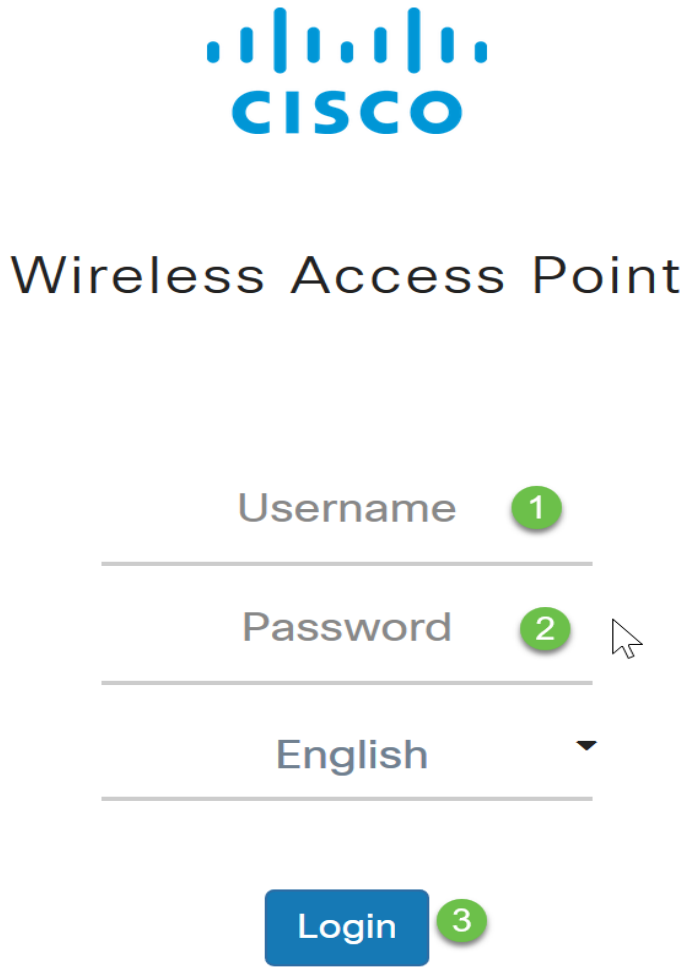
Softwareversion

- 1,0/1

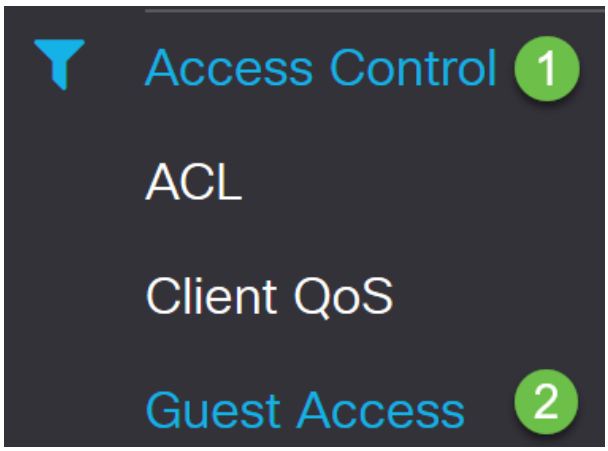
Active Directory-Gastauthentifizierung konfigurieren

Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm des WAP an, indem Sie den Benutzernamen und das Kennwort eingeben. Der Standard-Benutzername und das Kennwort lautet cisco/cisco. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie stattdessen die Anmeldeinformationen ein. Klicken Sie auf **Anmelden.**

HINWEIS: In diesem Artikel wird der WAP125 verwendet, um die Konfiguration der AD-Gastauthentifizierung zu veranschaulichen. Die Menüoptionen können je nach Gerät leicht variieren.



