

ACS 5.2 configureren voor poortgebaseerde verificatie met een LAP

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Aannames](#)

[Configuratiestappen](#)

[LAMP configureren](#)

[Switch configureren](#)

[RADIUS-server configureren](#)

[Netwerkbronnen configureren](#)

[Gebruikers configureren](#)

[Beleidselementen definiëren](#)

[Toegangsbeleid toepassen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u een lichtgewicht access point (LAP) kunt configureren als een 802.1x-applicatie om te verifiëren tegen een RADIUS-server zoals een Access Control Server (ACS) 5.2.

[Voorwaarden](#)

[Vereisten](#)

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

- Basiskennis hebben van de draadloze LAN-controller (WLC) en LAN's.
- Functionele kennis van de AAA-server hebben.
- Zorg voor een grondige kennis van draadloze netwerken en problemen met de 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
- Cisco Secure ACS-software-release 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.

Achtergrondinformatie

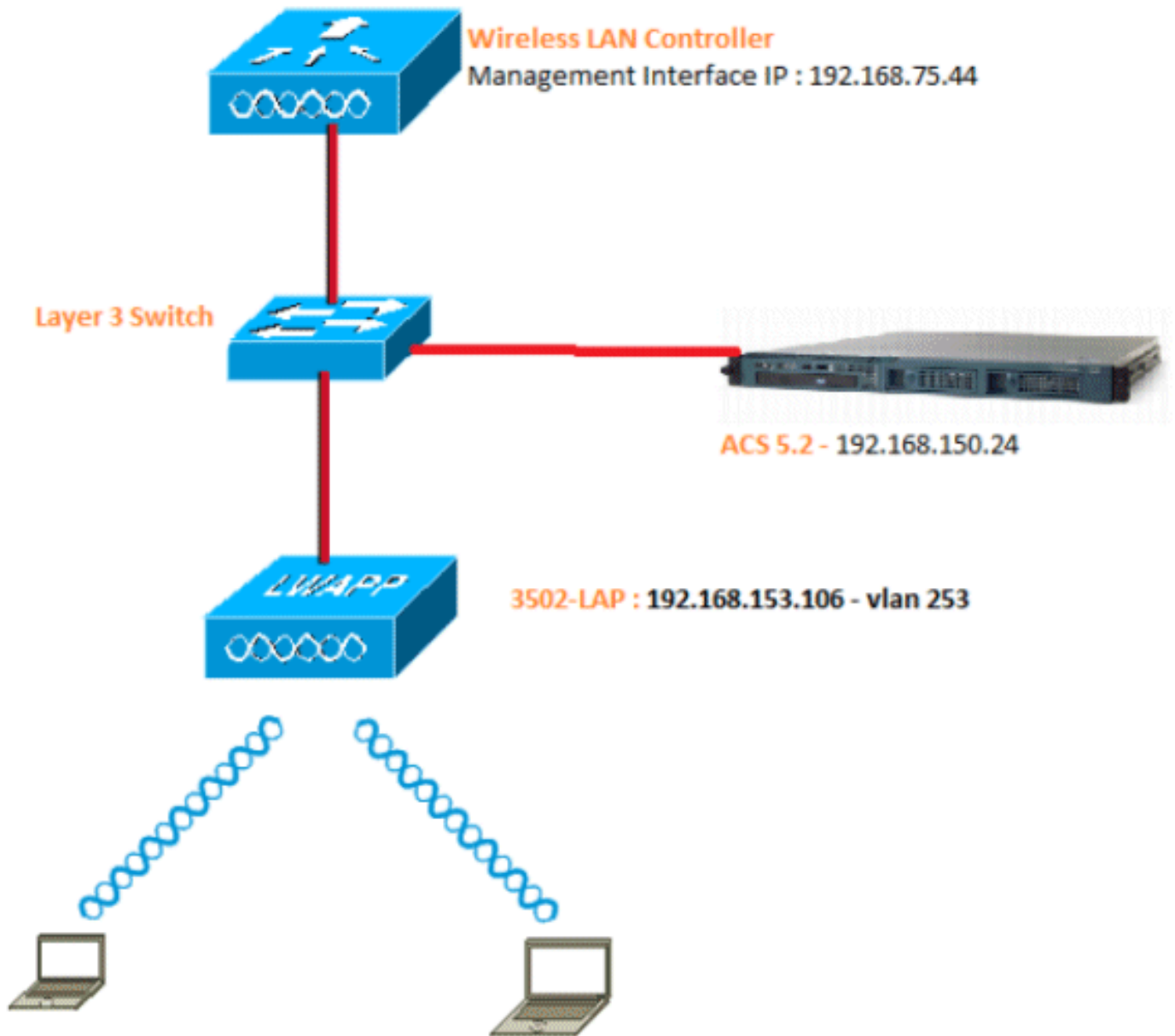
LAP's hebben in de fabriek X.509-certificaten geïnstalleerd - ondertekend door een privésleutel - die op het apparaat worden gebrand op het moment van productie. De LAP's gebruiken dit certificaat om bij het samenvoegen te authenticeren met de WLC. Deze methode beschrijft een andere manier om LAP's te verifiëren. Met WLC-software kunt u de 802.1x-verificatie configureren tussen een Cisco Aironet access point (AP) en een Cisco switch. In dit geval werkt het toegangspunt als de 802.1x-aanvrager en wordt het door de switch geverifieerd op basis van een RADIUS-server (ACS) die EAP-FAST gebruikt met anonieme PAC-levering. Zodra de switch is geconfigureerd voor 802.1x-verificatie, kan alleen 802.1x-verkeer door de poort worden doorgegeven totdat het apparaat dat is aangesloten op de poort, met succes wordt geverifieerd. Een AP kan worden geverifieerd voordat het zich aansluit bij een WLC of nadat het zich heeft aangesloten bij een WLC, in welk geval u 802.1x configureert op de switch nadat de LAP zich aansluit bij de WLC.

Configureren

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

Netwerkdigram

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.
- LAP wordt geplaatst in VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 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 categorieën:

1. [LAMP configureren.](#)
2. [Configureer de switch.](#)
3. [Configureer de RADIUS-server.](#)

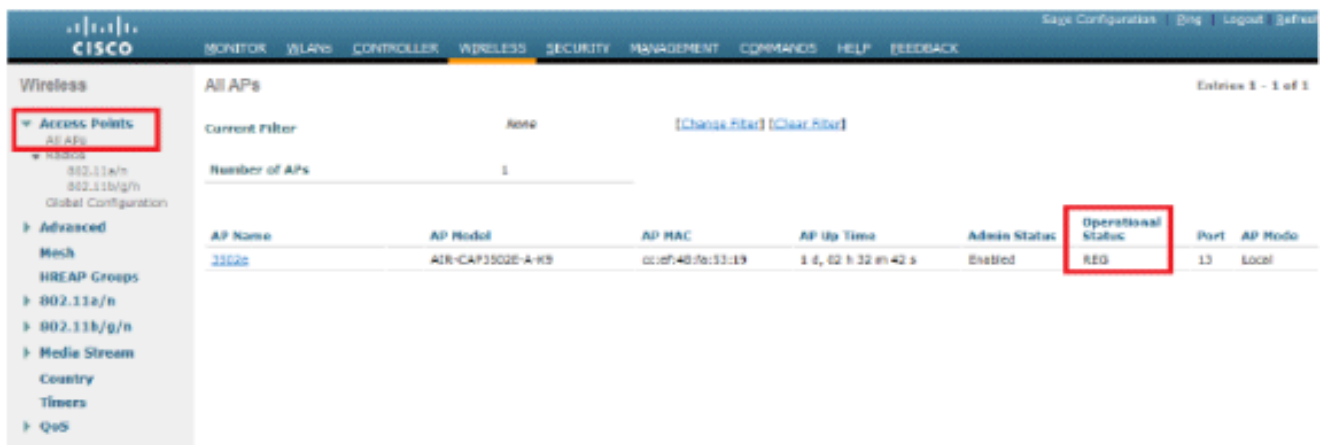
LAMP configureren

Aannames:

LAP is al geregistreerd in de WLC met optie 43, DNS of statisch geconfigureerde WLC-beheerinterface IP.

Voer de volgende stappen uit:

1. Ga naar **Wireless > Access points > Alle AP's** om LAP-registratie op de WLC te verifiëren.



The screenshot shows the Cisco WLC configuration interface. The 'Wireless' menu is expanded to 'Access Points', and the 'All APs' page is displayed. The table below shows the details of the AP '23202'.

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
23202	AIR-CT5502E-A-K9	cc:ef:40:7e:33:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. U kunt de 802.1x-referenties (dat wil zeggen, gebruikersnaam/wachtwoord) voor alle LAP's op twee manieren configureren: **Wereldwijd** Voor een reeds aangesloten bij LAP, kunt u de geloofsbrieven globaal plaatsen zodat elke LAP die zich bij WLC aansluit die geloofsbrieven zal erven.

