

ACS versie 5.2 en WLC voor per WLAN-verificatievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[De WLC configureren](#)

[Cisco beveiligde ACS configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document biedt een configuratievoorbeeld om de toegang voor elke gebruiker tot een Wireless LAN (WLAN) te beperken op basis van de Service set-identificer (SSID).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe u de draadloze LAN-controller (WLC) en het lichtgewicht access point (LAP) voor basisbediening kunt configureren
- Hoe u de Cisco Secure Access Control Server (ACS) configureren
- Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden

Gebruikte componenten

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

- Cisco 5500 Series WLC-software met firmware versie 7.4.10
- Cisco 1142 Series LAP
- Cisco Secure ACS Server versie 5.2.0.2.11

Configureren

Om de apparaten voor deze instelling te configureren hebt u het volgende nodig:

1. Configureer de WLC voor de twee WLAN's en RADIUS-server.

2. Configureer de Cisco beveiligde ACS.
3. Configureer de draadloze clients en controleer de configuratie.

De WLC configureren

Volg deze stappen om de WLC te configureren voor deze instelling:

1. Configureer de WLC om de gebruikersreferenties naar een externe RADIUS-server door te sturen. De externe RADIUS-server (Cisco Secure ACS in dit geval) bevestigt vervolgens de gebruikersreferenties en geeft toegang tot de draadloze clients. Voer de volgende stappen uit: Selecteer **Security > RADIUS-verificatie** van de controller GUI om de pagina RADIUS-verificatieservers weer te geven.



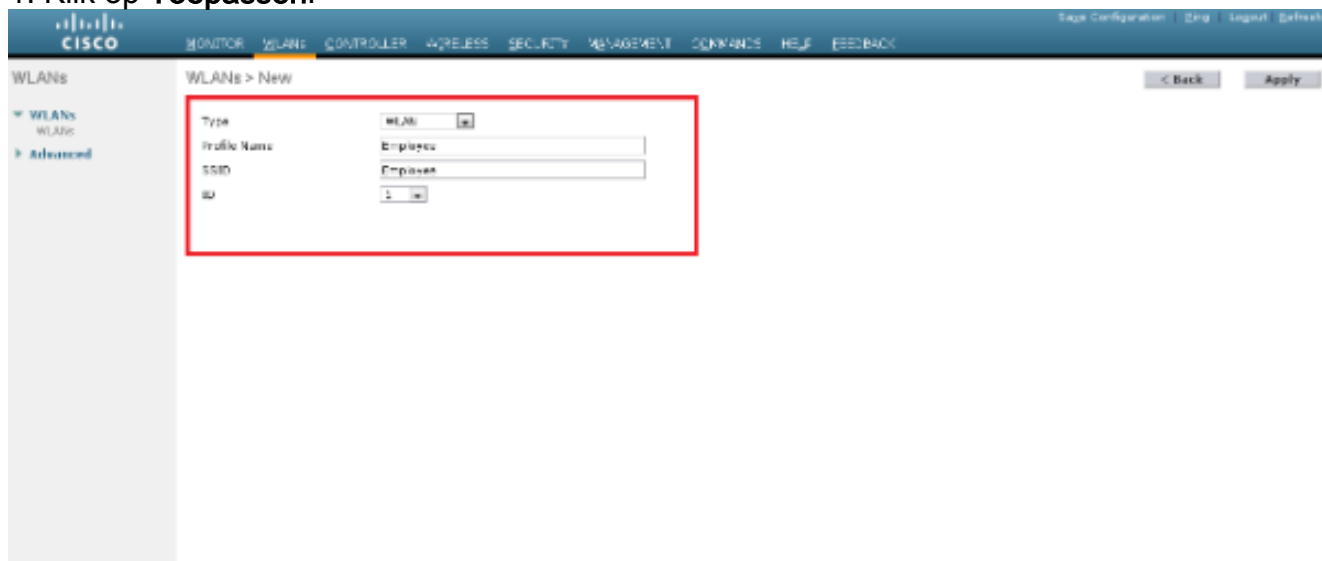
Klik op **New** om de RADIUS-serverparameters te definiëren. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. De selectieteksten Netwerkgebruiker en -beheer bepalen of de op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers. Dit voorbeeld gebruikt Cisco Secure ACS als de RADIUS-server met IP-adres 10.104.208.56.



Klik op **Toepassen**.

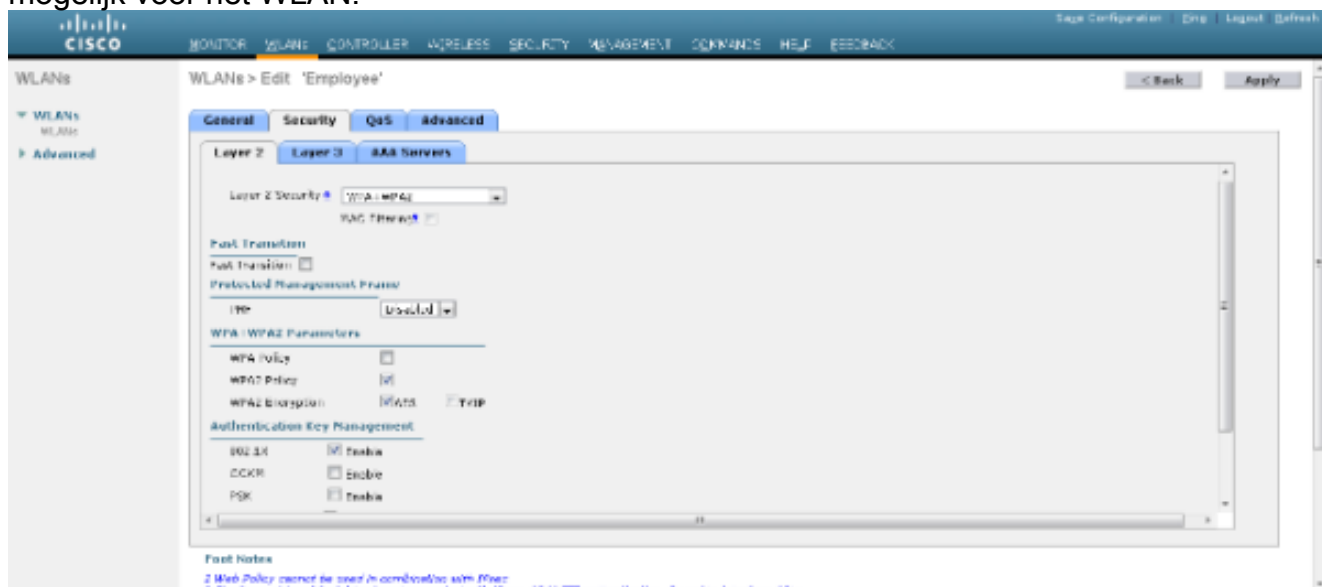
2. Voltooi deze stappen om één WLAN voor de werknemer met SSID **werknemer** en de andere WLAN's voor contracteurs met SSID **Contractor** te configureren. Klik op **WLAN's** van de controller GUI om een WLAN-functie te maken. Het WLAN-venster verschijnt. Dit venster

toont de WLAN's die op de controller zijn geconfigureerd. Klik op **New** om een nieuwe WLAN te configureren. Dit voorbeeld creëert een WLAN met de naam Werknemer en de WLAN-id is 1. Klik op **Toepassen**.