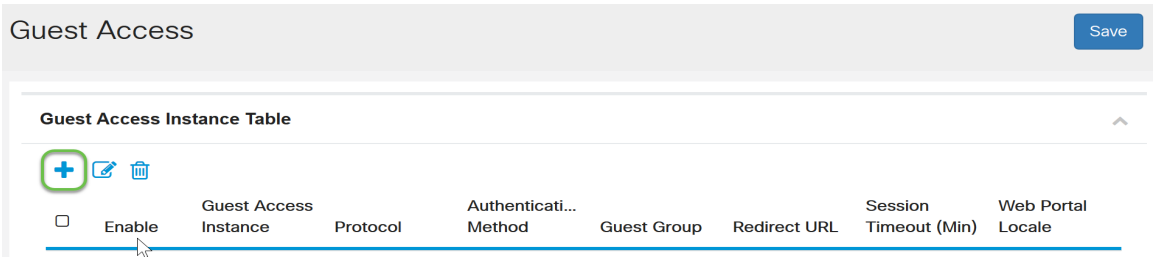
Schritt 2: Wählen Sie **Zugriffskontrolle > Gastzugriff aus**.



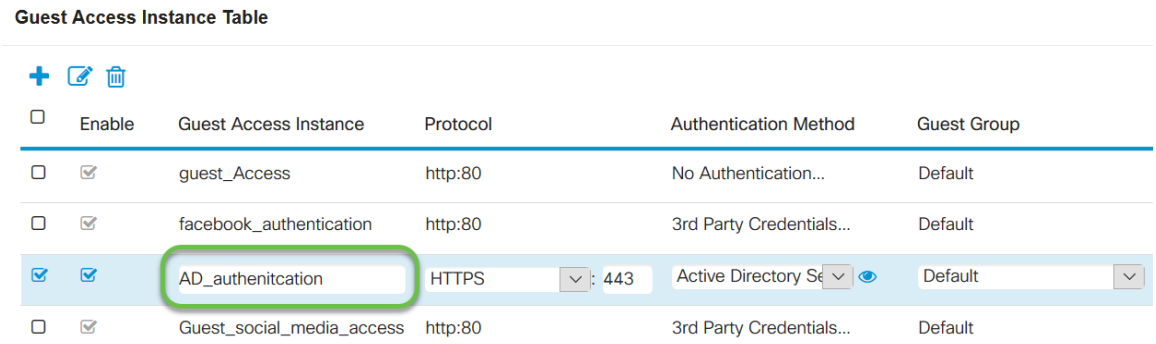
Schritt 3: In der *Gastzugriffs-Instanztabelle* können Sie entweder eine neue *Gastzugriffsinstanz* hinzufügen oder eine vorhandene bearbeiten. Die Gastzugangsfunktion des WAP125 oder WAP581-Zugangspunkts bietet Wireless-Verbindungen zu temporären Wireless-Clients im Bereich des Geräts. Der Access Point sendet zwei verschiedene Service Set Identifiers (SSIDs): eine für das Hauptnetzwerk und die andere für das Gastnetzwerk. Die Gäste werden dann zu einem Captive Portal weitergeleitet, wo sie ihre Anmeldeinformationen eingeben müssen. So bleibt das Hauptnetzwerk sicher, während die Gäste weiterhin auf das Internet zugreifen können.

Die Einstellungen des Captive Portals werden in der Guest Access Instance Table des webbasierten Dienstprogramms des WAP konfiguriert. Die Gastzugangsfunktion ist besonders in Hotel- und Bürolobbys, Restaurants und Einkaufszentren nützlich.

