PEAP en EAP-FAST configureren met ACS 5.2 en WLC

Inhoud

Inleiding

In dit document wordt uitgelegd hoe u de EAP-verificatie (Wireless LAN controller) voor uitbreidbare verificatie (EAP) kunt configureren met behulp van een externe RADIUS-server zoals Access Control Server (ACS) 5.2.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basiskennis hebben van WLC en Lichtgewicht access points (LAP's)
- Zorg voor een functionele kennis van de AAA-server
- Zorg voor een grondige kennis van draadloze netwerken en problemen met draadloze beveiliging

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5508 WLC met firmwarerelease 7.0.220.0
- Cisco 3502 Series router
- Microsoft Windows 7 Native Supplicant met Intel 6300-N driver versie 14.3
- Cisco Secure ACS-softwarerelease 5.2
- Cisco 3560 Series Switch

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

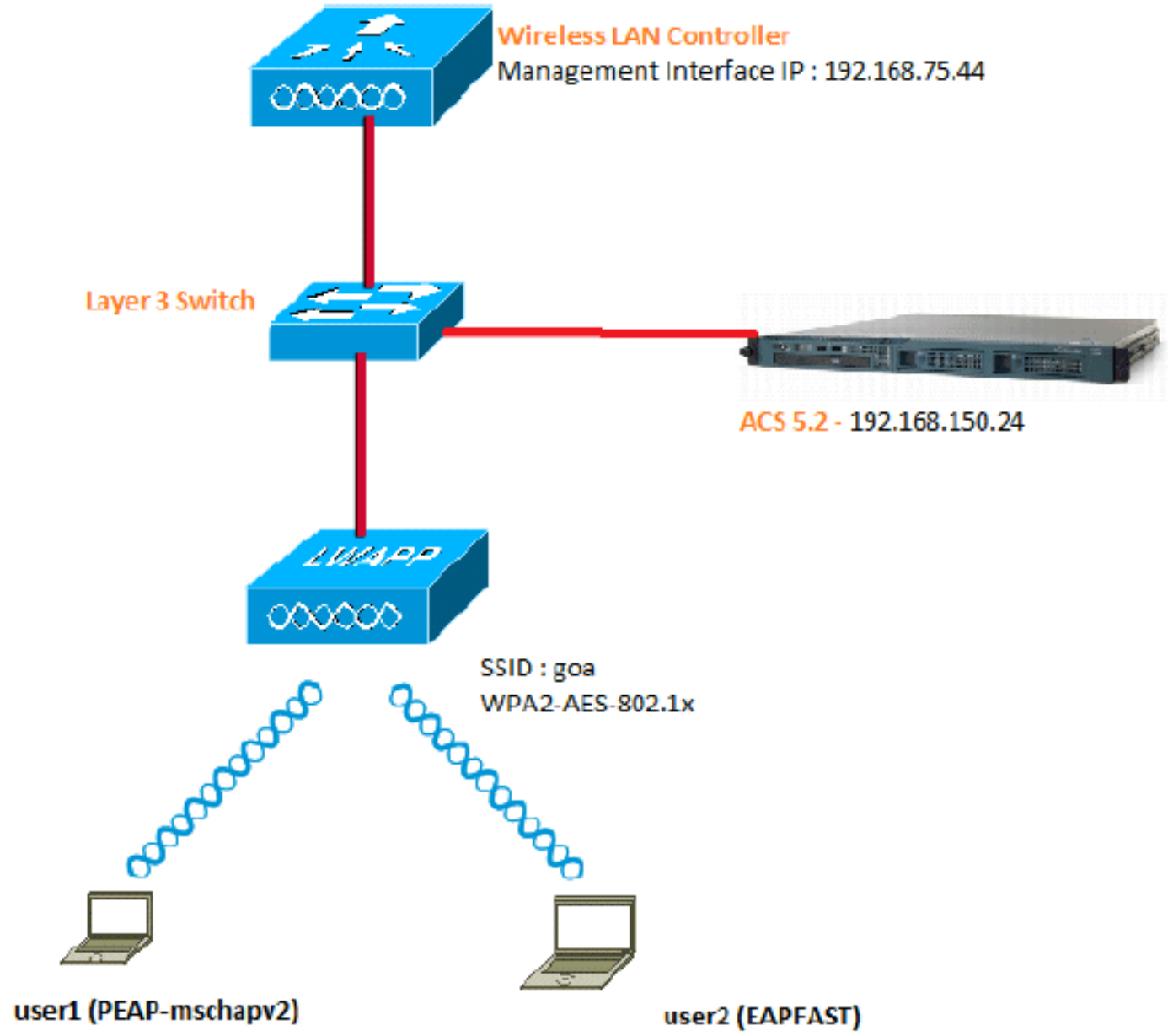
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde klanten) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit zijn de configuratiedetails van de componenten die in dit diagram worden gebruikt:

- Het IP-adres van de ACS-server (RADIUS) is 192.168.150.24.
- Het beheer en AP-manager interfaceadres van de WLC is 192.168.75.44.
- De DHCP-servers richten zich op 192.168.150.25.
- VLAN 253 wordt gebruikt in deze configuratie. Beide gebruikers verbinden met dezelfde SSID "goa". Gebruiker1 is echter ingesteld voor het verifiëren met PEAP-MSCHAPv2 en user2 met behulp van EAP-FAST.
- Gebruikers worden toegewezen in VLAN 253:VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Aannames

- Switches zijn geconfigureerd voor alle Layer 3 VLAN's.
- De DHCP-server is een DHCP-scope toegewezen.
- Layer 3-connectiviteit bestaat tussen alle apparaten in het netwerk.
- De LAP is al aangesloten bij de WLC.
- Elk VLAN heeft een /24 masker.

- ACS 5.2 heeft een zelfondertekend certificaat geïnstalleerd.

Configuratiestappen

Deze configuratie is verdeeld in drie stappen op hoog niveau:

1. Configureer de RADIUS-server.
2. Configureer de WLC.
3. Configureer het hulpprogramma draadloze client.

De RADIUS-server configureren

De RADIUS-serverconfiguratie is verdeeld in vier stappen:

1. Configureer de netwerkbronnen.
2. Gebruikers configureren.
3. Beleidselementen definiëren.
4. Toegangsbeleid toepassen.

ACS 5.x is een op beleid gebaseerd toegangscontrolesysteem. Dat wil zeggen dat ACS 5.x gebruikmaakt van een op regels gebaseerd beleidsmodel in plaats van het op groepen gebaseerde model dat gebruikt wordt in de 4.x-versies.

Het op regels gebaseerde ACS 5.x-beleidsmodel biedt krachtigere en flexibelere toegangscontrole in vergelijking met de oudere groepsgebaseerde aanpak.

In het oudere op groepen gebaseerde model definieert een groep beleid omdat het drie soorten informatie bevat en aan elkaar koppelt:

- Identiteitsinformatie - Deze informatie kan worden gebaseerd op lidmaatschap in AD- of LDAP-groepen of een statische toewijzing voor interne ACS-gebruikers.
- Andere beperkingen of voorwaarden - Tijdbeperkingen, apparaatbeperkingen, enzovoort.
- Rechten - VLAN's of Cisco IOS®-toegangsniveaus.

Het ACS 5.x-beleidsmodel is gebaseerd op de vormregels:

- Als de voorwaarde dan resultaat

Bijvoorbeeld, gebruiken wij de informatie die voor het op groep-gebaseerde model wordt beschreven:

- Indien identiteitsvoorwaarde, beperkingsvoorwaarde dan vergunningsprofiel.

Dit geeft ons de flexibiliteit om te beperken onder welke voorwaarden de gebruiker toegang tot het netwerk mag krijgen en welk autorisatieniveau is toegestaan als aan bepaalde voorwaarden wordt voldaan.

Netwerkbronnen configureren

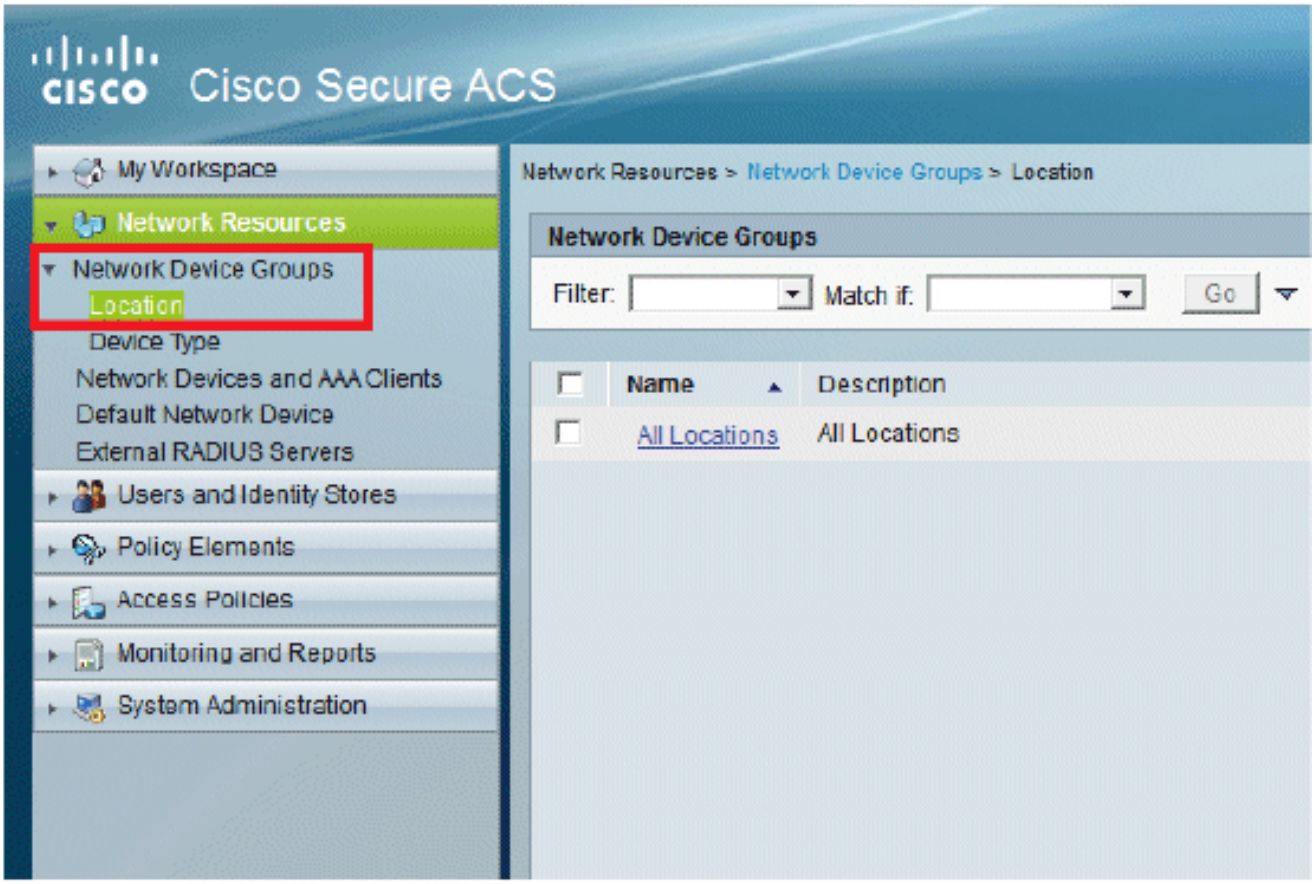
In dit gedeelte configureren we de AAA-client voor de WLC op de RADIUS-server.

Deze procedure legt uit hoe de WLC als AAA-client kan worden toegevoegd aan de RADIUS-

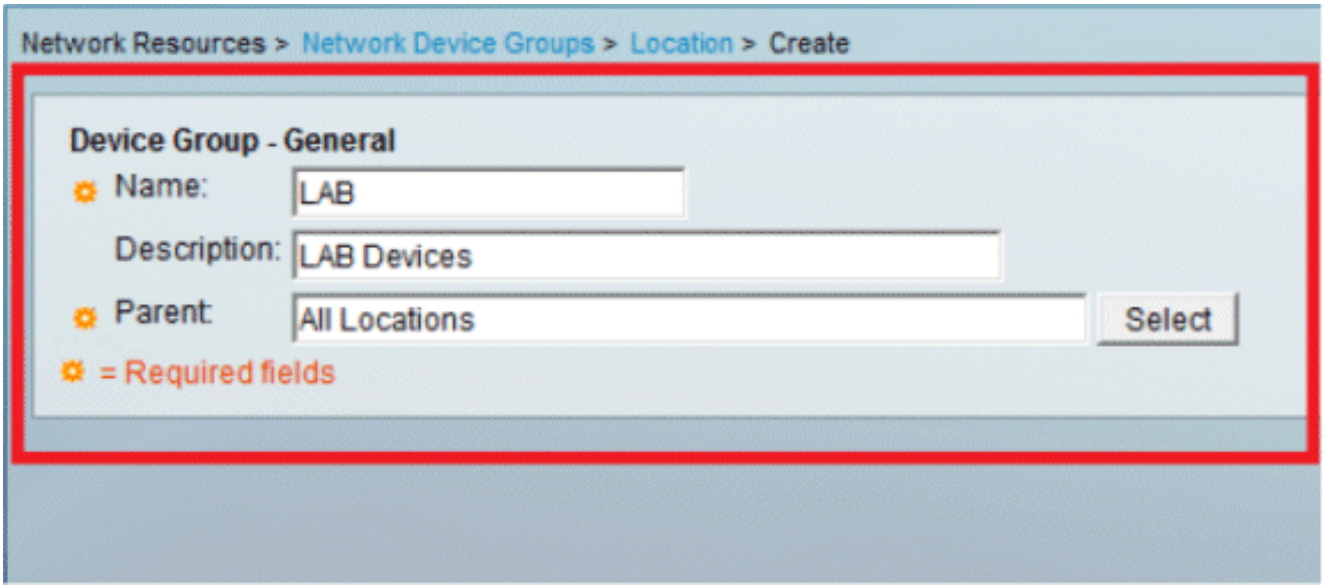
server, zodat de WLC de gebruikersreferenties kan doorgeven aan de RADIUS-server.

Voer de volgende stappen uit:

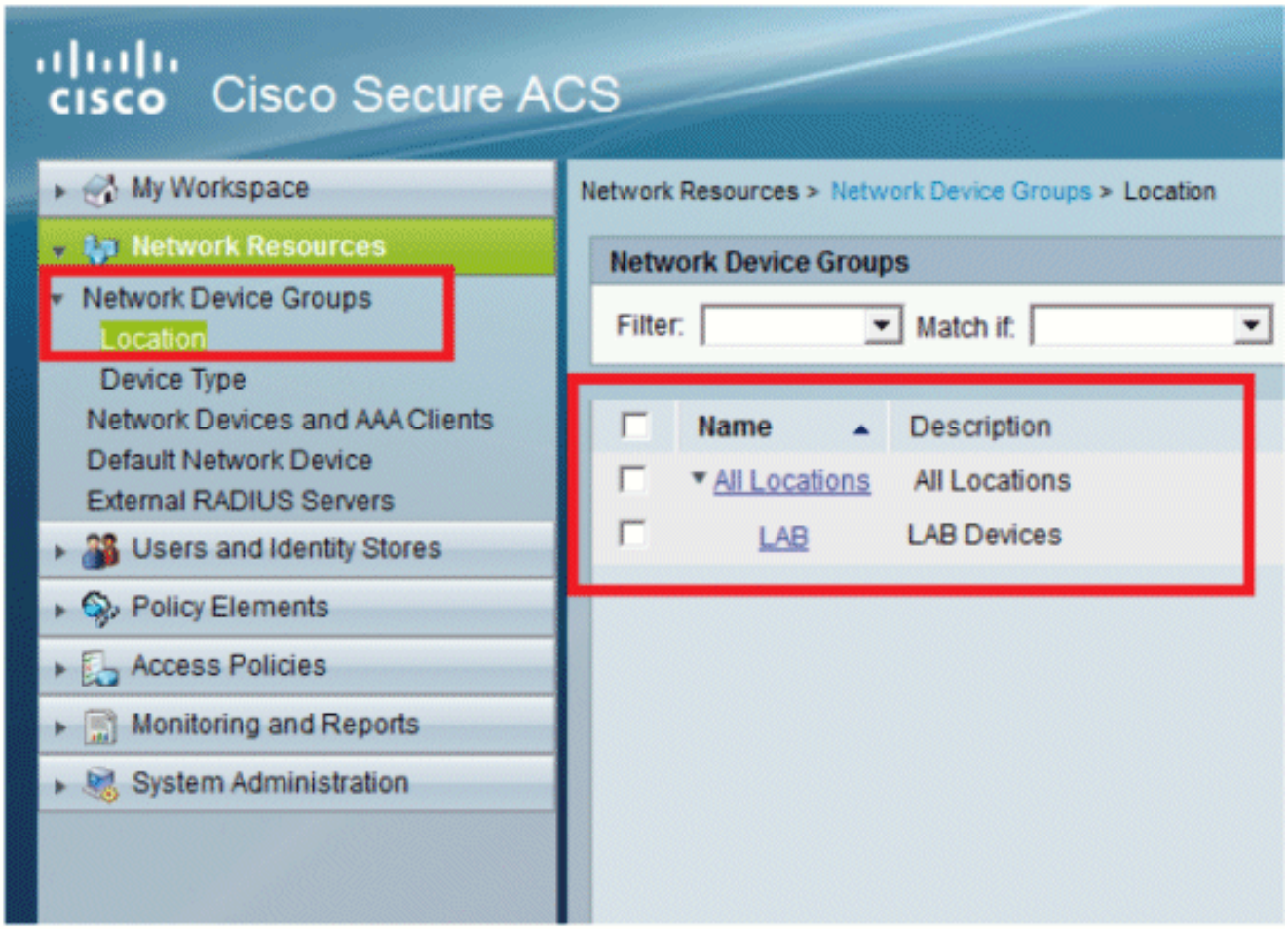
1. Ga vanuit de ACS GUI naar **Network Resources > Network Device Groepen > Location**, en klik op **Create** (onderaan
).



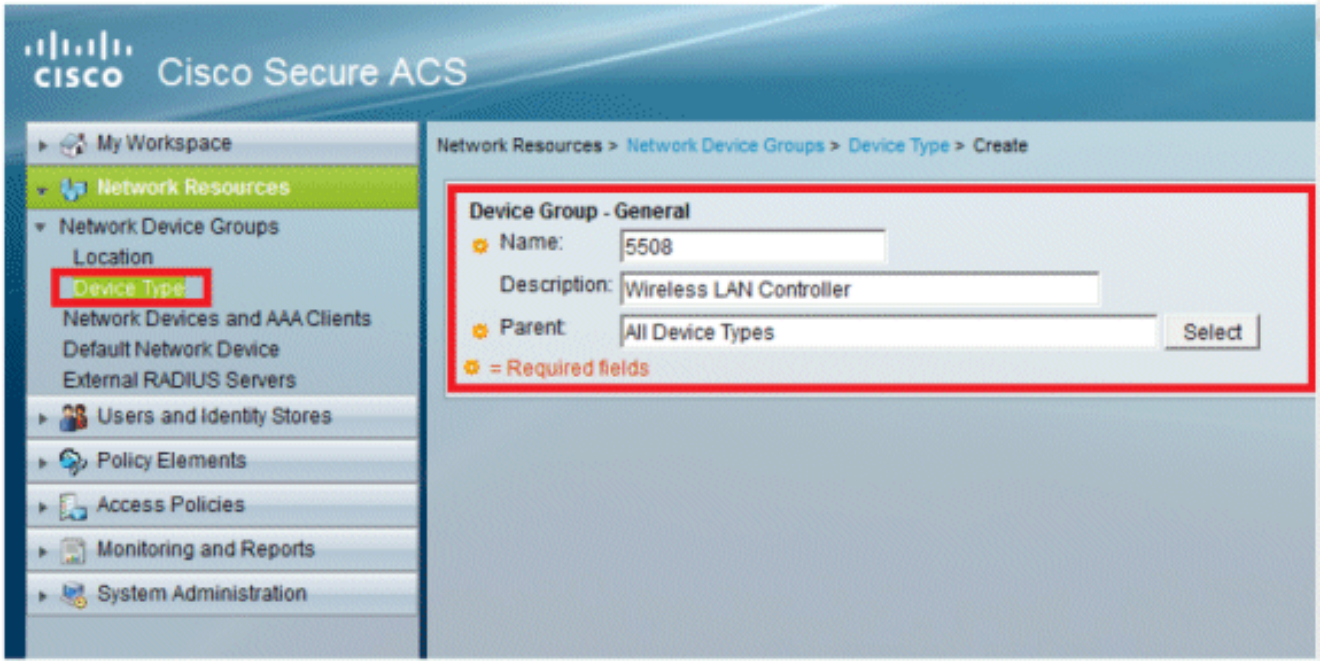
2. Voeg de vereiste velden toe en klik op
   Indienen.



