Configuratie van verificatie van derden op WAP571 of WAP571E

Doel

Dit artikel zal u door configuratie van derde authenticatie op een WAP571 of WAP71E access point leiden.

Inleiding

Netwerkgebruikers verbinden zich vaak met een draadloos access point (WAP) om snellere internetsnelheden te ontvangen in vergelijking met de dragerservice van hun mobiele apparaat. Een soepel inlogproces en een eenvoudige navigatie kunnen voor deze gebruikers een positieve ervaring garanderen. U kunt uw WAP571 of WAP571E configureren om een aantal gemakkelijke opties voor inloggen te hebben, terwijl u uw netwerk toch veilig houdt.

Verificatie door derden via Google of Facebook is een beschikbare functie met deze laatste update. Wanneer het gebruikt wordt, fungeert de rekening van de gebruiker als een soort "paspoort", waarmee de gebruiker toegang tot uw draadloos netwerk krijgt. Of je nu een koffietentje of een makelaarskantoor runt, het zorgt ervoor dat bezoekers gemakkelijk toegang hebben tot je netwerk en een geweldige bezoekerservaring hebben.

Toepasselijke apparaten

WAP571

WAP571E router

Softwareversie

1.1.03

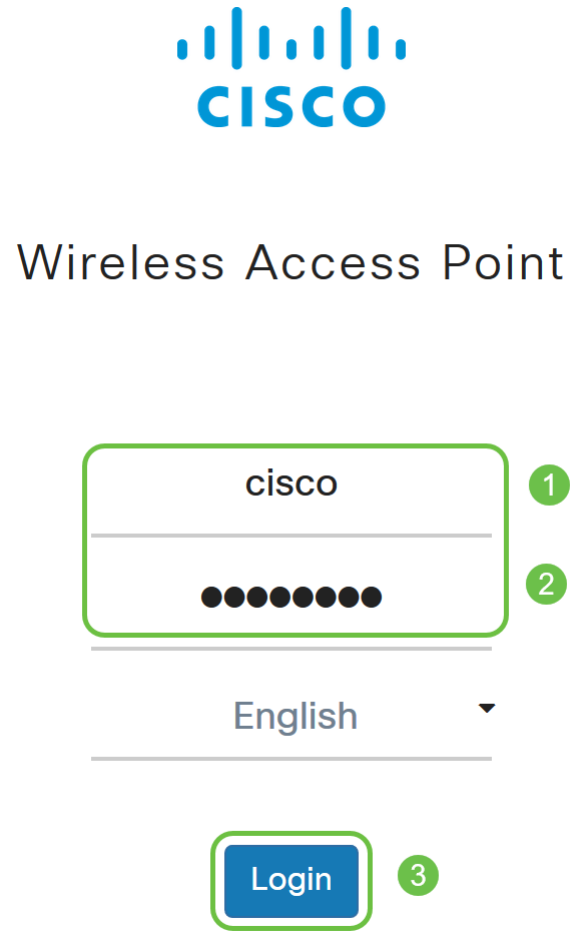
Vereisten

Internettoegang, zodat je verbinding kunt maken met Google en/of Facebook verificatieservers.

Gebruikers moeten een bestaand account hebben bij Google en/of Facebook.