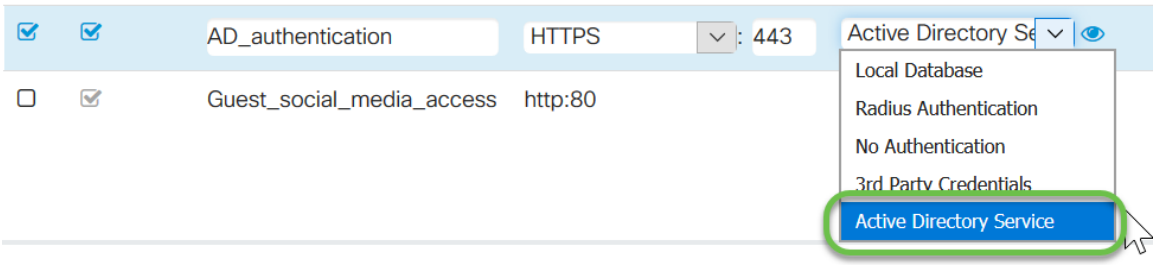
In diesem Beispiel wird eine neue *Gastzugriffsinstanz* durch Klicken auf das **Pluszeichen** hinzugefügt.



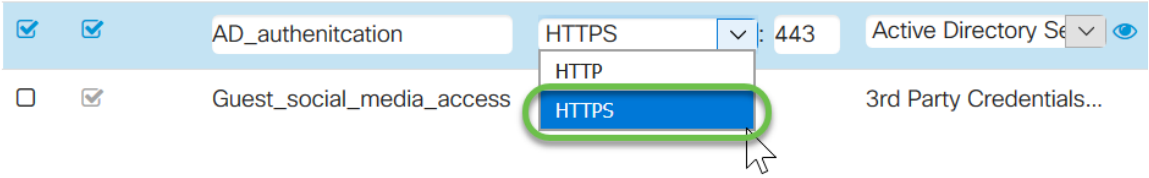
Schritt 4: Benennen Sie die *Gastzugriffsinstanz*. In diesem Beispiel wird es **AD_authentication** genannt.



Schritt 5: Wählen Sie die *Authentifizierungsmethode* als **Active Directory-Dienst aus**.

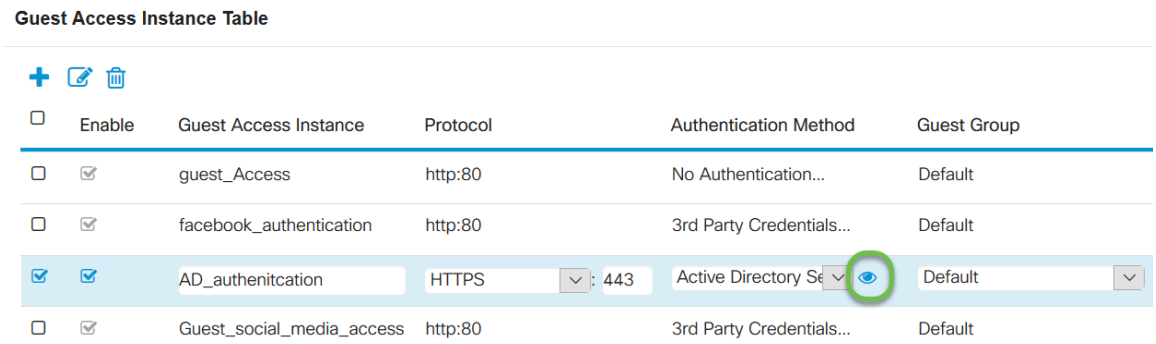


Schritt 6: Wenn Sie Active Directory-Dienst als *Authentifizierungsmethode* auswählen, wechselt das Protokoll von Hyper Text Transfer Protocol (HTTP) zu Hyper Text Transfer Protocol Secure (HTTPS).

