

Active Directory Guest Authentication on WAP125 of WAP581 configureren

Doel

Active Directory (AD) hostverificatie stelt een client in staat om een host-infrastructuur te configureren die gebruik maakt van hun interne Windows Directory-service voor verificatie. Captive Portal is een functie waarmee een beheerder klanten die verbinding maken met het Wireless Access Point (WAP)-netwerk kan blokkeren totdat deze toegang tot het netwerk hebben. Clients worden gericht op een webpagina voor verificatie en toegangsvoorwaarden voordat zij verbinding kunnen maken met het netwerk. De controle van het homopagina van het Captive Portal is voor zowel gasten als voor geauthentiseerde gebruikers van het netwerk. Deze functie maakt gebruik van de webbrowser en verandert deze in een verificatieapparaat.

Captive portal instanties zijn een gedefinieerde set configuraties die worden gebruikt om klanten op het WAP-netwerk voor authentiek te verklaren. Instanties kunnen zo worden geconfigureerd dat ze op verschillende manieren reageren op gebruikers terwijl ze proberen toegang te krijgen tot de bijbehorende virtuele access points. Klantenportaal wordt vaak gebruikt op Wi-Fi hotspotlocaties om te zorgen dat gebruikers akkoord gaan met voorwaarden en voorwaarden en om veiligheidsaanmeldingsgegevens te verstrekken voordat ze toegang krijgen tot internet.

Ter ondersteuning van AD-verificatie moet WAP met één of drie Windows-controllers communiceren om verificatie te kunnen leveren. Het kan meerdere domeinen voor authenticatie ondersteunen door domeincontrollers uit verschillende AD domeinen te kiezen.

Het doel van dit document is om u te tonen hoe u de AD gastauthenticatie op WAP125 of WAP581 moet configureren.

Toepasselijke apparaten

- WAP125
- WAP581

Softwareversie

- 1.0.1

Active Directory Guest-verificatie configureren

Stap 1. Meld u aan bij het web configuratie hulpprogramma van de WAP door de gebruikersnaam en het wachtwoord in te voeren. De standaardwaarden voor gebruikersnaam en wachtwoord zijn cisco/cisco. Als u een nieuwe gebruikersnaam of wachtwoord heeft geconfigureerd, moet u deze inloggegevens gebruiken. Klik op **Aanmelden**.


OPMERKING: In dit artikel wordt WAP125 gebruikt om de configuratie van AD-gastverificatie aan te tonen. De menuopties kunnen licht variëren afhankelijk van het model van het

apparaat.



Wireless Access Point

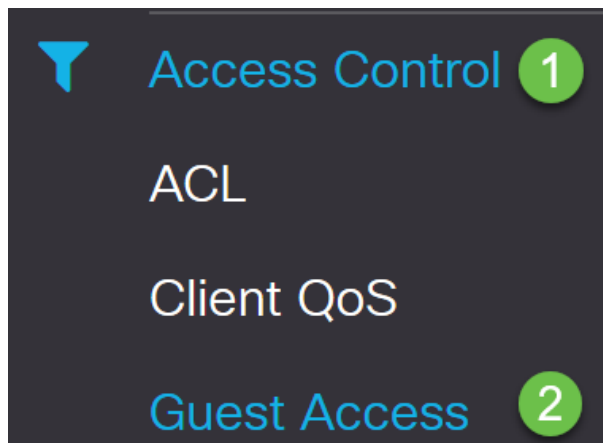
Username 1

Password 2 

English ▼

Login 3

Stap 2. Kies **toegangscontrole > Gasttoegang**.