   U ziet nu dit
   scherm:

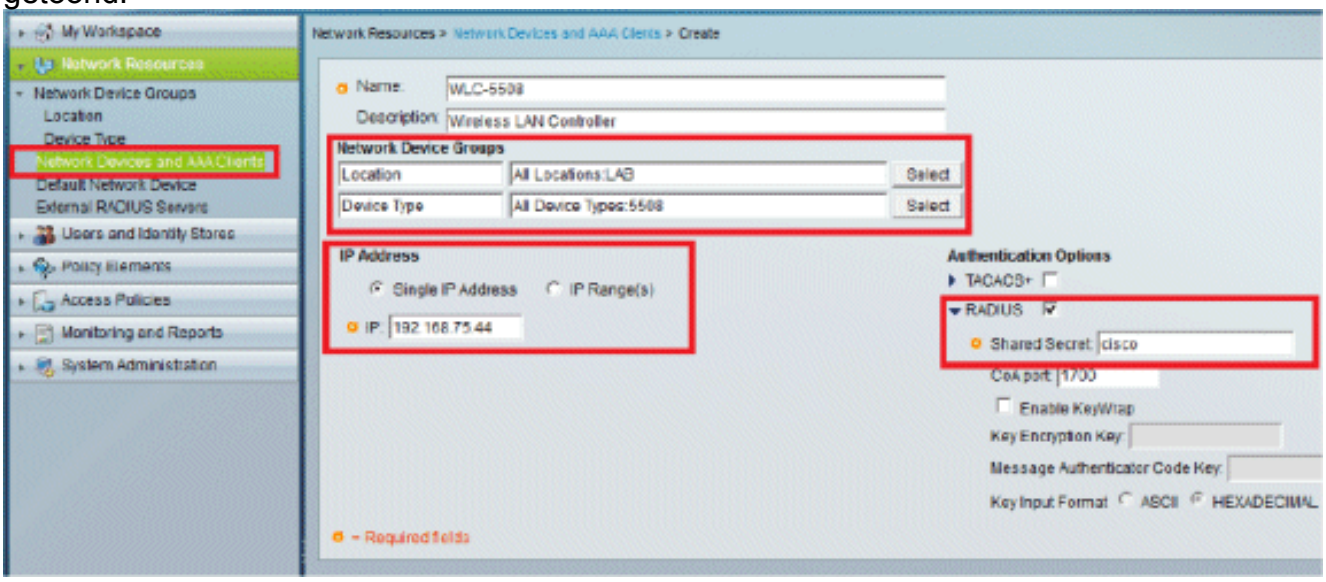


3. Klik op **Apparaattype** > **Aanmaken**.

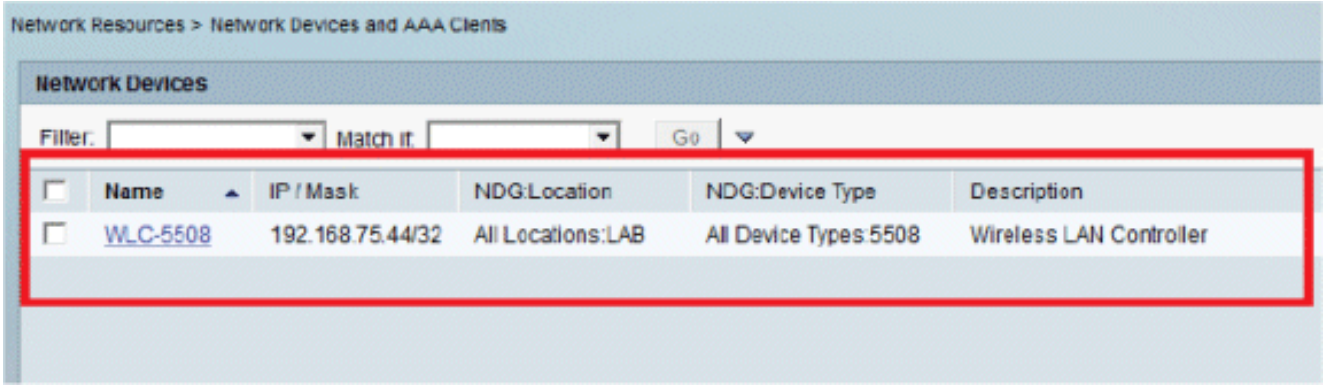


4. Klik op **Verzenden**. U ziet nu dit scherm:

5. Ga naar **Network Resources > Network Devices en AAA Clients**.
6. Klik op **Maken** en vul de details in zoals hier wordt getoond:



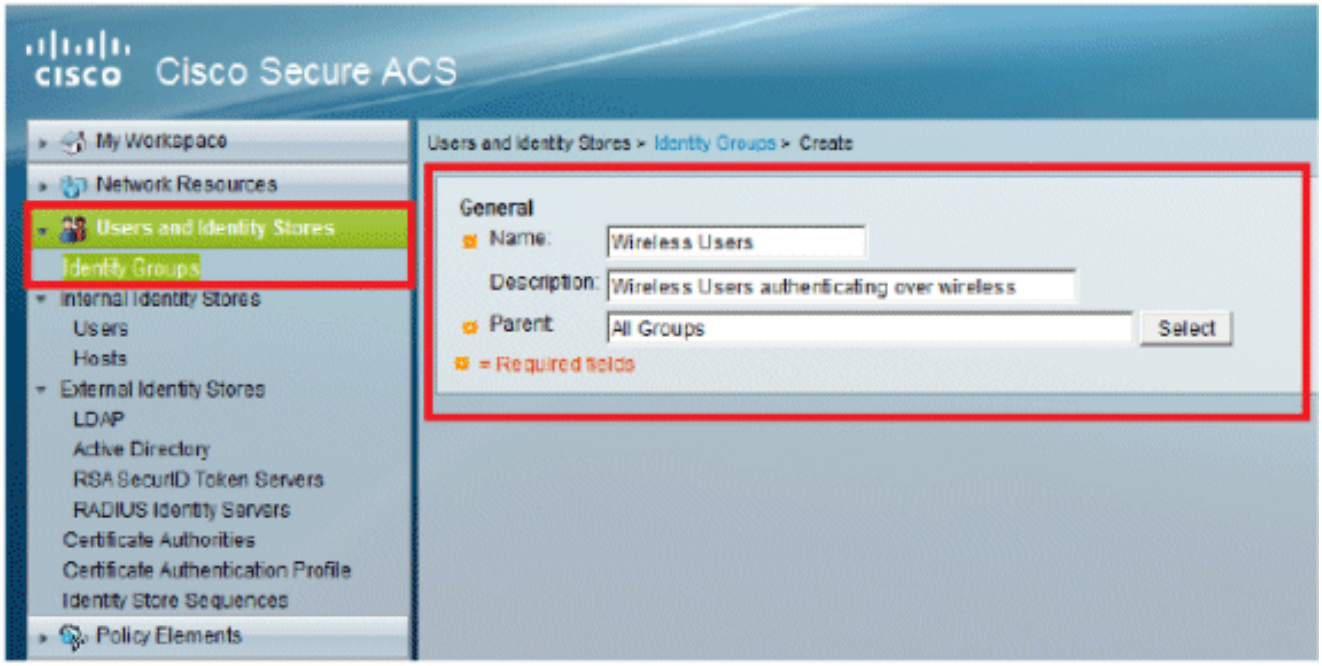
7. Klik op **Verzenden**. U ziet nu dit scherm:



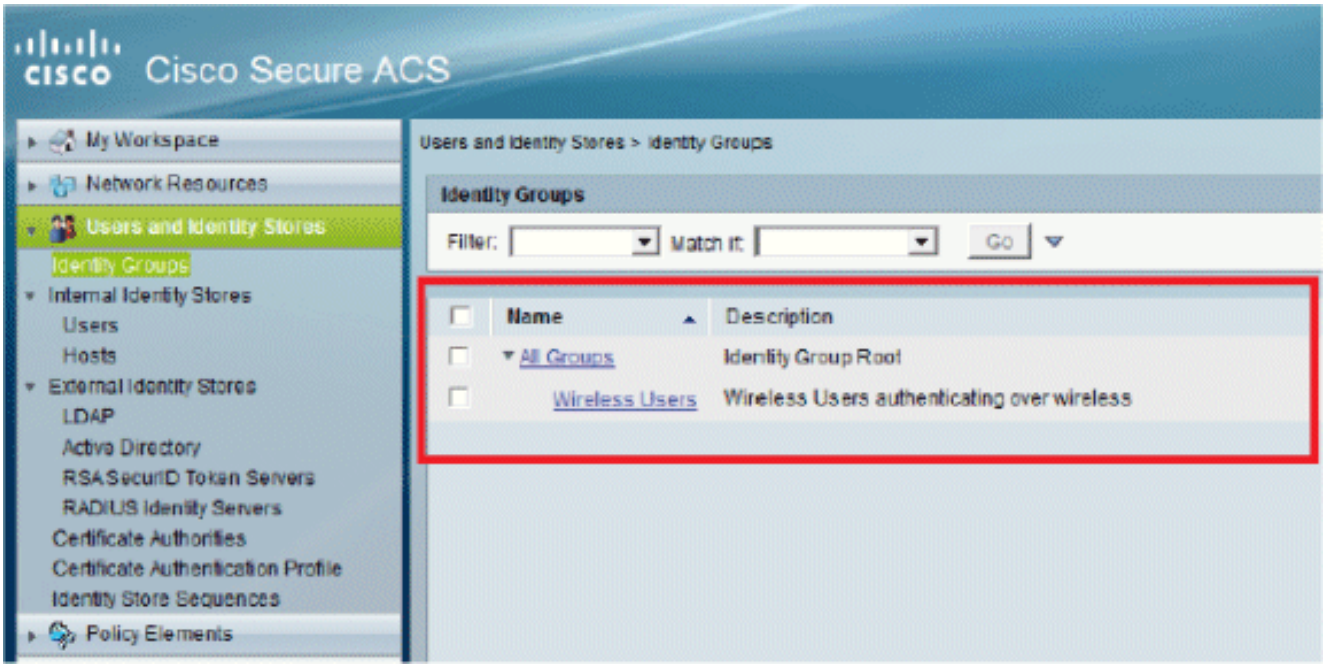
Gebruikers configureren

In deze sectie maken we lokale gebruikers op ACS. Beide gebruikers (user1 en user2) worden toegewezen in de groep die "Draadloze Gebruikers" wordt genoemd.

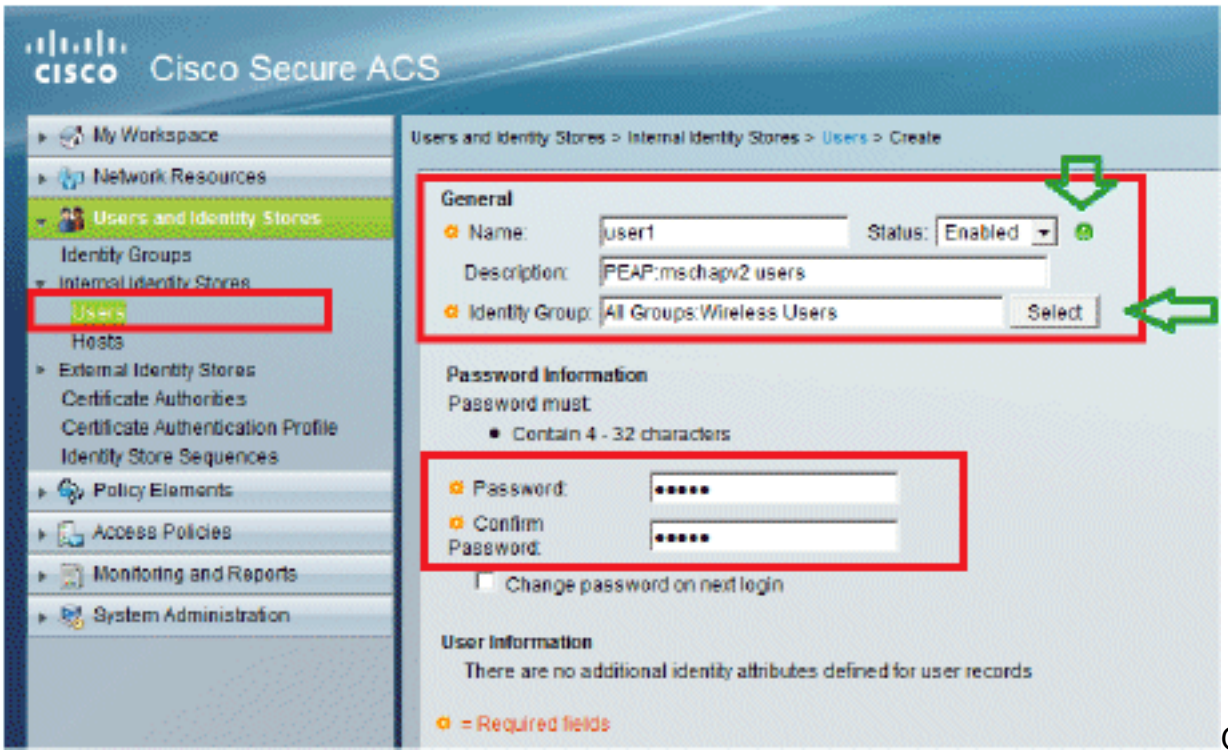
1. Ga naar **Gebruikers en Identiteitswinkels > Identiteitsgroepen > Aanmaken**.



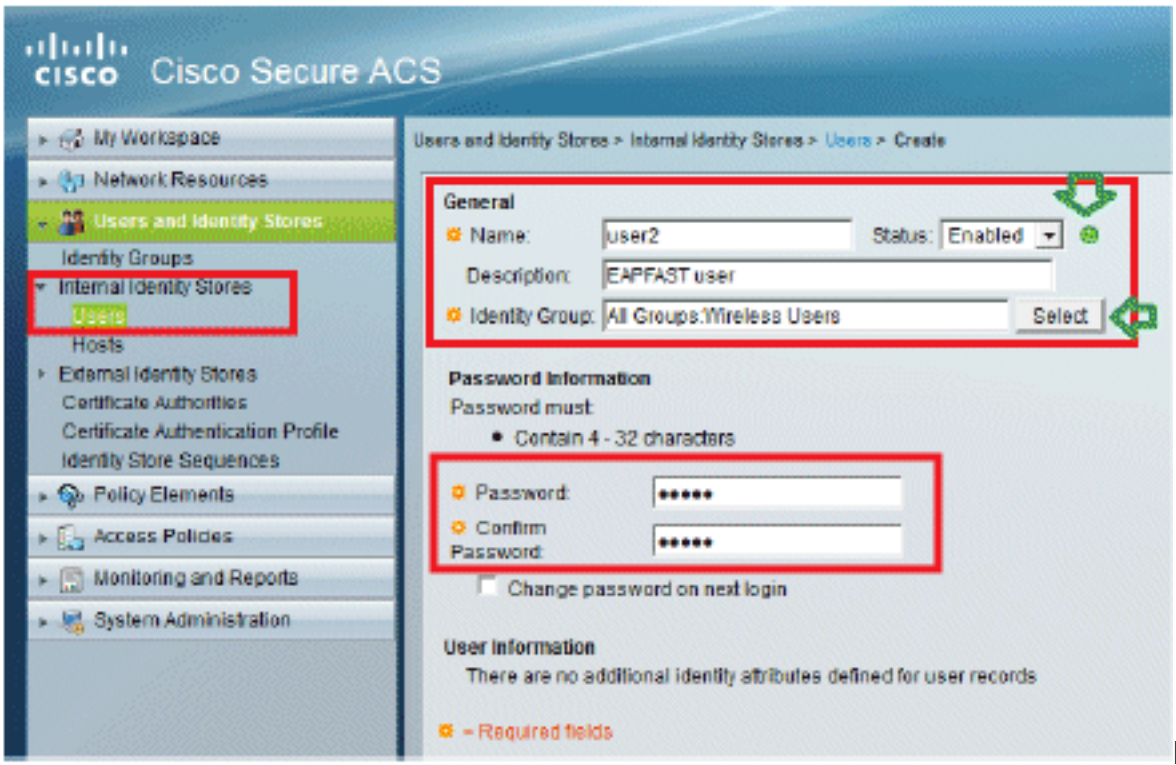
2. Zodra u op **Indienen** klikt, ziet de pagina er als volgt uit:

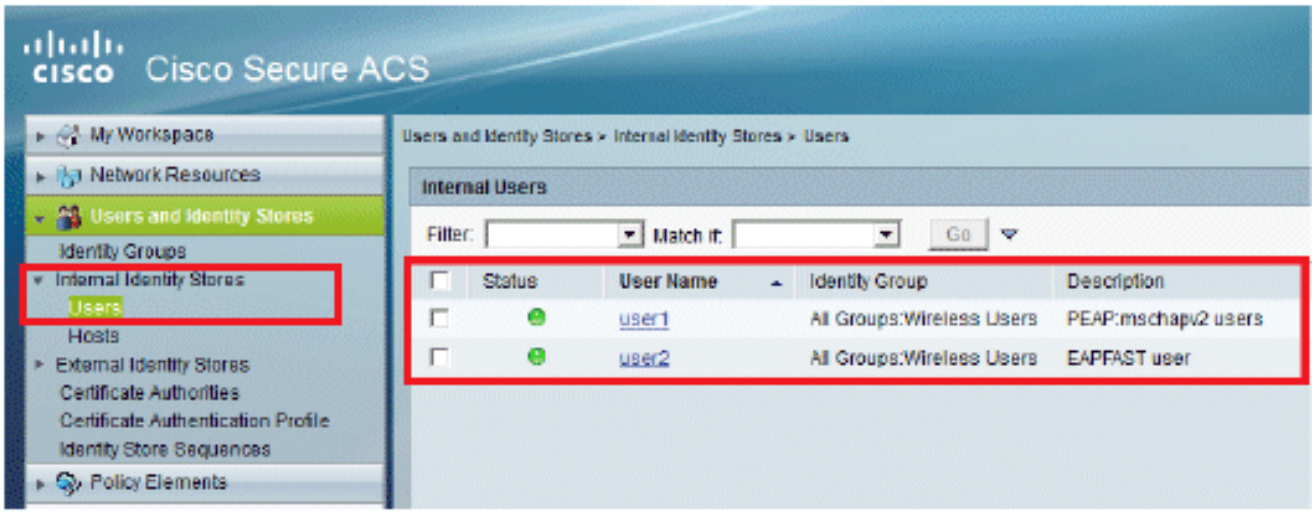


3. Maak gebruikers **user1** en **user2**, en wijs ze toe aan de groep "Draadloze gebruikers".Klik op **Gebruikers en identiteitswinkels > Identiteitsgroepen > Gebruikers > Aanmaken**.



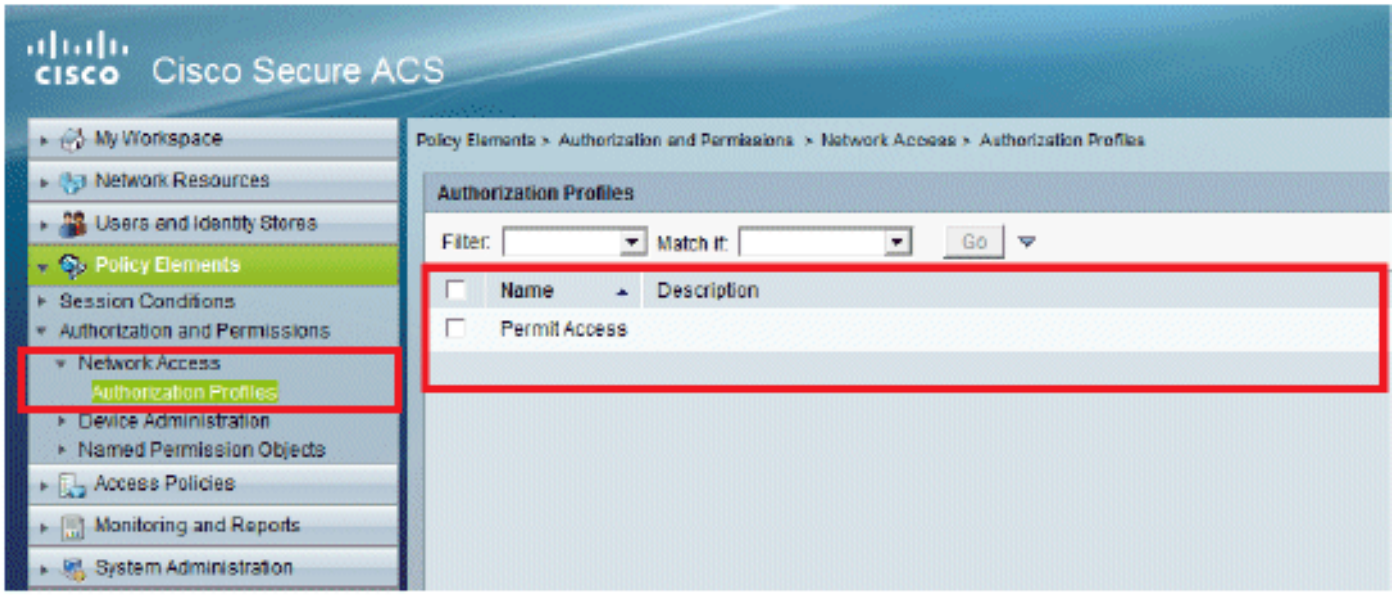
Op dezelfde manier maakt u user2. Het scherm zal er als volgt uitzien:





Beleidselementen definiëren

Controleer of **Permit Access** is ingesteld.

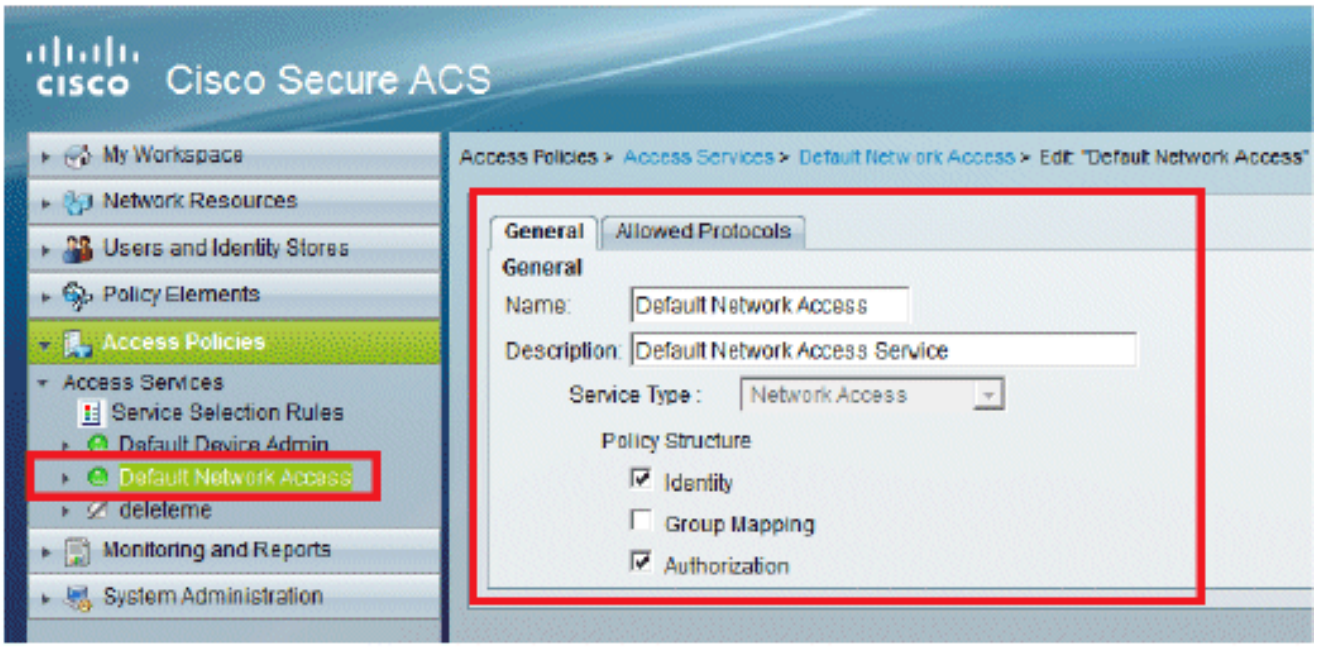


Toegangsbeleid toepassen

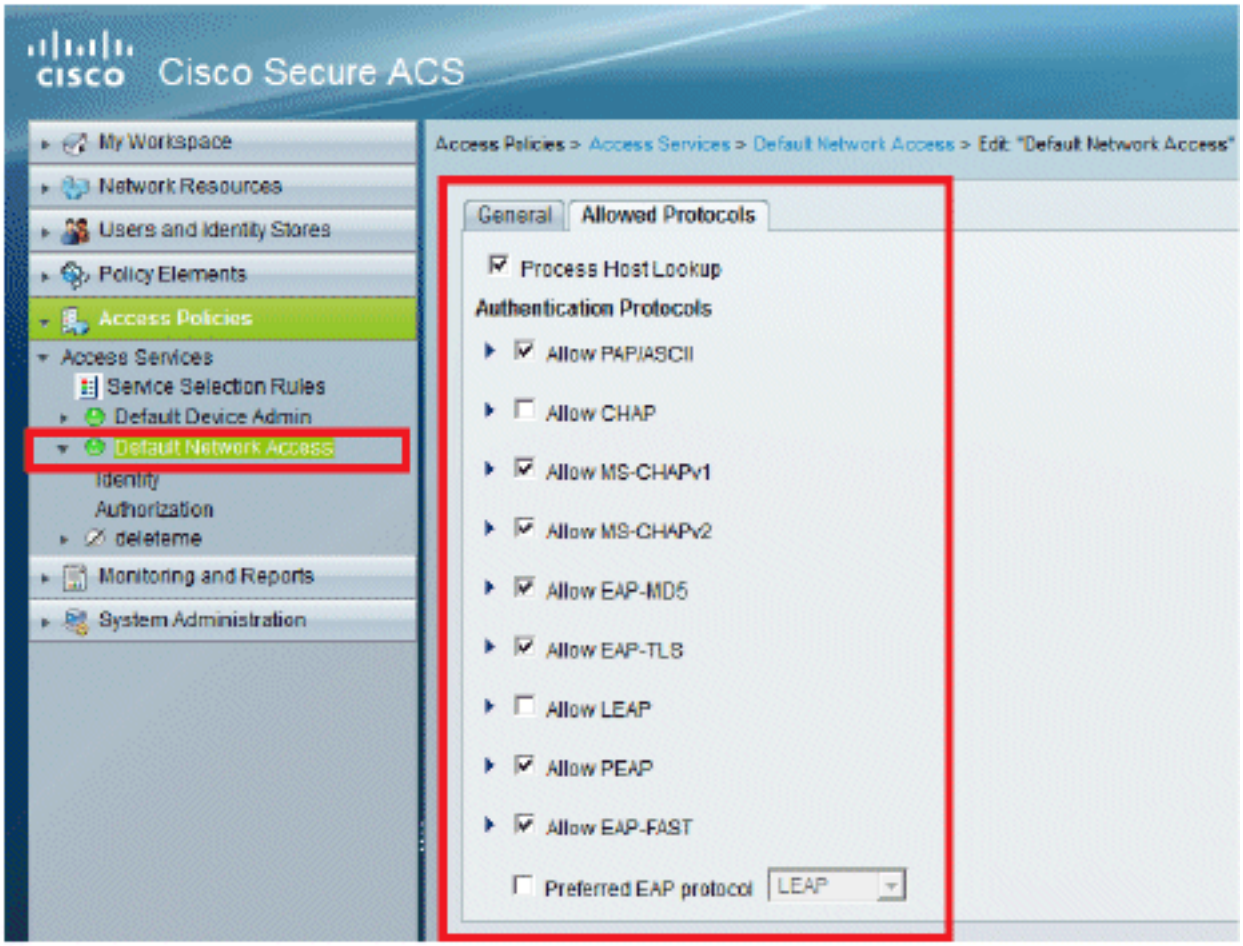
In dit gedeelte selecteren we welke verificatiemethoden moeten worden gebruikt en hoe de regels moeten worden geconfigureerd. We zullen regels opstellen op basis van de voorgaande stappen.