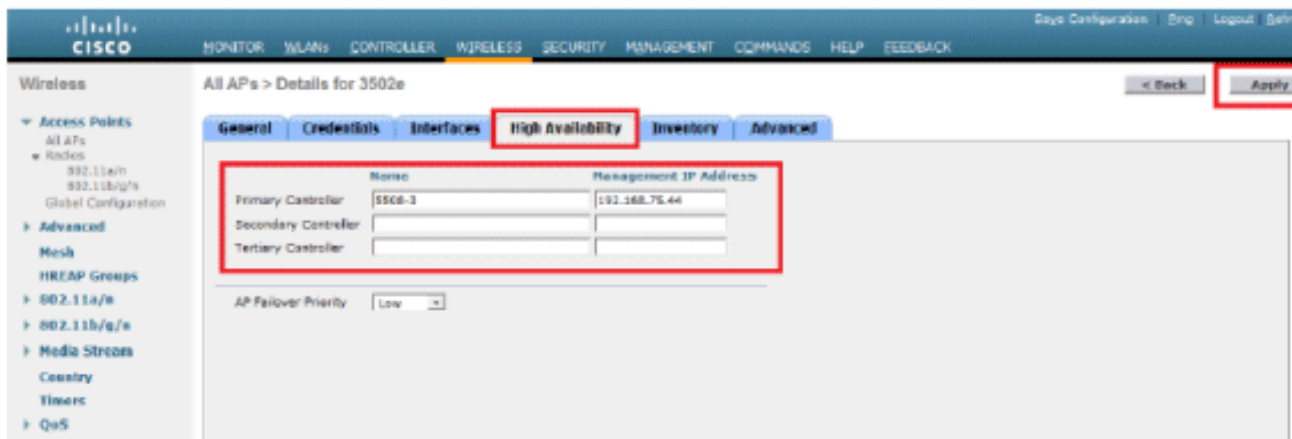
The screenshot shows the Cisco Wireless LAN Controller configuration interface. The 'Global Configuration' page is displayed, with the '802.1x Supplicant Credentials' section highlighted in red. This section includes a checkbox for '802.1x Authentication' (checked), and fields for 'Username', 'Password', and 'Confirm Password'. Other sections visible include CDP (with Ethernet and Radio State tables), High Availability (with heartbeat and backup controller settings), Login Credentials, and AP Image Pre-download (with download buttons).

Individueel Configureer 802.1 x profielen per AP. In ons voorbeeld, zullen wij geloofsbriefen per AP vormen. Ga naar **Draadloos > Alle toegangspunten** en selecteer het betreffende toegangspunt. Voeg de gebruikersnaam en het wachtwoord toe in de velden **802.1x Supplicant Credentials**.

The screenshot shows the 'All APs > Details for 3502e' configuration page. The 'Credentials' tab is selected and highlighted in red. The '802.1x Supplicant Credentials' section is also highlighted in red, showing the 'Over-ride Global credentials' checkbox checked and fields for 'Username', 'Password', and 'Confirm Password' filled with asterisks. Other tabs include General, Interfaces, High Availability, Inventory, and Advanced.

Opmerking: inlogreferenties worden gebruikt om Telnet, SSH of console in te schakelen op het toegangspunt.

- Configureer de sectie Hoge beschikbaarheid en klik op **Toepassen**.



Opmerking: na het opslaan blijven deze referenties behouden over de WLC en de AP-herstart. De referenties veranderen alleen wanneer de LAP zich aansluit bij een nieuwe WLC. De LAP gaat uit van de gebruikersnaam en het wachtwoord die op de nieuwe WLC zijn ingesteld. Als de AP zich nog niet bij een WLC heeft aangesloten, moet u in de LAP console om de referenties in te stellen. Geef deze CLI-opdracht uit in de inschakelmodus: **LAP#lwapp ap dot1x-gebruikersnaam <gebruikersnaam>wachtwoord <wachtwoord>** of **LAP#capwap ap dot1x gebruikersnaam <gebruikersnaam> wachtwoord <wachtwoord>** **Opmerking:** deze opdracht is alleen beschikbaar voor AP's die het herstelbeeld uitvoeren. De standaardgebruikersnaam en het wachtwoord voor de LAP zijn respectievelijk Cisco en Cisco.

Switch configureren

De switch fungeert als een vericator voor de LAP en verifieert de LAP op een RADIUS-server. Als de switch niet over de juiste software beschikt, upgrade dan de switch. In de switch CLI, geef deze opdrachten uit om de 802.1x-verificatie op een switch poort in te schakelen:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

Opmerking: als u andere AP's op dezelfde switch hebt en u wilt niet dat ze 802.1x gebruiken, kunt u de poort niet geconfigureerd laten voor 802.1x of deze opdracht geven:

```
switch(config-if)authentication port-control force-authorized
```

[RADIUS-server configureren](#)

LAP is geverifieerd met EAP-FAST. Zorg ervoor dat de RADIUS-server die u gebruikt deze EAP-methode ondersteunt als u geen Cisco ACS 5.2 gebruikt.

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 beleidsgebaseerde ACS. Met andere woorden, ACS 5.x gebruikt een op regel gebaseerd beleidsmodel in plaats van het op groep gebaseerde model dat in de 4.x-versies wordt gebruikt.

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.
- **Toestemmingen** - VLAN's of Cisco IOS[®]-prioriteitsniveaus.

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 de voorwaarden waaronder de gebruiker toegang tot het netwerk krijgt te beperken en ook het toegestane autorisatieniveau te beperken wanneer aan bepaalde voorwaarden wordt voldaan.

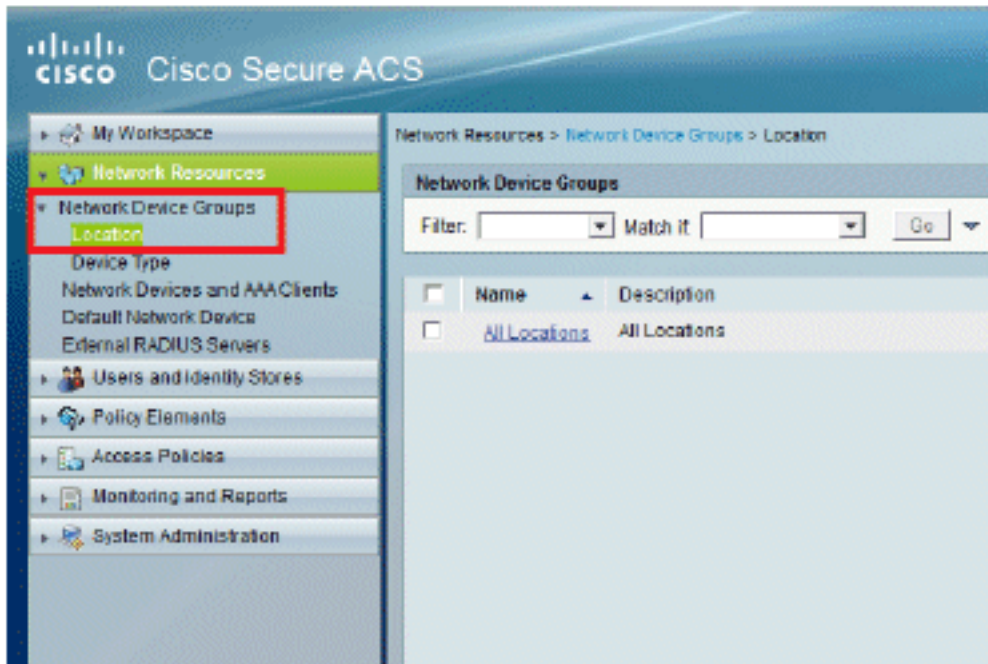
[Netwerkbronnen configureren](#)

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

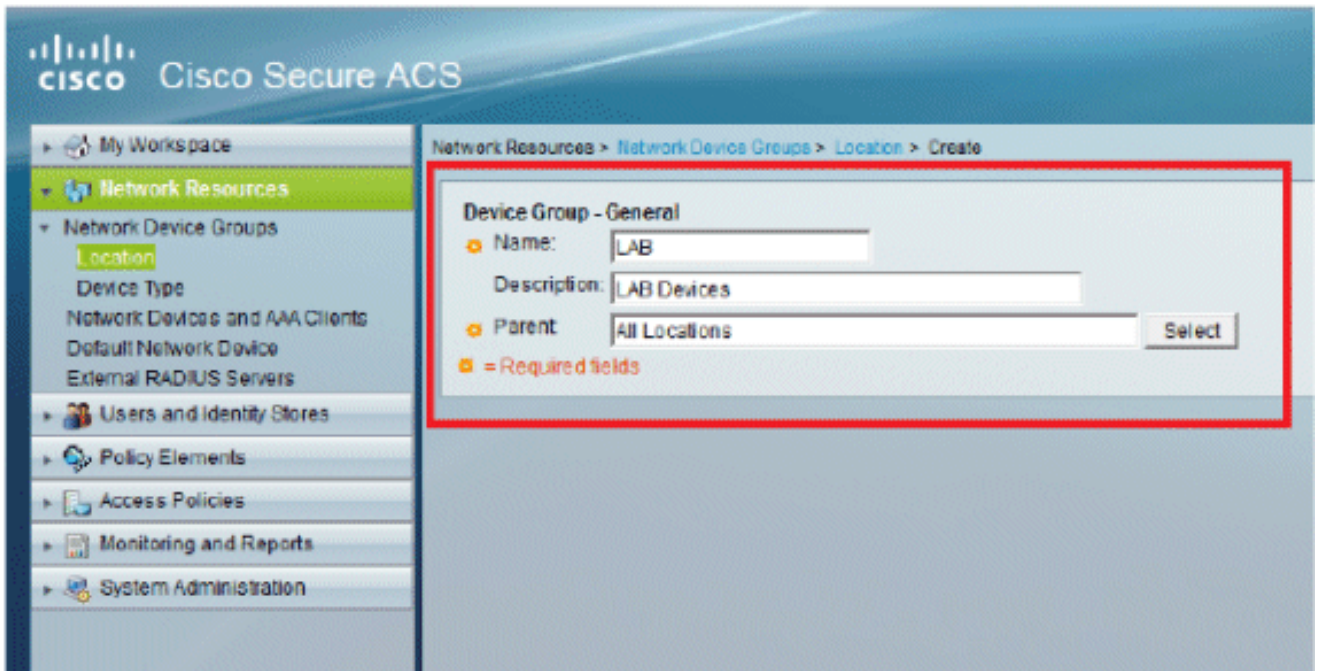
Deze procedure legt uit hoe u de switch als AAA-client aan de RADIUS-server kunt toevoegen, zodat de switch de gebruikersreferenties van de LAP aan de RADIUS-server kan doorgeven.