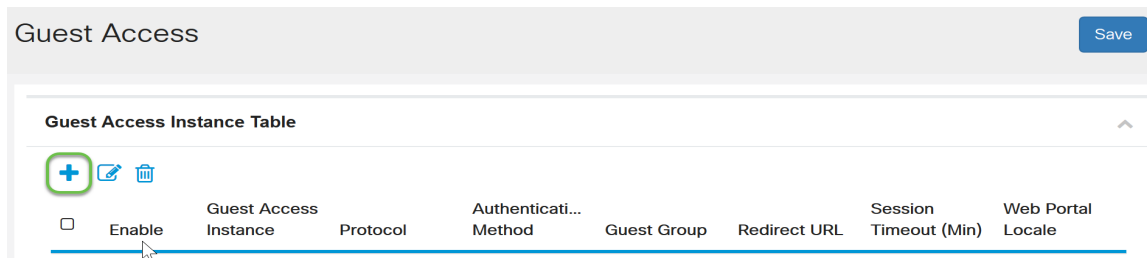


Stap 3. In de *tabel van het instel van de toegang* kunt u een nieuw *exemplaar* van de *Gast* toevoegen of een bestaand exemplaar bewerken. De Guest Access-functie van WAP125 of WAP581 access point biedt draadloze verbindingen aan tijdelijke draadloze klanten binnen het bereik van het apparaat. Het werkt door het toegangspunt uitzendt twee verschillende Service Set Identificatoren (SSID's) uit: één voor het hoofdnetwerk, en de andere voor het gastnetwerk. Gegeven worden dan opnieuw naar een Captive Portal verwezen, waar zij nodig zijn om hun geloofsbrieven in te voeren. In feite houdt dit het hoofdnetwerk veilig terwijl het gasten toegang tot het internet geeft.

De instellingen van het Captive Portal worden ingesteld in de tabel van het Guest Access

Instance van het webgebaseerde hulpprogramma van WAP. De functie Gasttoegang is vooral bruikbaar in hotels en kantoorlobby's, restaurants en winkelcentra.

In dit voorbeeld wordt er een nieuw *exemplaar* van de *Gast Access* toegevoegd door op het pictogram plus te klikken.

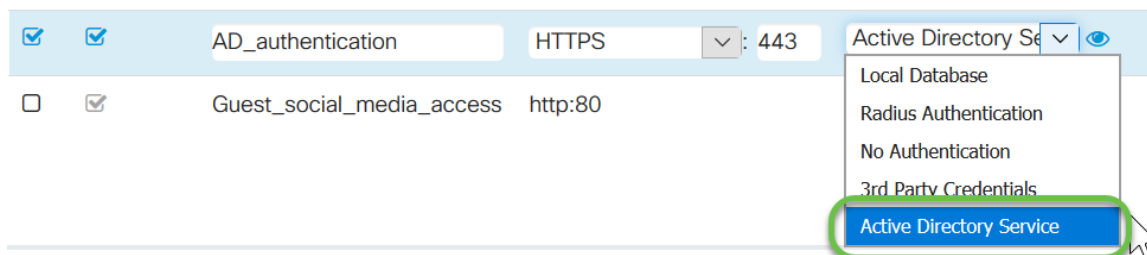


Stap 4. Geef het *Guest Access Instance* een naam. In dit voorbeeld heet het **AD_authentication**.

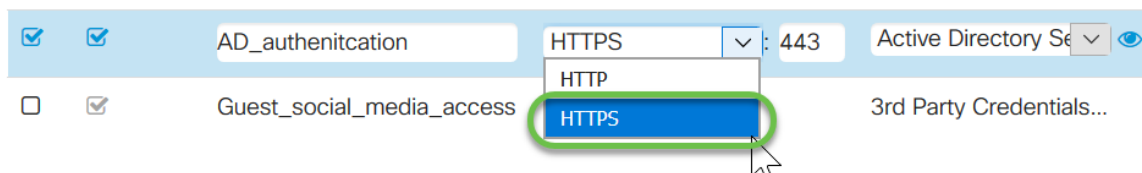
Guest Access Instance Table

Enable	Guest Access Instance	Protocol	Authenticati...	Guest Group
<input type="checkbox"/>	guest_Access	http:80	No Authentication...	Default
<input type="checkbox"/>	facebook_authentication	http:80	3rd Party Credentials...	Default
<input checked="" type="checkbox"/>	AD_authentication	HTTPS	Active Directory Se	Default
<input type="checkbox"/>	Guest_social_media_access	http:80	3rd Party Credentials...	Default

Stap 5. Kies de *verificatiemethode* als **Active Directory Service**.