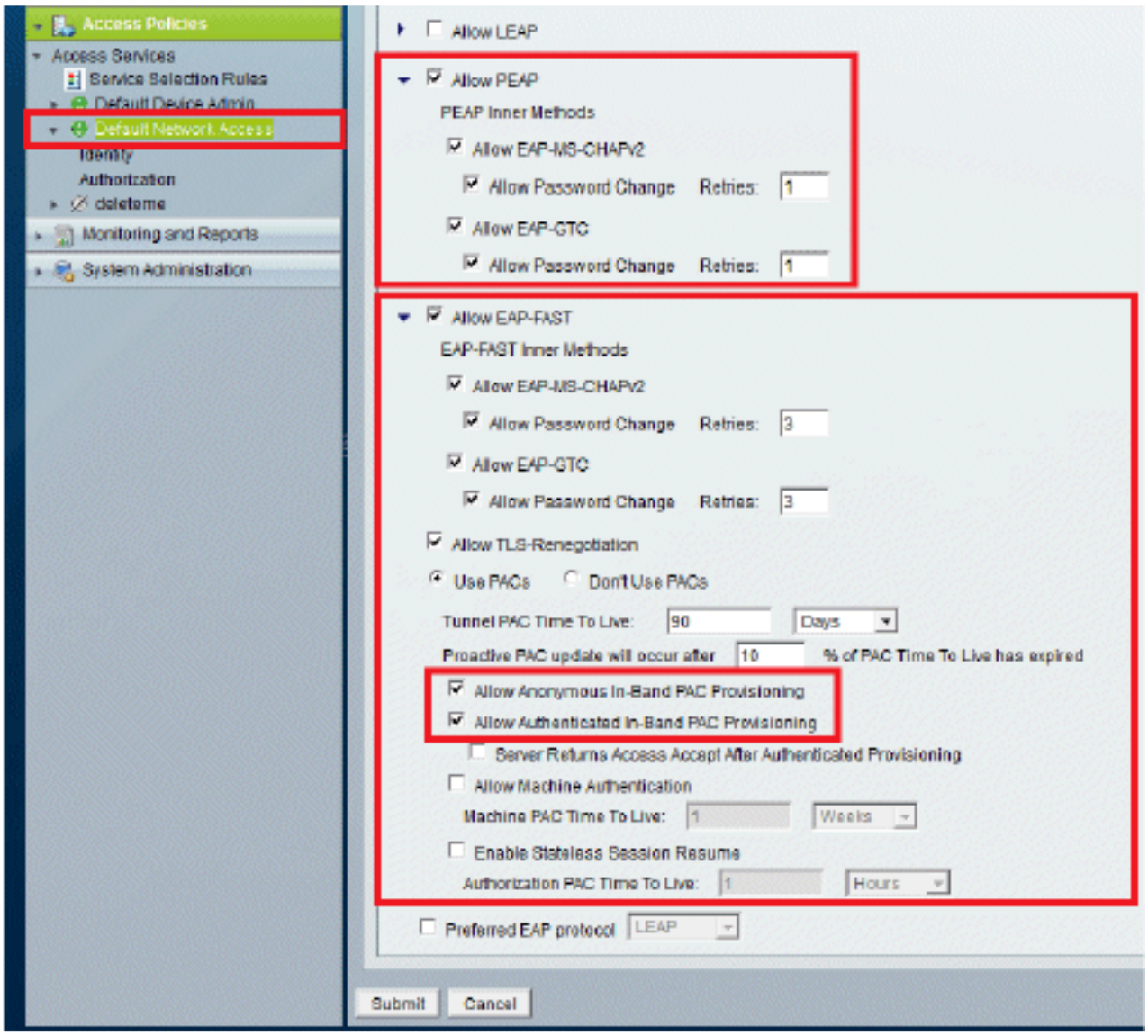
Voer de volgende stappen uit:

1. Ga naar **Toegangsbeleid > Toegangsservices > Standaard netwerktoegang > Bewerken: "Standaard netwerktoegang"**.

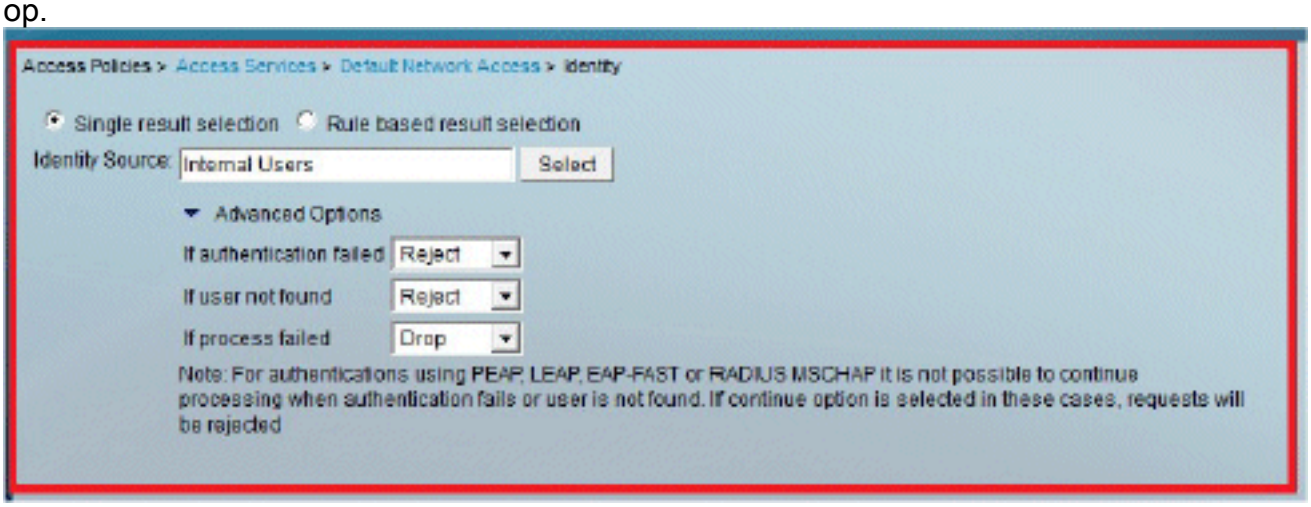


2. Selecteer de EAP-methode die u wilt laten verifiëren door de draadloze clients. In dit voorbeeld gebruiken we **PEAP-MSCHAPv2** en **EAP-FAST**.



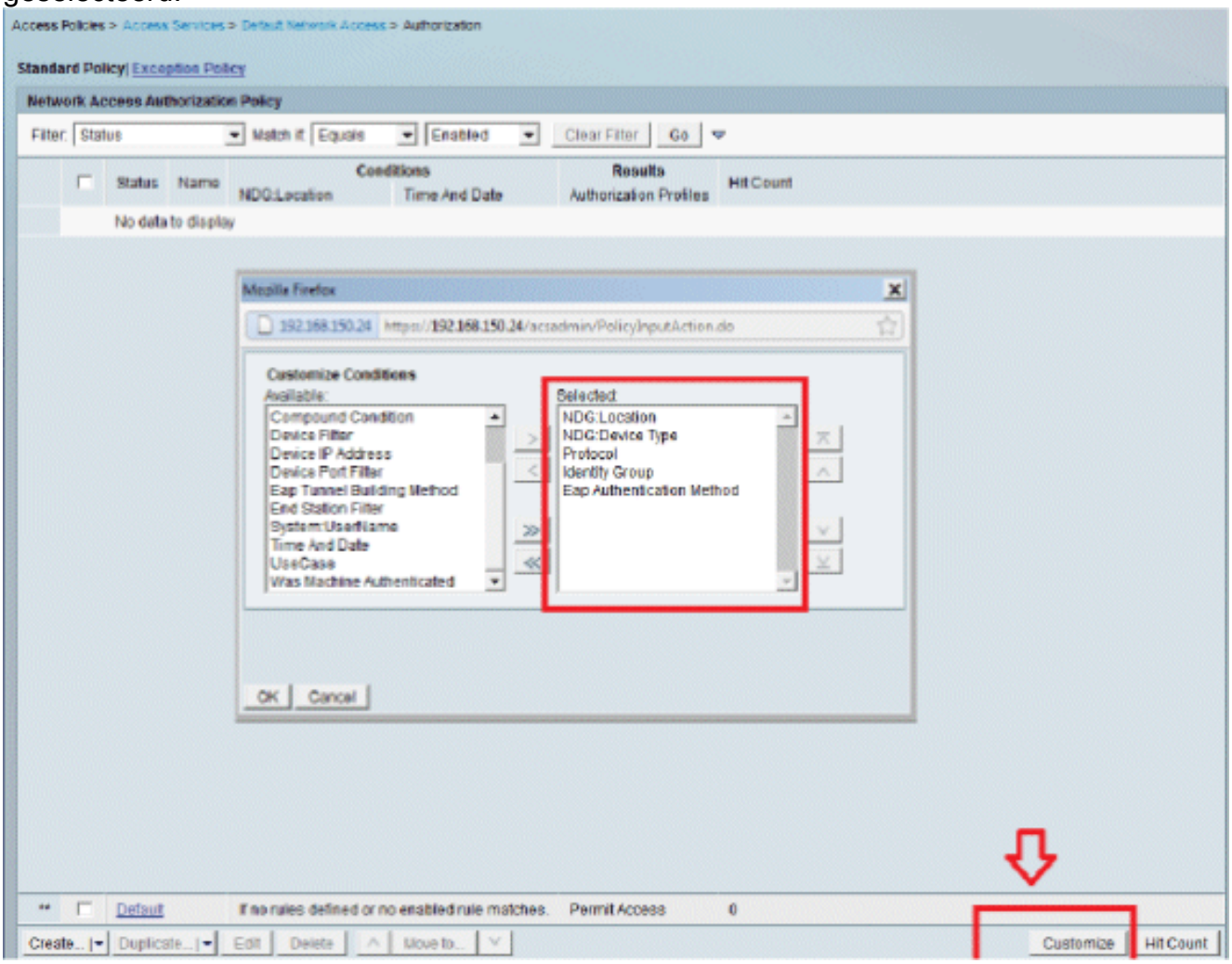


3. Klik op **Verzenden**.
4. Controleer de groep Identity die u hebt geselecteerd. In dit voorbeeld gebruiken we **Interne Gebruikers**, die we hebben gemaakt op ACS. **Sla** de wijzigingen op.

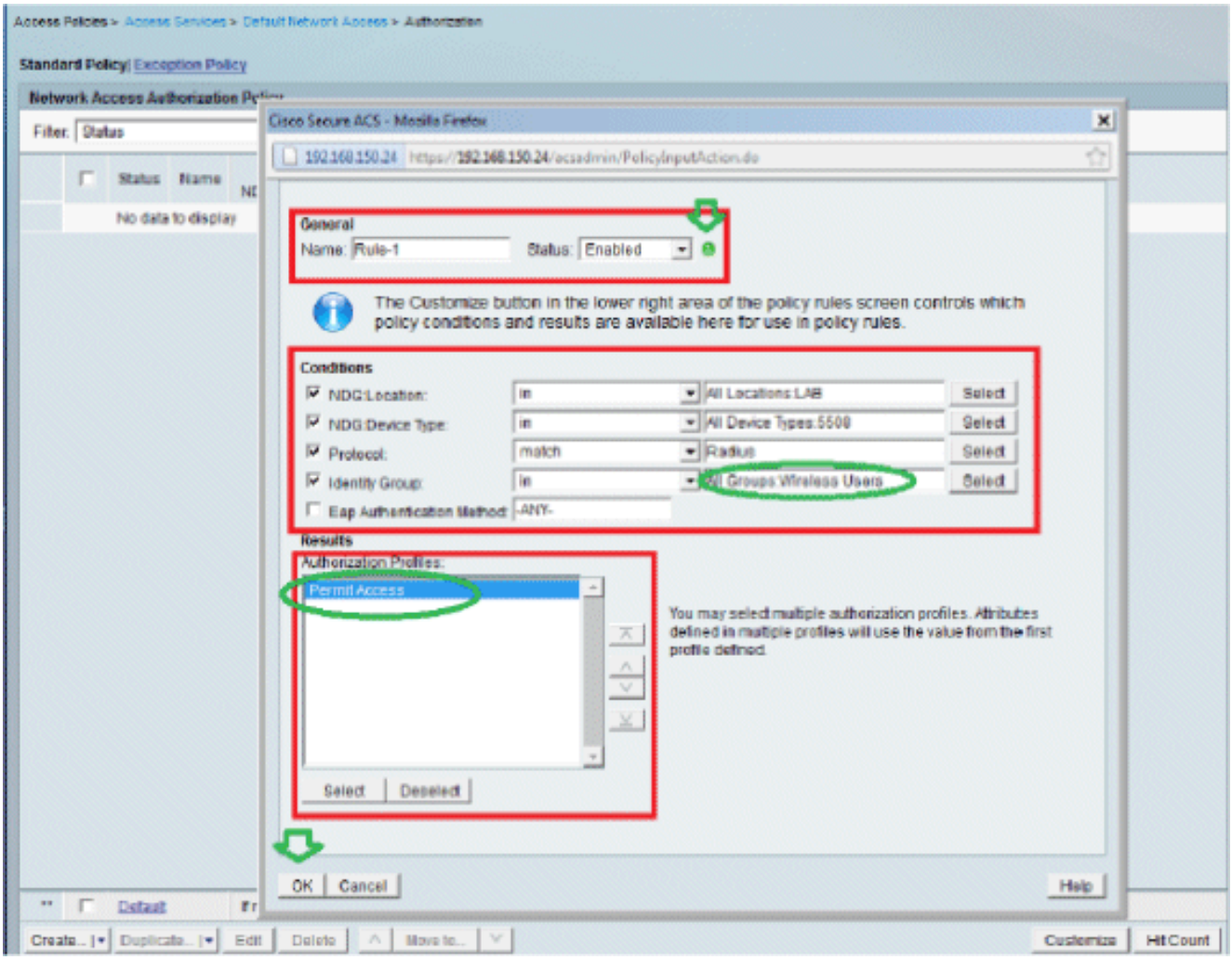


5. Als u het autorisatieprofiel wilt controleren, gaat u naar **Toegangsbeleid > Toegangsservices > Standaard netwerktoegang > Autorisatie**.U kunt aanpassen onder welke voorwaarden u gebruikerstoegang tot het netwerk zult verlenen en welk autorisatieprofiel (attributen) u zal overgaan zodra het is geverifieerd. Deze granulariteit is alleen beschikbaar in ACS 5.x. In dit voorbeeld hebben we de optie Locatie, **Apparaattype**, **Protocol**, **Identity Group** en **EAP-**

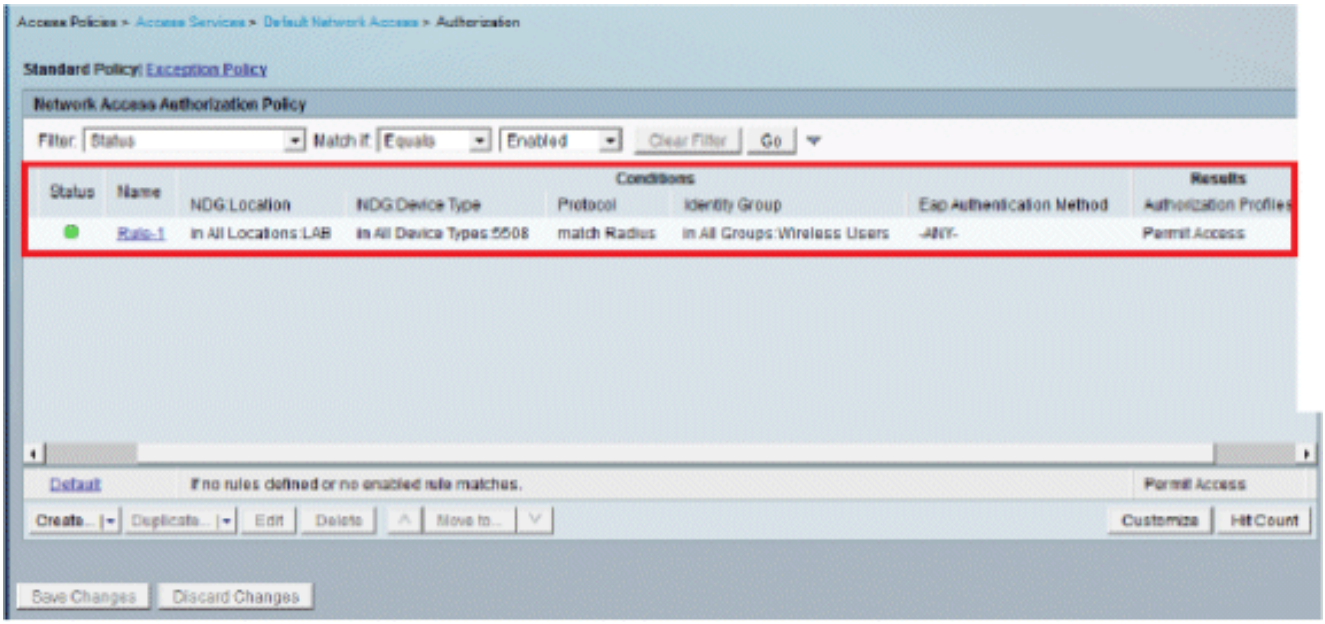
verificatiemethode
geselecteerd.



6. Klik op **OK** en **sla wijzigingen op**.
7. De volgende stap is het opstellen van een regel. Als er geen regels zijn vastgesteld, krijgt de klant zonder enige voorwaarden toegang.Klik op **Aanmaken > Regel-1**. Deze regel is voor gebruikers in de groep "Draadloze gebruikers".

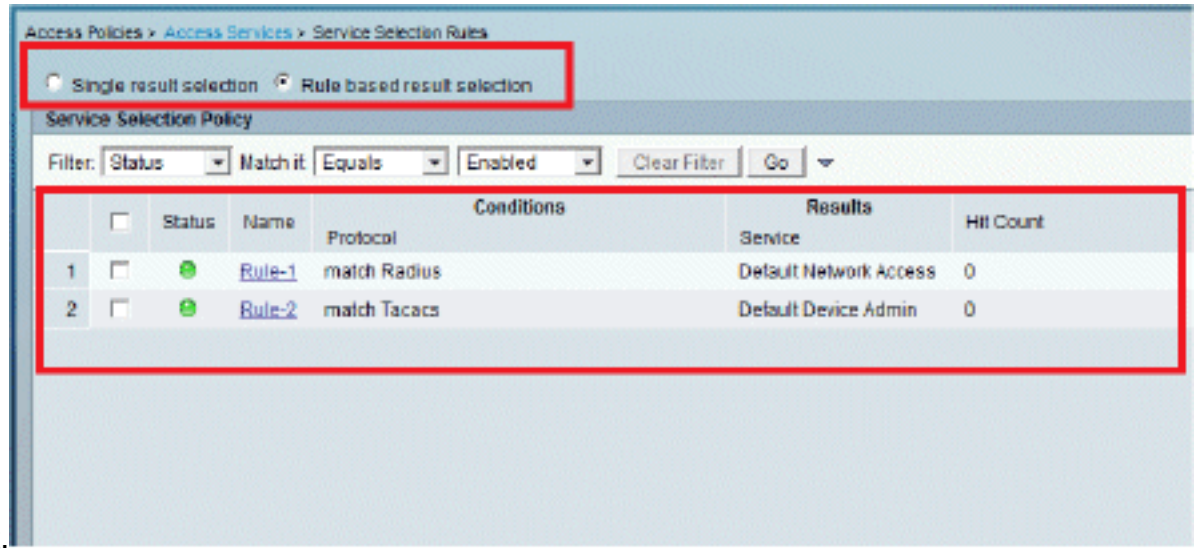


8. Sla de wijzigingen op. Het scherm zal er als volgt uitzien:



Als u wilt dat gebruikers die niet voldoen aan de voorwaarden die worden geweigerd, bewerk dan de standaardregel om "ontkennen toegang" te zeggen.