Voer de volgende stappen uit:

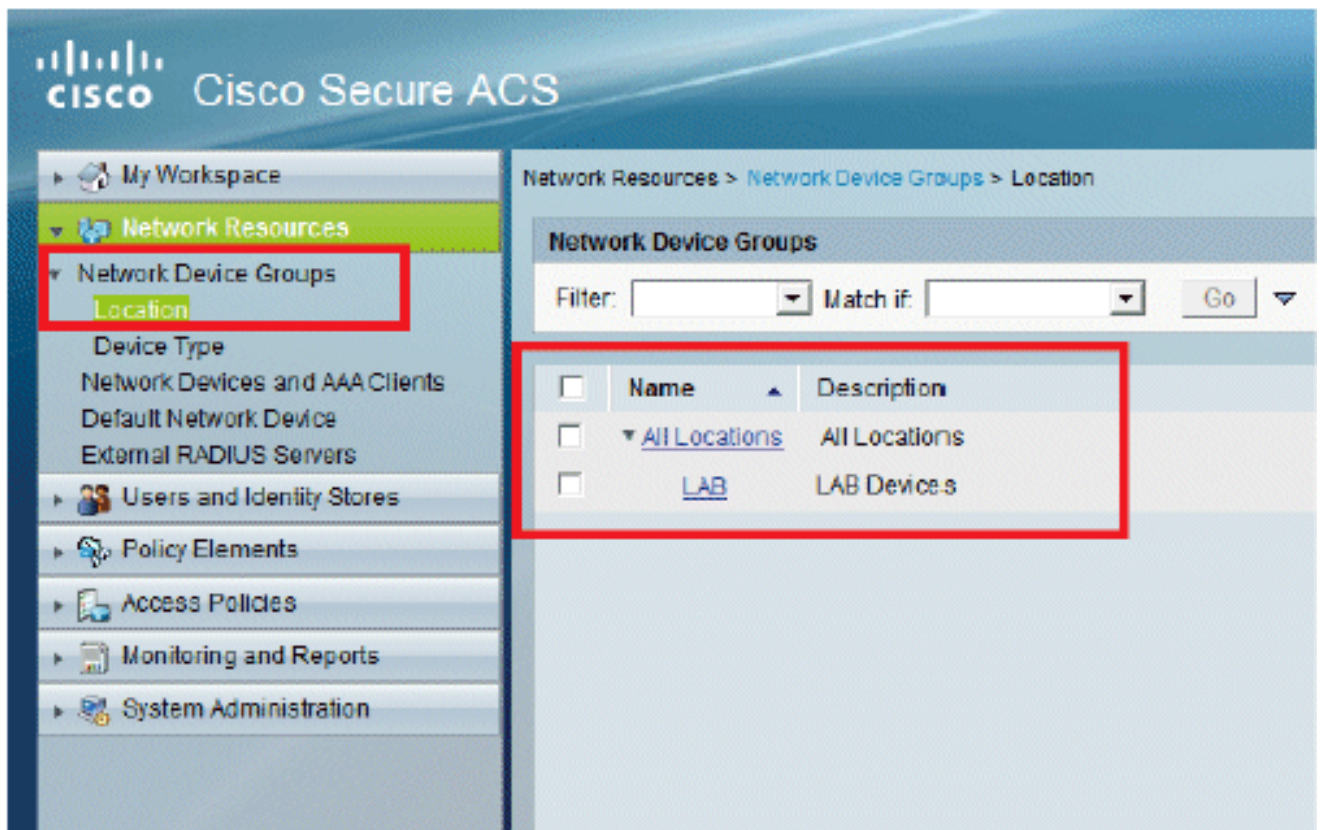
1. Klik vanuit de ACS GUI op **Netwerkbronnen**.
2. Klik op **Netwerkapparaatgroepen**.
3. Ga naar **Locatie > Aanmaken** (onderaan



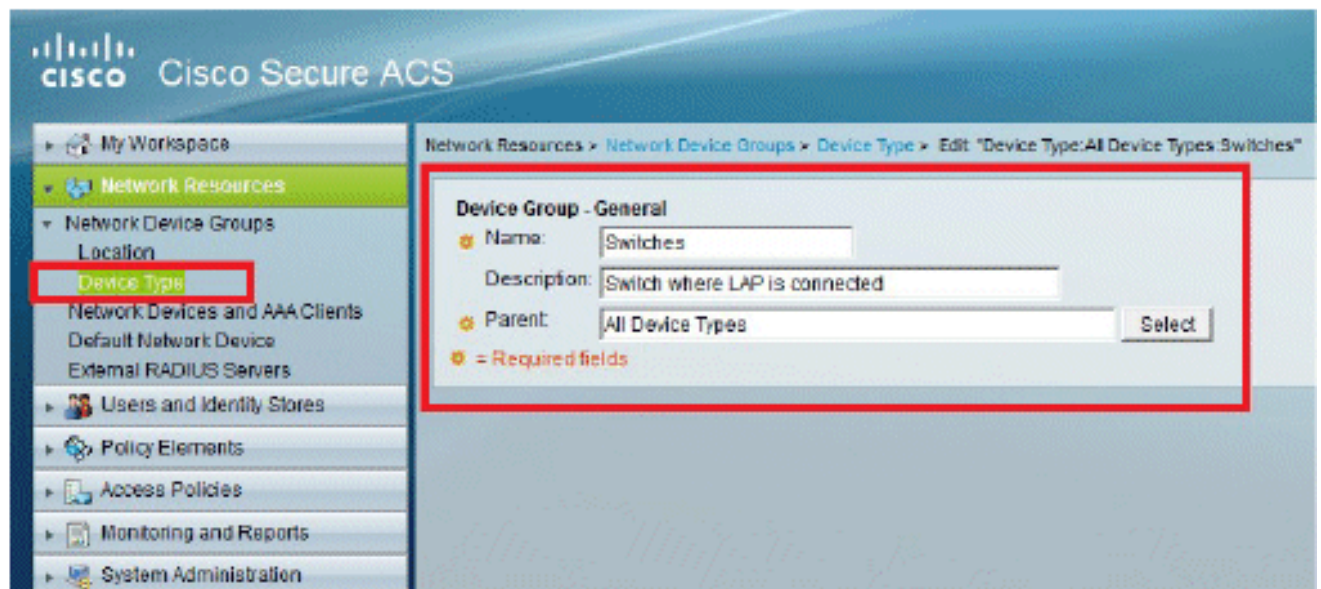
-).
- Voeg de vereiste velden toe en klik op **Indienen**.



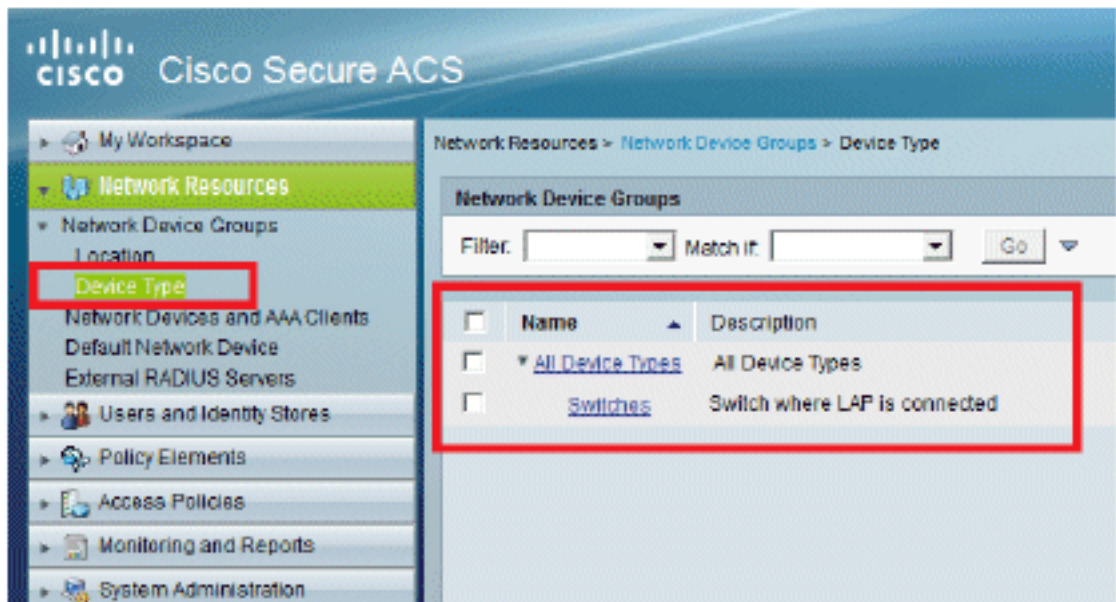
- Het venster vernieuwt:



6. Klik op **Apparaattype** > **Aanmaken**.



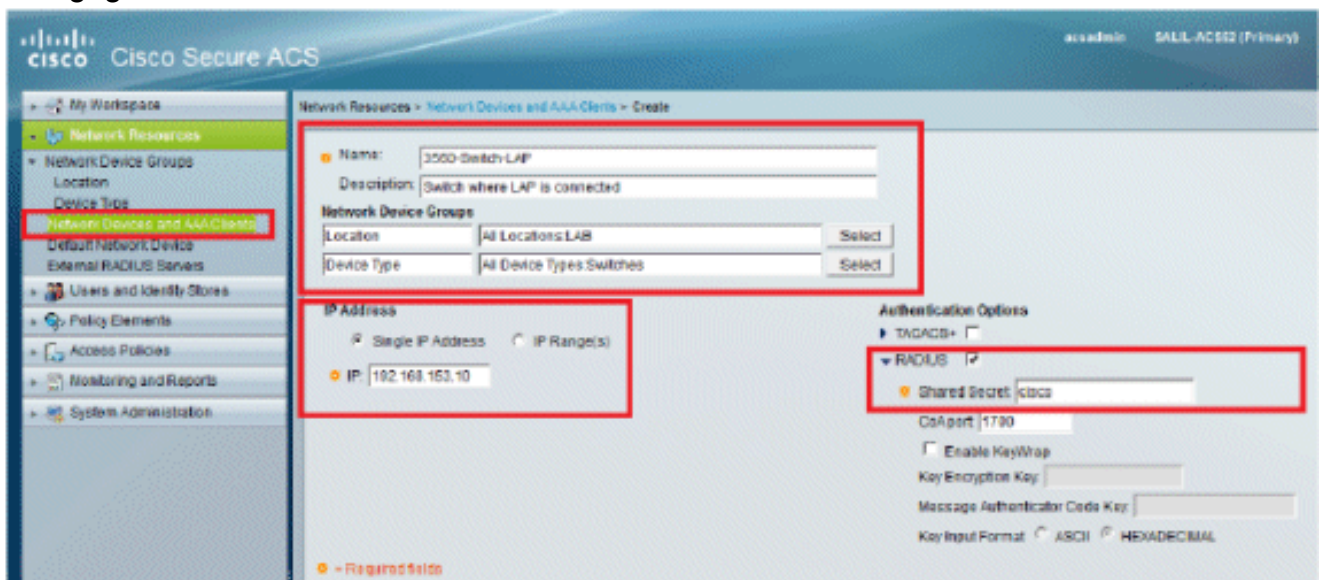
7. Klik op **Verzenden**. Als het venster is voltooid, wordt het



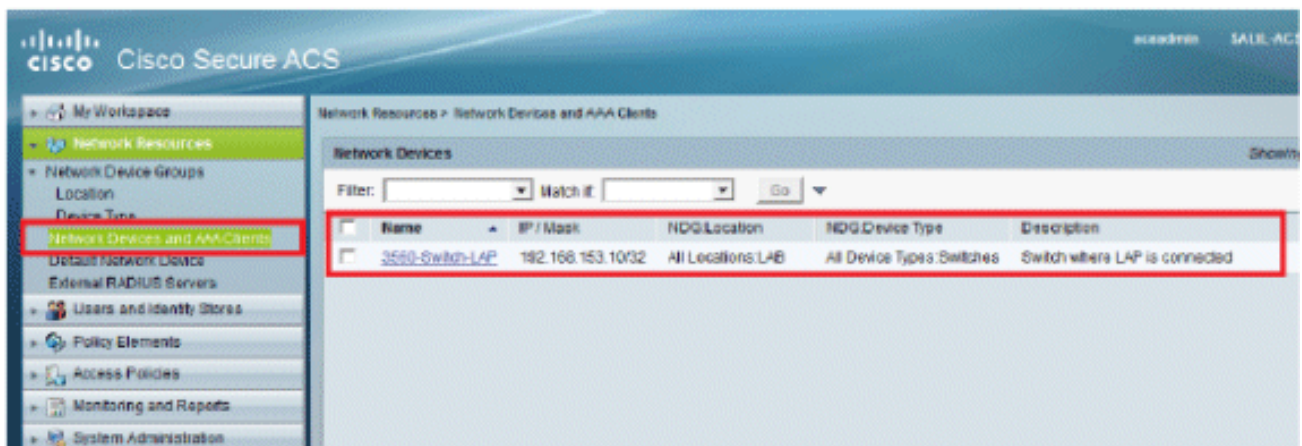
vernieuwd:

8. Ga naar **Network Resources > Network Devices en AAA Clients**.

9. Klik op **Maken** en vul de details in zoals hier wordt weergegeven:



10. Klik op **Verzenden**. Het venster vernieuwt:

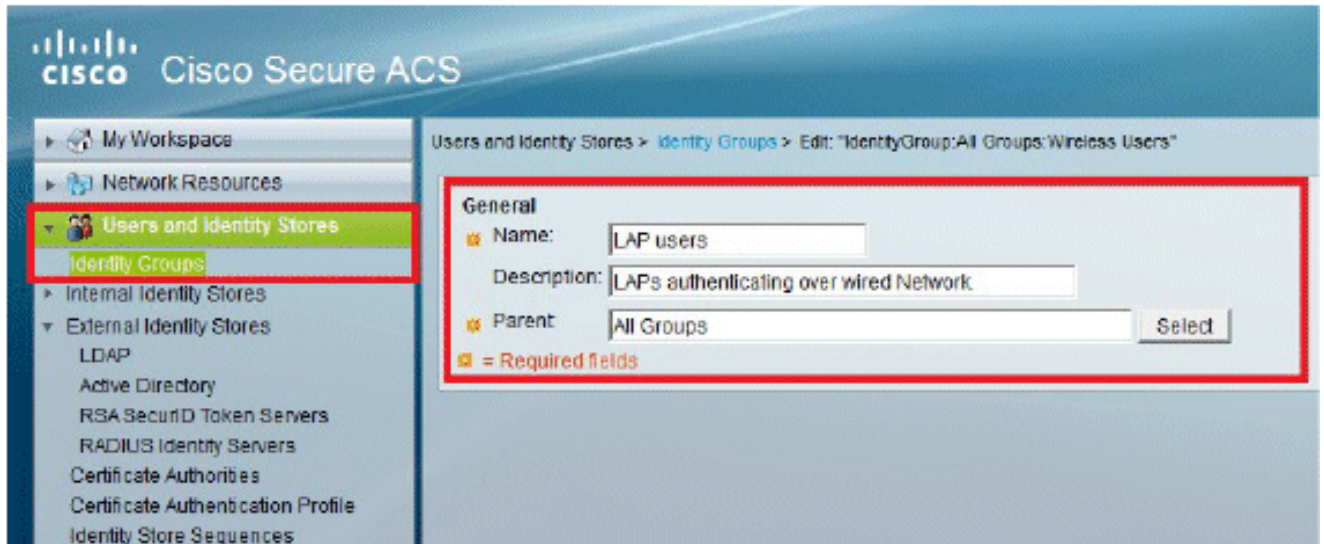


Gebruikers configureren

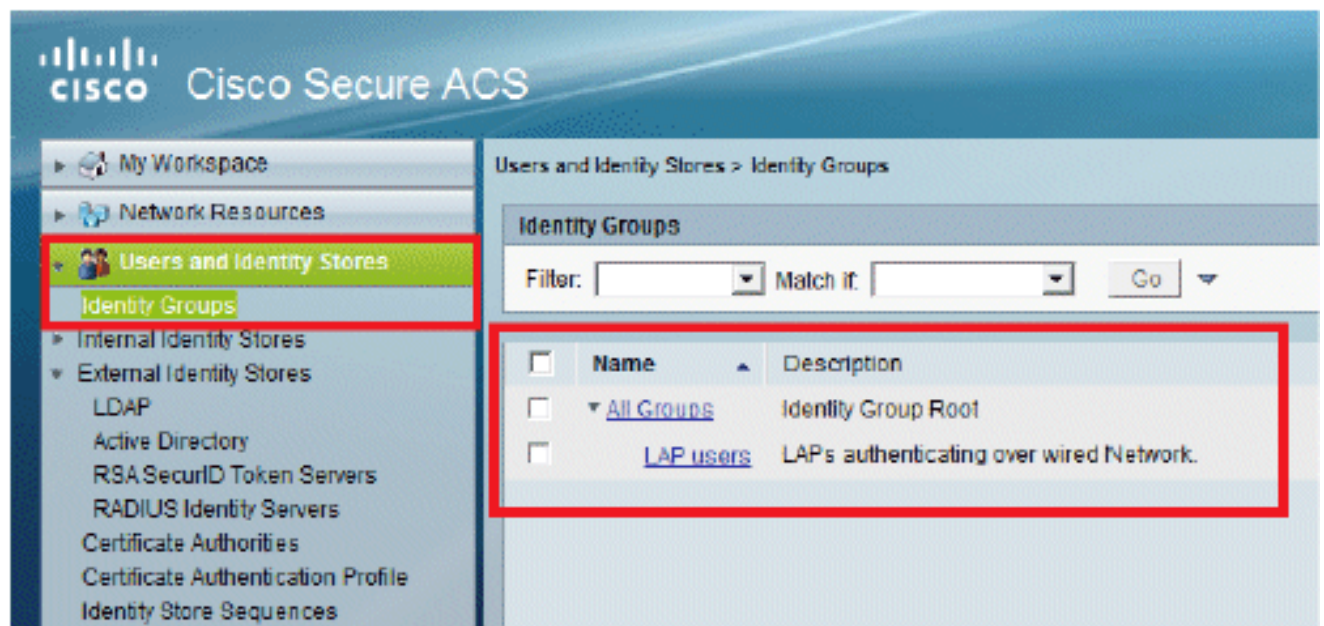
In deze sectie, zult u zien hoe u een gebruiker op eerder gevormde ACS te creëren. U wijst de gebruiker toe aan een groep die "LAP-gebruikers" wordt genoemd.