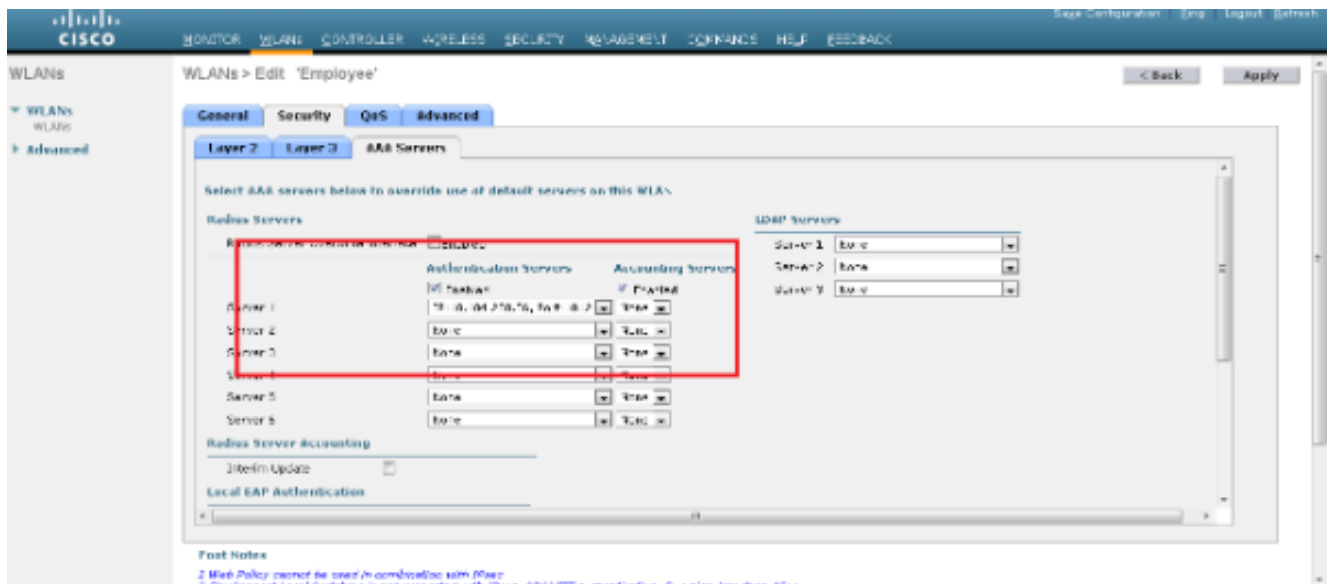
The screenshot shows the Cisco configuration interface for creating a new WLAN. The page title is 'WLANs > New'. A red box highlights the configuration fields: 'Type' is set to 'WLAN', 'Profile Name' is 'Employee', 'SSID' is 'Employee', and 'ID' is '1'. The interface includes a navigation menu at the top with options like MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. There are also 'Back' and 'Apply' buttons at the top right.

Selecteer het **WLAN > Bewerken** venster en definieer de parameters die specifiek zijn voor WLAN: Selecteer in het tabblad Layer 2 Security de optie **802.1x**. Layer 2 Security optie is standaard 802.1x. Dit maakt 802.1 x/Extensible Authentication Protocol (EAP) authenticaties mogelijk voor het WLAN.



The screenshot shows the Cisco configuration interface for editing an existing WLAN named 'Employee'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'AAA Servers' section is visible, showing a list of RADIUS servers. The interface includes a navigation menu at the top with options like MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. There are also 'Back' and 'Apply' buttons at the top right.

Selecteer in het tabblad AAA-servers de juiste RADIUS-server in de vervolgkeuzelijst onder RADIUS-servers. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk. Klik op **Toepassen**.



Op dezelfde manier herhaalt u stappen b tot d om een WLAN-oplossing voor contractanten te maken.

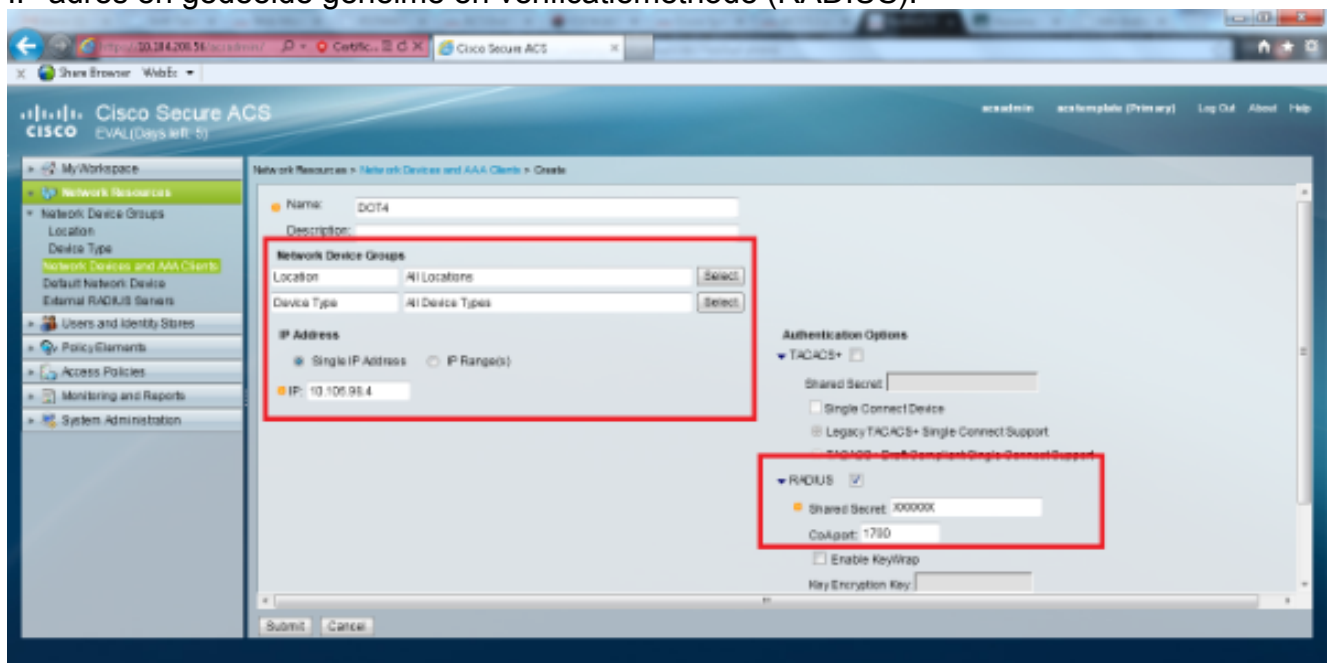
Cisco beveiligde ACS configureren

Op de Cisco Secure ACS-server moet u:

1. Configureer de WLC als een AAA-client.
2. Maak de gebruikersdatabase (Credentials) voor op SSID gebaseerde verificatie.
3. MAP-verificatie inschakelen.

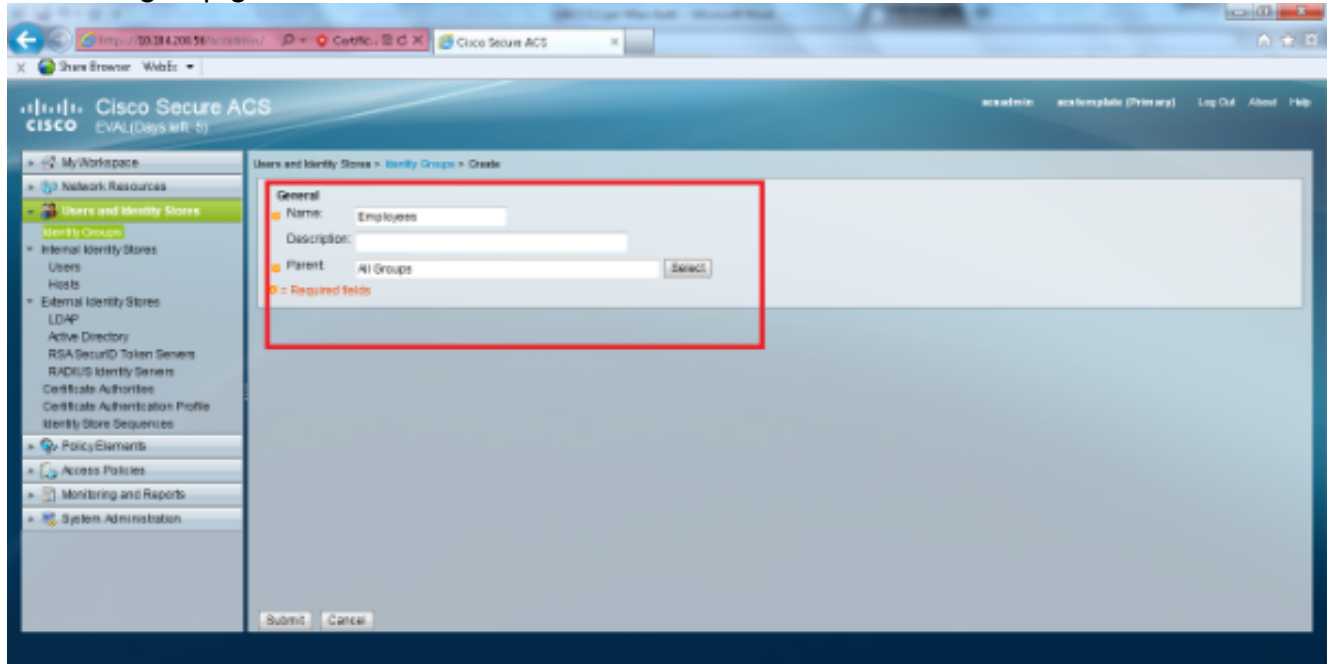
Voltooi deze stappen op Cisco Secure ACS:

1. Om de controller als een AAA-client op de ACS-server te definiëren, selecteert u **Netwerkbronnen > Netwerkapparaten en AAA-clients** vanuit de ACS-GUI. Klik onder Netwerkapparaten en AAA-clients op **Maken**.
2. Wanneer de pagina Network Configuration verschijnt, specificeert u de naam van de WLC, IP-adres en gedeelde geheime en verificatiemethode (RADIUS).

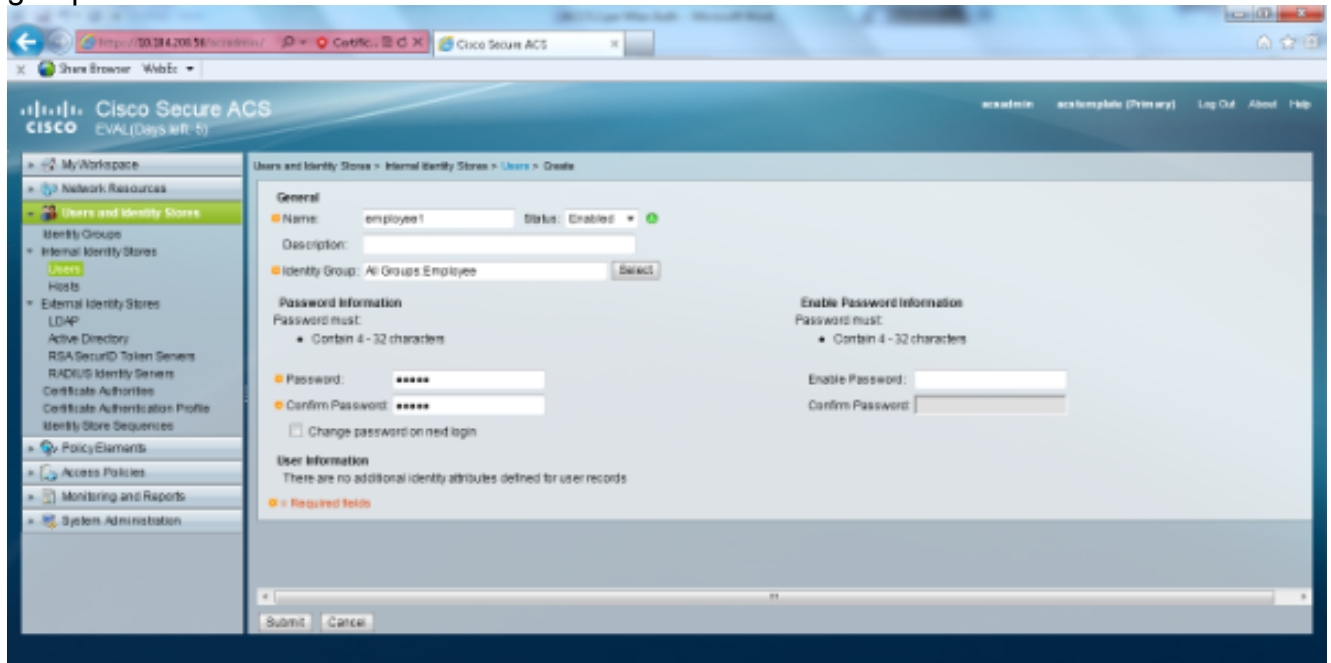


3. Selecteer **Gebruikers- en identiteitsopslag > Identiteitsgroepen** uit de ACS-GUI. Maak de

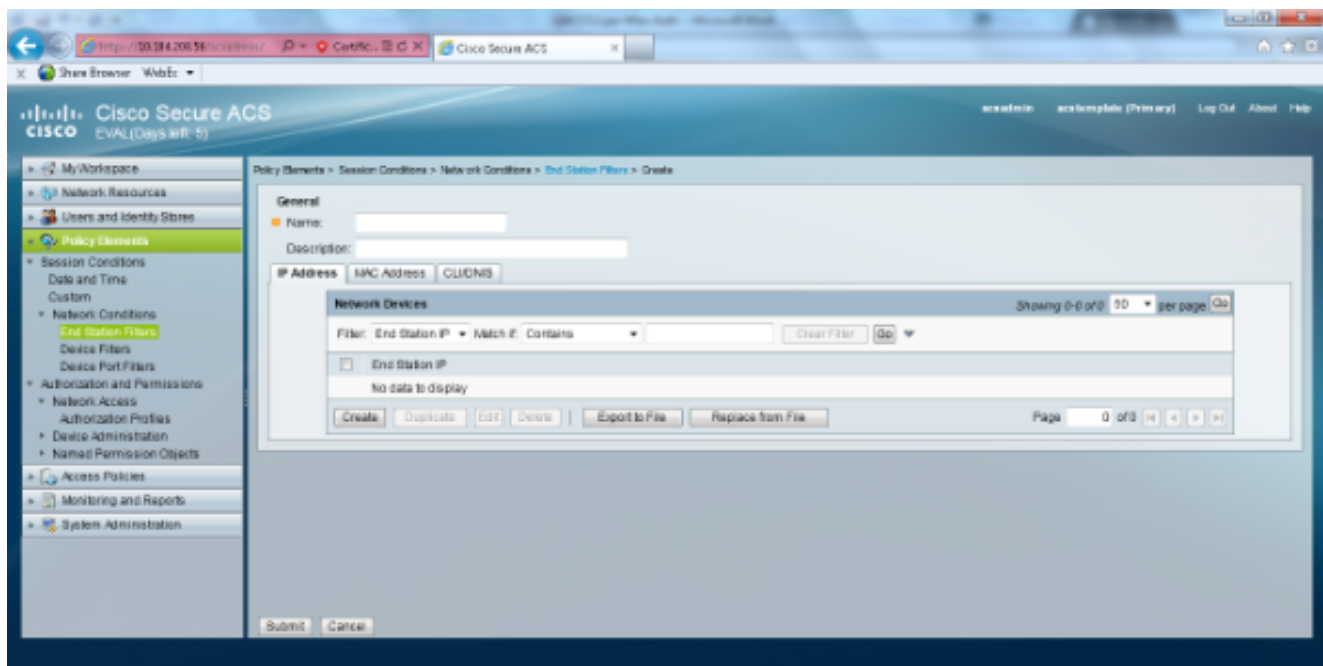
respectievelijke groepen voor Werknemer en Contractor en klik op **Maken**. In dit voorbeeld wordt de groep gemaakt met de naam Werknemers.