9. Wij zullen nu **regels voor de selectie van de dienst** vaststellen. Gebruik deze pagina om een eenvoudig of regel-gebaseerd beleid te vormen om te bepalen welke dienst om op inkomende verzoeken van toepassing te zijn. In dit voorbeeld wordt een op regels gebaseerd beleid

gebruikt. 

De WLC configureren

Deze configuratie vereist de volgende stappen:

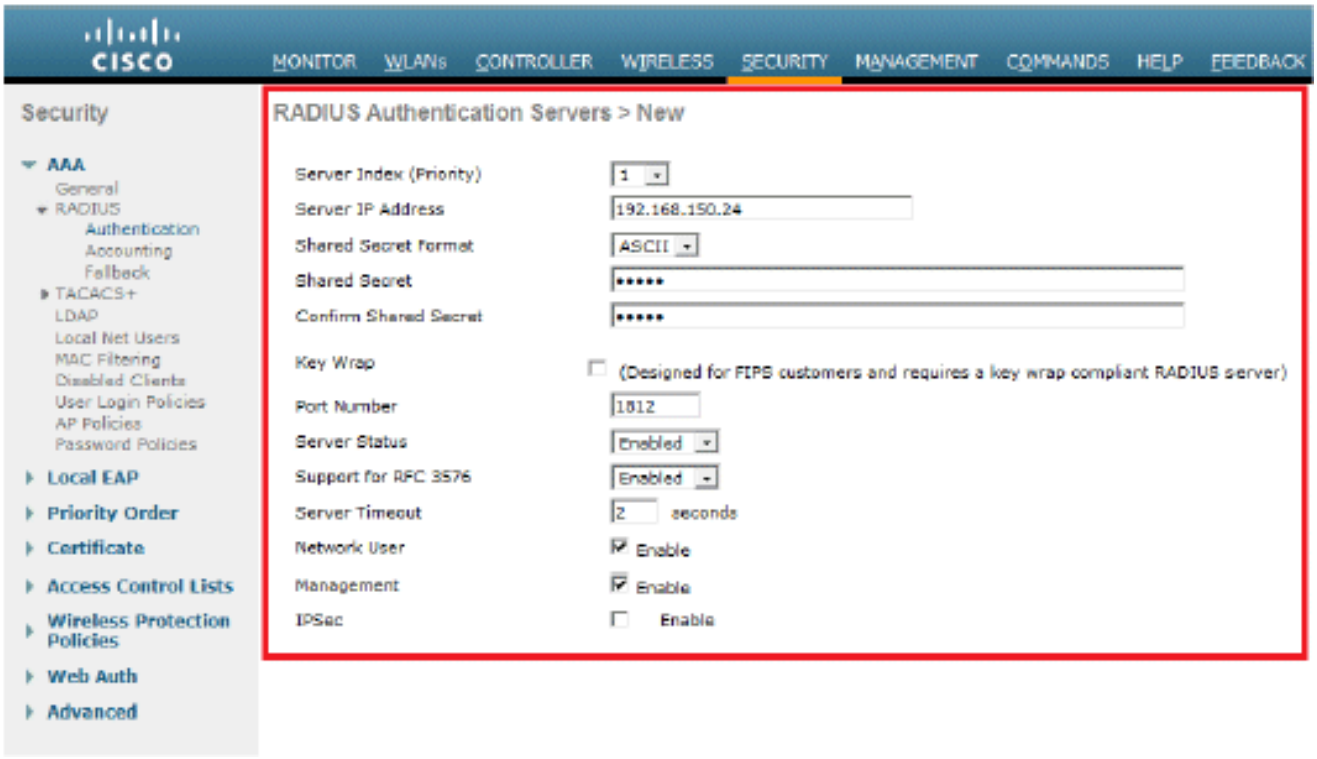
1. Configureer de WLC met de gegevens van de verificatieserver.
2. Configureer de Dynamische interfaces (VLAN's).
3. Configureer de WLAN's (SSID).

Configureer de WLC met de gegevens van de verificatieserver

Het is noodzakelijk om de WLC te configureren zodat het kan communiceren met de RADIUS-server om de clients te verifiëren, en ook voor andere transacties.

Voer de volgende stappen uit:

1. Klik vanuit de controller-GUI op **Security**.
2. Voer het IP-adres van de RADIUS-server en de gedeelde geheime sleutel in die wordt gebruikt tussen de RADIUS-server en de WLC.Deze gedeelde geheime sleutel moet dezelfde zijn als die welke in de RADIUS-server is geconfigureerd.

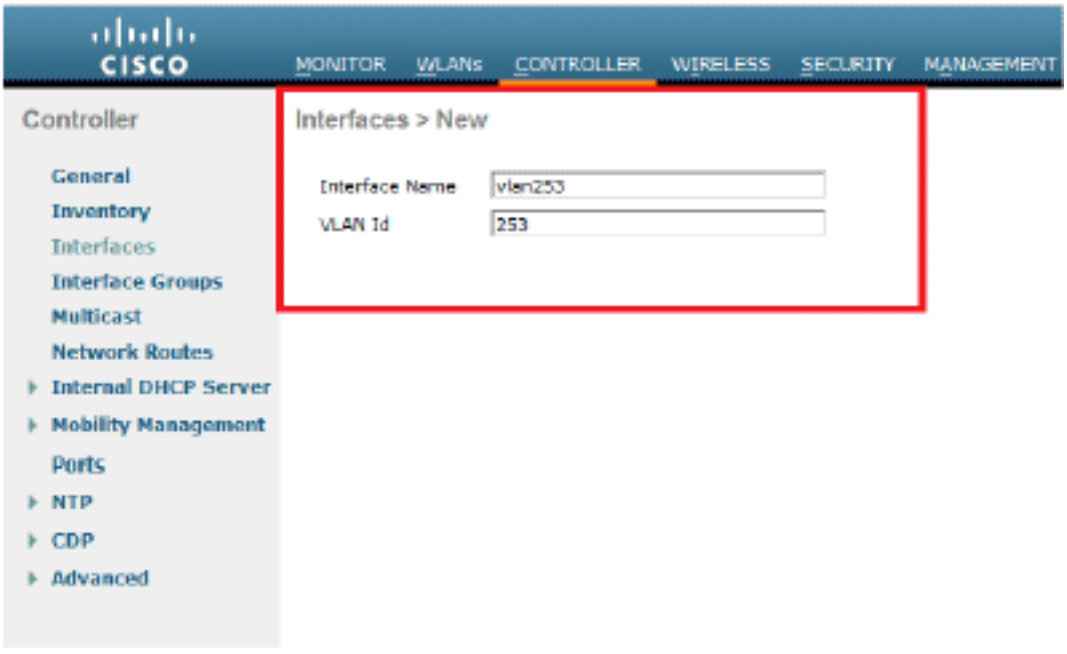


De dynamische interfaces (VLAN's) configureren

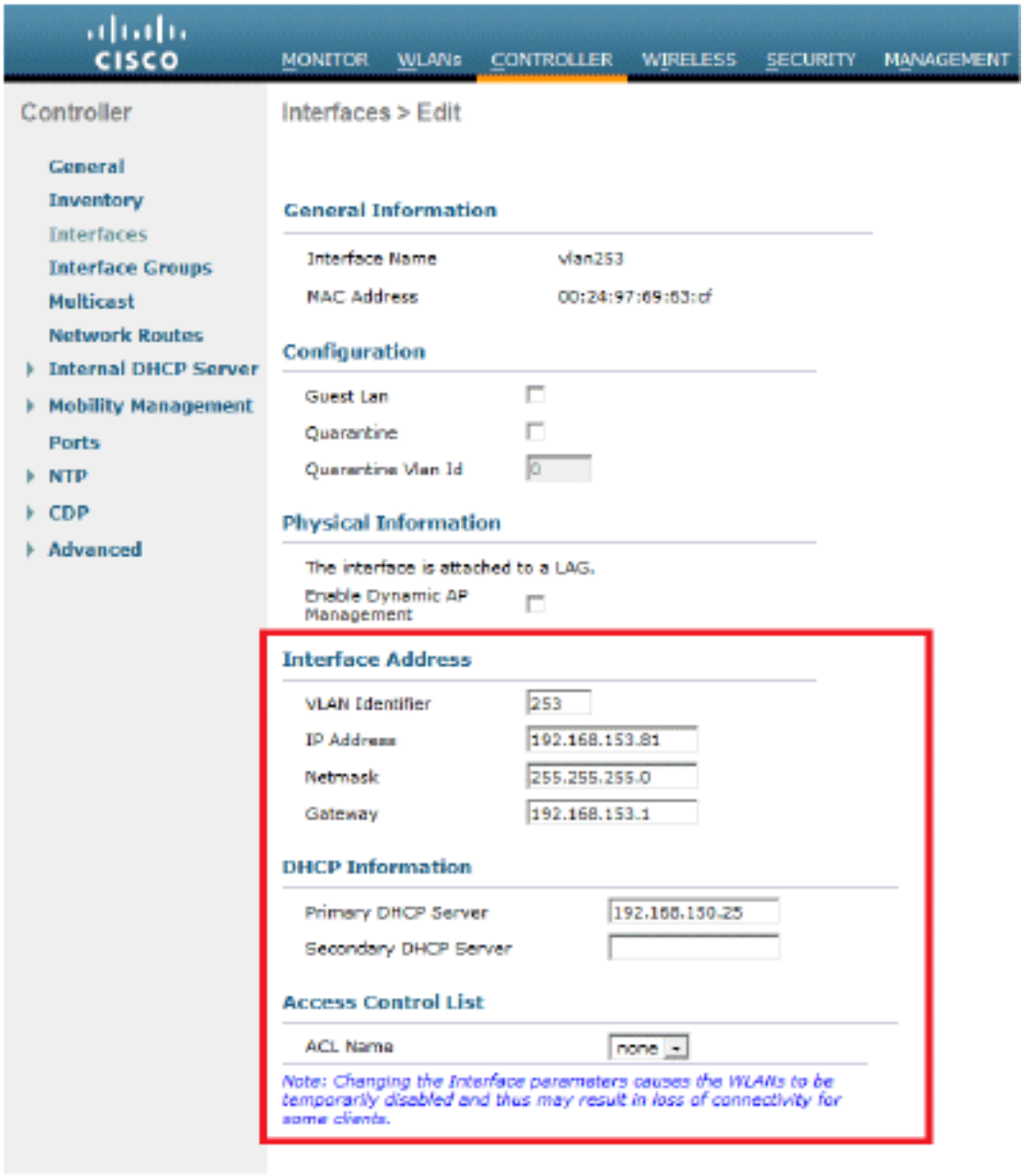
Deze procedure beschrijft hoe u dynamische interfaces op de WLC kunt configureren.

Voer de volgende stappen uit:

1. De dynamische interface wordt geconfigureerd vanuit de controller-GUI, in het venster **Controller >**

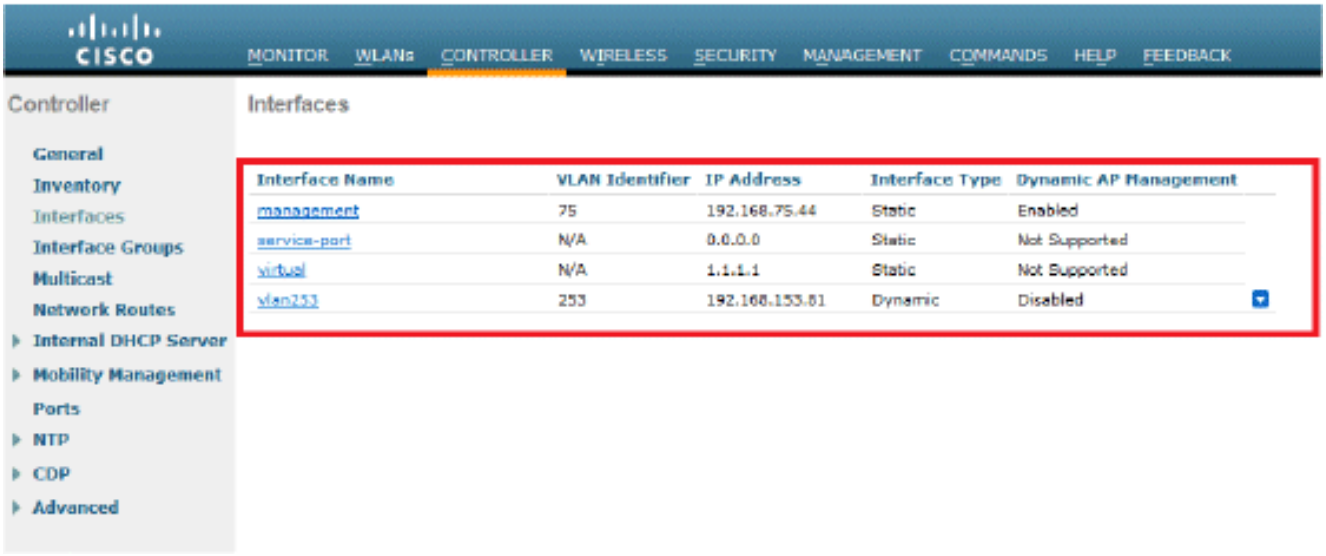


Interfaces.
2. Klik op **Apply** (Toepassen).Dit brengt u naar het venster Bewerken van deze dynamische interface (VLAN 253 hier).
3. Voer het IP-adres en de standaardgateway van deze dynamische interface



in.

4. Klik op **Apply** (Toepassen).
5. De geconfigureerde interfaces zien er als volgt uit:

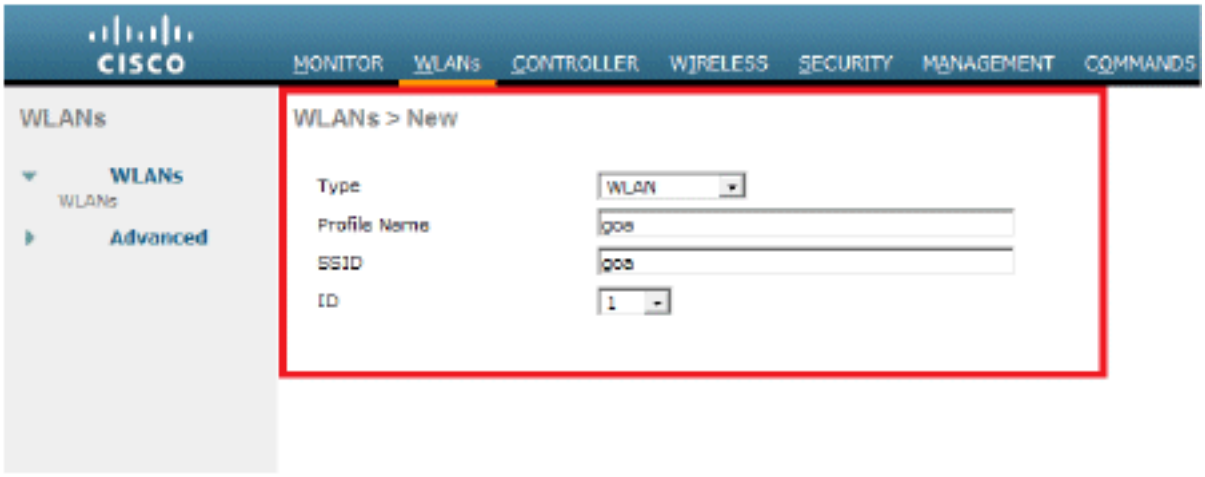


De WLAN's (SSID) configureren

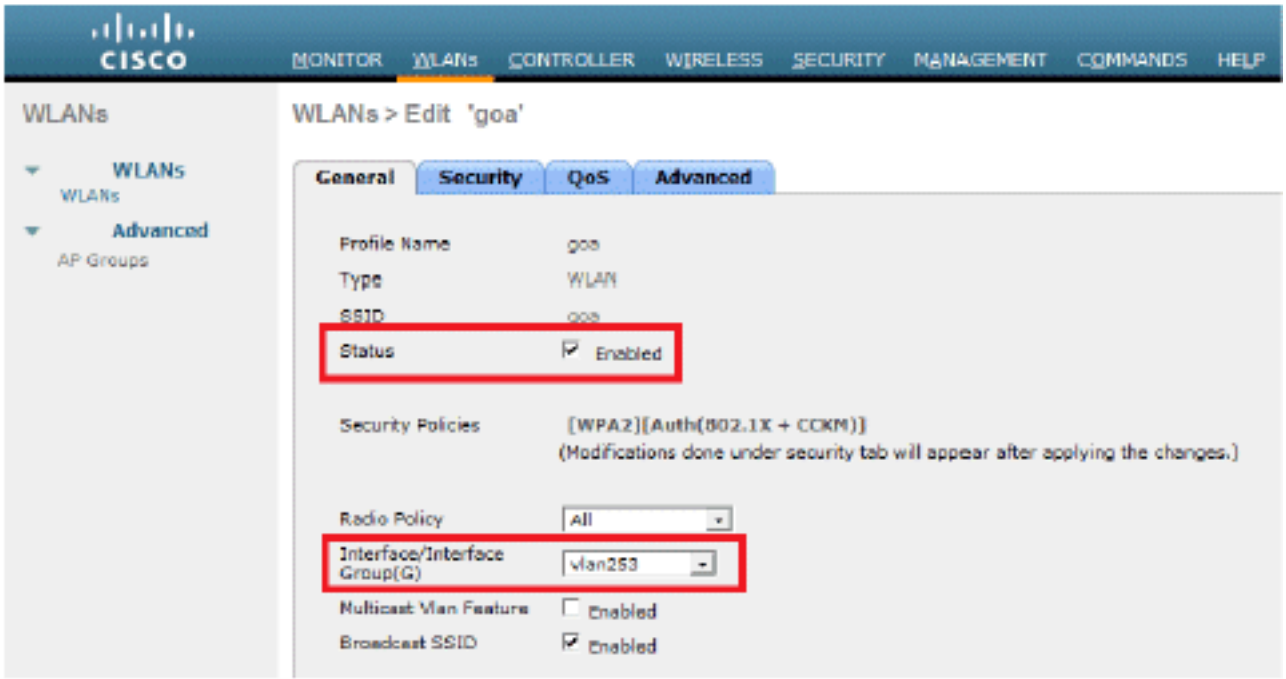
Deze procedure verklaart hoe te om WLANs in WLC te vormen.

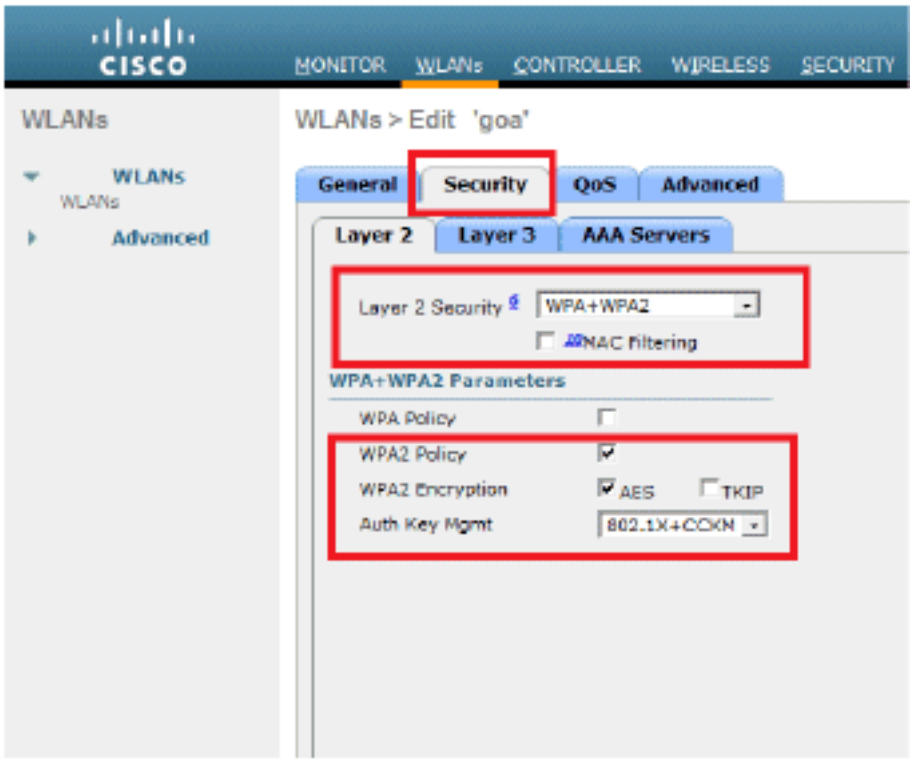
Voer de volgende stappen uit:

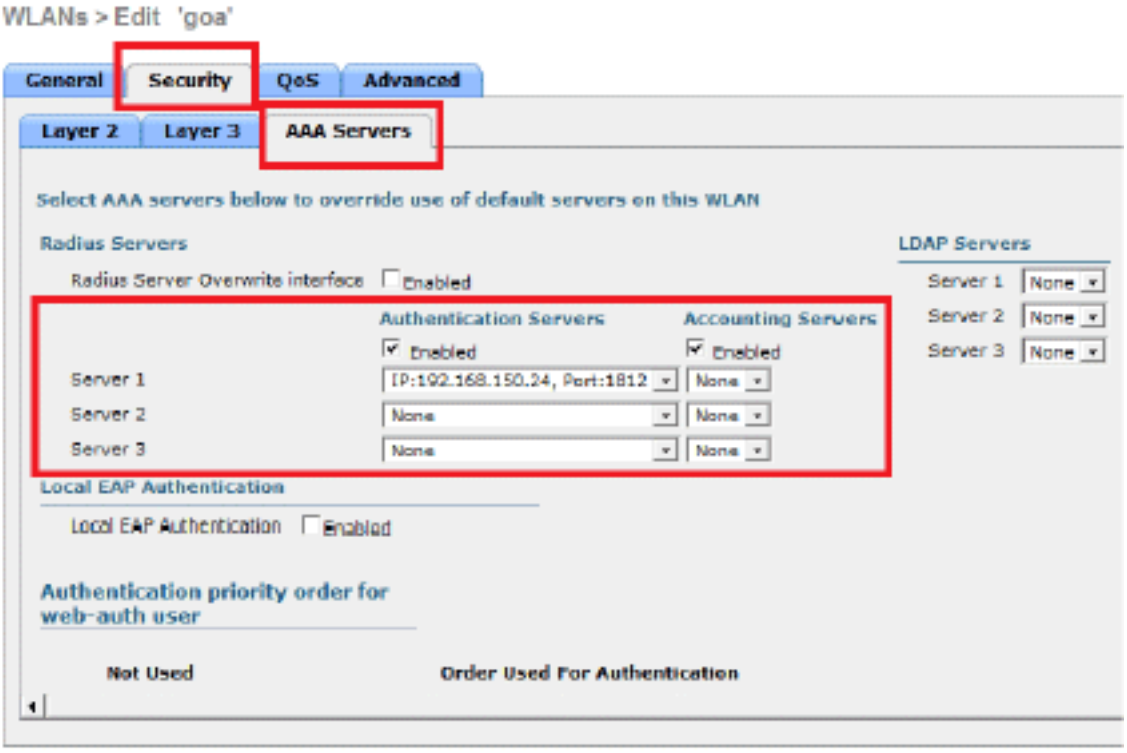
1. Van de controller GUI, ga naar **WLAN's > Create New** om een nieuw WLAN te maken. Het nieuwe WLAN-venster wordt weergegeven.
2. Voer de informatie over WLAN-id en WLAN-SSID in.U kunt om het even welke naam als WLAN SSID ingaan. In dit voorbeeld wordt **goa** gebruikt als WLAN-SSID.