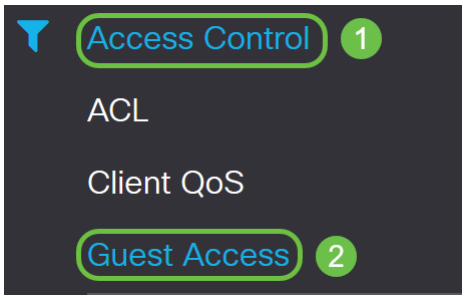
Verificatie van derden configureren

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.**



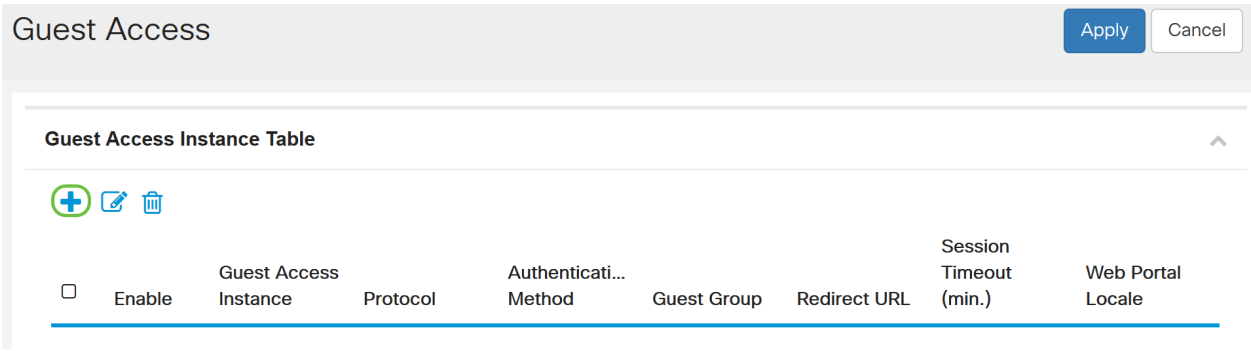
Opmerking: In dit artikel wordt WAP571E gebruikt om de configuratie van externe gastverificatie aan te tonen. De menuopties kunnen licht variëren afhankelijk van het model van het apparaat.

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

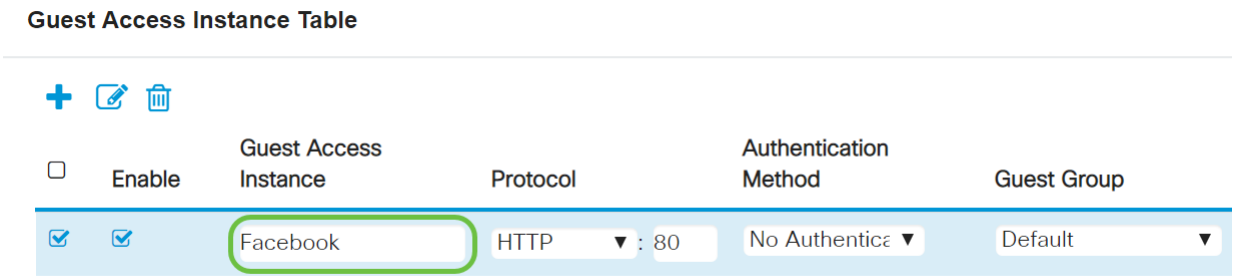


Stap 3. In de *tabel van het instel van de toegang* kunt u een nieuw *exemplaar* van de *Gast* toevoegen of een bestaand exemplaar bewerken.

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 **Facebook**.

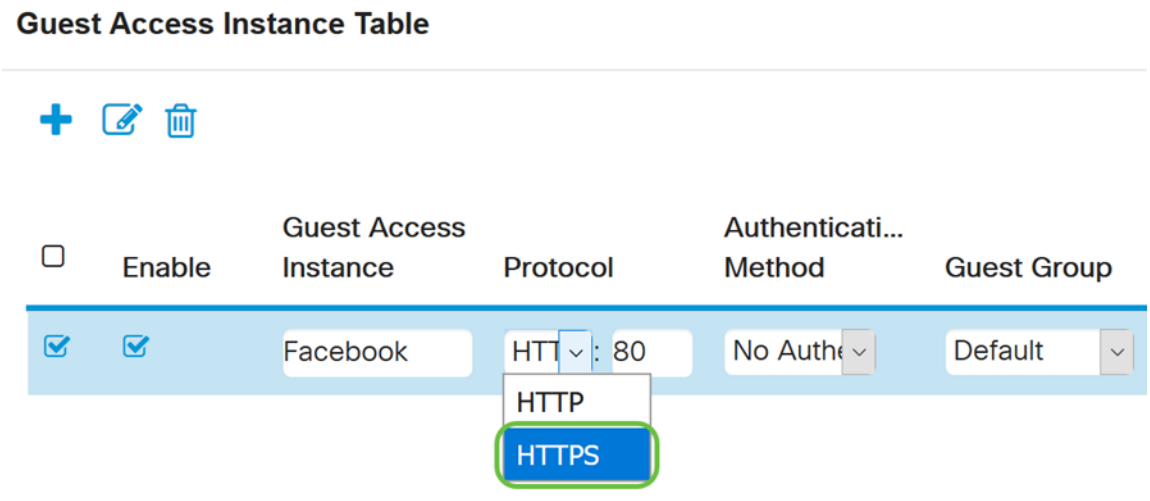


Stap 5. Kies het *protocol* dat u tijdens het verificatieproces wilt gebruiken in het vervolgkeuzemenu.