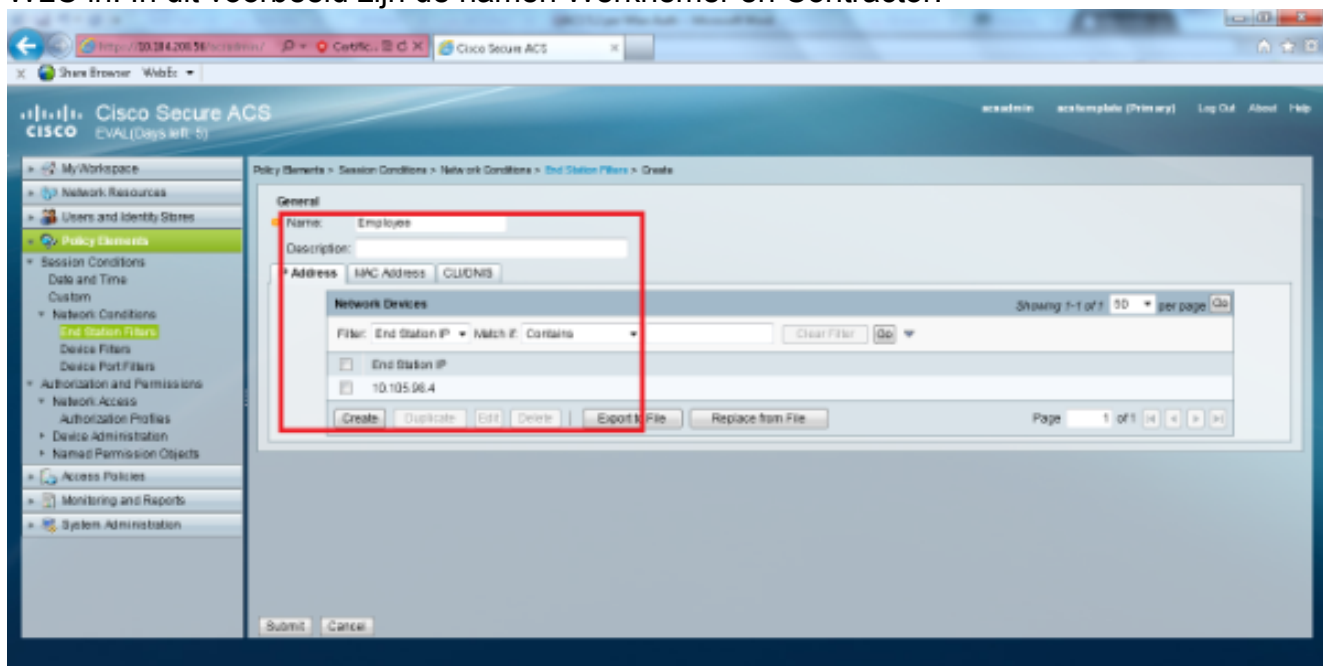
4. Selecteer **Gebruikers en identiteitsopslag > Interne identiteitsopslag**. Klik op **Maken** en voer de gebruikersnaam in. Plaats ze in de juiste groep, definieer hun wachtwoord en klik op **Inzenden**. In dit voorbeeld wordt een gebruiker met de naam worker1 in de groep Werknemer gecreëerd. Creëer ook een gebruiker met de naam contractant1 onder de groepsaannemers.



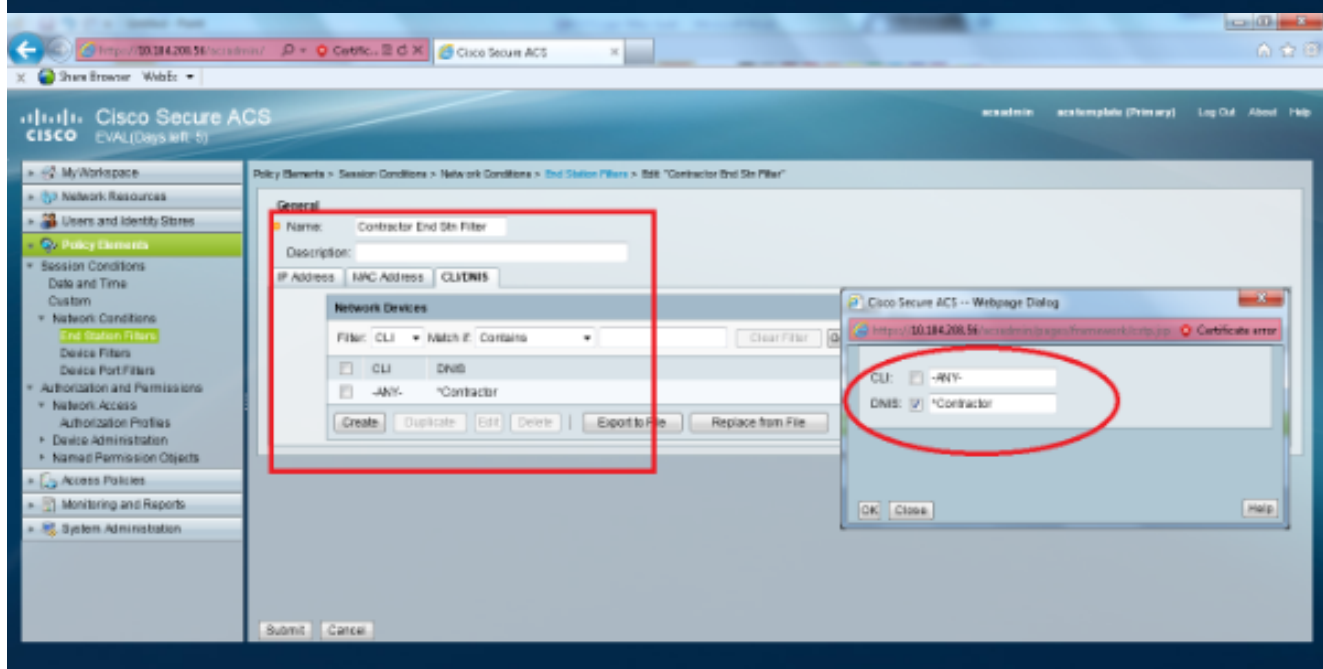
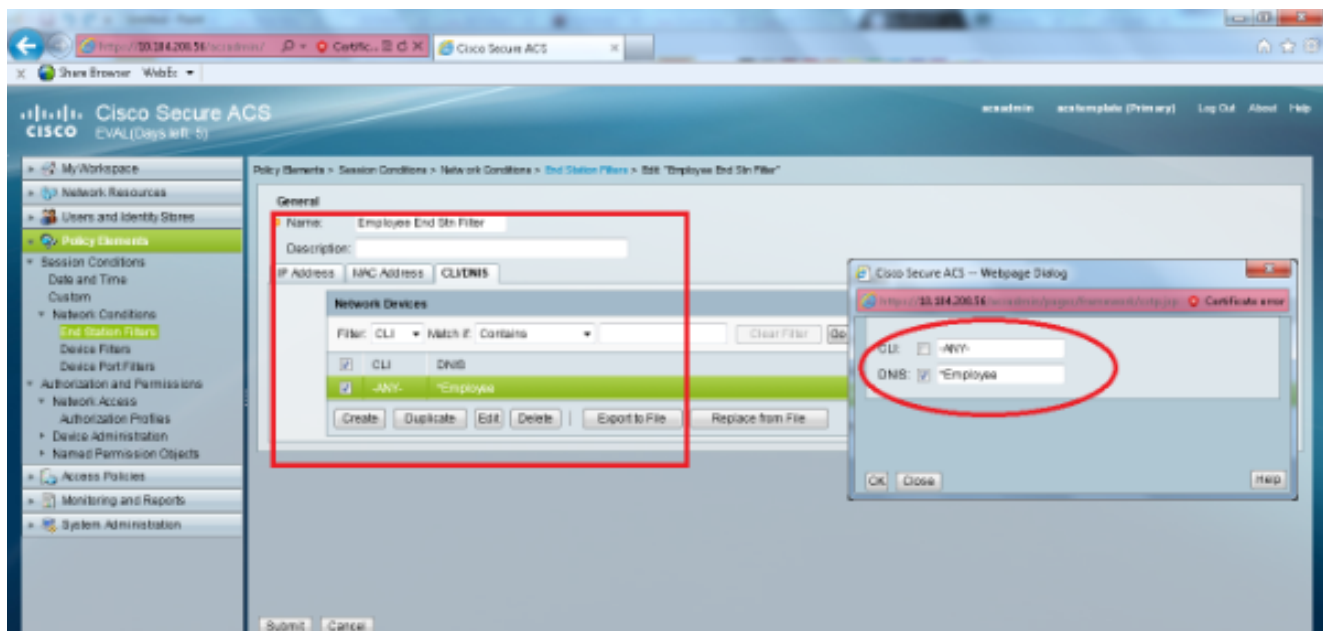
5. Selecteer **Beleidselementen > Netwerkomstandigheden > Filters van het eindstation**. Klik op **Maken**.