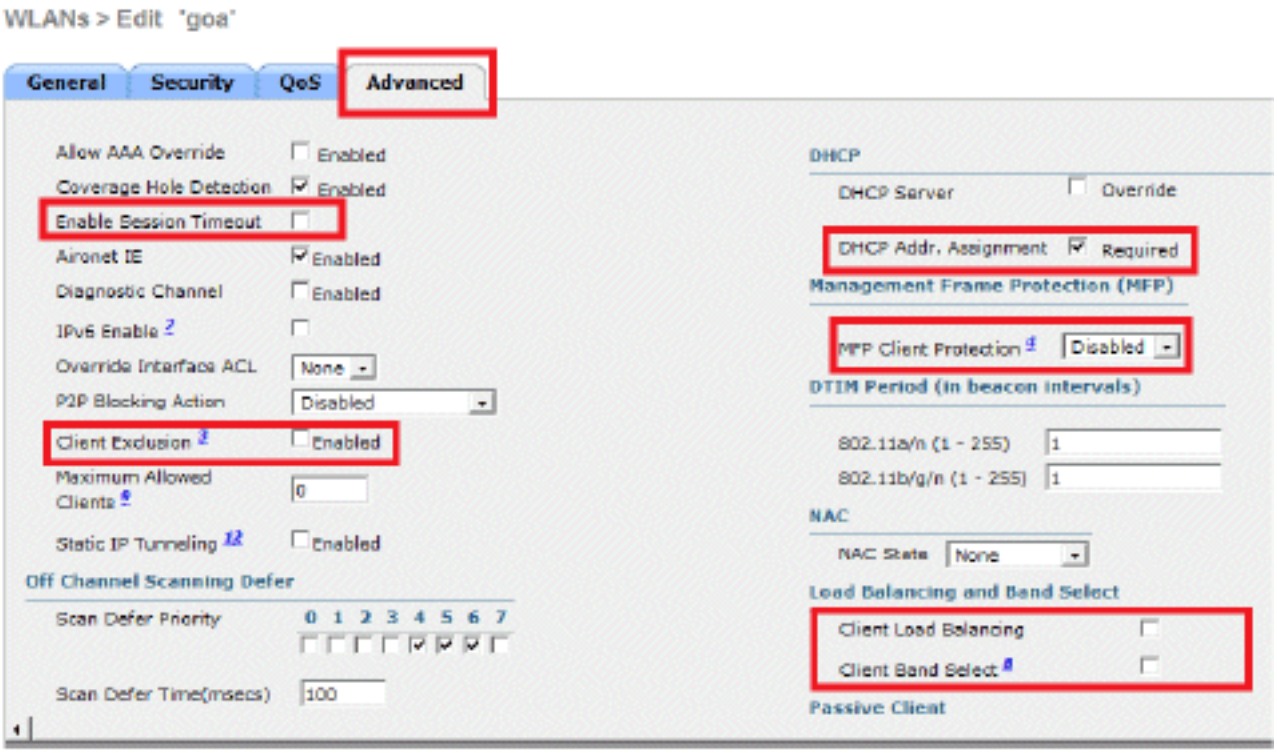


3. Klik op **Toepassen** om naar het venster Bewerken van het WLAN-doel te gaan.




MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
WLANs
WLANs > Edit 'goa'
WLANs
WLANs
Advanced
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Auth Key Mgmt
802.1X+CCKM


WLANs > Edit 'goa'
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Radius Server Overwrite interface
Enabled
Authentication Servers
Accounting Servers
Enabled
Enabled
Server 1
IP:192.168.150.24, Port:1812
None
Server 2
None
None
Server 3
None
None
LDAP Servers
Server 1
None
Server 2
None
Server 3
None
Local EAP Authentication
Local EAP Authentication
Enabled
Authentication priority order for web-auth user
Not Used
Order Used For Authentication



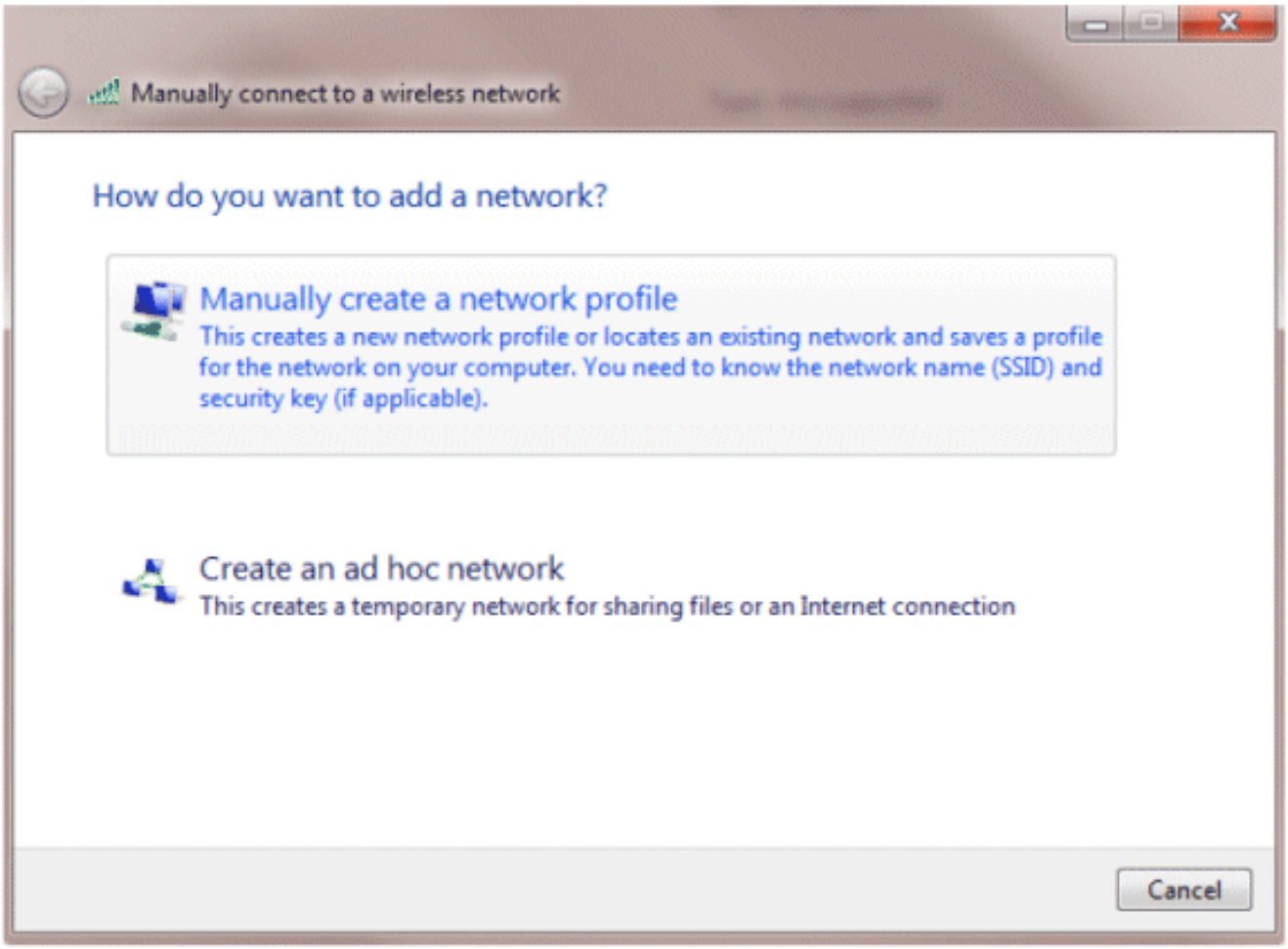
Het hulpprogramma voor draadloze clients configureren

PEAP-MSCHAPv2 (gebruiker1)

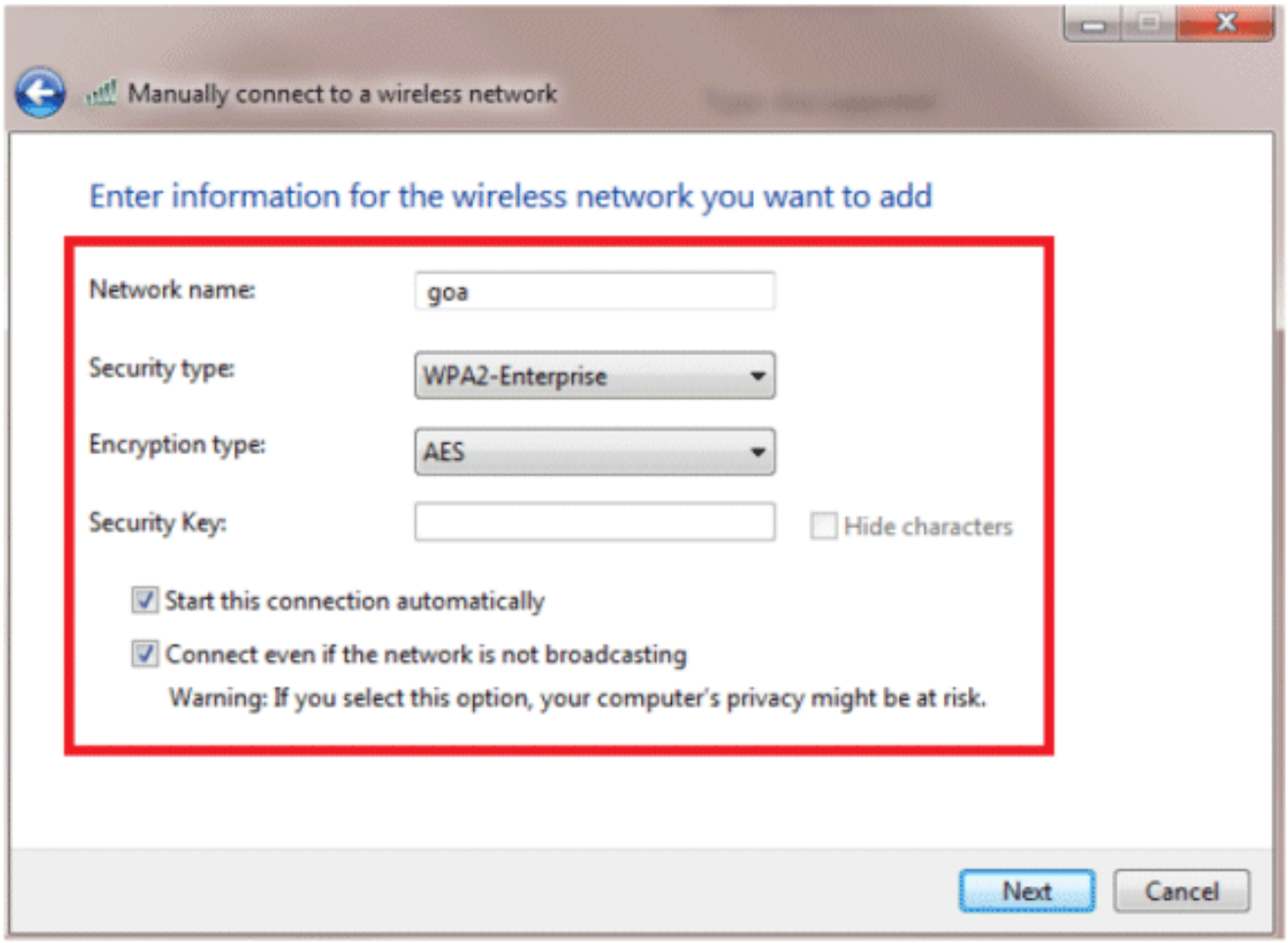
In onze testclient gebruiken we Windows 7 Native Supplicant met een Intel 6300-N kaart waarop 14.3 driver-versie draait. Het is aan te raden om te testen met de nieuwste drivers van leveranciers.

Voltooi de volgende stappen om een profiel te maken in Windows Zero Config (WZC):

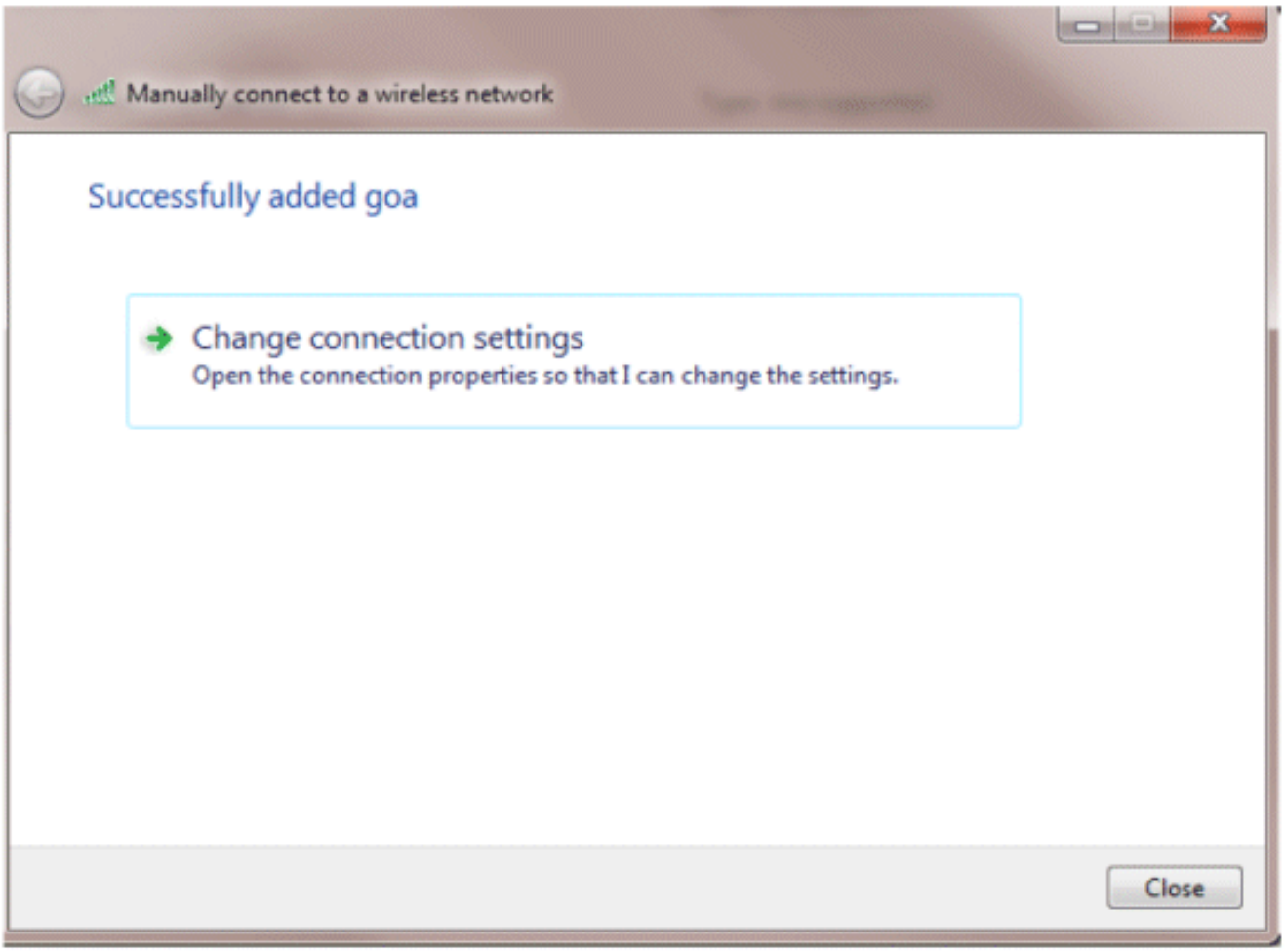
1. Ga naar **Configuratiescherm > Netwerk en internet > Draadloze netwerken beheren**.
2. Klik op het tabblad **Toevoegen**.
3. Klik op **Handmatig een netwerkprofiel maken**.



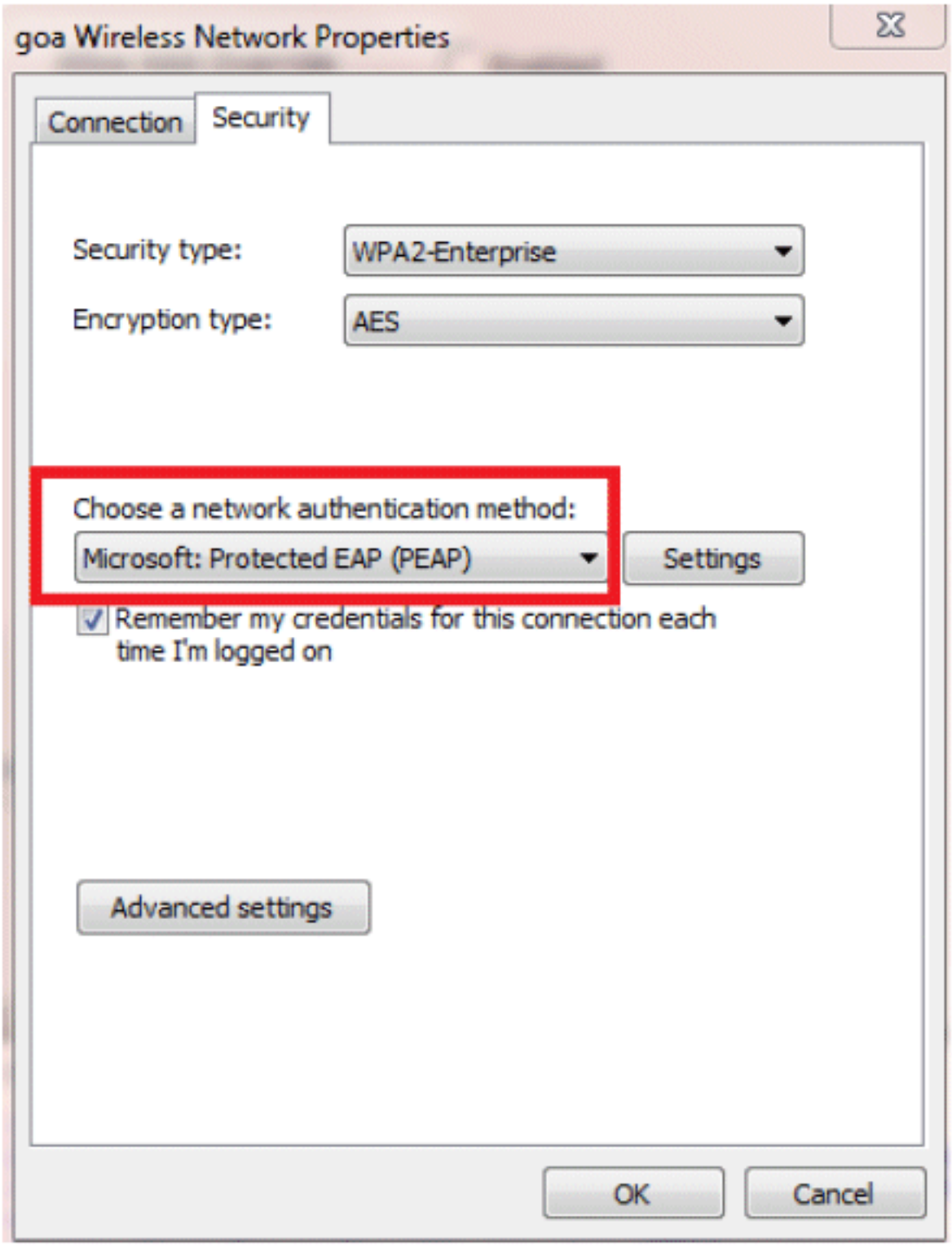
4. Voeg de details toe zoals die op WLC worden gevormd.**Opmerking:** de SSID is hoofdlettergevoelig.
5. Klik op **Next**
   (Volgende).