Stap 6. Zodra u de Active Directory Service als *verificatiemethode* kiest, wordt het protocol gewijzigd van Hyper-Text Transfer Protocol (HTTP) naar Hyper-Text Transfer Protocol (HTTPS) Secure.



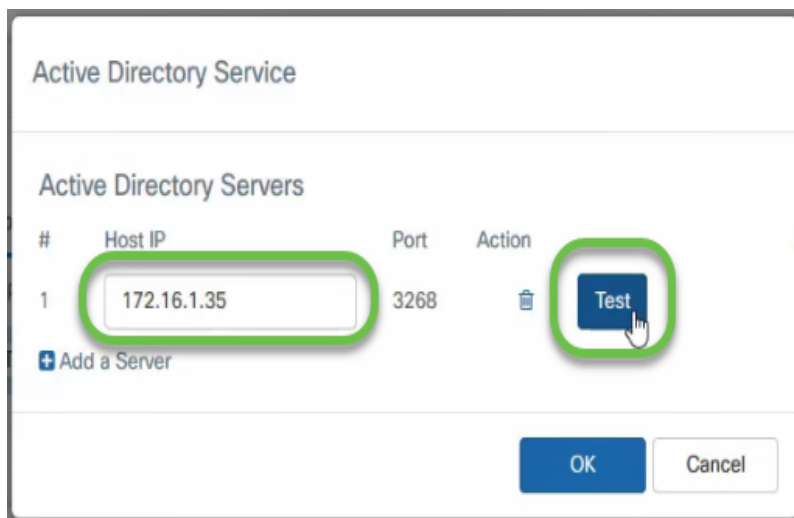
OPMERKING: Het is heel belangrijk dat een cliënt de pagina voor een gevangen portaal aanpast om HTTPS te gebruiken en niet HTTP zoals de eerste veiliger is. Als een client HTTP kiest, kunnen ze onbedoeld gebruikersnamen en wachtwoorden blootstellen door ze in ongecodeerde, duidelijke tekst te verzenden. Het is de beste praktijk om een HTTPS-portaalpagina te gebruiken.

Stap 7. Configureer het IP-adres van de AD-server door op het pictogram blauw oog te klikken naast de Active Directory Service in de kolom *Verificatiemethode*.

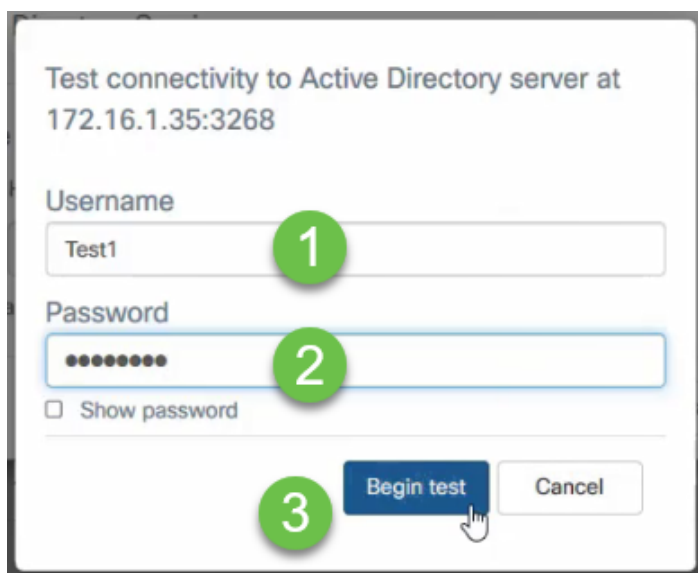
Guest Access Instance Table

<input type="checkbox"/>	<input type="checkbox"/>	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input type="checkbox"/>	<input checked="" type="checkbox"/>	guest_Access	http:80	No Authentication...	Default
<input type="checkbox"/>	<input checked="" type="checkbox"/>	facebook_authentication	http:80	3rd Party Credentials...	Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_authentication	HTTPS : 443	Active Directory Se	Default
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Guest_social_media_access	http:80	3rd Party Credentials...	Default