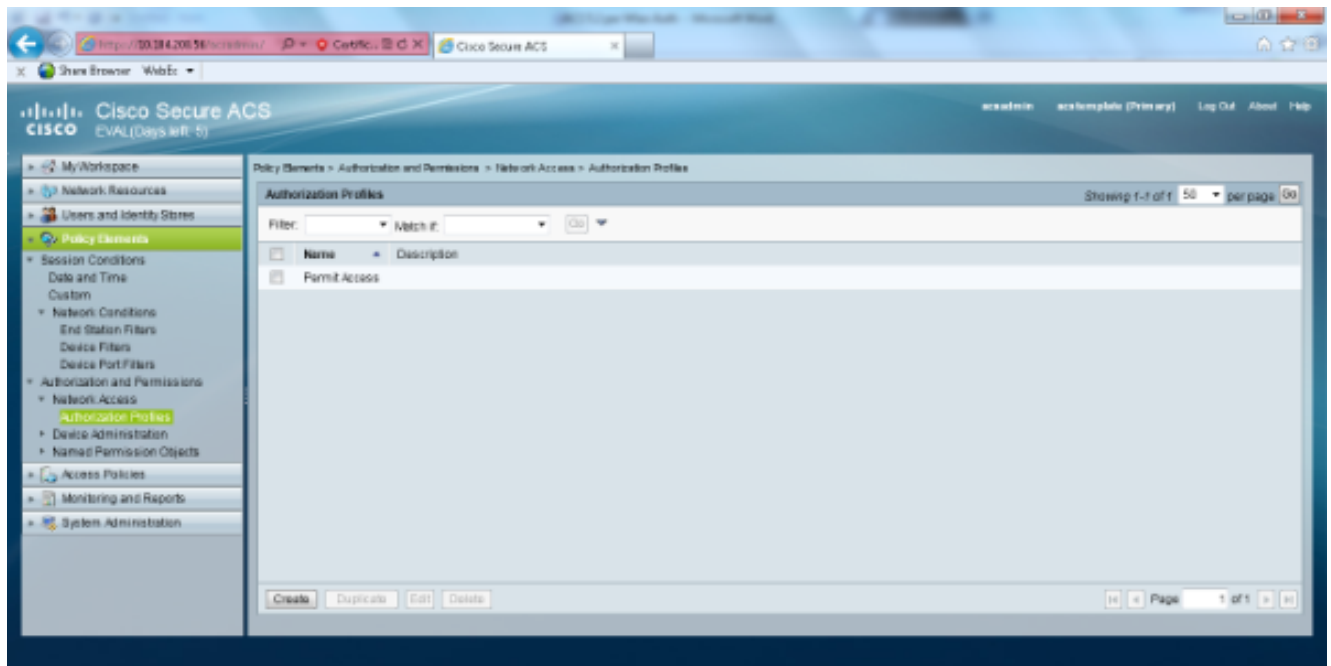
Voer een betekenisvolle naam in en voer onder het tabblad **IP-adres** het IP-adres van de WLC in. In dit voorbeeld zijn de namen Werknemer en Contractor.



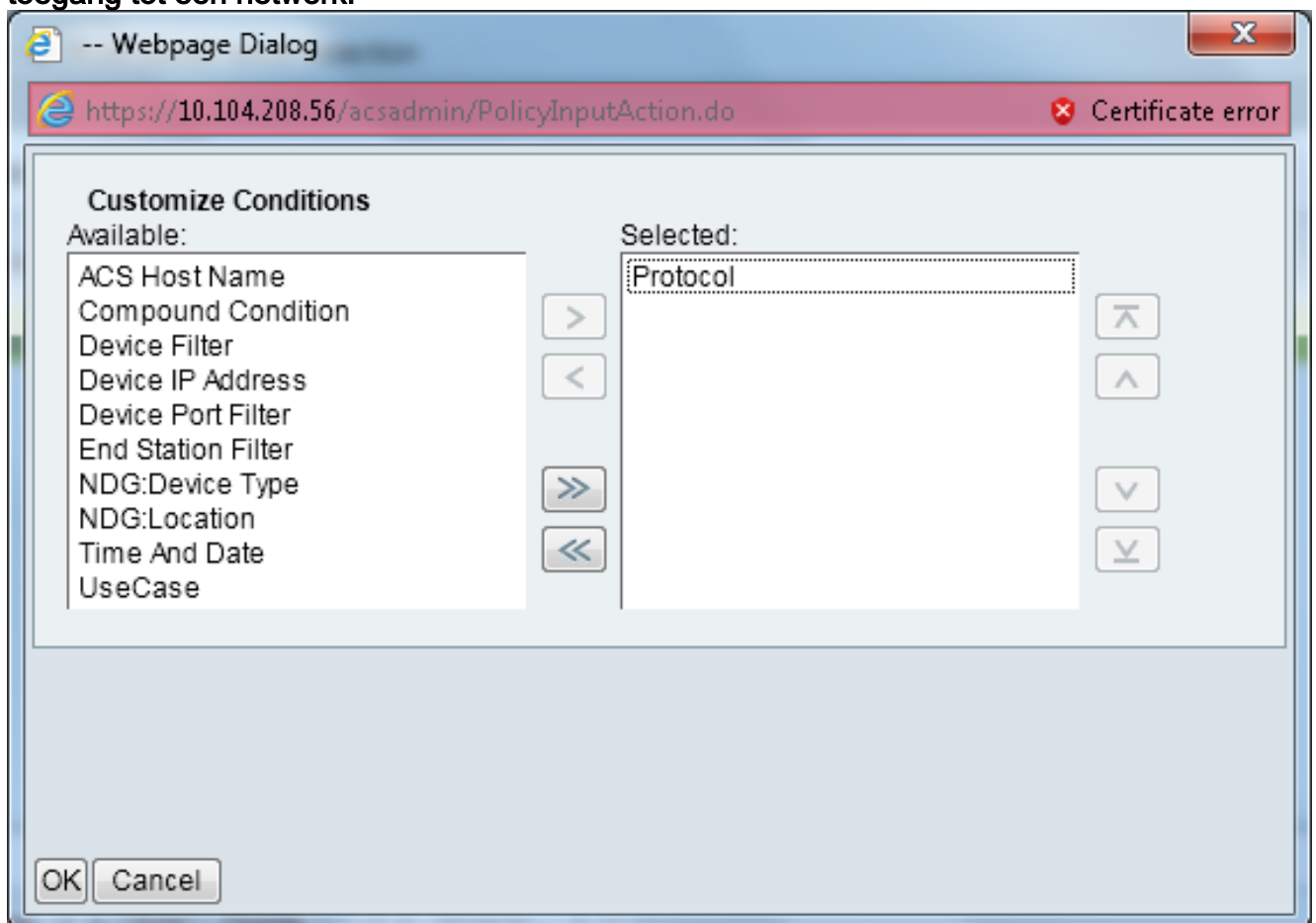
Onder het tabblad CLI/DNIS, laat CLI als ALLE-bestanden en voer DNIS in als *<SSID>. In dit voorbeeld, wordt het DNIS-veld ingevoerd als *Werknemer aangezien dit End-station filter wordt gebruikt om alleen de toegang tot het WLAN-adres van de werknemer te beperken. De DNIS - eigenschap definieert SSID dat de gebruiker toegang mag krijgen. De WLC stuurt de SSID in de DNIS-eigenschap naar de RADIUS-server. Herhaal dezelfde stappen voor het filter van het Eindstation van de Contractor.