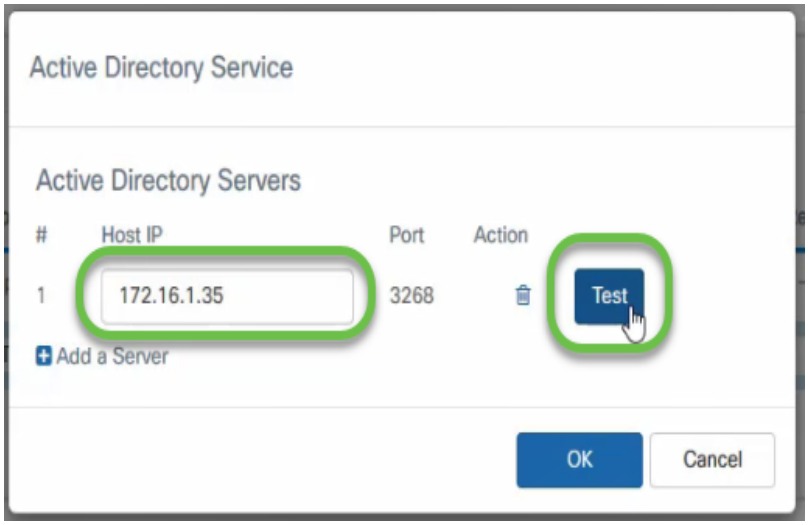


HINWEIS: Es ist sehr wichtig, dass ein Client die Captive Portal-Seite so konfiguriert, dass sie HTTPS und nicht HTTP verwendet, da erstere sicherer ist. Wenn ein Client HTTP auswählt, kann er Benutzernamen und Kennwörter versehentlich verfügbar machen, indem er sie in unverschlüsseltem Klartext überträgt. Es empfiehlt sich, eine HTTPS-Seite für das Captive Portal zu verwenden.

Schritt 7: Konfigurieren Sie die IP-Adresse des AD-Servers, indem Sie in der Spalte *Authentifizierungsmethode* neben dem Active Directory-Dienst auf das **blaue Symbol** klicken.

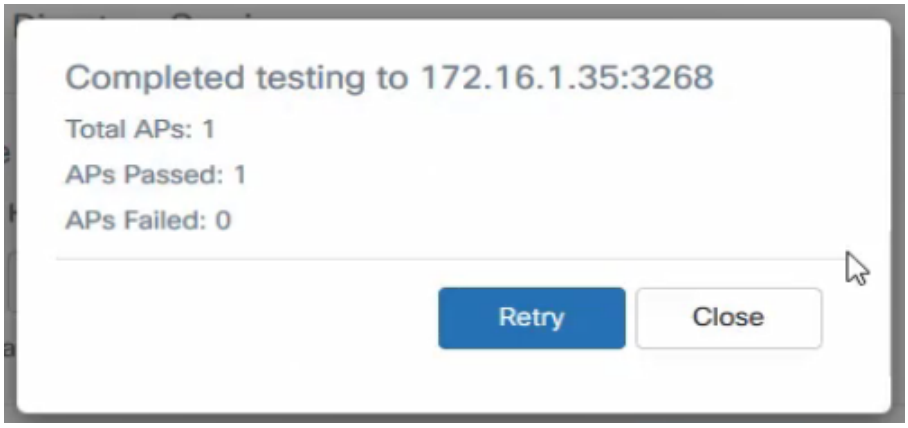


Schritt 8: Ein neues Fenster wird geöffnet. Geben Sie die IP-Adresse für den AD-Server ein. In diesem Beispiel wird die Host-IP-Adresse **172.16.1.35** verwendet. Als optionalen Schritt können Sie auf **Test** klicken, um die Gültigkeit zu überprüfen.



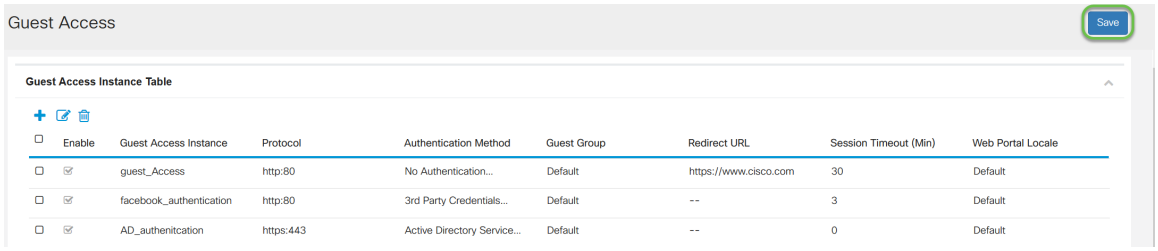
Schritt 9: (Optional) Wenn Sie im vorherigen Schritt auf **Test** klicken, wird ein weiteres Popup-Fenster geöffnet, in dem Sie *Benutzername* und *Kennwort* des Benutzers in AD eingeben können und auf **Test starten** klicken.