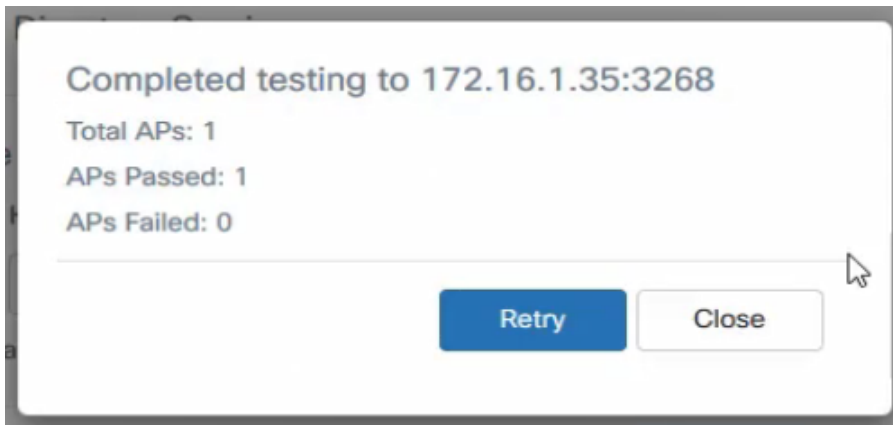
Stap 8. Er wordt een nieuw venster geopend. Voer het IP-adres in voor de AD-server. In dit voorbeeld is het gebruikte Host IP-adres **172.16.1.35**. Als optionele stap kunt u op **Test** klikken om te controleren of het adres geldig is.



Stap 9. (Optioneel) Zodra u op **Test** klikt in de vorige stap, wordt een ander pop-upvenster geopend en kunt u de *gebruikersnaam* en *wachtwoord* van de gebruiker invoeren in AD en op **Start test** klikken.

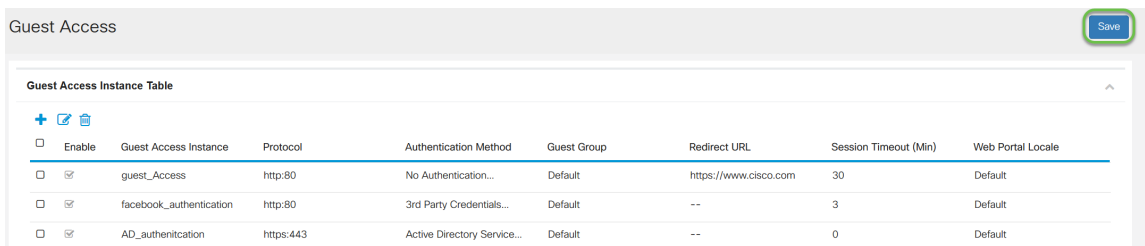


Als deze geldig is, wordt de test succesvol doorlopen en verschijnt het volgende scherm. Dit bevestigt dat u verbinding kunt maken met de domeincontroller en u authentiek kunt verklaren.

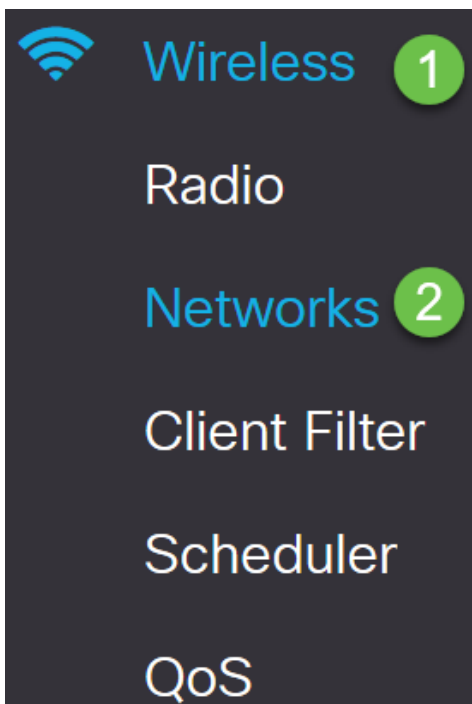


OPMERKING: U kunt maximaal 3 AD-servers toevoegen.

