

# Active Directory Guest Authentication on WAP571 of WAP571E configureren

## Doel

Het doel van dit document is om u te tonen hoe u de Actieve Gastverificatie van de Map op WAP571 of WAP571E moet configureren.

## Inleiding

Microsoft biedt Windows Active Directory Service, een interne actieve map (AD). Hiermee slaat u alle essentiële informatie voor het netwerk op, inclusief gebruikers, apparaten en beleid. Beheerders gebruiken de AD als één enkele plaats om het netwerk te maken en te beheren. AD-gastverificatie maakt het mogelijk dat een cliënt een interne portaalinfrastructuur vormt met behulp van de AD voor authenticatie. Captive Portal (CP) is een functie waarmee een beheerder toegang kan verlenen aan vooraf gedefinieerde gebruikers die verbinding maken met een Wireless Access Point (WAP). Clients worden gericht op een webpagina voor verificatie en toegangsvoorwaarden voordat zij verbinding kunnen maken met het netwerk. De CP-verificatie is voor zowel gasten als voor geauthentiseerde gebruikers van het netwerk. Deze functie maakt gebruik van de webbrowser en verandert deze in een verificatieapparaat.

CP 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 (VAP's) die meerdere toegangspunten simuleren binnen één fysiek WAP-apparaat. Om meer te weten te komen over VAP en de stappen die bij het configureren ervan betrokken zijn, klikt u [hier](#).

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. Voor sommige organisaties bieden zij de toetredende gebruiker de mogelijkheid om in de toekomst contact met het merk op te nemen. Er zijn veel gevallen van marketinggebruik naar een functie als deze. Ter ondersteuning van AD-verificatie moet WAP met één tot drie Windows-domeincontrollers (ook bekend als servers) communiceren om verificatie te kunnen leveren. Het kan meerdere domeinen voor authenticatie ondersteunen door domeincontrollers uit verschillende AD domeinen te kiezen.

## Toepasselijke apparaten

WAP571

WAP571E router

## Softwareversie

## 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 hebt ingesteld, voert u die aanmeldingsgegevens in. Klik op **Aanmelden**.

Opmerking: In dit artikel wordt WAP571E 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

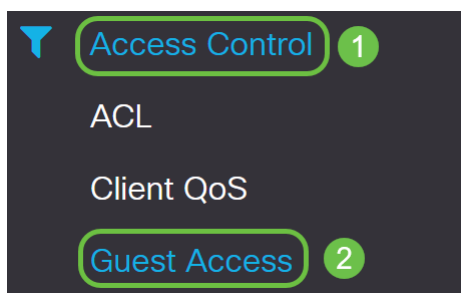
English



Login

3

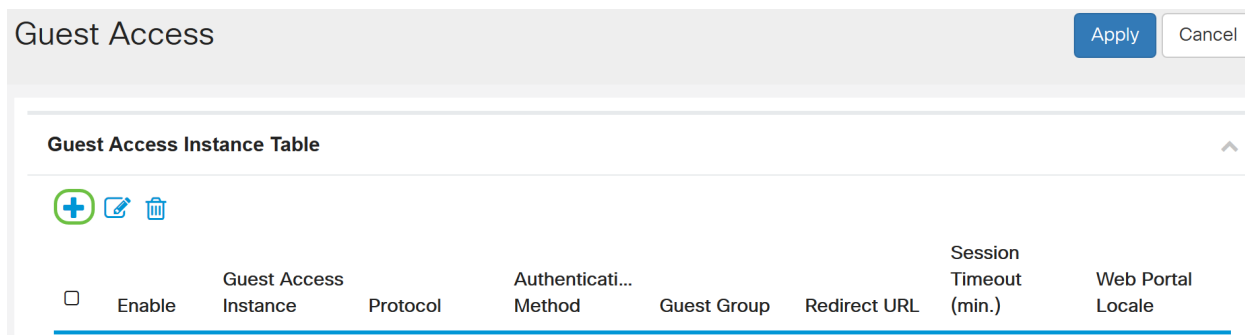
Stap 2. Kies **toegangscontrole > Gasttoegang**.



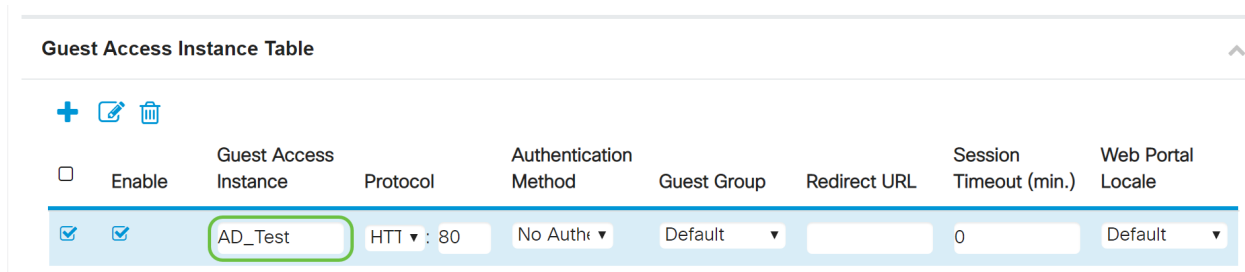
Stap 3. In de *tabel* met *GEREEDSCHAP* kunt u het **plus-pictogram** selecteren om een nieuw *Guest Access Instance* toe te voegen of het **potlood- en papieren pictogram** om een bestaand exemplaar te bewerken. De Guest Access-functie van WAP571 of WAP571E access point biedt draadloze verbindingen aan tijdelijke draadloze klanten binnen het bereik van het apparaat. Het toegangspunt zal de Service Set Identifier (SSID) uitzenden, specifiek voor het gastnetwerk. Gegeven worden dan opnieuw naar een CP geleid waar ze 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 de CP 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\_Test**.