Voer de volgende stappen uit:

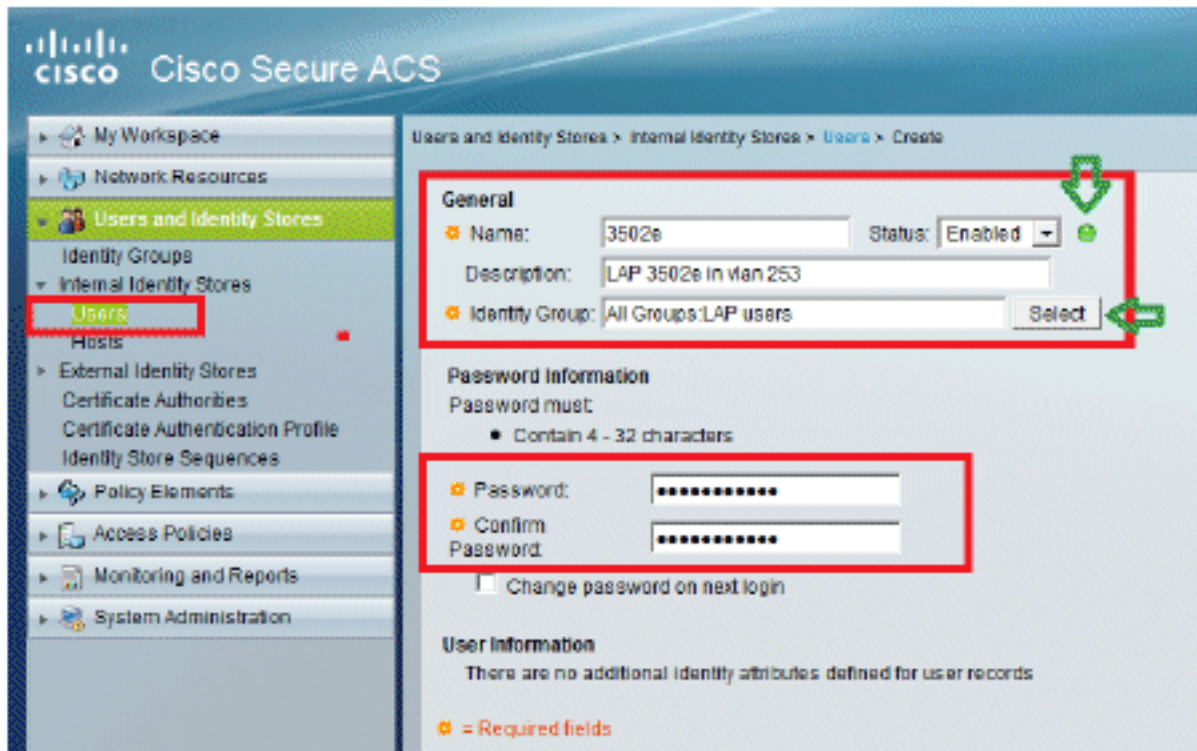
1. Ga naar **Gebruikers en Identiteitswinkels > Identiteitsgroepen > Aanmaken**.



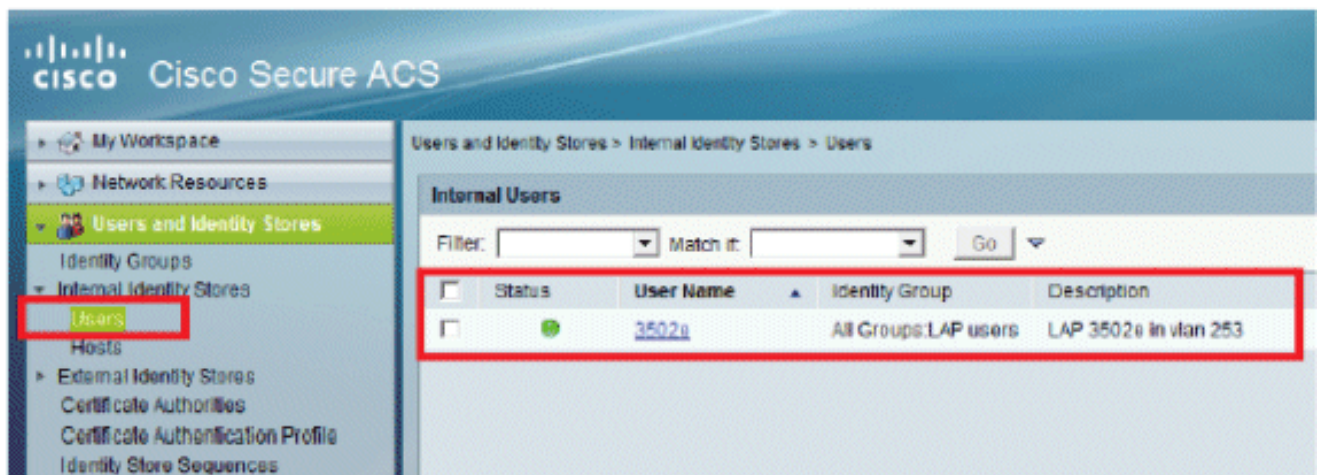
2. Klik op **Verzenden**.



3. Maak **3502e** en wijs het toe aan groep "LAP-gebruikers".
4. Ga naar **Gebruikers en Identiteitswinkels > Identiteitsgroepen > Gebruikers > Aanmaken**.

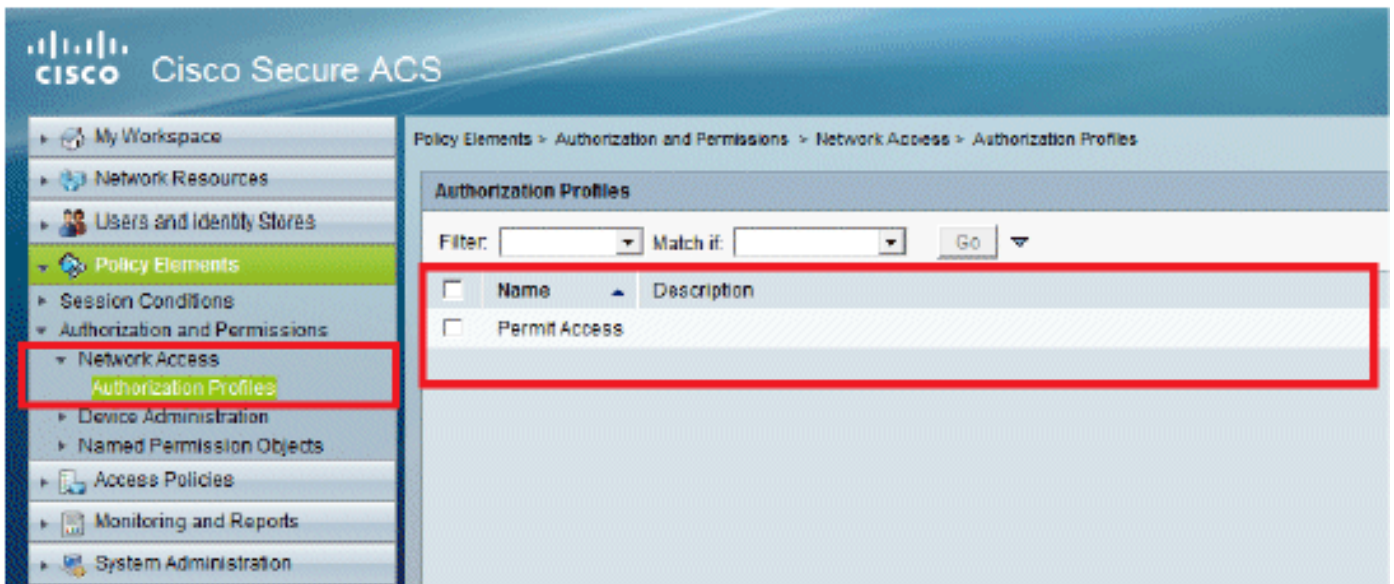


5. U ziet de bijgewerkte informatie:



Beleidselementen definiëren

Controleer of **Permit Access** is ingesteld.