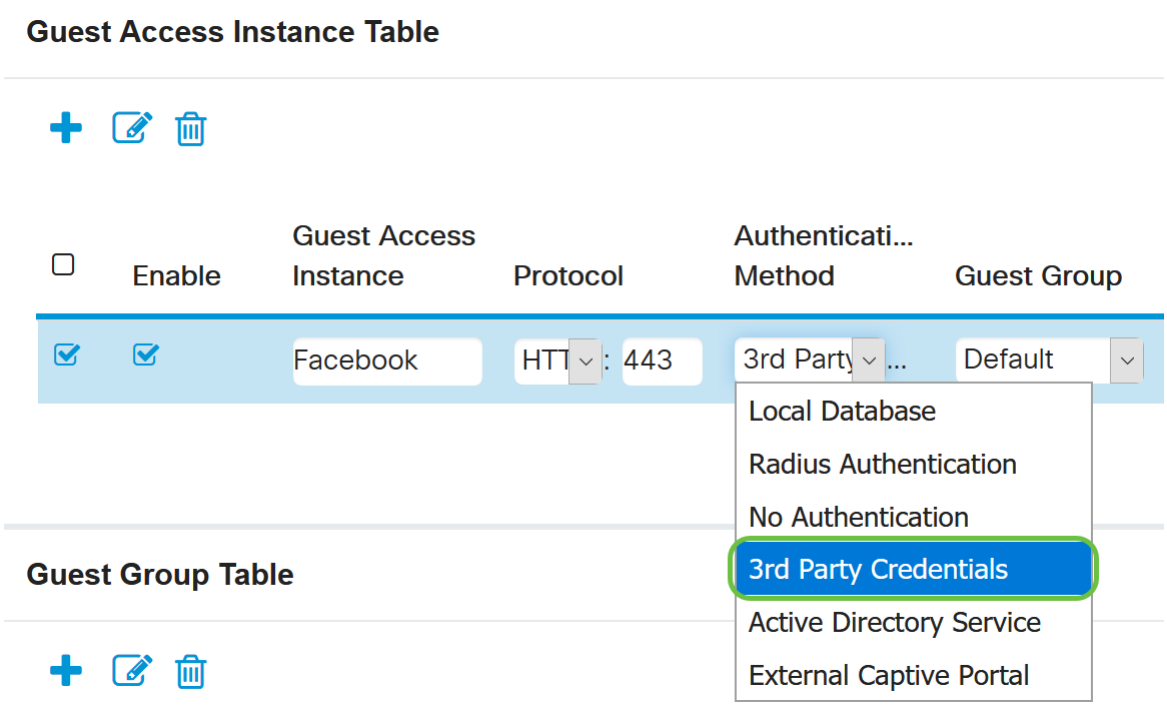
HTTP - gebruikt geen encryptie tijdens verificatie.

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 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.

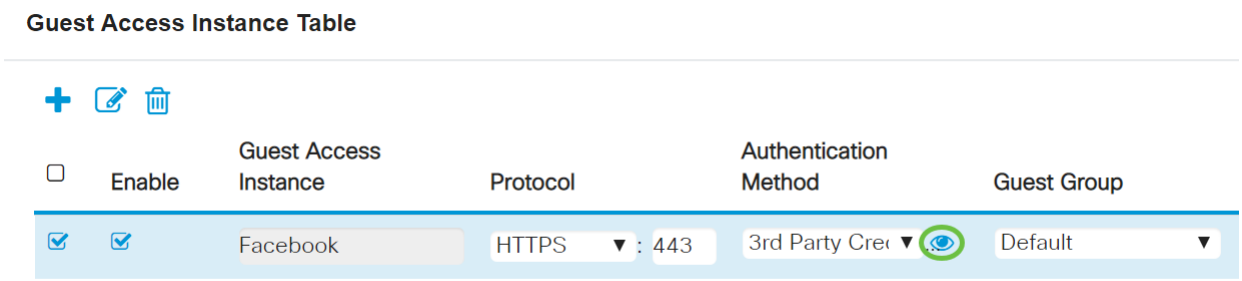


Stap 6. Kies de *verificatiemethode* als **3e-mails van derden.**



Opmerking: Het WAP-apparaat gebruikt de aanmeldingsgegevens op de sociale media-account om de gebruikers echt te maken.