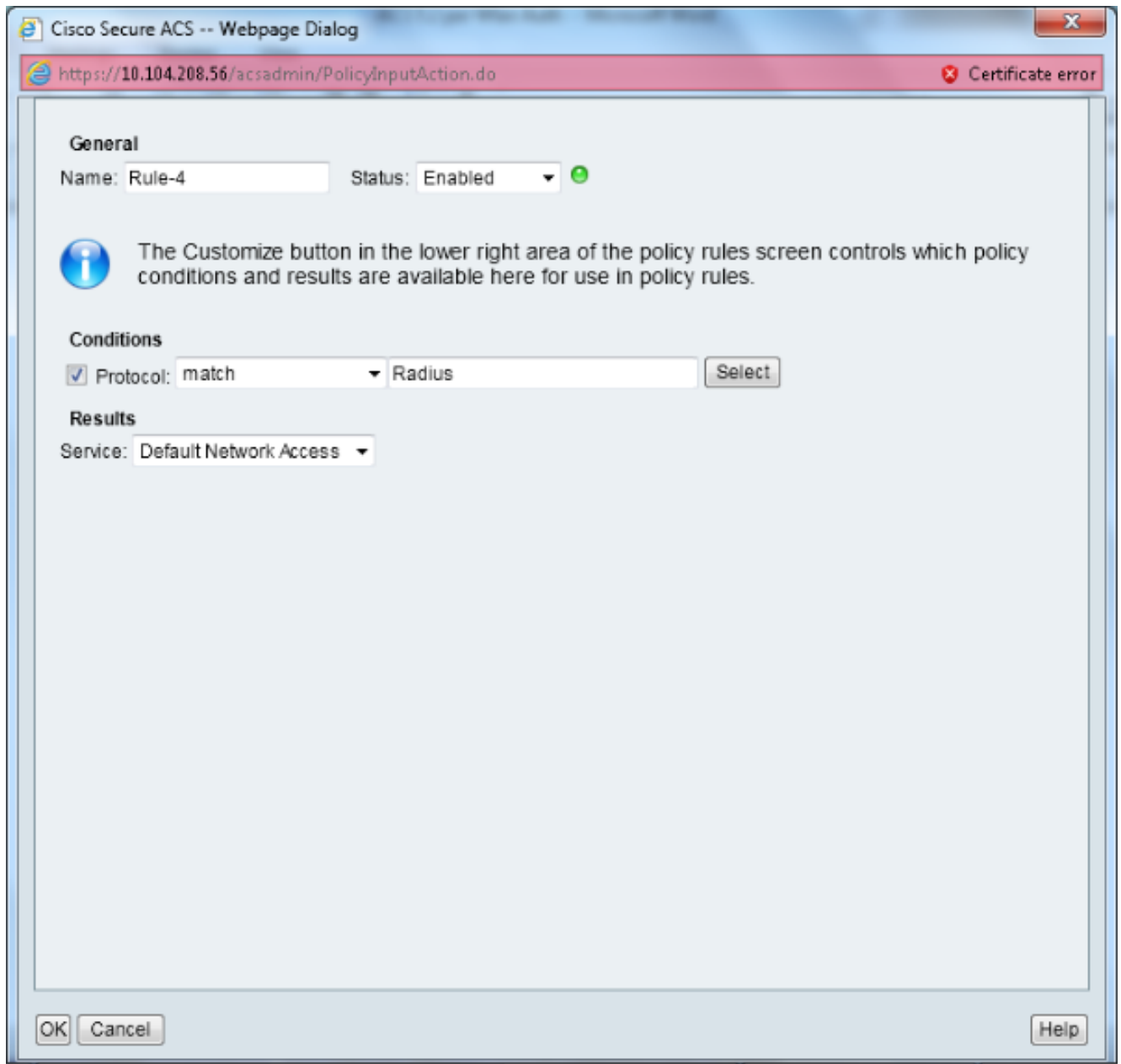


6. Selecteer **Beleids-elementen > Vergunningen en toegangsrechten > Netwerktogang > Verificatieprofielen**. Er moet een standaardprofiel zijn voor toegangsrechten.

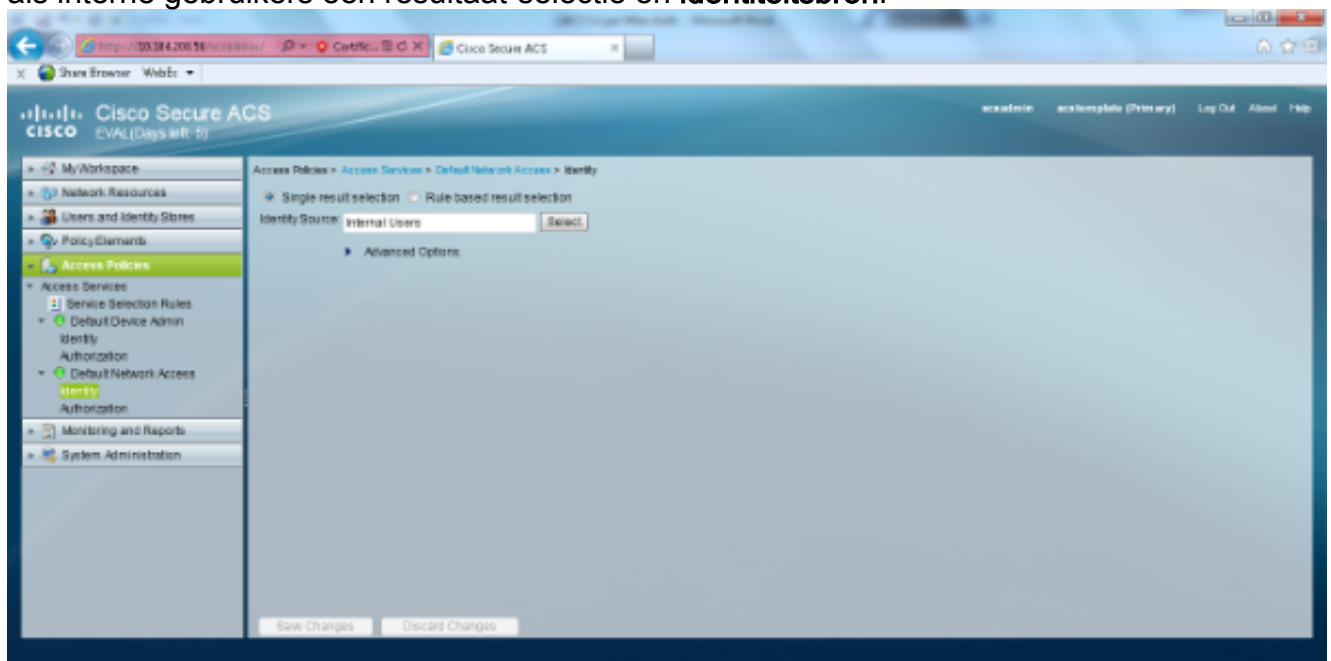


7. Selecteer **Toegangsbeleid > Toegangsservices > Service- en serviceselectieregels**. Klik op **Aanpassen**. Voeg een geschikte toestand toe. Dit voorbeeld gebruikt Protocol als Straal als de matchingsvoorwaarde. Klik op **Maken**. Naam de regel. Selecteer **Protocol** en selecteer **Straal**. Kies onder **Resultaten** de juiste toegangsservice. In dit voorbeeld blijft het standaard **toegang tot een netwerk**.