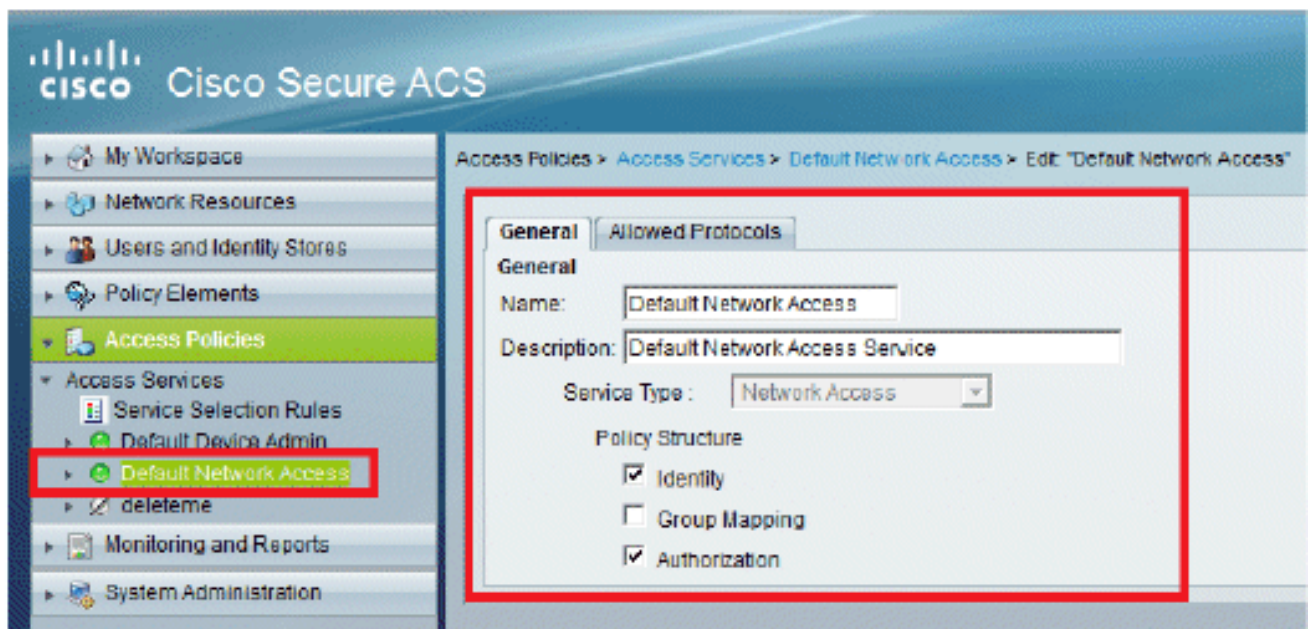


Toegangsbeleid toepassen

In dit gedeelte selecteert u EAP-FAST als de verificatiemethode die wordt gebruikt voor LAP's om te verifiëren. U maakt vervolgens regels op basis van de vorige stappen.

Voer de volgende stappen uit:

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



2. Zorg ervoor dat u **EAP-FAST** en **Anonymous In-Band PAC Provisioning** hebt ingeschakeld.

- ▶ My Workspace
- ▶ Network Resources
- ▶ Users and Identity Stores
- ▶ Policy Elements
- ▶ Access Policies
- ▶ Access Services
 - ▶ Service Selection Rules
 - ▶ Default Device Admin
 - ▶ **Default Network Access**
 - ▶ Identity
 - ▶ Authorization
 - ▶ delete me
- ▶ Monitoring and Reports
- ▶ System Administration

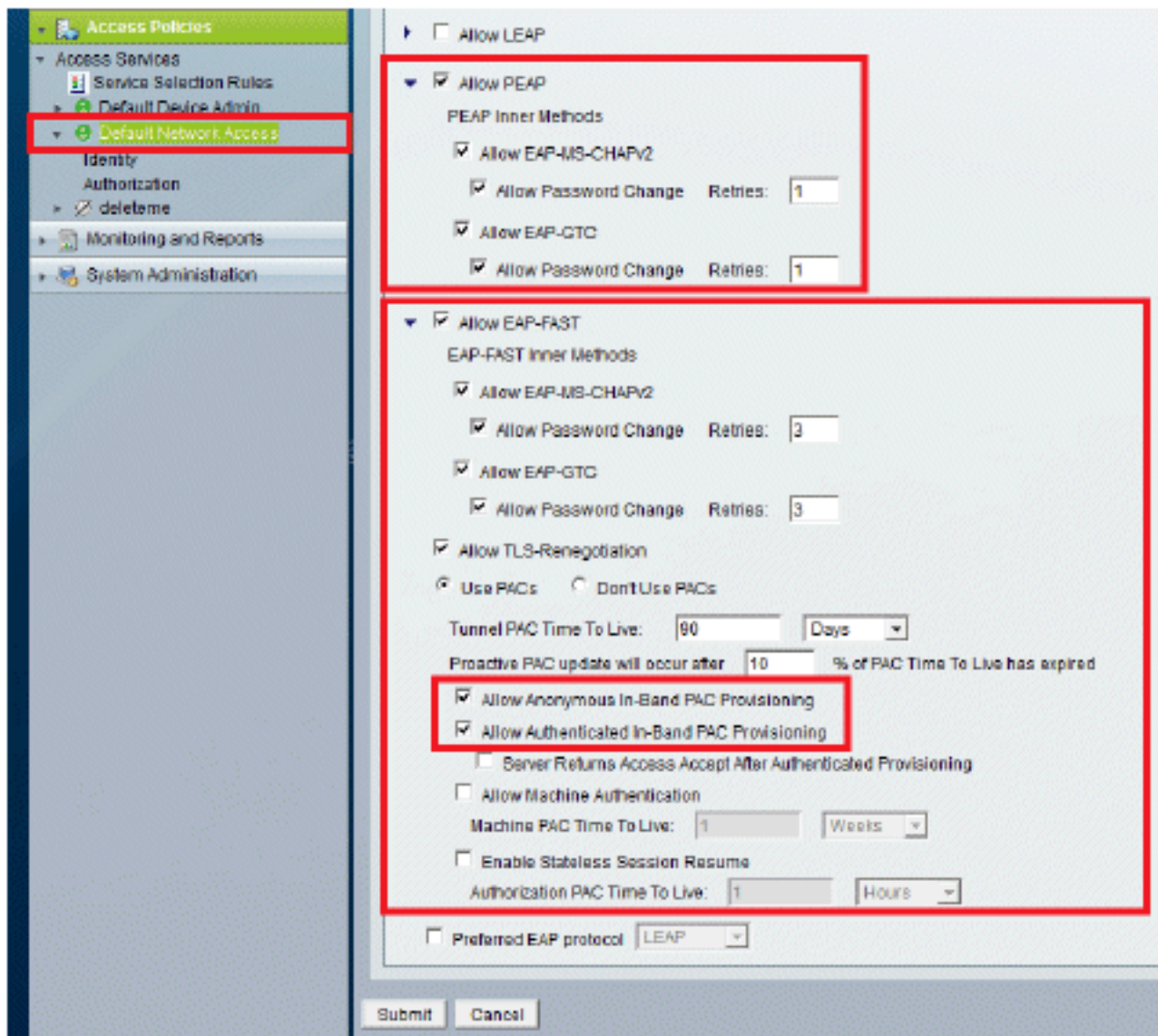
General | **Allowed Protocols**

Process Host Lookup

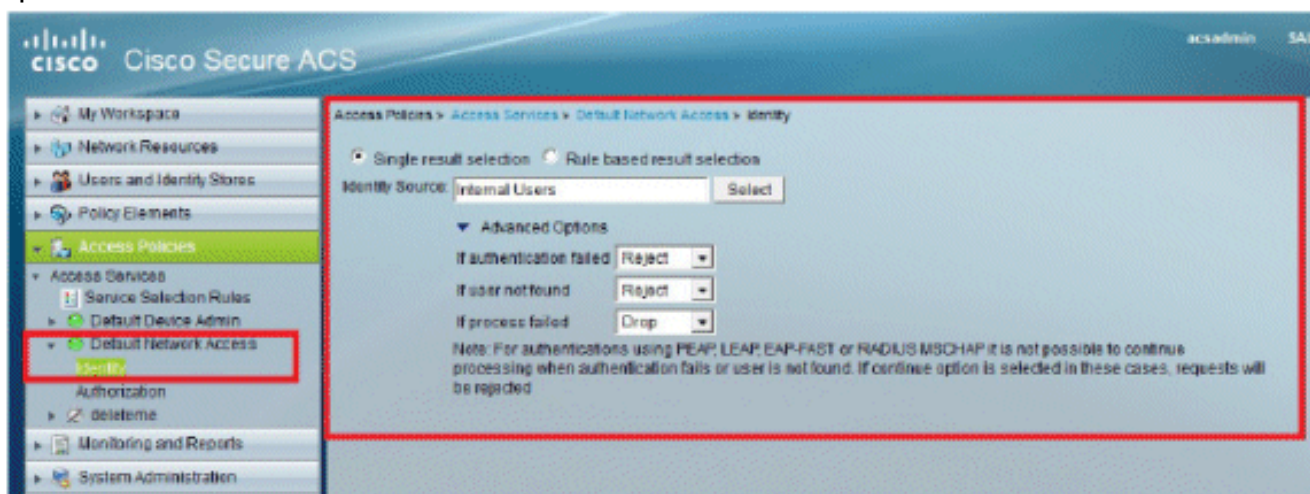
Authentication Protocols

- ▶ Allow PAP/ASCII
- ▶ Allow CHAP
- ▶ Allow MS-CHAPv1
- ▶ Allow MS-CHAPv2
- ▶ Allow EAP-MD5
- ▶ Allow EAP-TLS
- ▶ Allow LEAP
- ▶ Allow PEAP
- ▶ Allow EAP-FAST