Stap 7. Klik op het **pictogram Blauw oog** naast de Credentials van 3 partijen in de kolom *Verificatiemethode*.

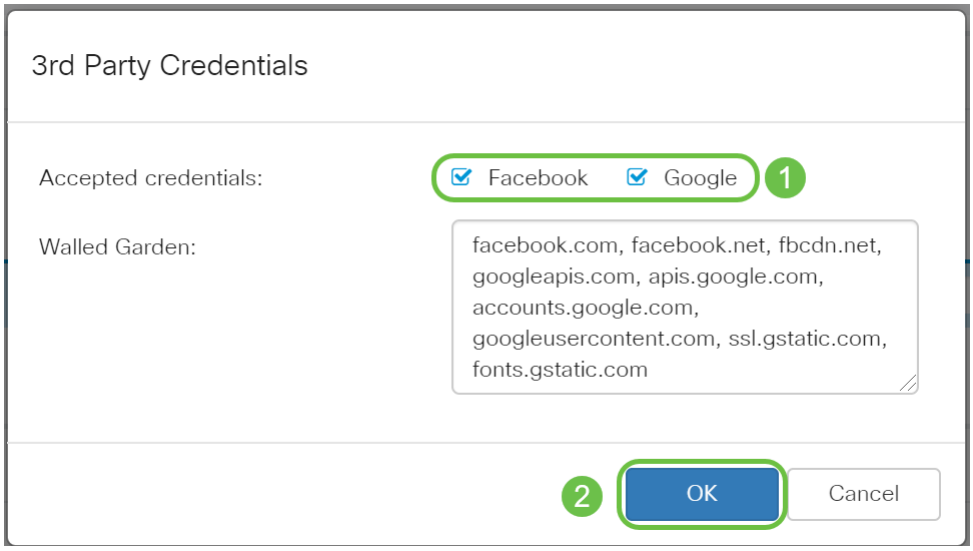


Stap 8. Configureer de volgende instellingen voor *3de* echtheidscontrole van *derden*.

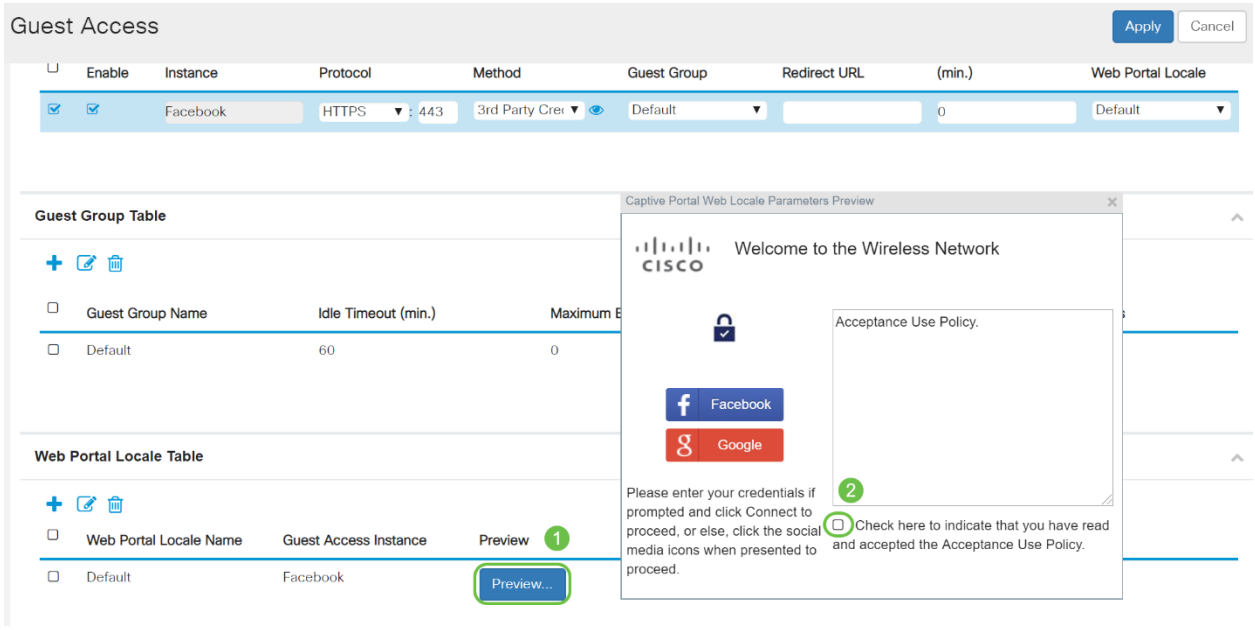
Accepteerde aanmeldingsgegevens - selecteer Facebook, Google of beide.