Wenn sie gültig ist, besteht der Test erfolgreich, und der folgende Bildschirm wird angezeigt. Dadurch wird bestätigt, dass Sie eine Verbindung zum Domänen-Controller herstellen und sich authentifizieren können.

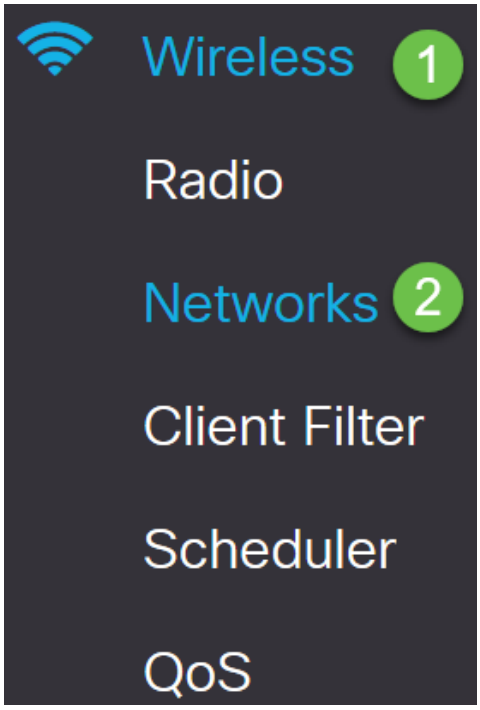


HINWEIS: Sie können bis zu 3 AD-Server hinzufügen.

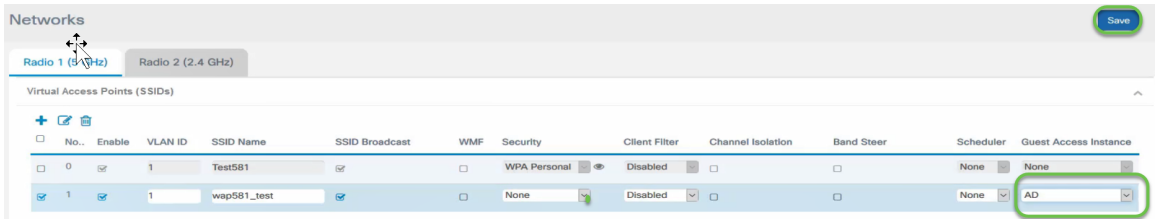
Schritt 10: Speichern Sie die Änderungen.



Schritt 11: Gehen Sie zum Menü, und wählen Sie **Wireless > Networks** aus.