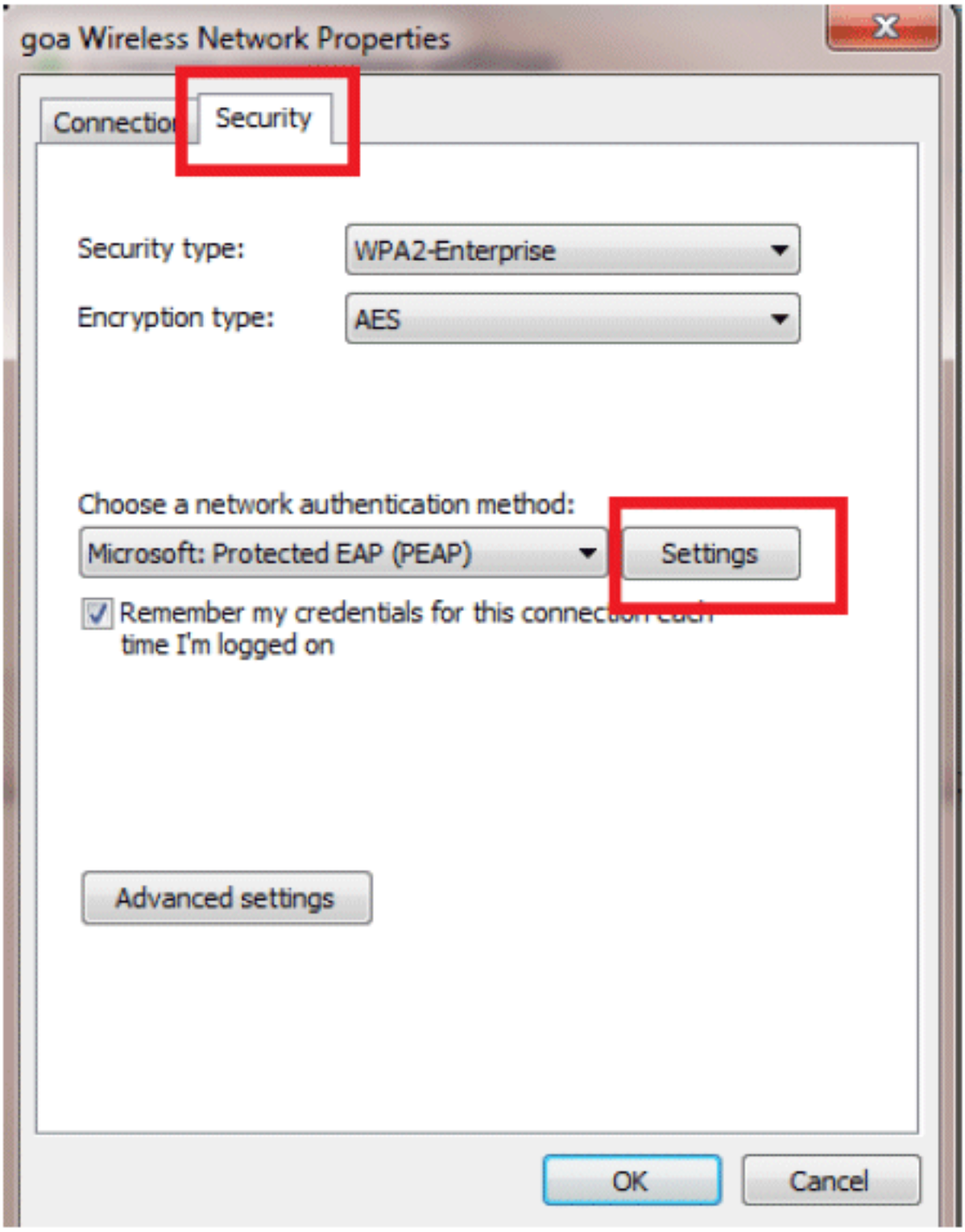


6. Klik op **Verbindingsinstellingen wijzigen** om de instellingen te controleren.

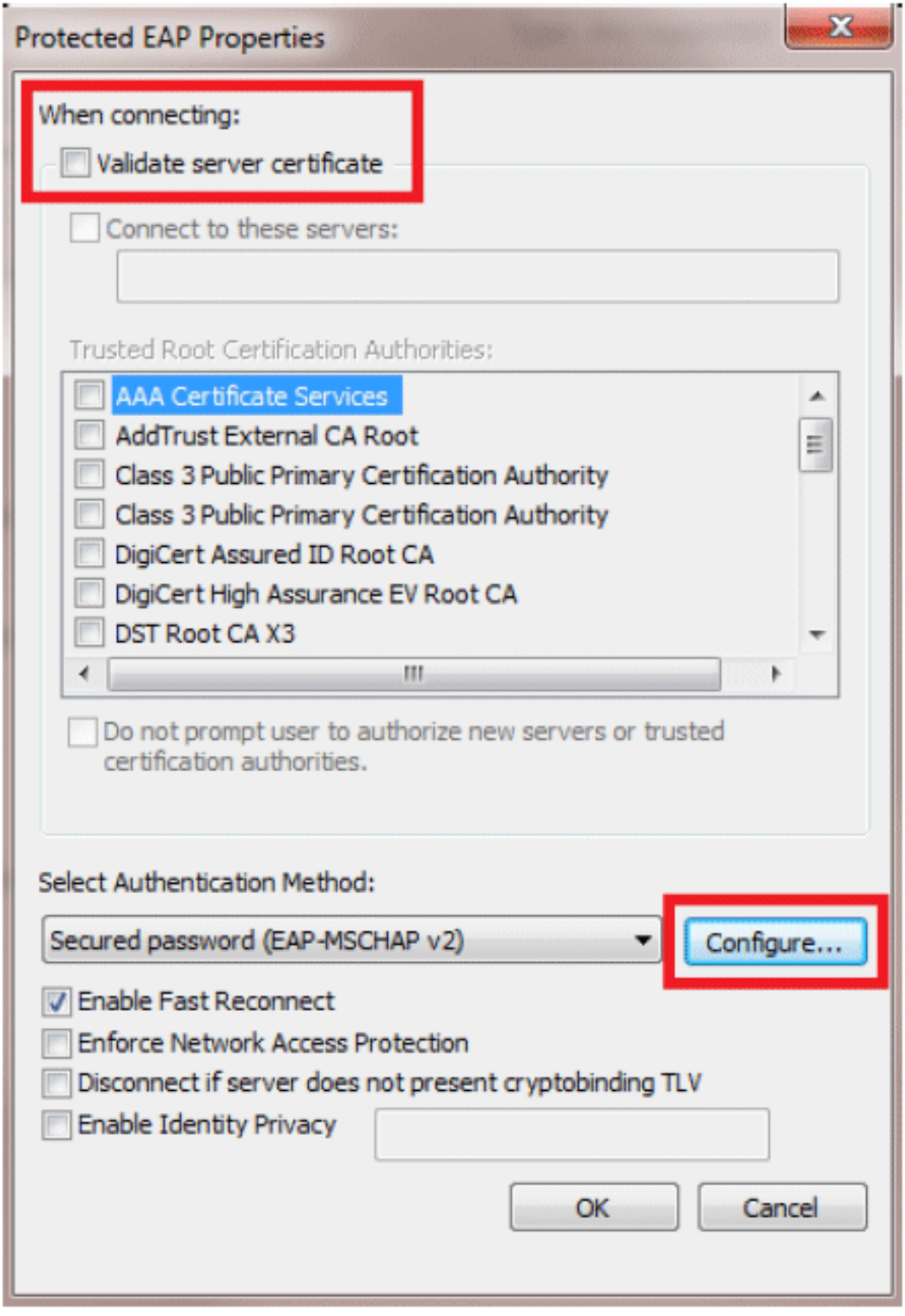


7. Controleer of **PEAP** is ingeschakeld.



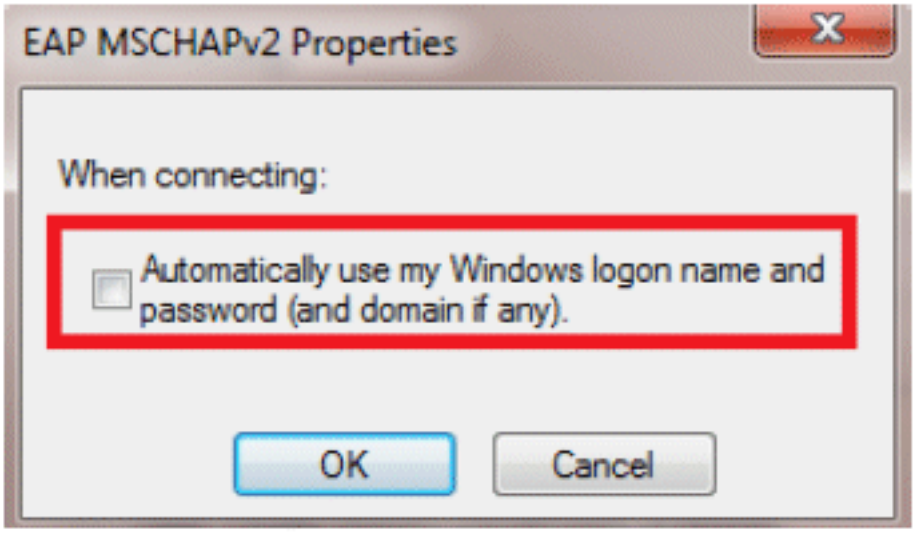


8. In dit voorbeeld valideren we het servercertificaat niet. Als u dit selectievakje inschakelt en geen verbinding kunt maken, probeer dan de functie uit te schakelen en weer te



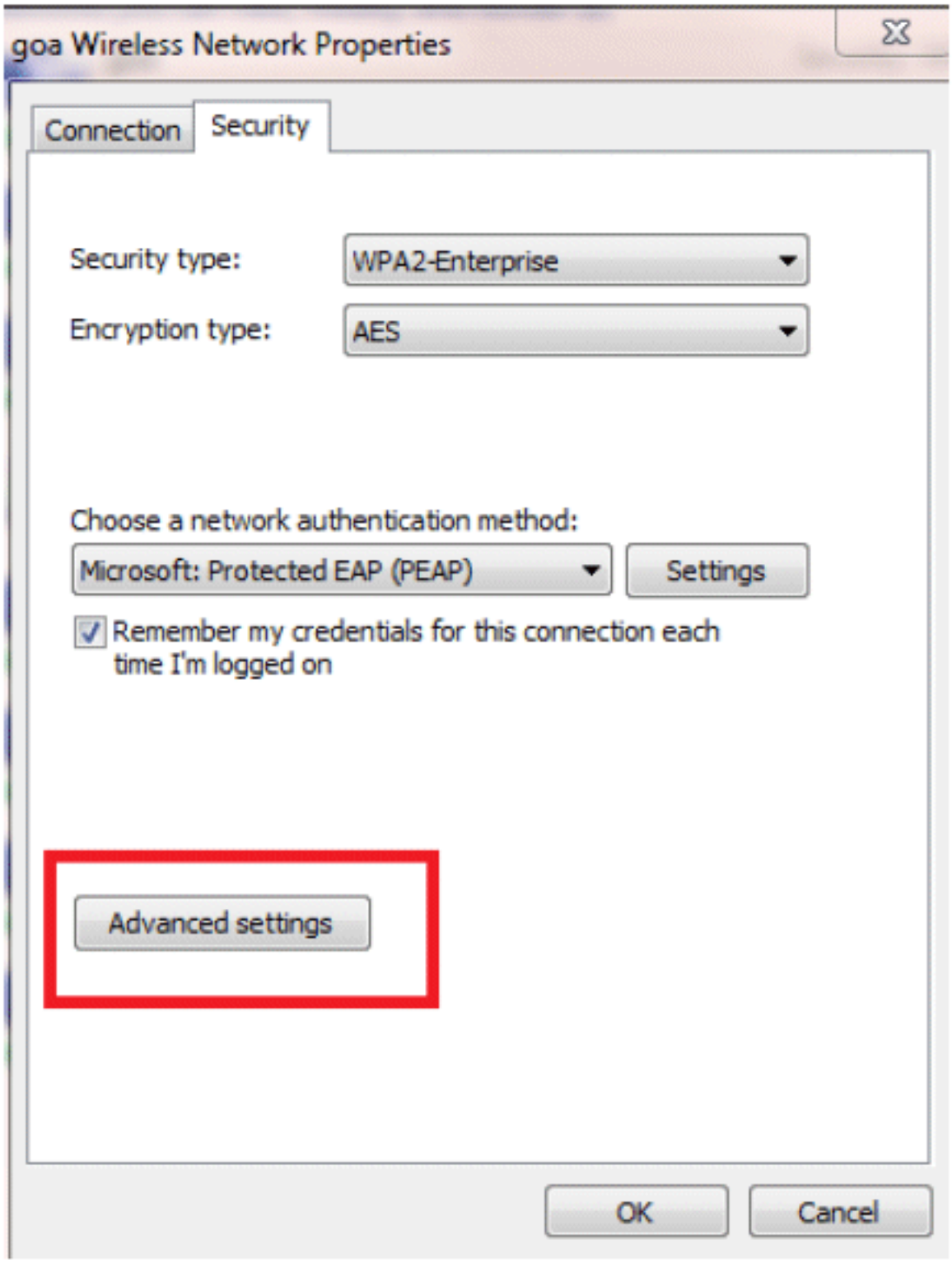
testen.

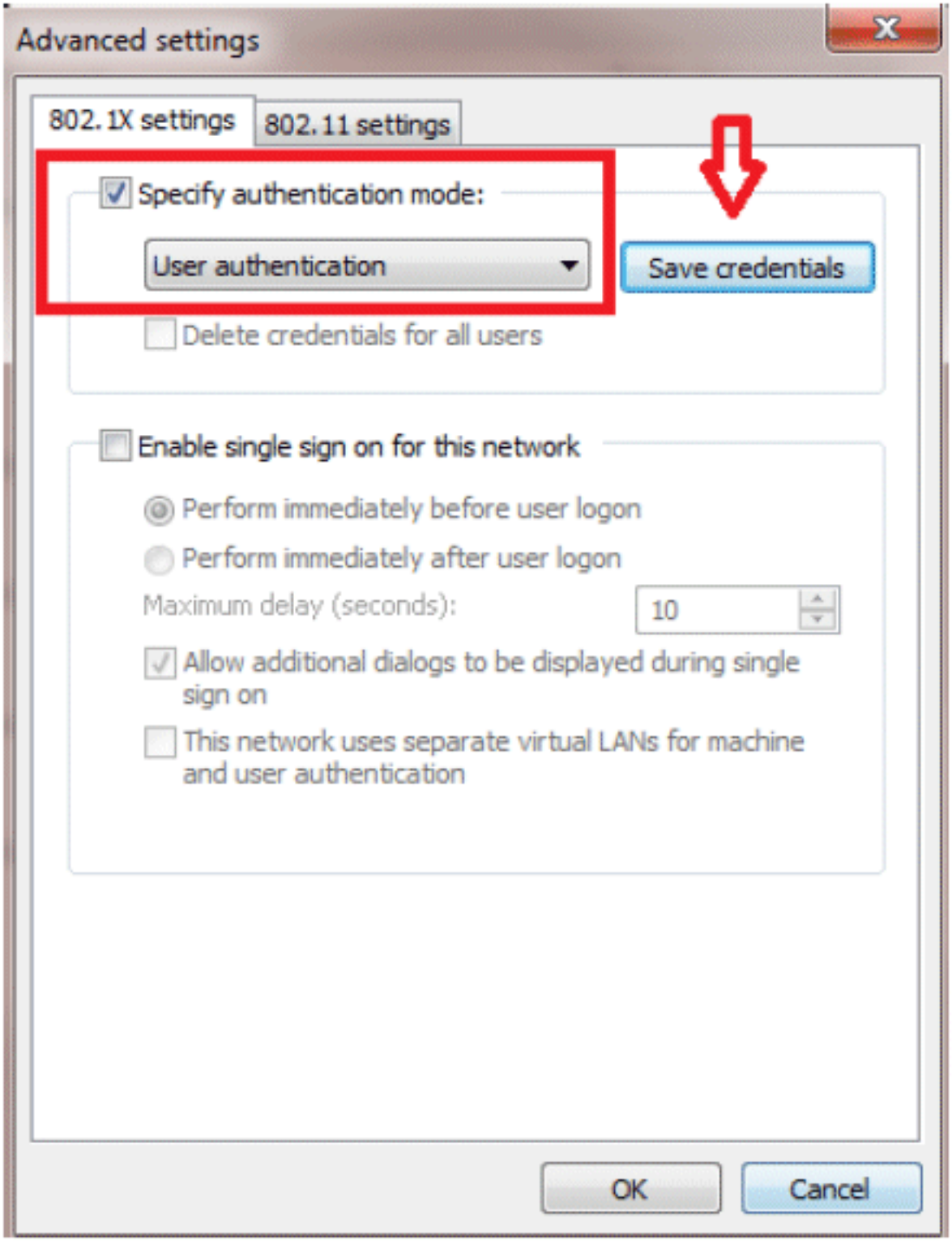
9. U kunt ook uw Windows-referenties gebruiken om in te loggen. In dit voorbeeld zullen we dat echter niet gebruiken. Klik op

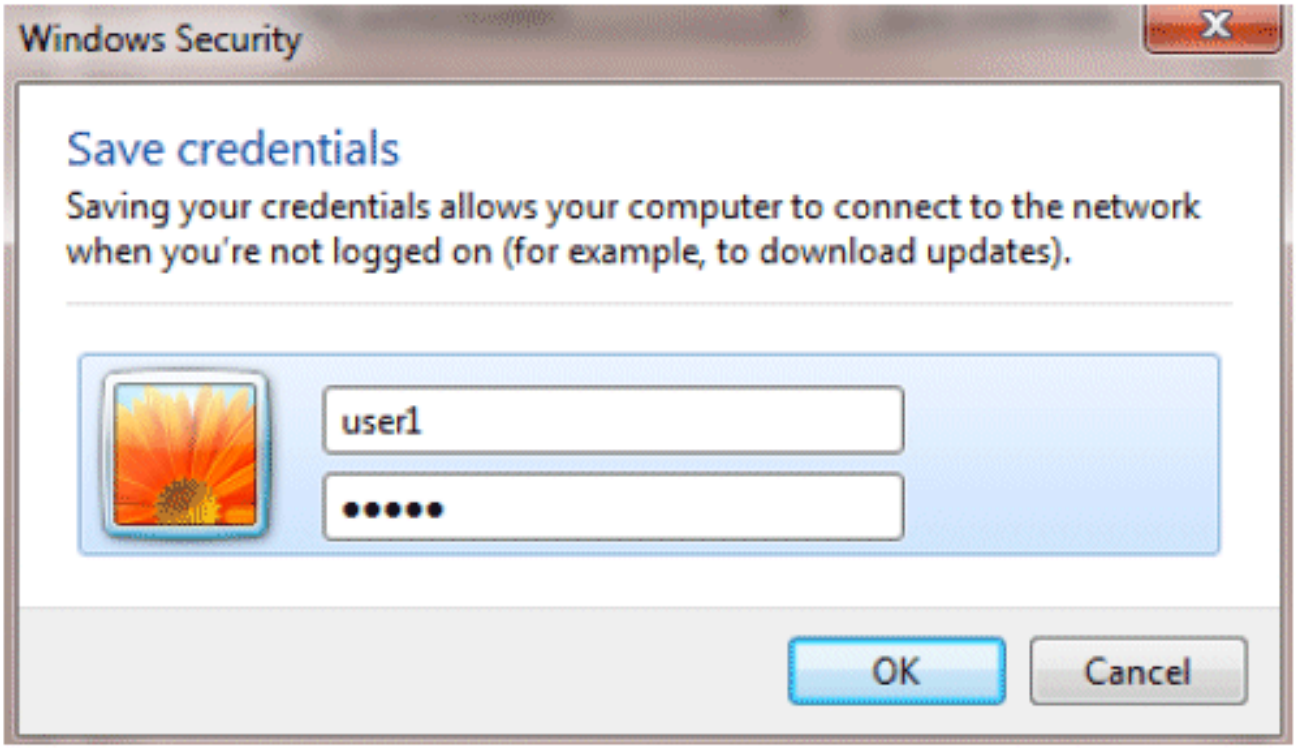


OK.

10. Klik op **Geavanceerde instellingen** om Gebruikersnaam en wachtwoord te configureren.


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



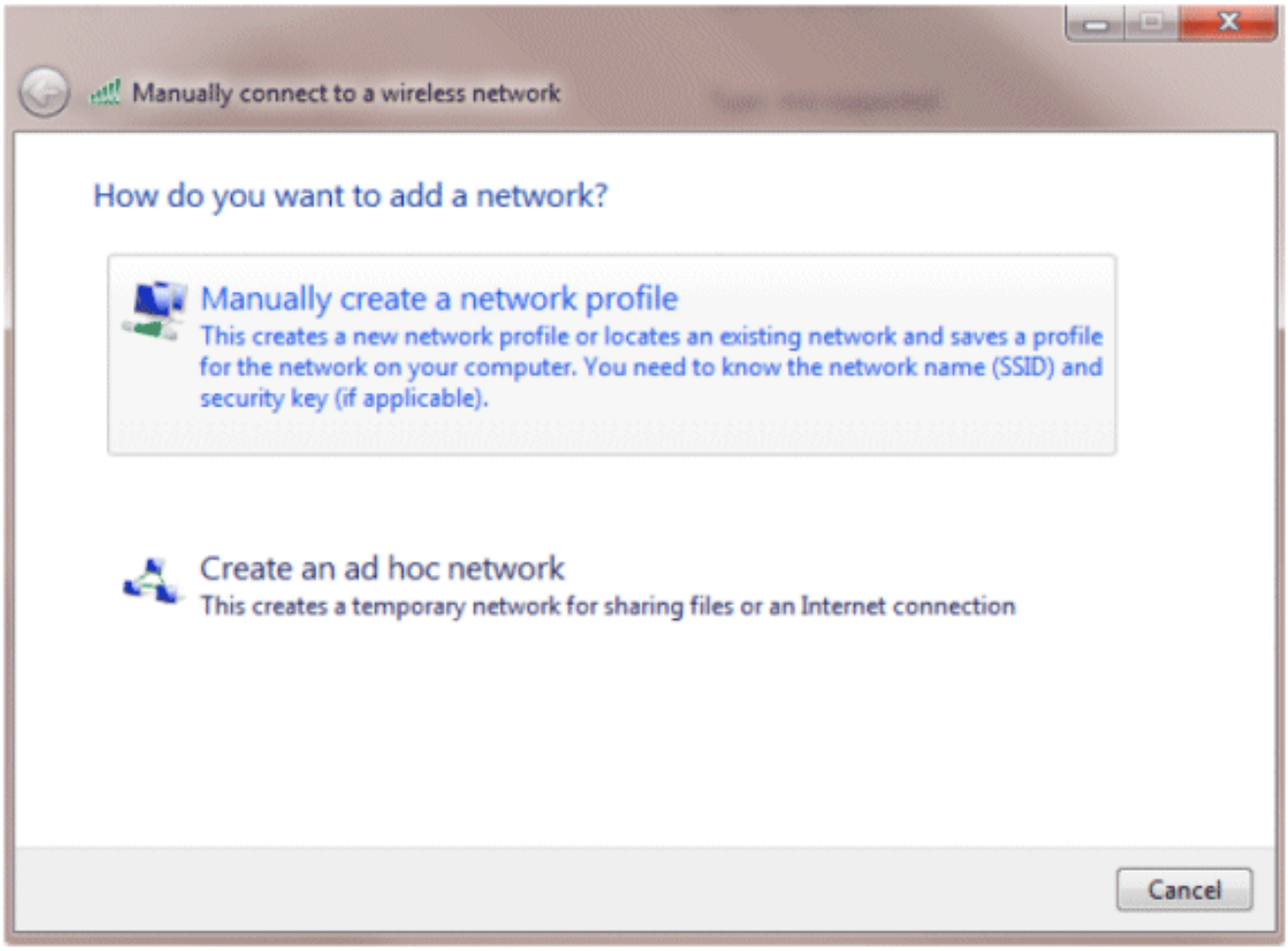
Uw clientprogramma is nu klaar voor verbinding.