Uitgeschakeld *Garden* - De relevante standaardconfiguratie wordt automatisch ingesteld terwijl Accepted Credentials geselecteerd zijn.

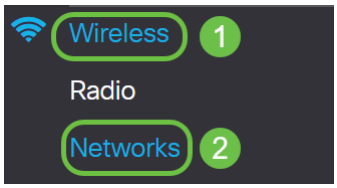
In dit voorbeeld worden **Facebook** en **Google** geselecteerd. Klik op **OK**.



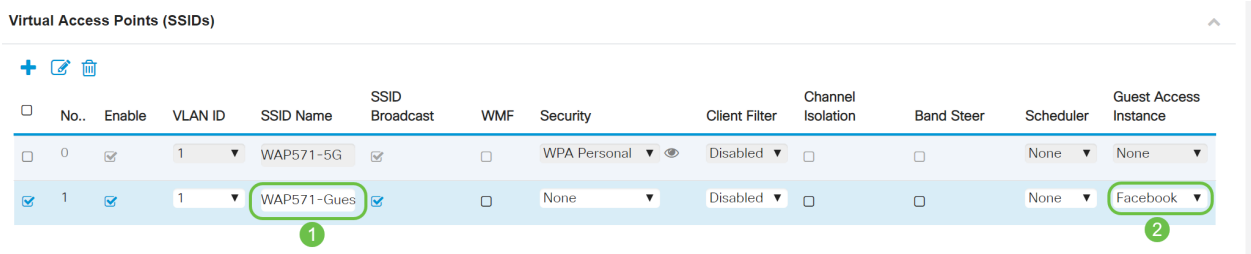
Stap 9. (Optioneel) Klik om de pagina Captive Portal te bekijken op de knop **Voorbeeld** onder de *Locale Tabel van Web Portal*. In een nieuw venster wordt de voorbeeldpagina weergegeven waarop gebruikers worden gevraagd hun Facebook- of Google-referenties in te voeren. De gebruikers moeten ook het vakje voor Acceptatiebeleid aankruisen.



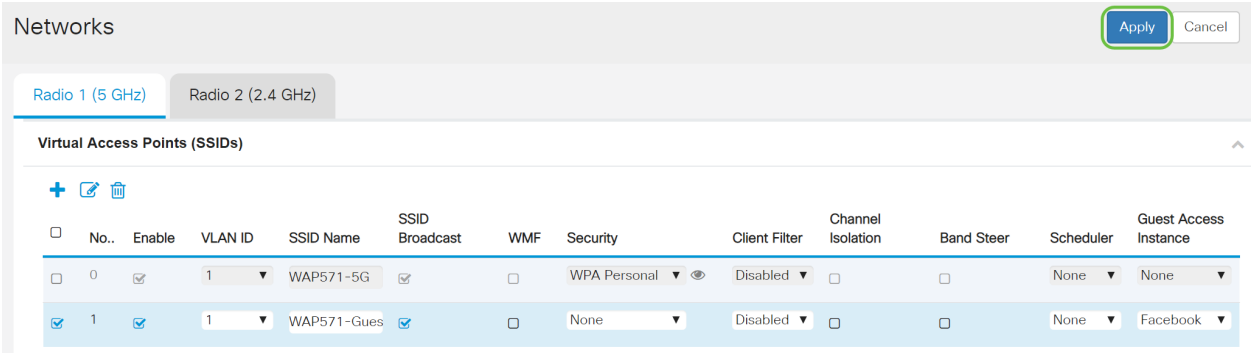
Stap 10. Ga naar het menu en kies **Draadloos > netwerken.**



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



Stap 12. Klik op **Toepassen**.



Conclusie

Je hebt 'derde' authenticatie ingesteld via Google, Facebook of beide op een WAP571 of WAP571E.