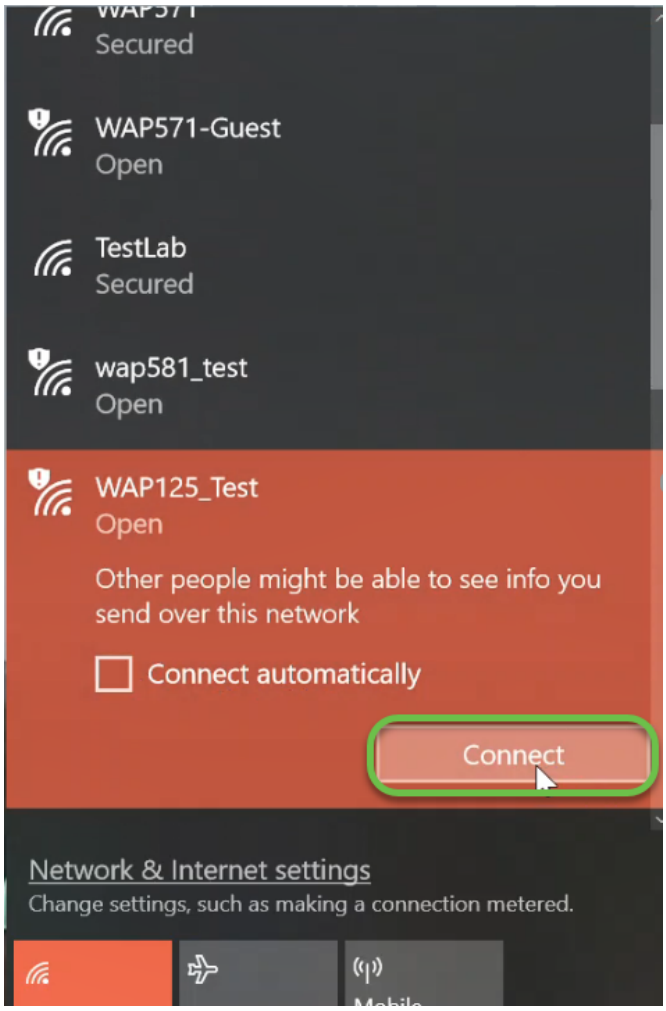


Schritt 12: Wählen Sie das Netzwerk aus, und geben Sie an, dass **AD** als *Gastzugriffsinstanz* für die Authentifizierung ausgewählt wird. Klicken Sie auf **Speichern.**