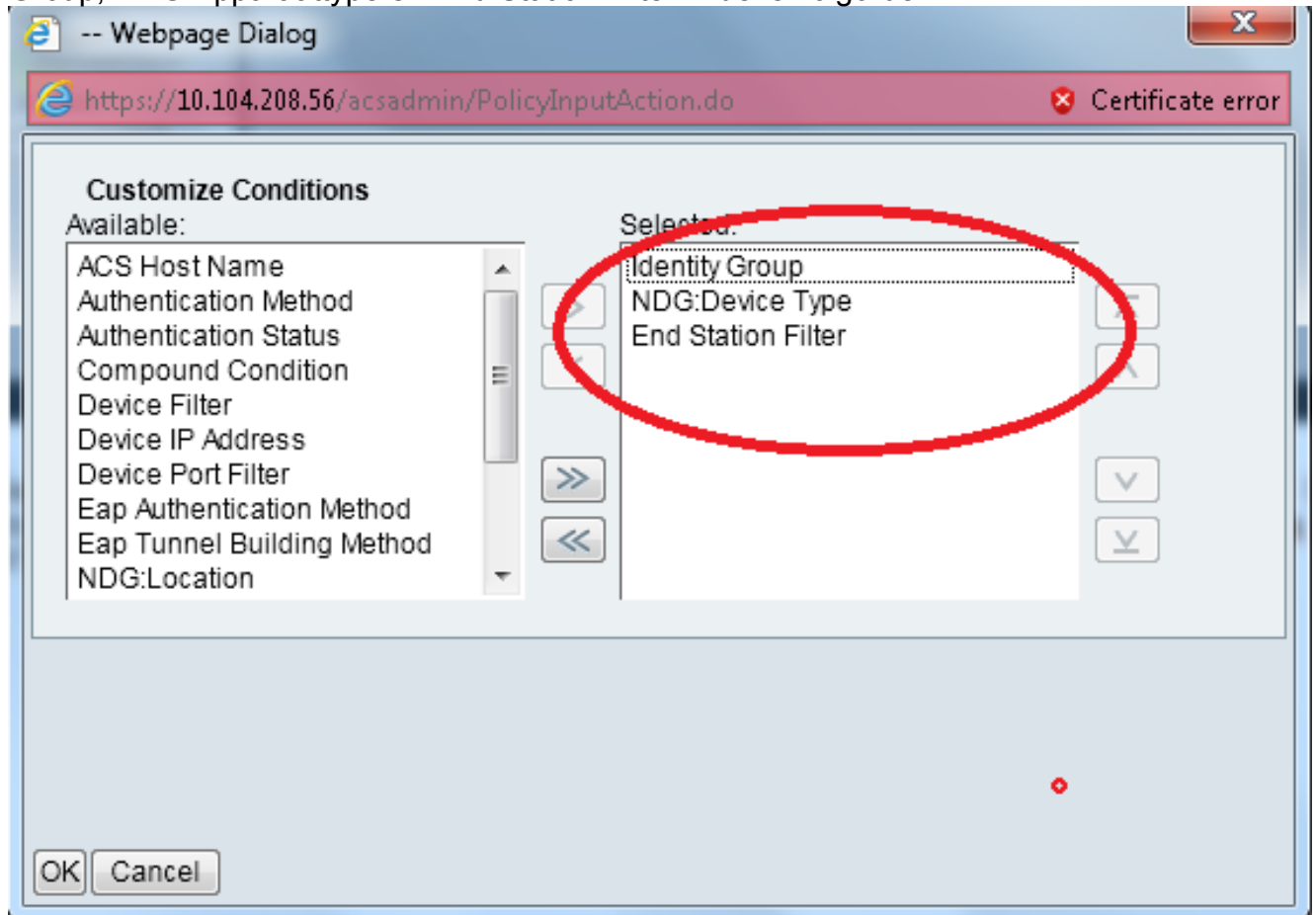




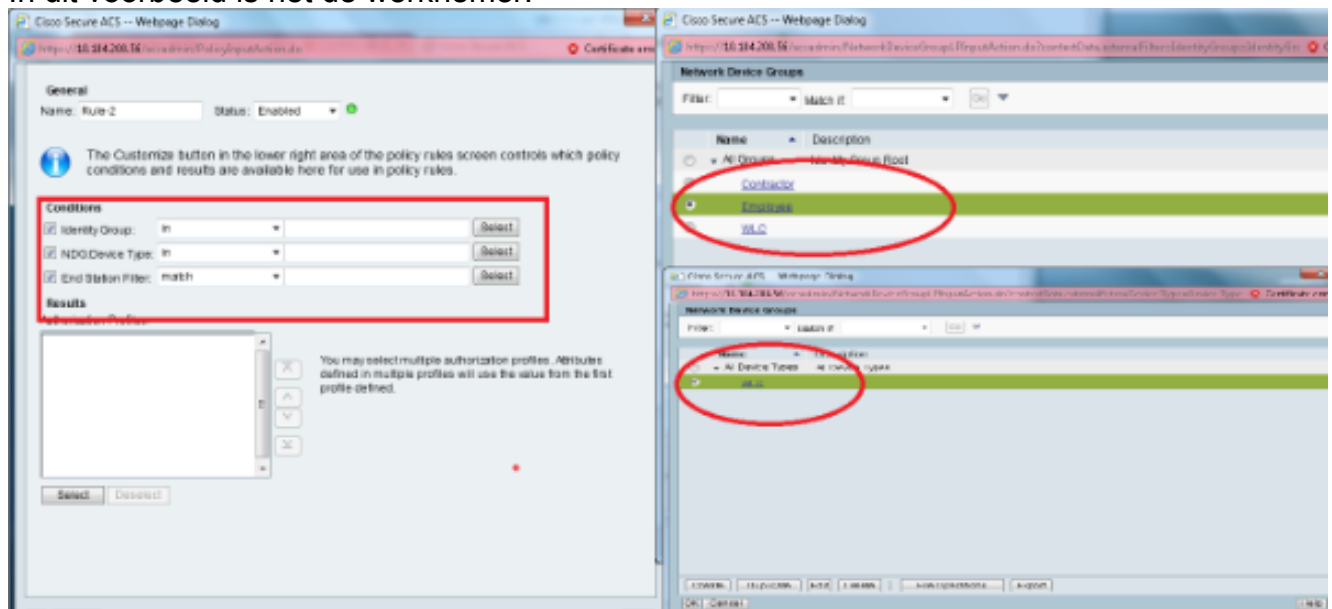
8. Selecteer Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > Identity. Kies als interne gebruikers één resultaat-selectie en identiteitsbron.