Preferred EAP protocol

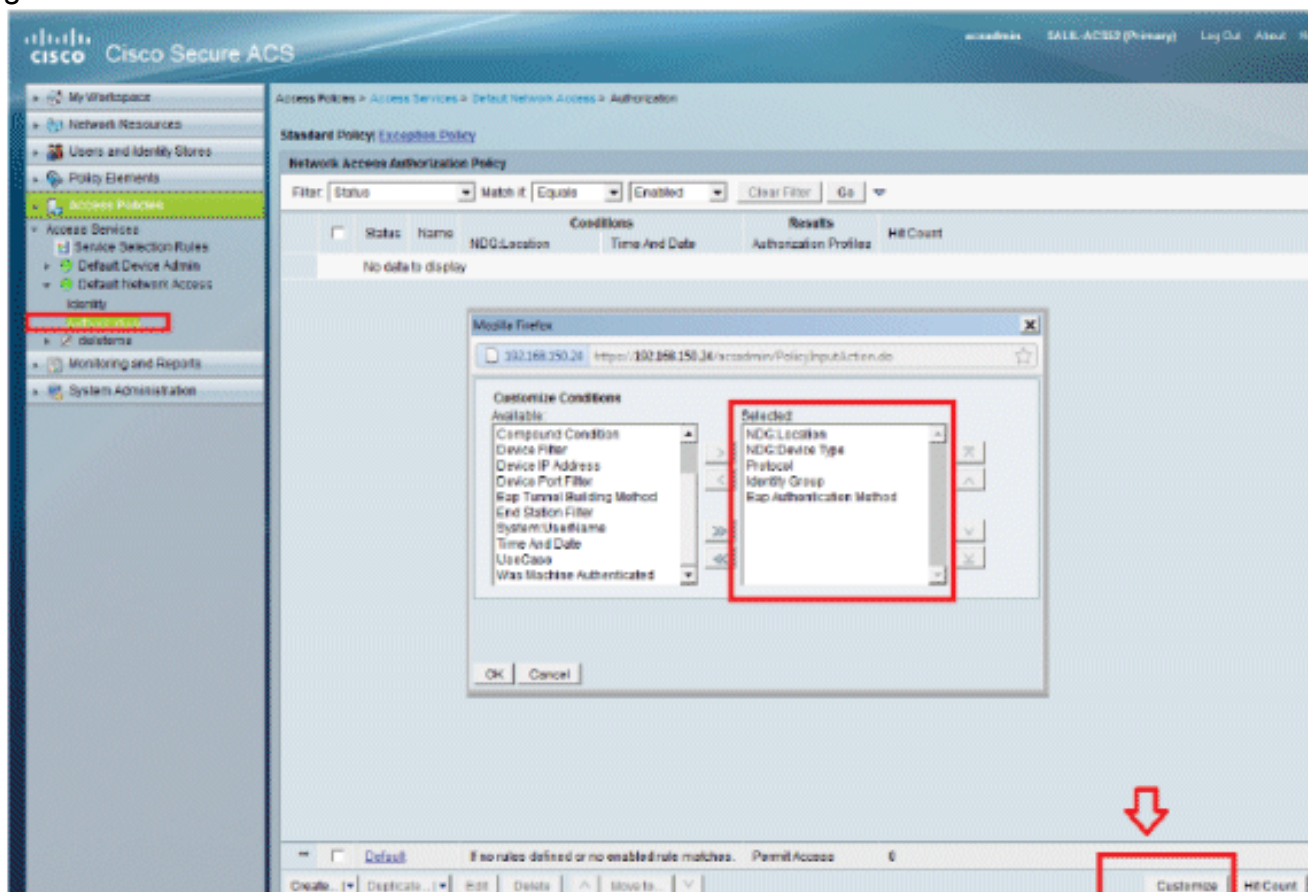


3. Klik op **Verzenden**.
4. Controleer de groep Identity die u hebt geselecteerd. In dit voorbeeld, gebruik **Interne Gebruikers** (die op ACS) werd gemaakt en sla de veranderingen op.

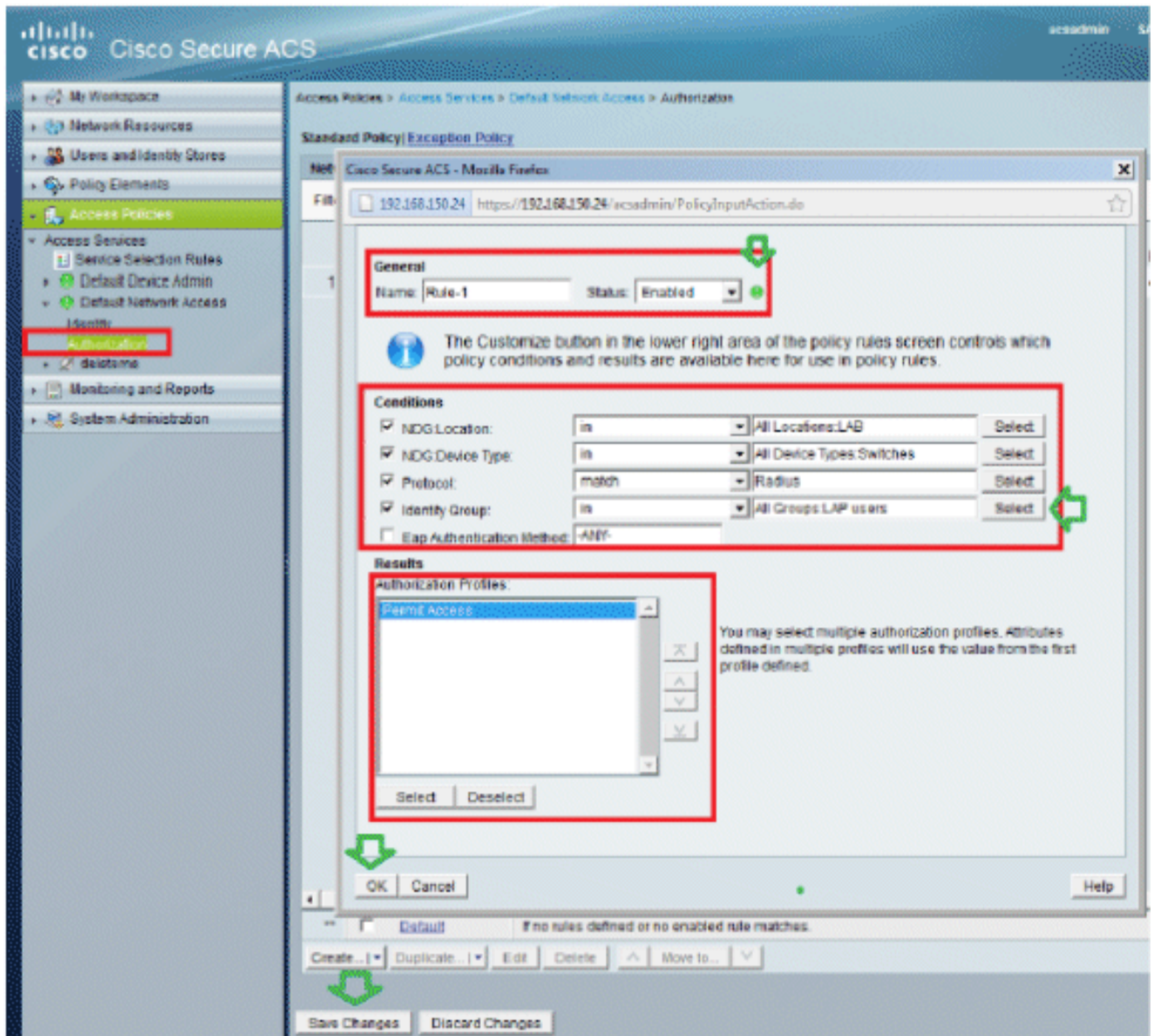


5. Ga naar **Toegangsbeleid > Toegangsservices > Standaard netwerktoegang > Autorisatie** om het autorisatieprofiel te verifiëren. U kunt aanpassen onder welke voorwaarden u een gebruiker toegang tot het netwerk zal verlenen en welk autorisatieprofiel (attributen) u zal overgaan zodra het is geverifieerd. Deze granulariteit is alleen beschikbaar in ACS 5.x. In dit