EAP-FAST (gebruiker2)

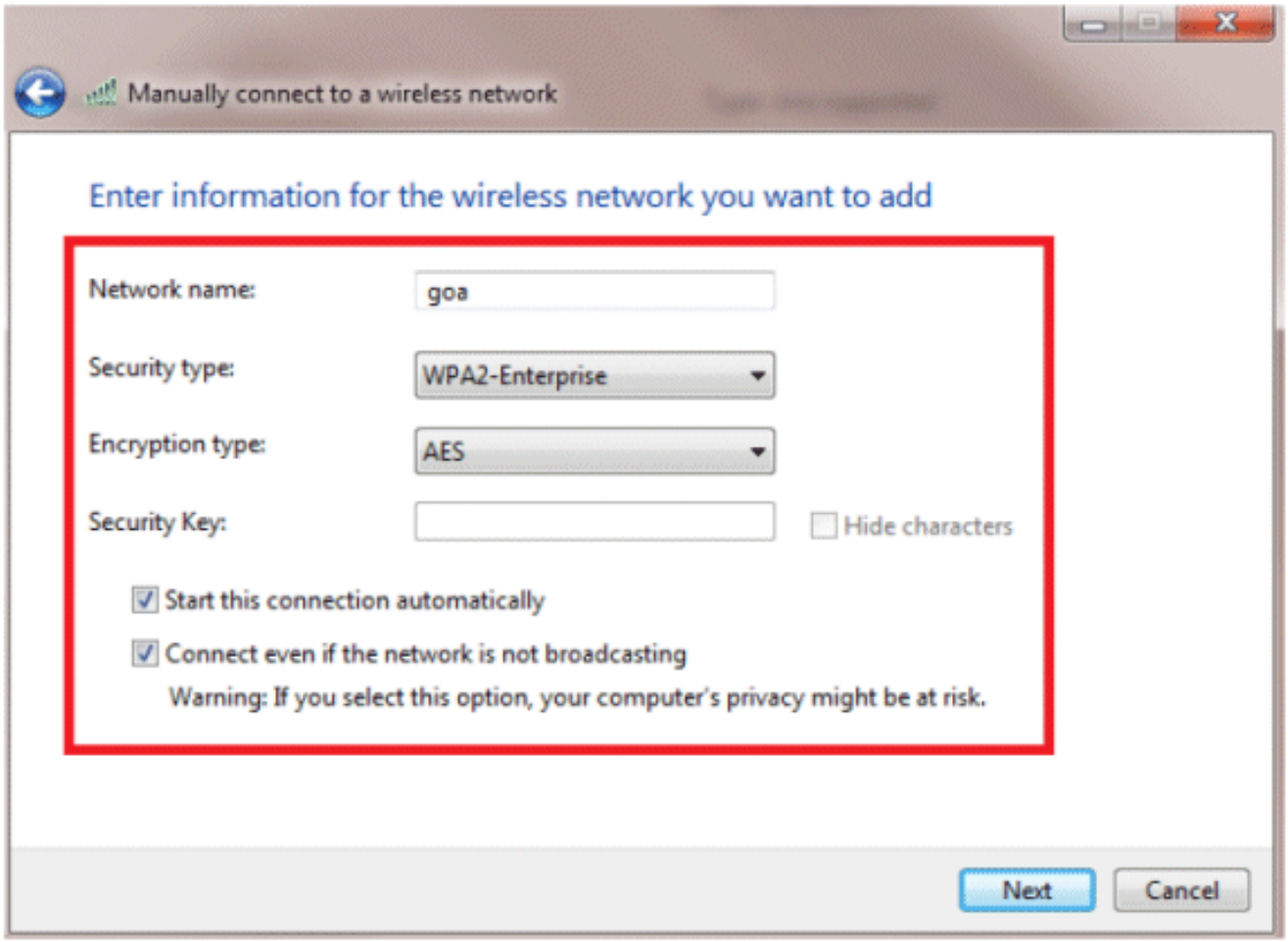
In onze testclient gebruiken we Windows 7 Native Supplicant met een Intel 6300-N kaart waarop 14.3 driver-versie draait. Het is aan te raden om te testen met de nieuwste drivers van leveranciers.

Voltooi de volgende stappen om een profiel in WZC te maken:

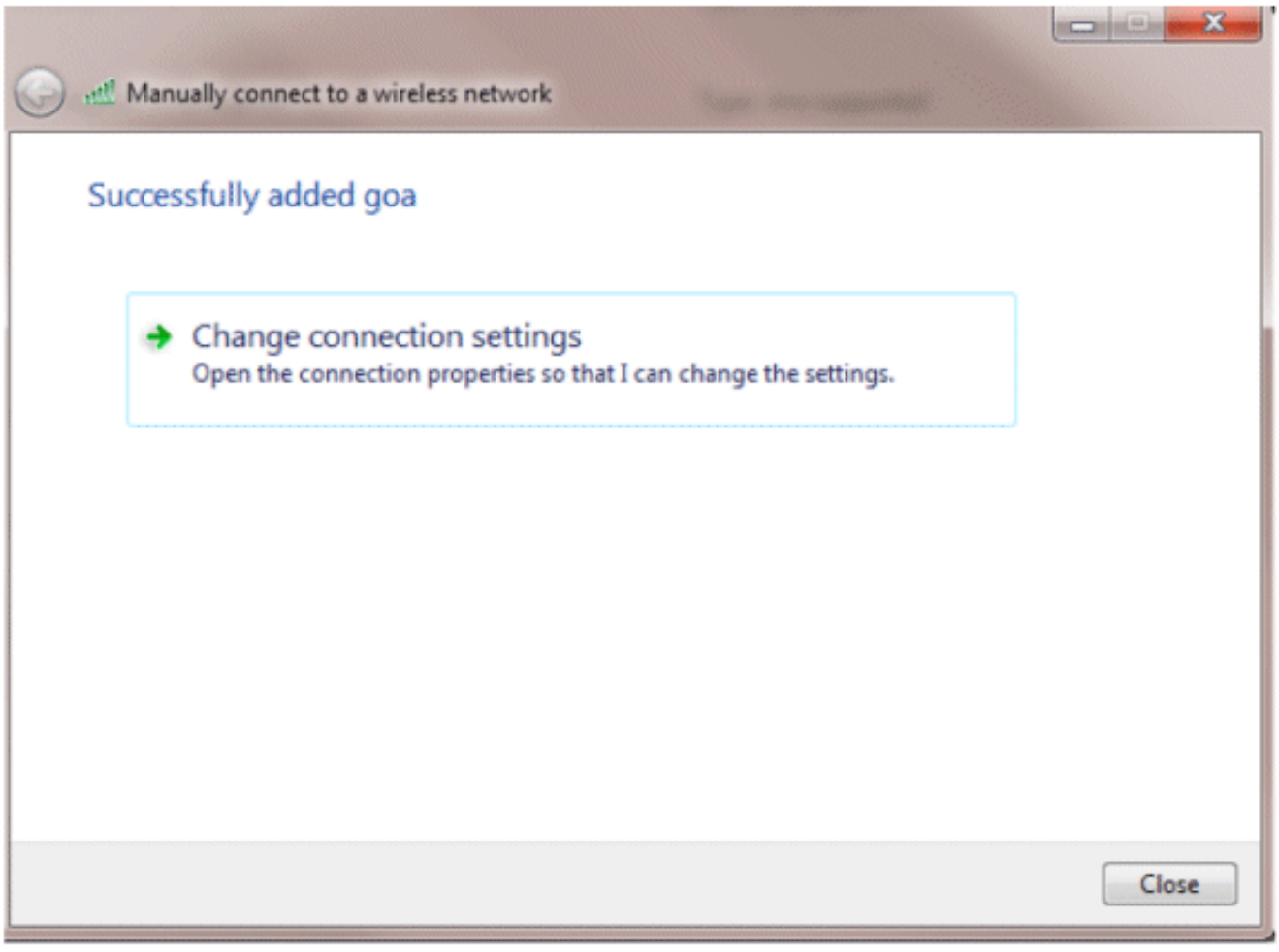
1. Ga naar **Configuratiescherm > Netwerk en internet > Draadloze netwerken beheren**.
2. Klik op het tabblad **Toevoegen**.
3. Klik op **Handmatig een netwerkprofiel maken**.



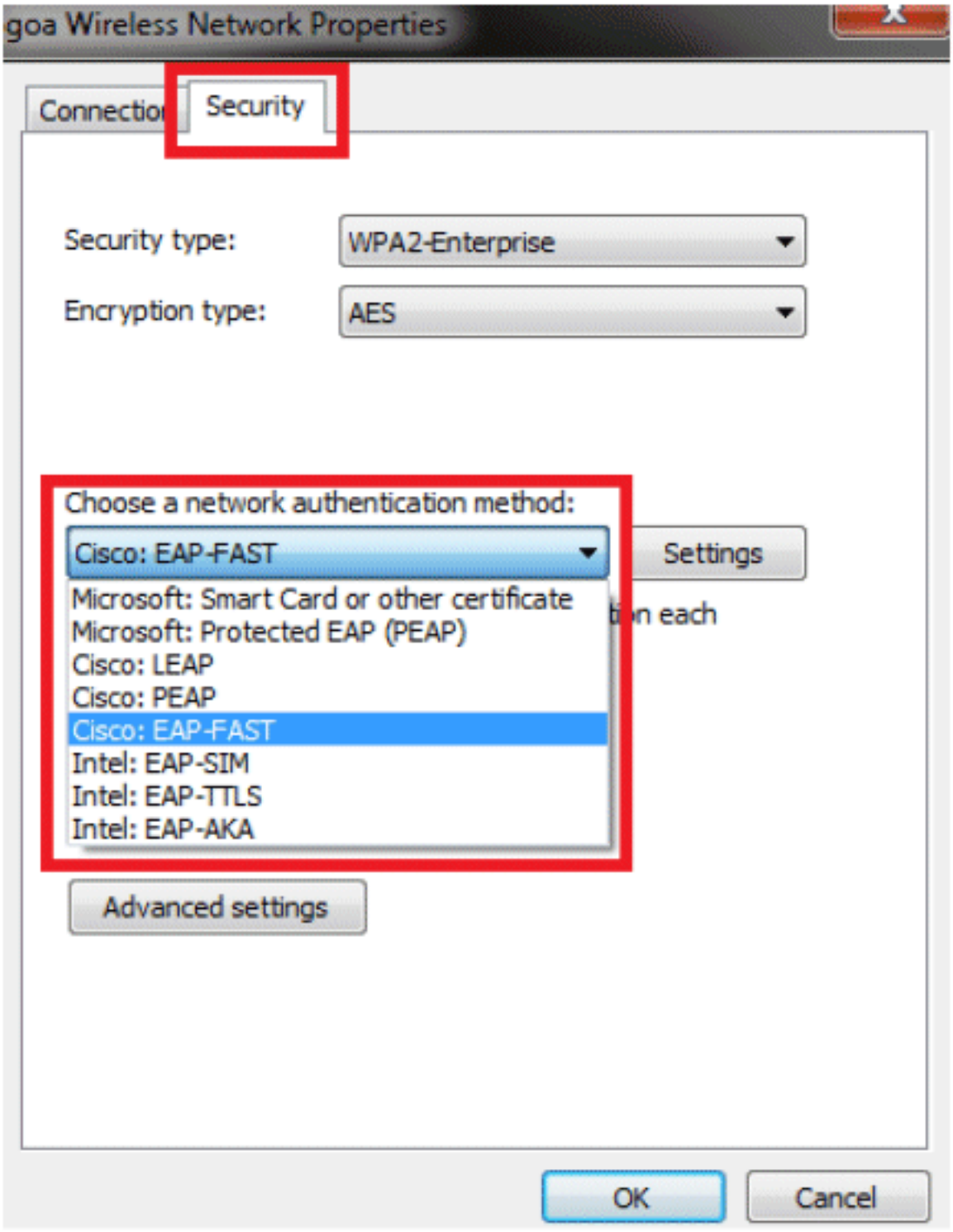
4. Voeg de details toe zoals die op WLC worden gevormd.**Opmerking:** de SSID is hoofdlettergevoelig.
5. Klik op **Next**
   (Volgende).

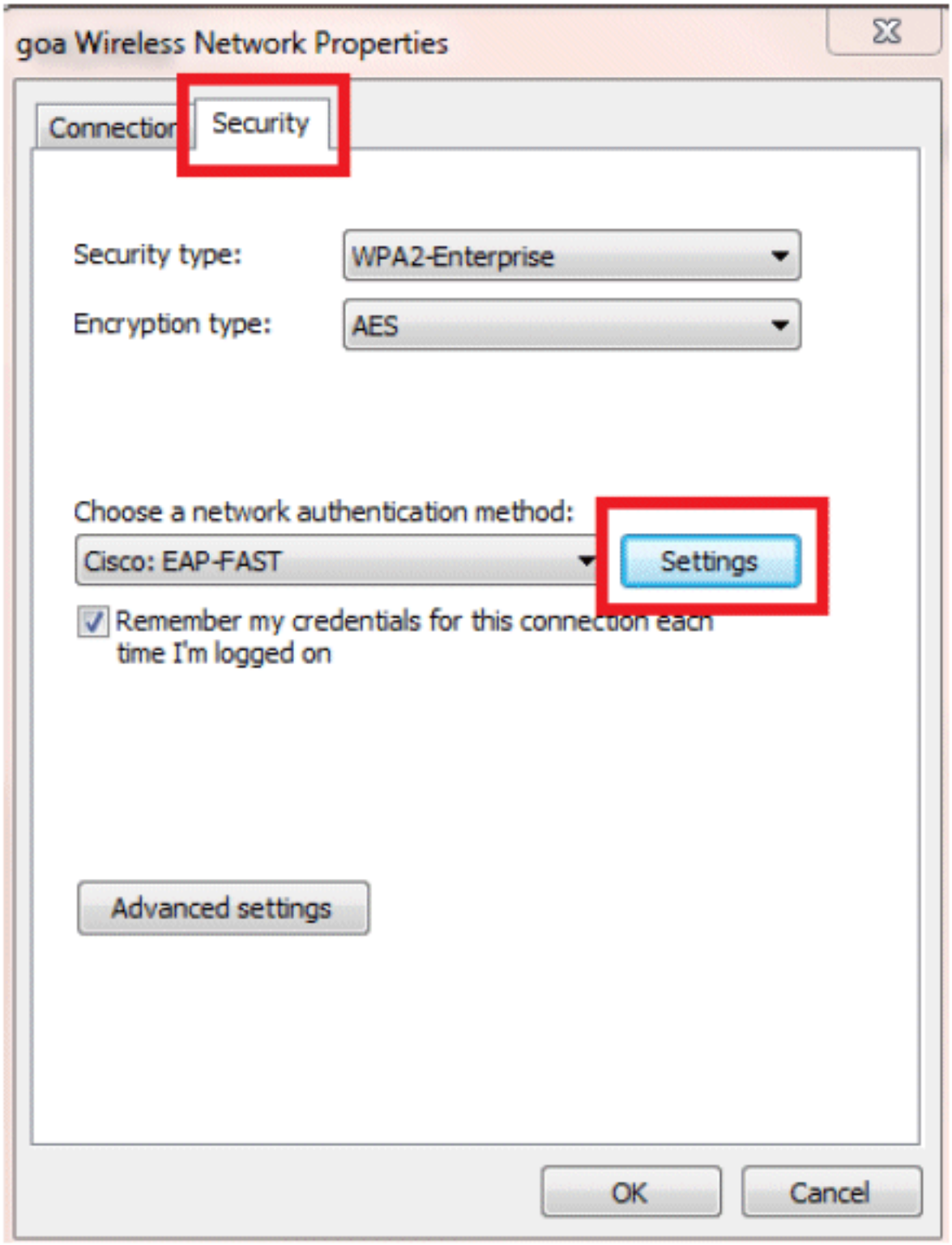


6. Klik op **Verbindingsinstellingen wijzigen** om de instellingen te controleren.

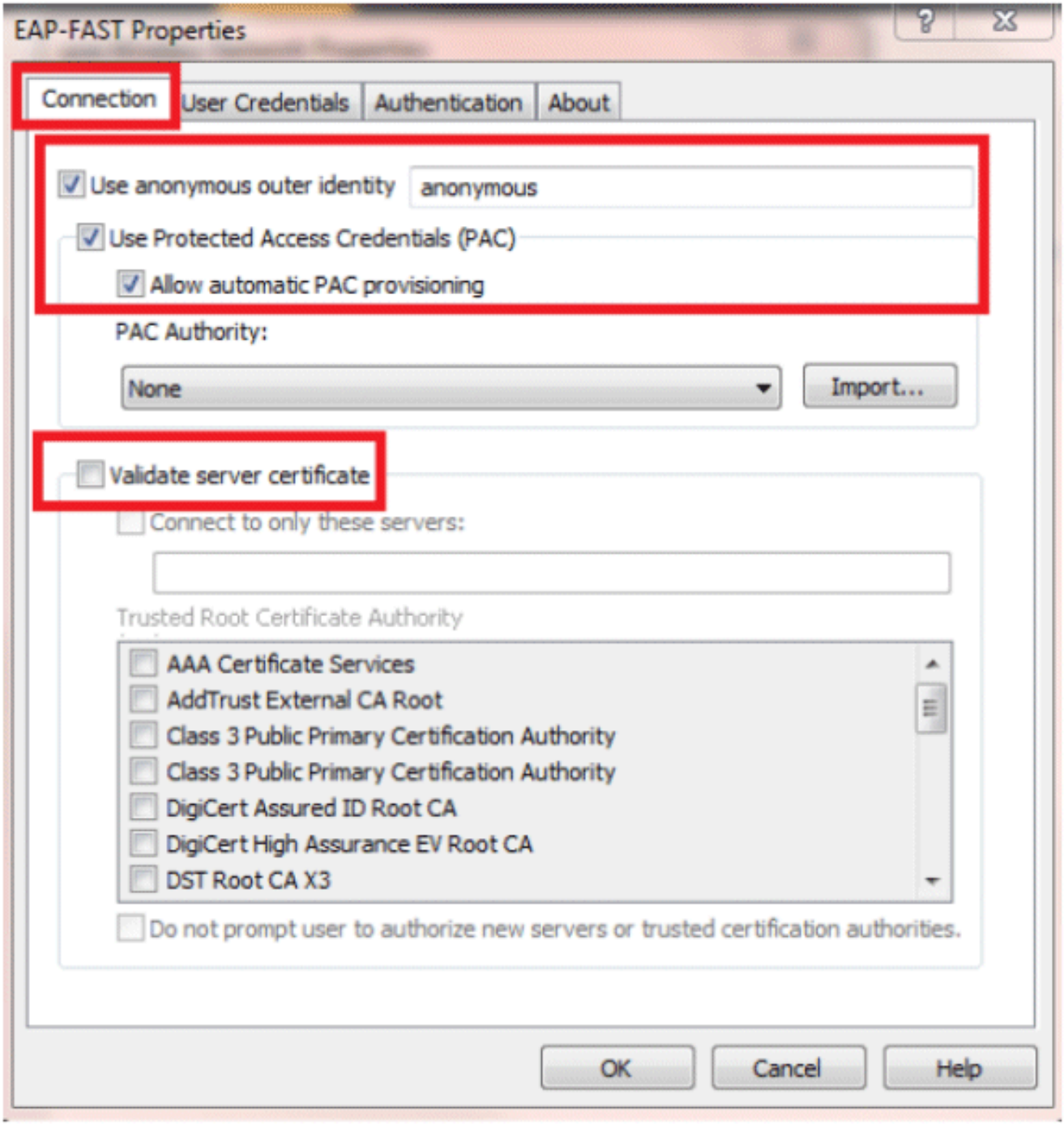


7. Zorg ervoor dat EAP-FAST is ingeschakeld.**Opmerking:** WZC heeft standaard geen EAP-FAST als verificatiemethode. U moet het hulpprogramma downloaden van een externe leverancier. In dit voorbeeld, aangezien het een Intel-kaart is, is Intel PROSet op het systeem geïnstalleerd.