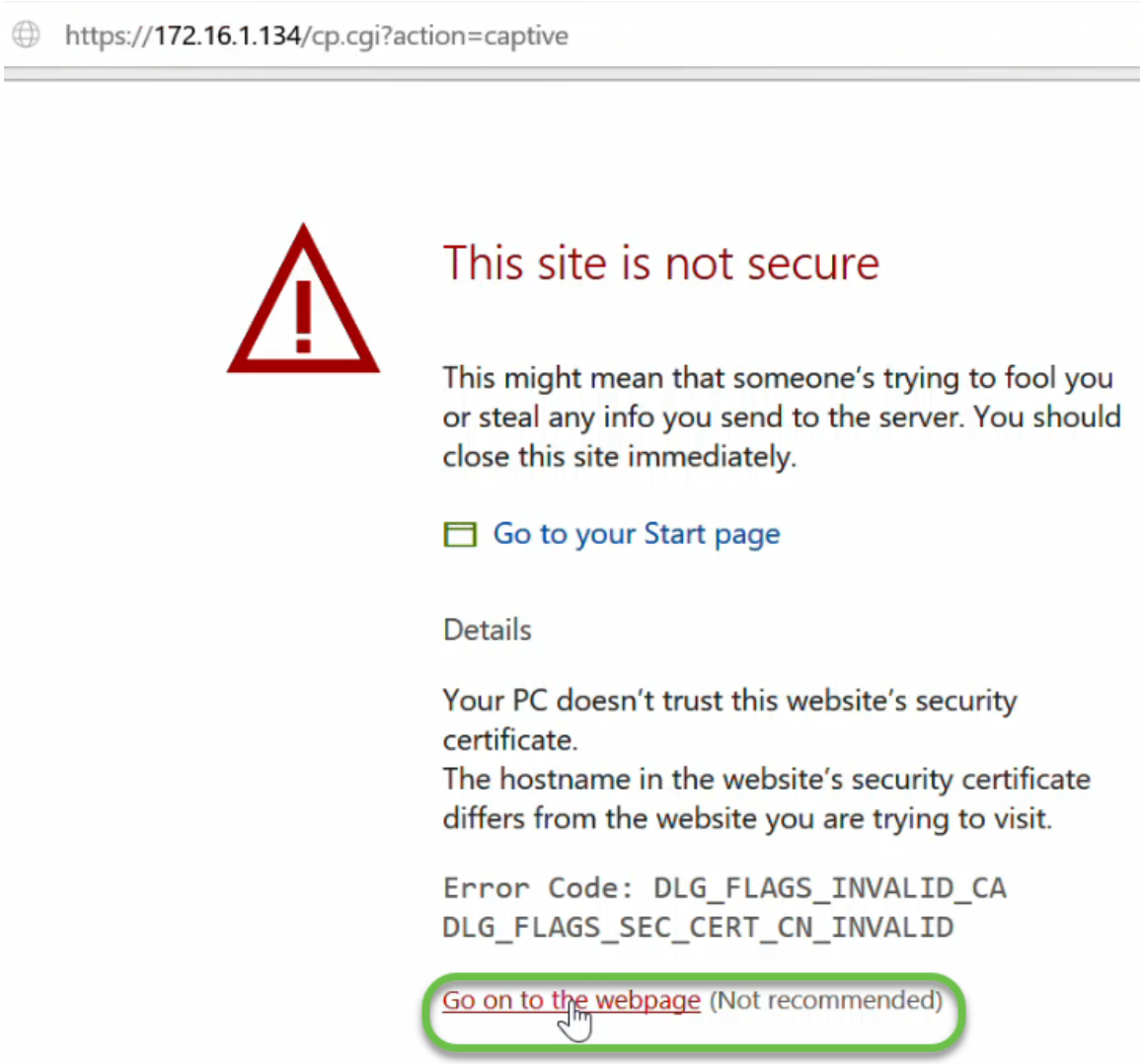


Schritt 13: Um über AD-Authentifizierung eine Verbindung zum Wireless-Gastnetzwerk

herzustellen, gehen Sie zur Wireless-Option Ihres PCs, wählen Sie das Netzwerk aus, das für die AD-Authentifizierung konfiguriert wurde, und klicken Sie auf **Verbinden.**