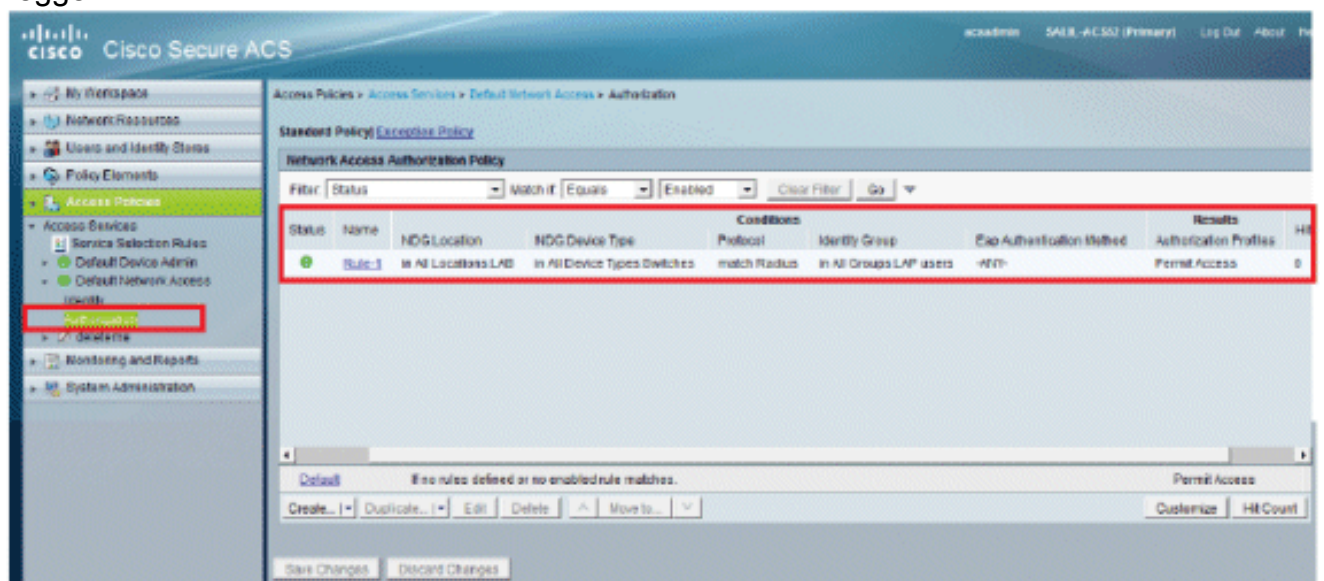
voorbeeld worden Locatie, Apparaattype, Protocol, Identity Group en EAP-verificatiemethode geselecteerd.



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



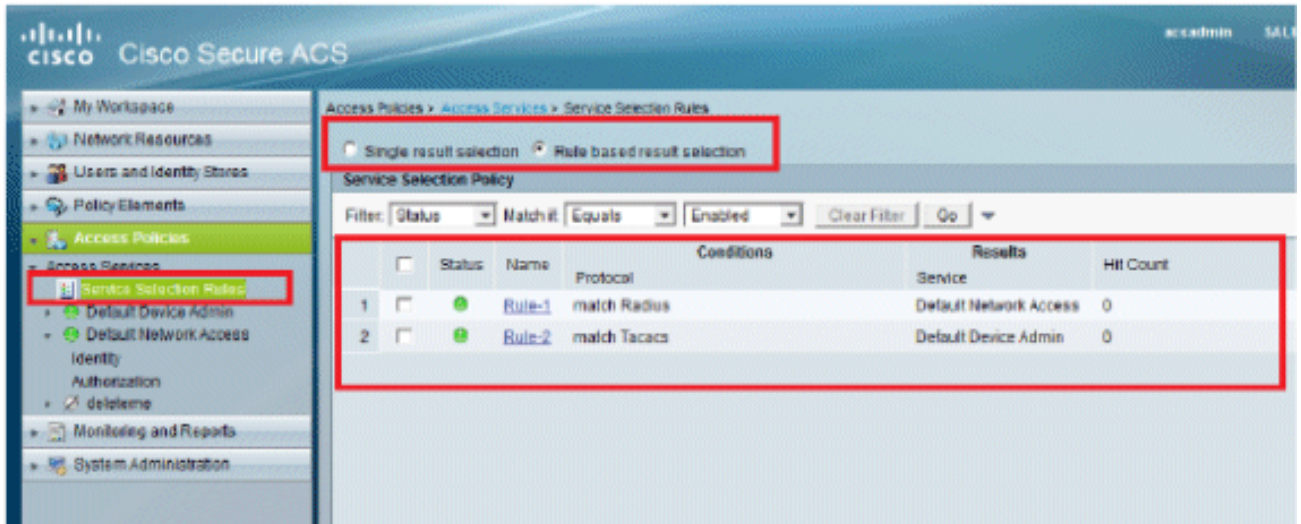
9. Klik op **Wijzigingen opslaan**. Als u wilt dat gebruikers die niet voldoen aan de voorwaarden die moeten worden geweigerd, bewerk de standaardregel om "Deny Access" te zeggen.



10. De laatste stap is het definiëren van regels voor serviceselectie. 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.

Voorbeeld:



Verifiëren

Als 802.1x is ingeschakeld op de poortpoort, wordt al het verkeer behalve het 802.1x-verkeer geblokkeerd door de switch. De LAP, die al bij de WLC is geregistreerd, wordt losgekoppeld. Enkel na een succesvolle 802.1x-verificatie mag ander verkeer door. Succesvolle registratie van de LAP naar de WLC nadat de 802.1x is ingeschakeld op de switch geeft aan dat de LAP-verificatie succesvol is.

AP-console:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
```

```

down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.

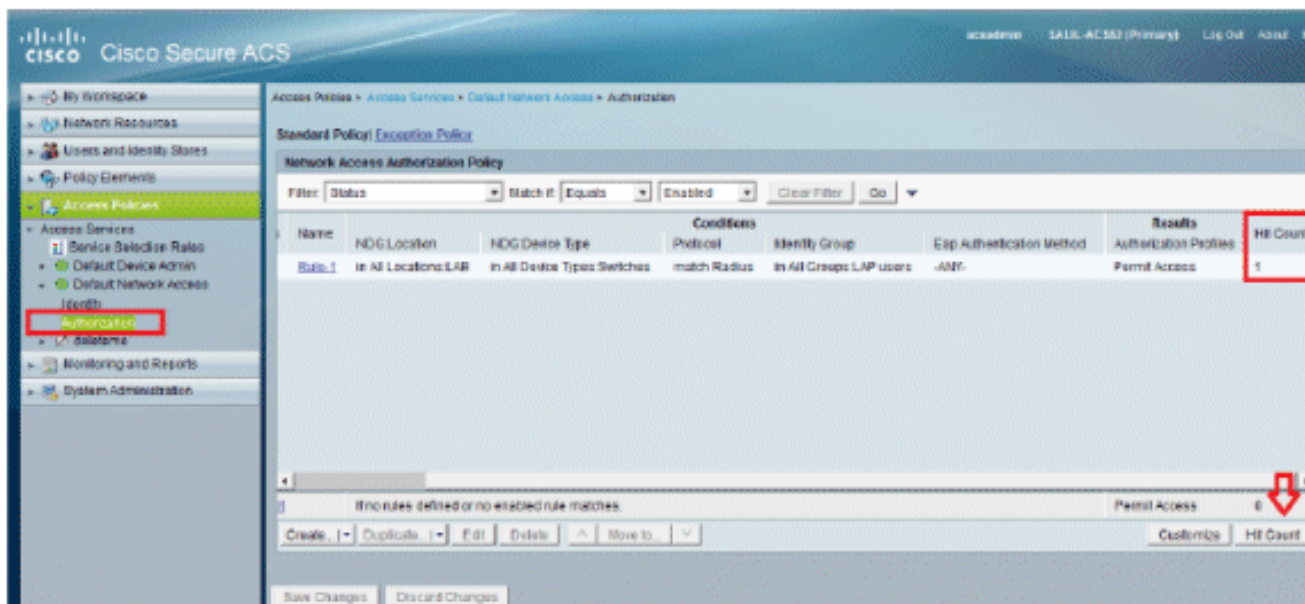
```

ACS-logs:

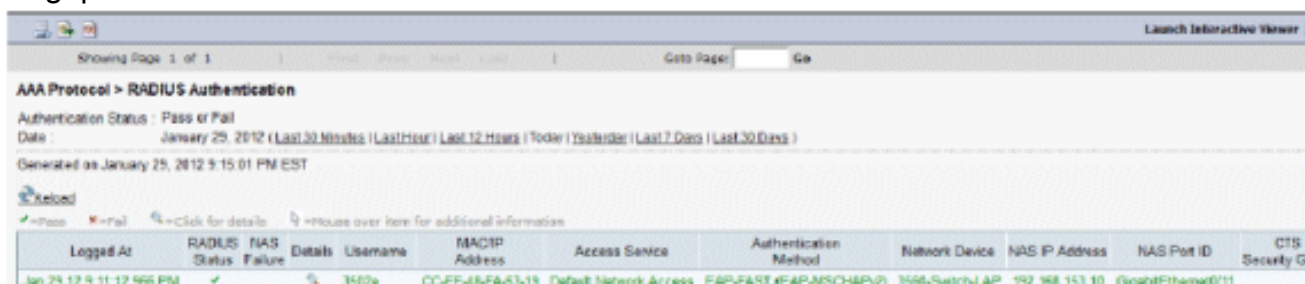
1. Bekijk de Hit tellingen: Als u logbestanden controleert binnen 15 minuten van verificatie, zorg er dan voor dat u de Hit Count ververs. Op dezelfde pagina, onderaan heb je een Hit Count tabblad.

The screenshot shows the Cisco Secure ACS web interface. The left sidebar has 'Service Selection Rules' highlighted. The main content area shows a table of rules. The 'Hit Count' column is highlighted with a red box.

	<input type="checkbox"/>	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>	●	Rule-1	match Radius		Default Network Access	1
2	<input type="checkbox"/>	●	Rule-2	match Tacacs		Default Device Admin	0



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



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Cisco Secure Access Control System](#)
- [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.