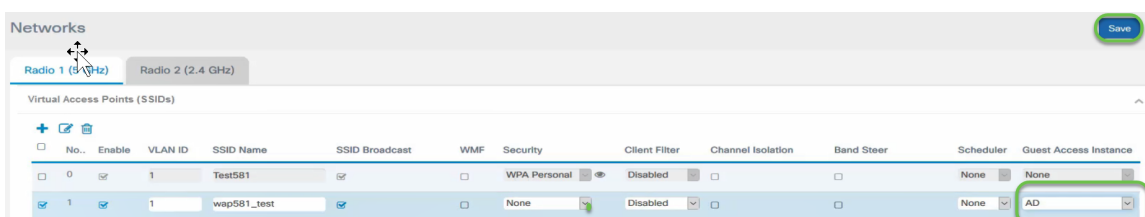
Stap 10. Sla de wijzigingen op.



Stap 1. Ga naar het menu en kies **Draadloos > netwerken**

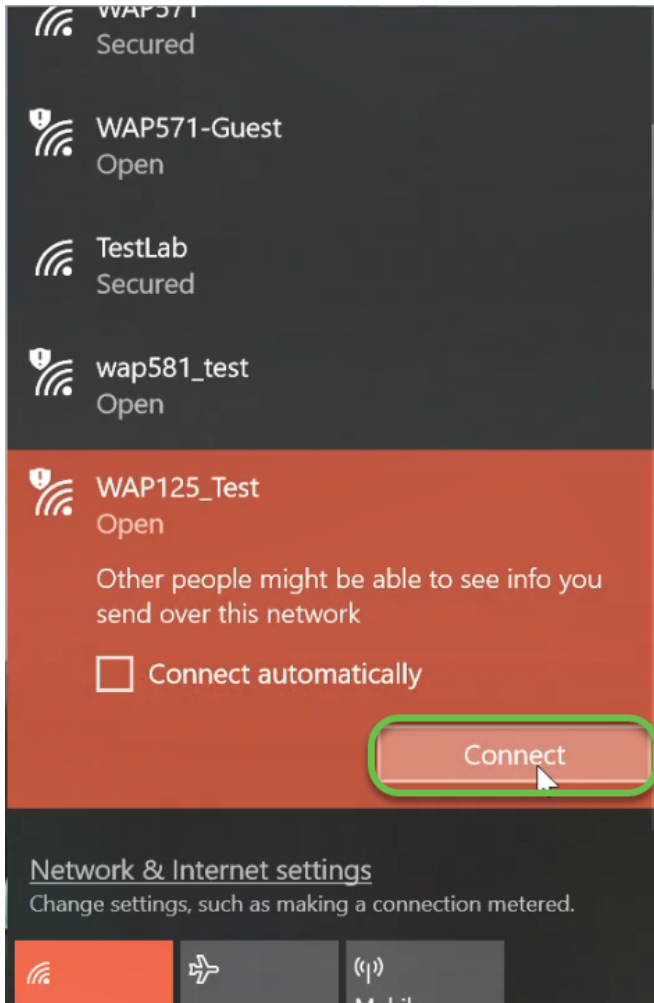


Stap 12. Kies het netwerk en specificeer dat het **AD** zal kiezen als het *Guest Access Instance* voor verificatie. Klik op **Opslaan**.



Stap 13. Om met AD-verificatie op het netwerk te kunnen aansluiten, gaat u naar de

draadloze optie op uw PC (PC) en selecteert u het netwerk dat voor AD-verificatie is geconfigureerd en klikt u op **Connect**.