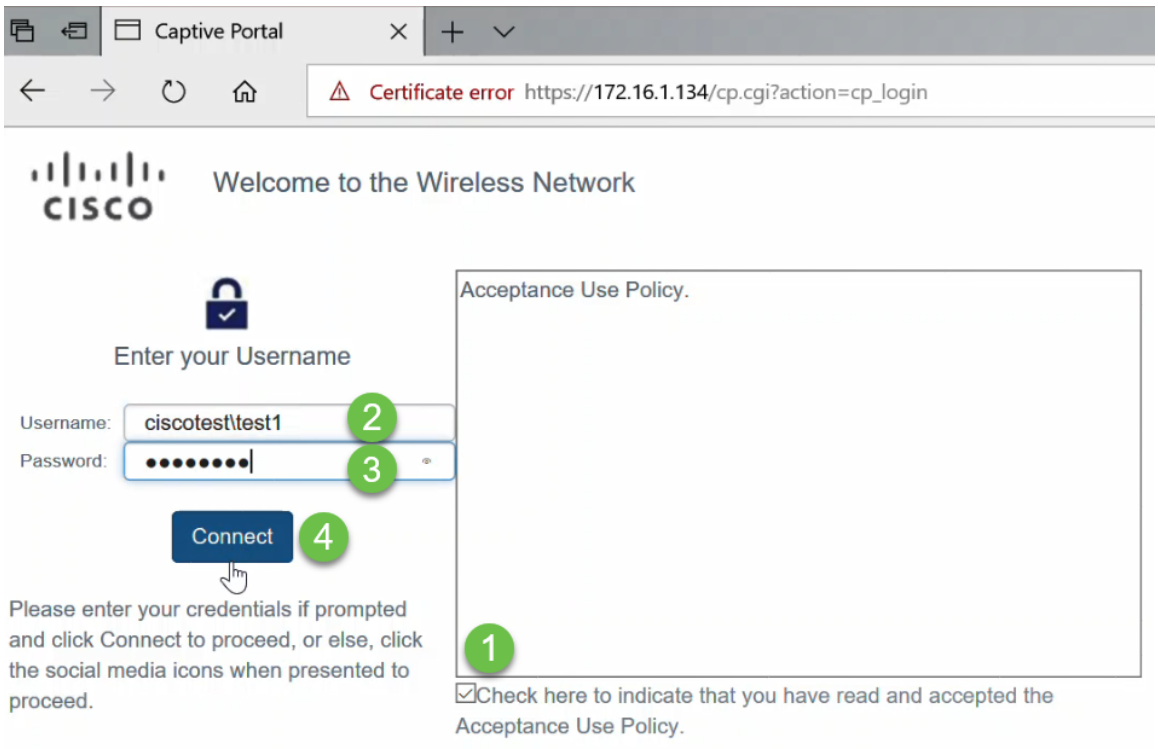


Schritt 14: Nach dem Herstellen der Verbindung wird ein Webbrowser mit der Warnung für das Standard-Sicherheitszertifikat geöffnet. Klicken Sie auf **Weiter zur Webseite**.



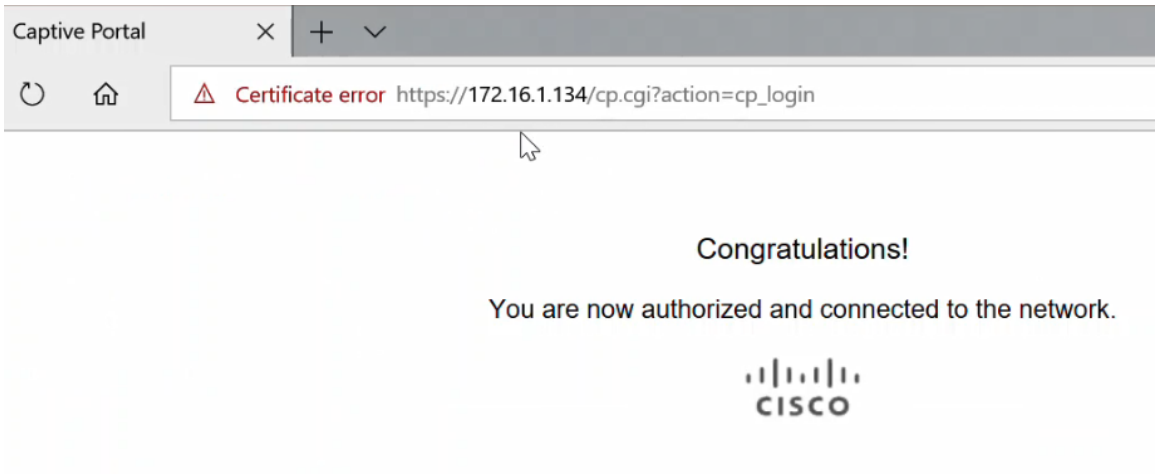
HINWEIS: Der Bildschirm wird möglicherweise je nach Browser, den Sie verwenden, unterschiedlich angezeigt.

Schritt 15: Die Seite *Captive Portal* wird aufgerufen. Aktivieren Sie das Kontrollkästchen Acceptance Use Policy (Richtlinie für Akzeptanz verwenden), um die Richtlinie zu akzeptieren, und geben Sie den *Benutzernamen* und das *Kennwort* des Benutzers in AD ein. Klicken Sie auf **Verbinden**, um eine Verbindung zum Netzwerk herzustellen.



HINWEIS: Wenn es mehrere Domänen gibt, enthält der Benutzername den Domänennamen\Benutzernamen. In diesem Beispiel ist es ciscotest\test1.

Schritt 16: Sie sind nun authentifiziert und haben Internetzugang.



Schlussfolgerung

Sie sollten jetzt die Active Directory-Gastauthentifizierung für WAP125 oder WAP581 erfolgreich konfiguriert und deren Funktionalität überprüft haben.