Stap 5. Kies het *Protocol* voor de CP-instantie die u tijdens het verificatieproces wilt gebruiken in het vervolkeuzemenu.

HTTP - gebruikt geen encryptie tijdens verificatie.

HTTPS - gebruikt de Secure Socket Layer (SSL), wat een certificaat vereist om encryptie te leveren. Het certificaat wordt op het aansluitingstijdstip aan de gebruiker getoond.

Opmerking: Het is heel belangrijk dat een cliënt de pagina van het gevangen portaal aanpast om HTTPS te gebruiken en niet HTTP zoals het 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.

#### Guest Access Instance Table

	Enable	Guest Access Instance	Protocol	Authenticati... Method	Guest Group	Redirect URL	Session Timeout (min.)	Web Portal Locale
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 80	No Auth	Default		0	Default

Dropdown menu for Protocol: HTTP, **HTTPS**

Stap 6. Kies de *verificatiemethode* als **Active Directory Service**.

#### Guest Access Instance Table

	Enable	Guest Access Instance	Protocol	Authenticati... Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D ...	Default

Dropdown menu for Authentication Method: Local Database, Radius Authentication, No Authentication, 3rd Party Credentials, **Active Directory Service**, External Captive Portal

#### Guest Group Table



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

	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D	Default

Stap 8. Er wordt een nieuw venster geopend. Voer het IP-adres in voor de AD-server. In dit voorbeeld is het IP-adres van de host **172.16.1.35**. Klik op **OK**.

## Active Directory Service

### Active Directory Servers

#	Host IP	Port	Action
1	172.16.1.35	3268	 <input type="button" value="Test"/>

 Add a Server



Opmerking: Als een optionele stap kunt u op **Test** klikken om te verifiëren dat het IP-adres voor de AD server geldig is. Klik [hier](#) voor meer informatie over de verificatiestappen. U kunt maximaal 3 AD-servers toevoegen.

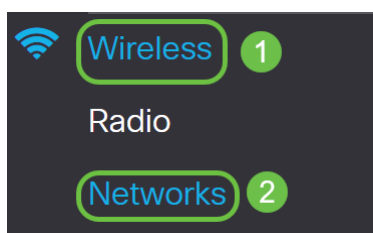
Stap 9. Klik op **Toepassen** om de wijzigingen op te slaan.

Guest Access

Guest Access Instance Table

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group	Redirect URL	Session Timeout (min.)	Web Portal Locale
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AD_Test	HTT : 443	Active D	Default		0	Default

Stap 10. Ga naar het menu en kies **Draadloos > netwerken**.



Stap 1. Kies het netwerk en specificeer dat het **AD** zal kiezen als het *Guest Access Instance* voor verificatie. In dit voorbeeld is het netwerk **WAP571\_test**.

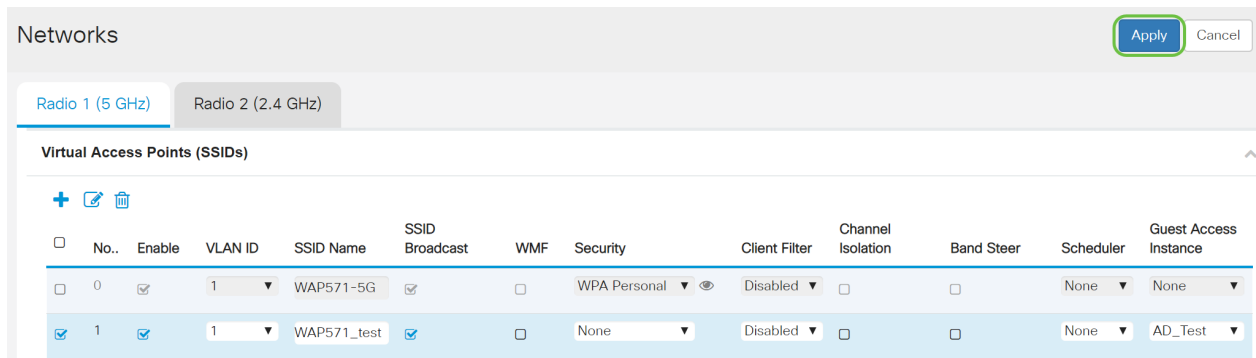
Networks

Radio 1 (5 GHz) Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)

<input type="checkbox"/>	No..	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	WAP571_test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	AD_Test

Stap 12. Klik op **Toepassen**.



Networks Apply Cancel

Radio 1 (5 GHz) Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	WAP571_test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	AD_Test

## Conclusie

U hebt nu met succes de actieve authenticatie van telefoongidsen ingesteld op WAP571 of WAP571E.

Raadpleeg voor stappen om verbinding te maken met het netwerk van gast draadloze netwerken met behulp van AD-verificatie en om de functionaliteit ervan te controleren het artikel op [Configure Active Directory Guest Authentication on WAP125 of WAP581](#).