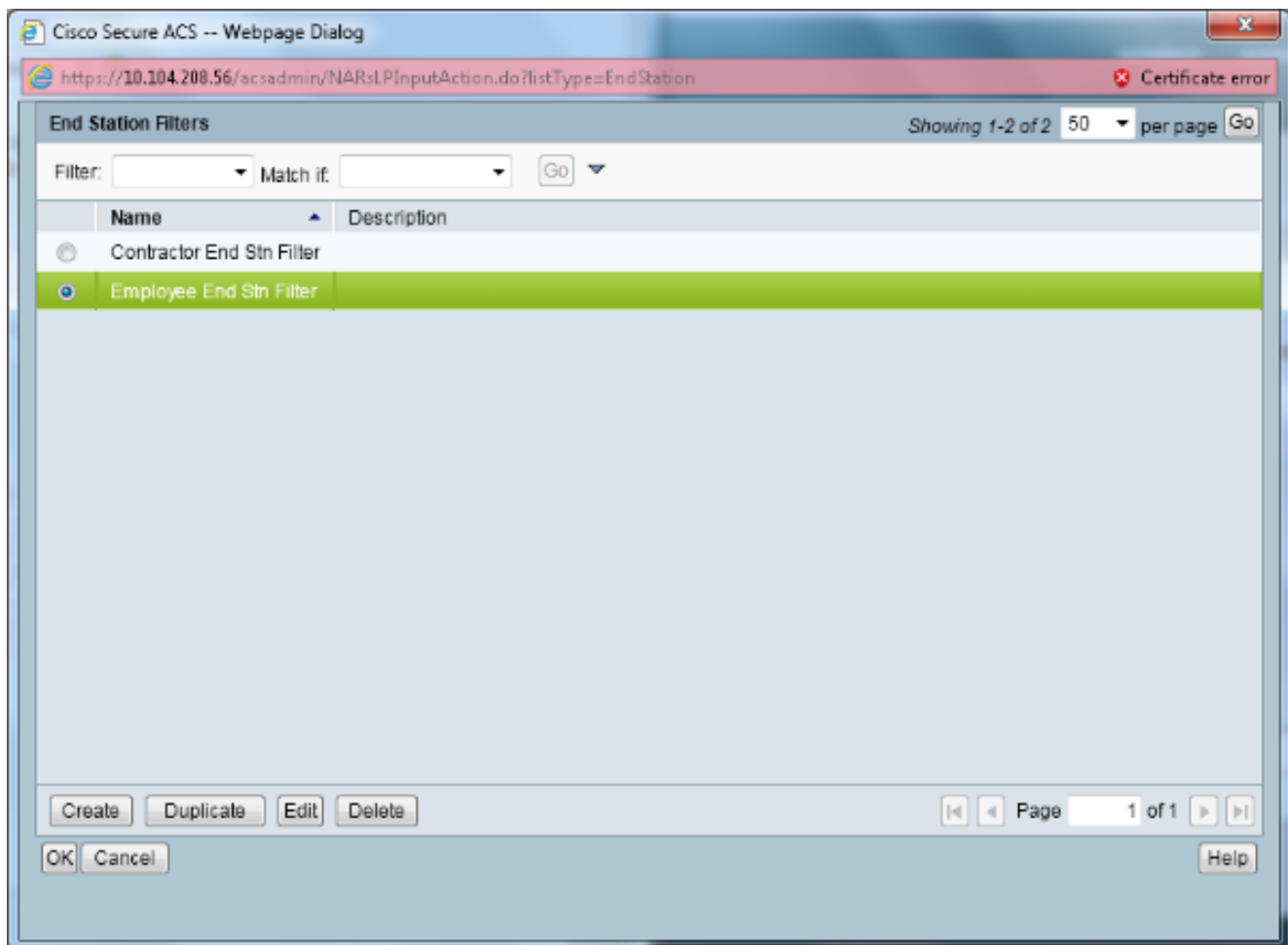
Selecteer **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > autorisatie**.
Klik op **Aanpassen** en voeg de aangepaste voorwaarden toe. Dit voorbeeld gebruikt Identity Group, NDG:Apparaattype en End Station Filter in deze volgorde.



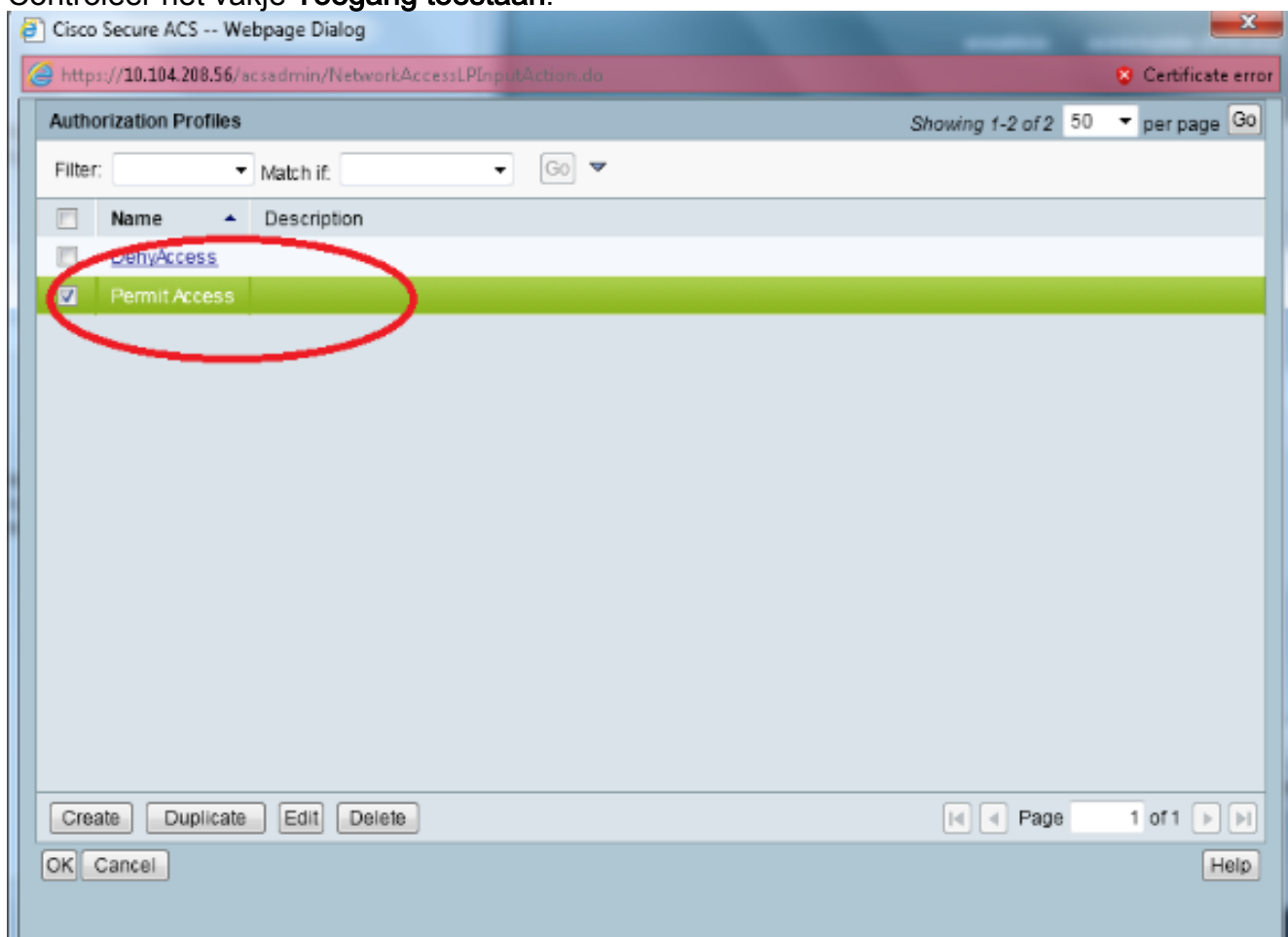
Klik op **Maken**. Geef de regel een naam en kies de juiste identiteitsgroep onder Alle groepen. In dit voorbeeld is het de werknemer.



Klik op de radioknop **End-of-support** van **Werknemers** of voer de naam in die u in Stap 1b hebt ingevoerd in de sectie "Configure the WLC".



Controleer het vakje Toegang toestaan.



Herhaal de bovenstaande stappen voor Contractorregels. Zorg ervoor dat de

standaardinstelling is om **toegang te weigeren**. Zodra u stap e hebt voltooid, zouden uw regels er als dit voorbeeld uit moeten zien:

The screenshot shows the Cisco Secure ACS web interface. The breadcrumb navigation is: Access Policies > Access Services > Default Network Access > Authorization. The main content area is titled 'Standard Policy Exception Policy' and 'Network Access Authorization Policy'. A table lists the policy rules:

Filter	Status	Match If	Equals	Clear Filter	Del																
1	<input type="checkbox"/>	Enabled	Contractor	In All Groups	Contractor	In All Device Types	WLC	match	Contractor	End Stn Filter	Permit Access	7									
2	<input type="checkbox"/>	Enabled	Employee	In All Groups	Employee	In All Device Types	WLC	match	Employee	End Stn Filter	Permit Access	5									
	<input type="checkbox"/>	Default	If no rules defined or no enabled rule matches.										Deny Access	3							

Below the table are buttons for 'Create...', 'Duplicate...', 'Edit', 'Delete', 'Move to...', 'Customize', and 'Hit Count'. At the bottom, there are 'Save Changes' and 'Discard Changes' buttons.

Dit sluit de configuratie af. Na deze sectie moet de client dienovereenkomstig met de SSID en de veiligheidsparameters worden geconfigureerd om verbinding te maken.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

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