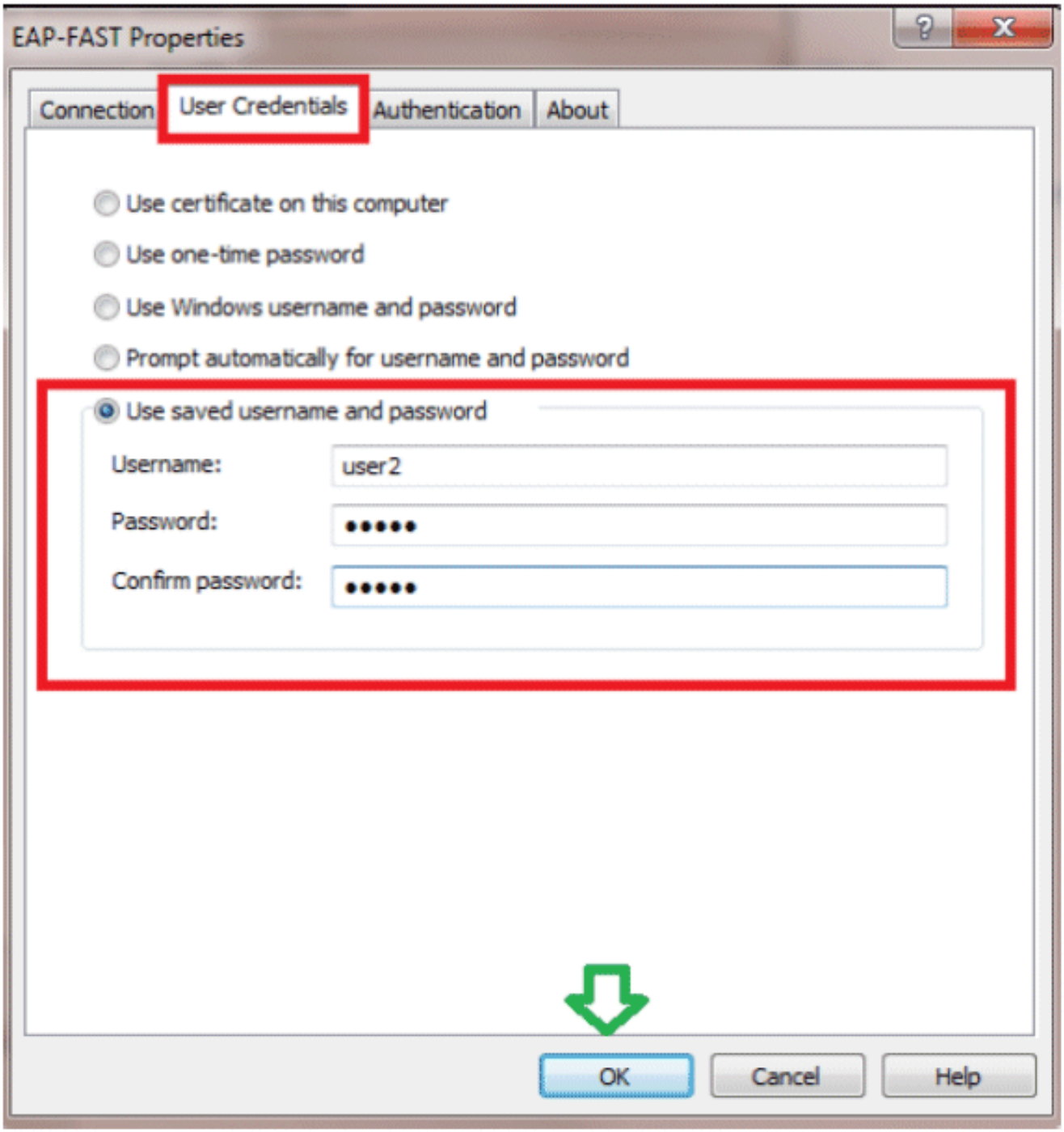




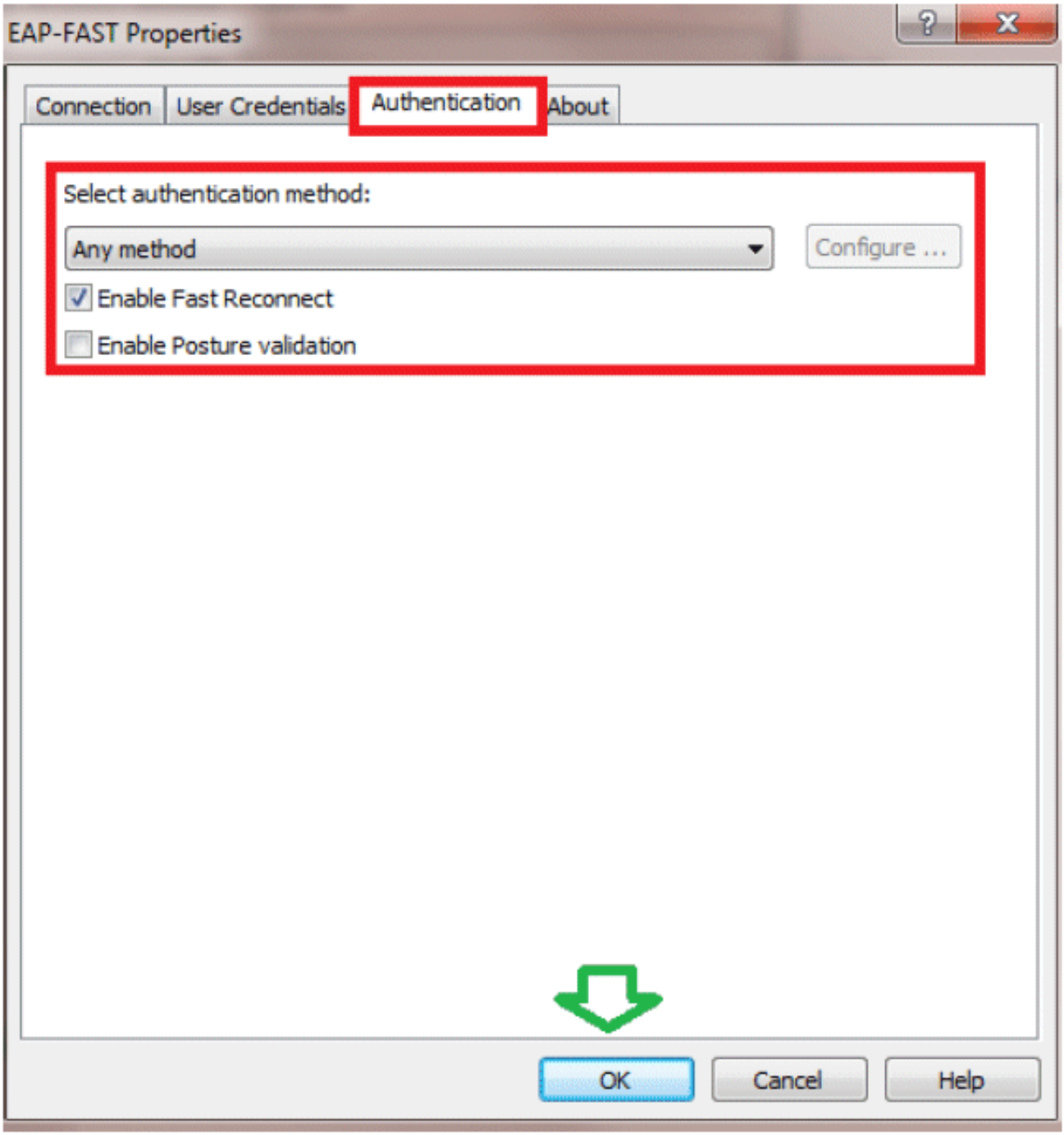
8. Schakel **automatische PAC-levering** in en controleer of **het servercertificaat voor valideren** niet is
ingeschakeld.



9. Klik op het tabblad **Gebruikersreferenties** en voer de referenties van gebruiker2 in. U kunt ook uw Windows-referenties gebruiken om in te loggen. In dit voorbeeld zullen we dat echter niet
gebruiken.

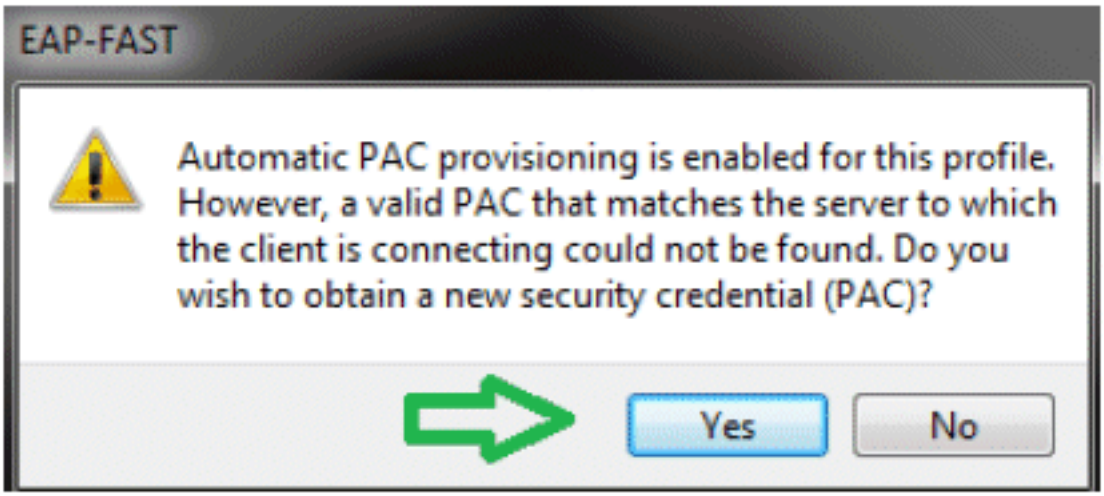

EAP-FAST Properties
Connection
User Credentials
Authentication
About
Use certificate on this computer
Use one-time password
Use Windows username and password
Prompt automatically for username and password
Use saved username and password
Username:
user2
Password:
Confirm password:
OK
Cancel
Help

10. Klik op **OK**.



Uw clientprogramma is nu klaar om verbinding te maken voor gebruiker2.

Opmerking: Wanneer gebruiker2 probeert te verifiëren, zal de RADIUS-server een PAC verzenden. Accepteer de PAC om de verificatie te voltooien.



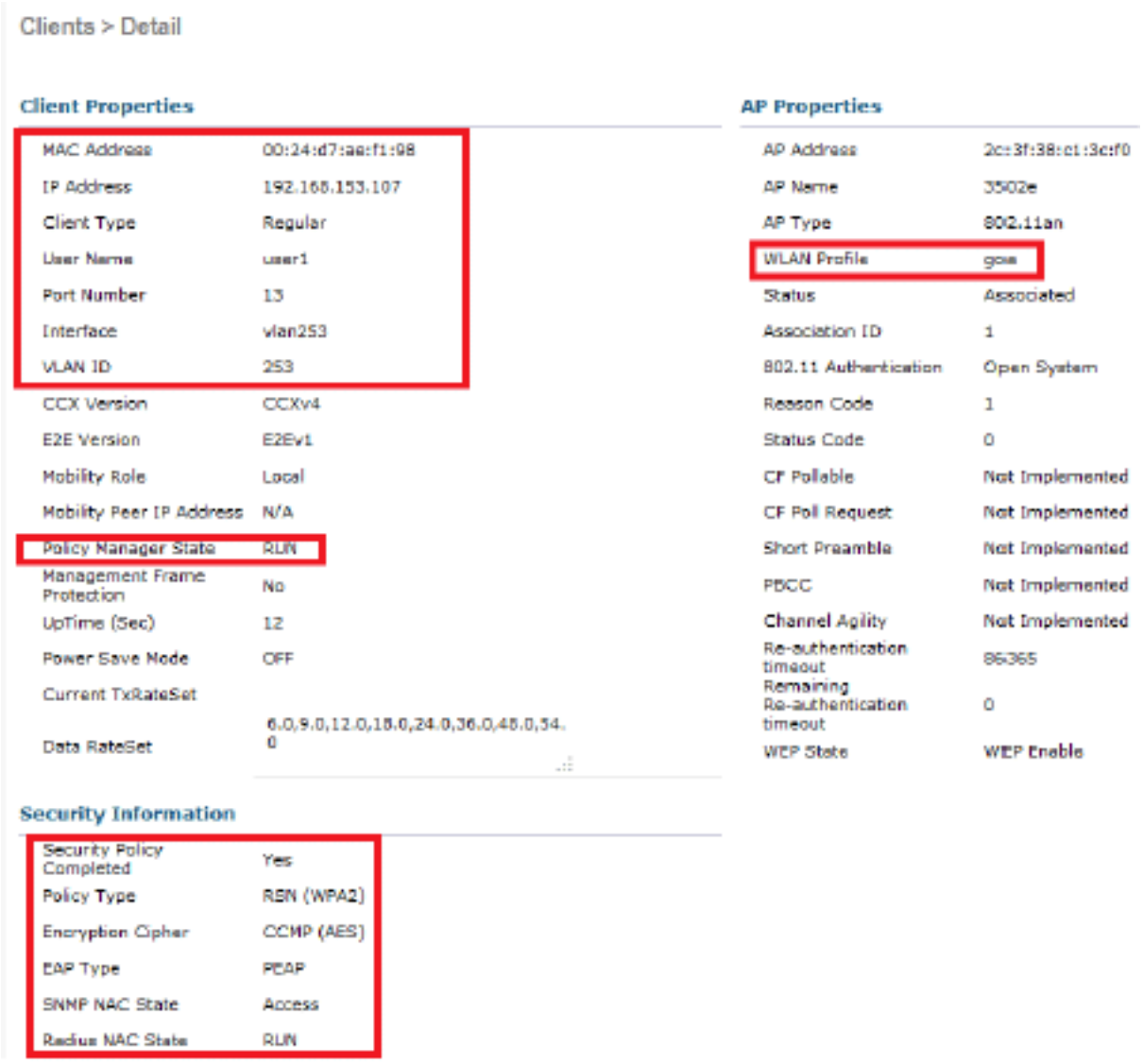
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De Output Interpreter Tool (OIT) (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show**. Gebruik de OIT om een analyse te bekijken van de output van de opdracht **show**.

Controleer gebruiker1 (PEAP-MSCHAPv2)

Ga vanuit de WLC GUI naar **Monitor** > **Clients** en selecteer het MAC-adres.

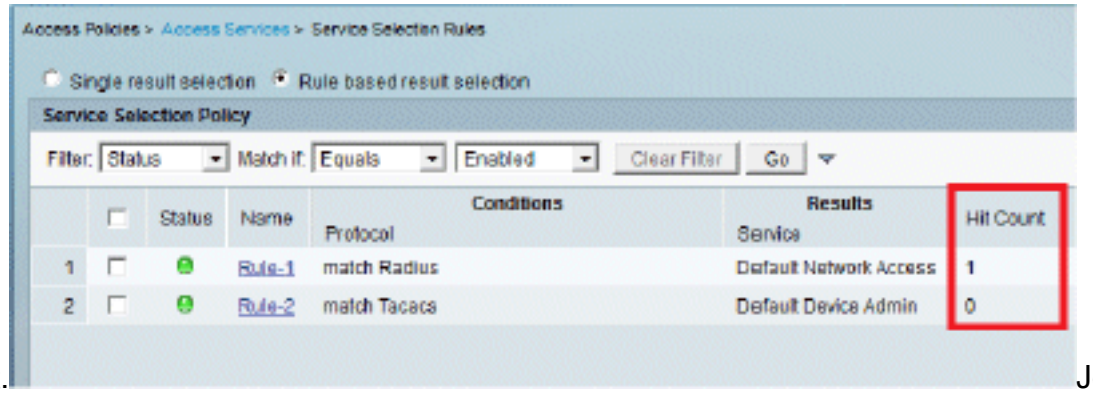


WLC RADIUS-status:

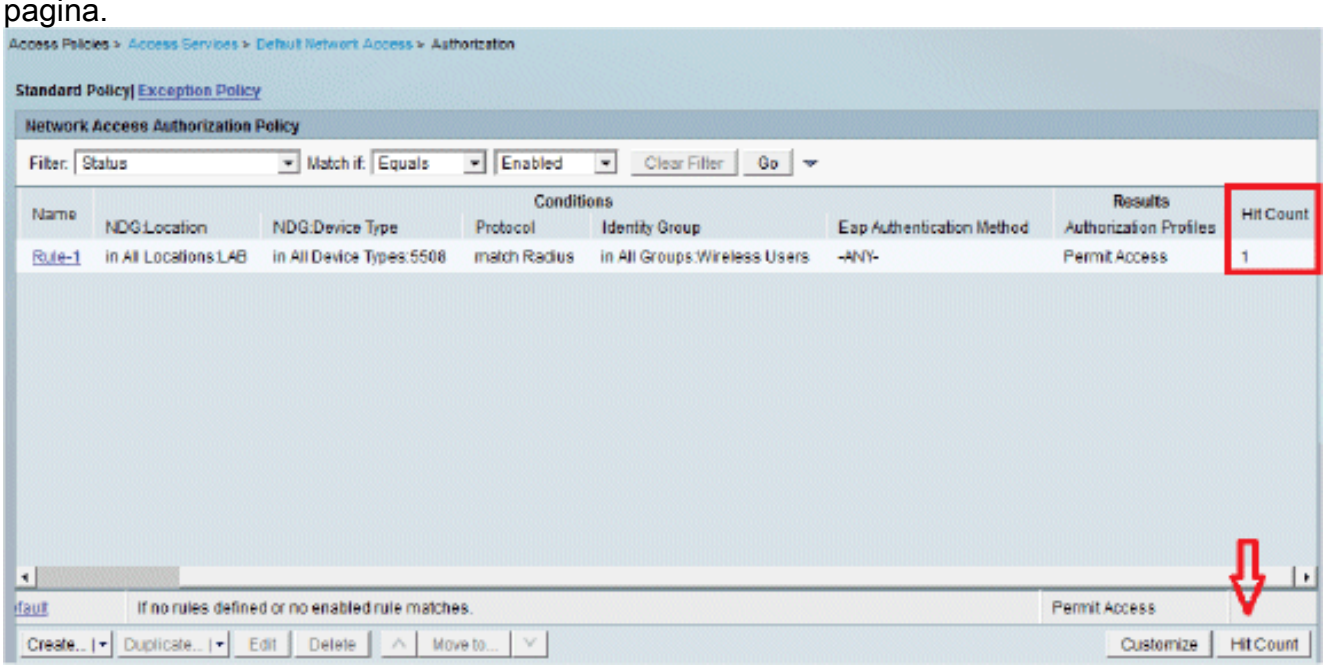
```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

ACS-logbestanden:

1. Voltooi de volgende stappen om de Hit-tellingen te bekijken:Als u de logbestanden binnen 15 minuten na verificatie controleert, zorg er dan voor dat u de Hit-telling



ververst. Je hebt een tab voor **Hit Count** onderaan dezelfde pagina.



2. Klik op **Bewaking en rapporten** en er verschijnt een nieuw pop-upvenster. Ga naar **Verificaties - Radius -Vandaag**. U kunt ook op **Details** klikken om te verifiëren welke serviceselectieregel is toegepast.

Controleer gebruiker2 (EAP-FAST)

Ga vanuit de WLC GUI naar **Monitor > Clients** en selecteer het MAC-adres.

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

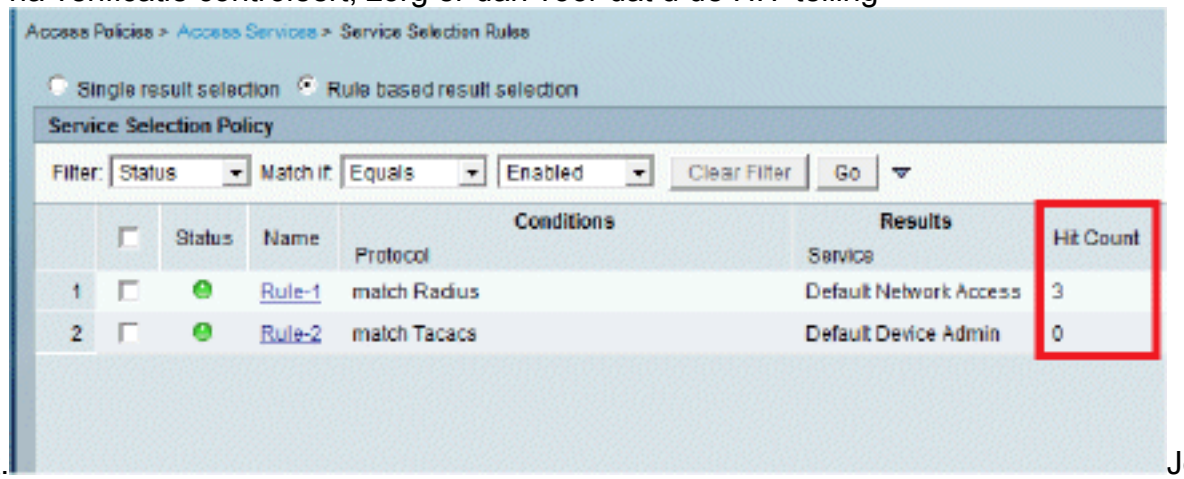
AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

ACS-logbestanden:

1. Voltooi de volgende stappen om de Hit-tellingen te bekijken:Als u de logbestanden binnen 15 minuten na verificatie controleert, zorg er dan voor dat u de HIT-telling ververst. 
Access Policies > Access Services > Service Selection Rules

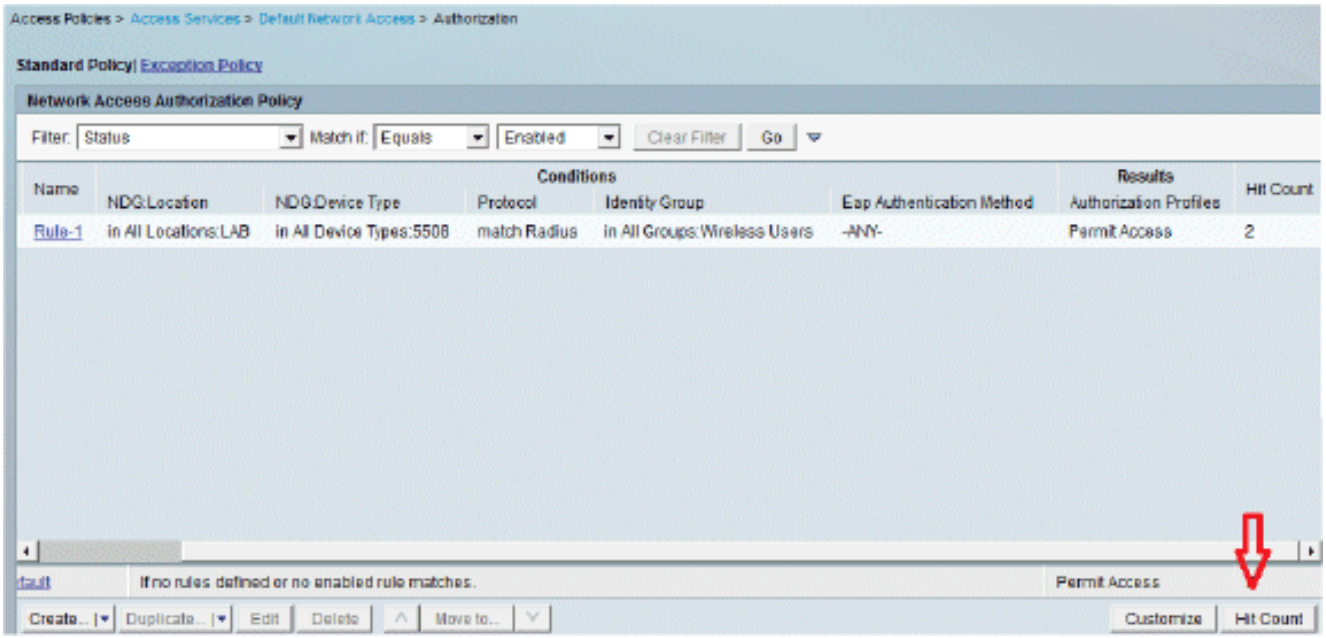
Single result selection Rule based result selection

Service Selection Policy

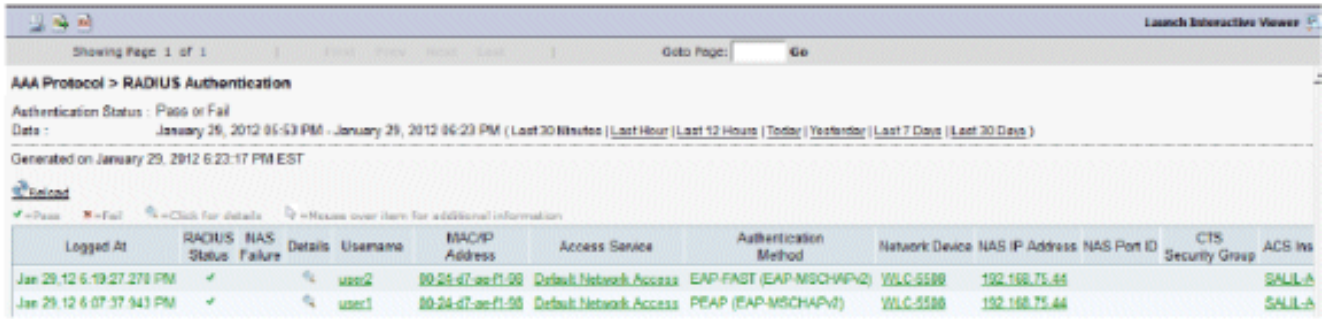
Filter: Status Match if: Equals Enabled Clear Filter Go

		Status	Name	Conditions: Protocol	Results: Service	Hit Count
1			Rule-1	match Radius	Default Network Access	3
2			Rule-2	match Tacacs	Default Device Admin	0

Je hebt een tab voor **Hit Count** onderaan dezelfde pagina.



2. Klik op **Bewaking en rapporten** en er verschijnt een nieuw pop-upvenster. Ga naar **Verificaties - Radius -Vandaag**. U kunt ook op **Details** klikken om te verifiëren welke serviceselectieregel is
toegepast.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

De Output Interpreter Tool (OIT) (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show**. Gebruik de OIT om een analyse te bekijken van de output van de opdracht **show**.

N.B.: Raadpleeg Belangrijke informatie over debug-opdrachten voordat u **debug-**opdrachten gebruikt.

1. Als u problemen ondervindt, geeft u deze opdrachten op de WLC uit:**debug client** *<mac add of the client>***debug aaa all enable****toon cliëntdetail** *<mac addr>* - Controleer de staat van de beleidsmanager.**toon radius auth statistieken** - Verifieer de mislukkingsreden.**debug deactiveren-all** - debugs uitschakelen.**duidelijke stats radius auth all** - Duidelijke radius statistieken op de WLC.
2. Controleer de logbestanden in de ACS en noteer de reden van de fout.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.