Stap 14. Na verbinding wordt een venster van een webbrowser geopend met de standaardwaarschuwing voor beveiligingscertificaten. Klik op **Ga naar de webpagina**.



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

[Go to your Start page](#)

Details

Your PC doesn't trust this website's security certificate.

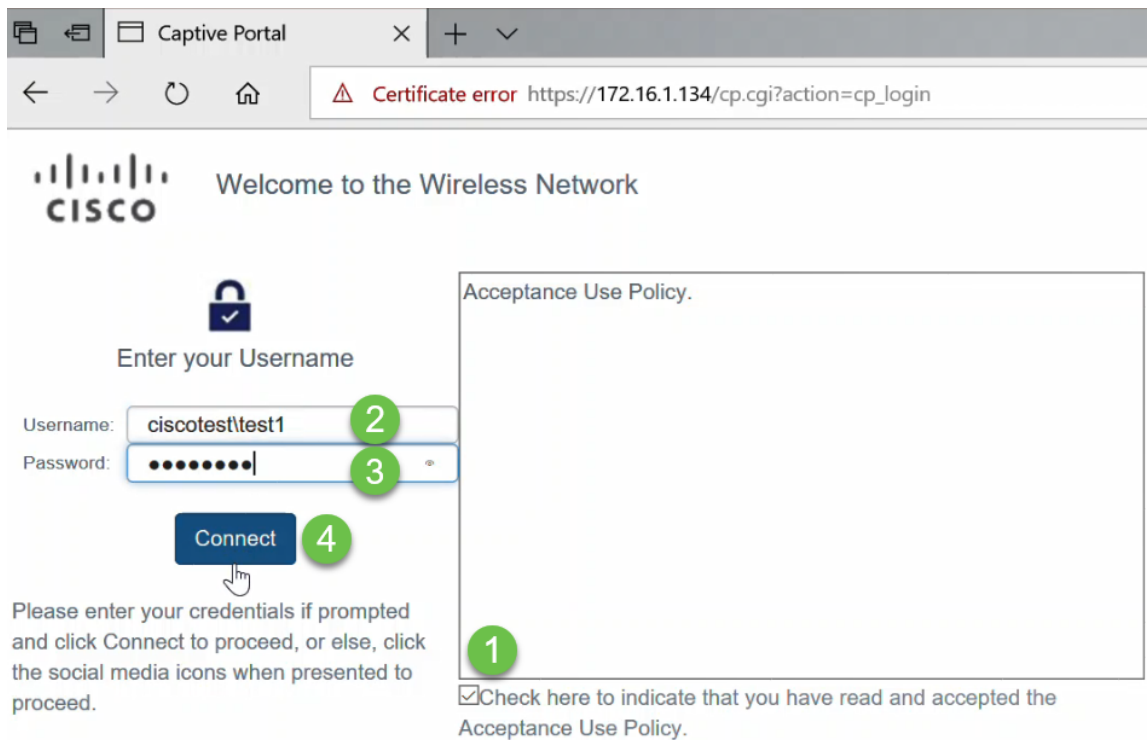
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[Go on to the webpage](#) (Not recommended)

OPMERKING: Het scherm kan op een andere manier worden weergegeven, afhankelijk van de browser die u gebruikt.

Stap 15. De pagina *Captive Portal* is gestart. Controleer het vakje Aanvaarding Gebruik beleid om het beleid te aanvaarden en voer de *gebruikersnaam* en het *wachtwoord* van de gebruiker in in. Klik op **Connect** om verbinding te maken met het netwerk.



OPMERKING: Als er meerdere domeinen zijn, dan zal de gebruikersnaam de domeinnaam\username omvatten. In dit voorbeeld is het ciscotest\test1.

Stap 16. Je bent nu echt bevonden en hebt toegang tot internet.



Congratulations!

You are now authorized and connected to the network.



Conclusie

U zou nu met succes de actieve authenticatie van telefoongidsen op WAP125 of WAP581 hebben ingesteld en de functionaliteit ervan hebben geverifieerd.