

ACS 5.x: Verificatie en autorisatie voor TACACS+ op basis van configuratievoorbeeld voor AD-groepslidmaatschap

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configuratie](#)

[ACS 5.x configureren voor verificatie en autorisatie](#)

[Configureer het Cisco IOS-apparaat voor verificatie en autorisatie](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt een voorbeeld van het configureren van TACACS+ verificatie en commando-autorisatie op basis van AD-groepslidmaatschap van een gebruiker met Cisco Secure Access Control System (ACS) 5.x en hoger. ACS gebruikt Microsoft Active Directory (AD) als een externe identiteitsopslag om resources zoals gebruikers, machines, groepen en eigenschappen op te slaan.

[Voorwaarden](#)

[Vereisten](#)

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

- ACS 5.x is volledig geïntegreerd in het gewenste AD-domein. Als ACS niet met het gewenste AD-domein is geïntegreerd, raadpleeg [ACS 5.x en hoger: Integratie met Microsoft Active Directory Configuration Voorbeeld](#) voor meer informatie om de integratietaak uit te voeren.

[Gebruikte componenten](#)

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

- Cisco beveiligde ACS 5.3
- Cisco IOS-software release 12.2(44)SE6.**Opmerking:** Deze configuratie kan worden uitgevoerd

op alle Cisco IOS-apparaten.

- Microsoft Windows Server 2003-domein

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 de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

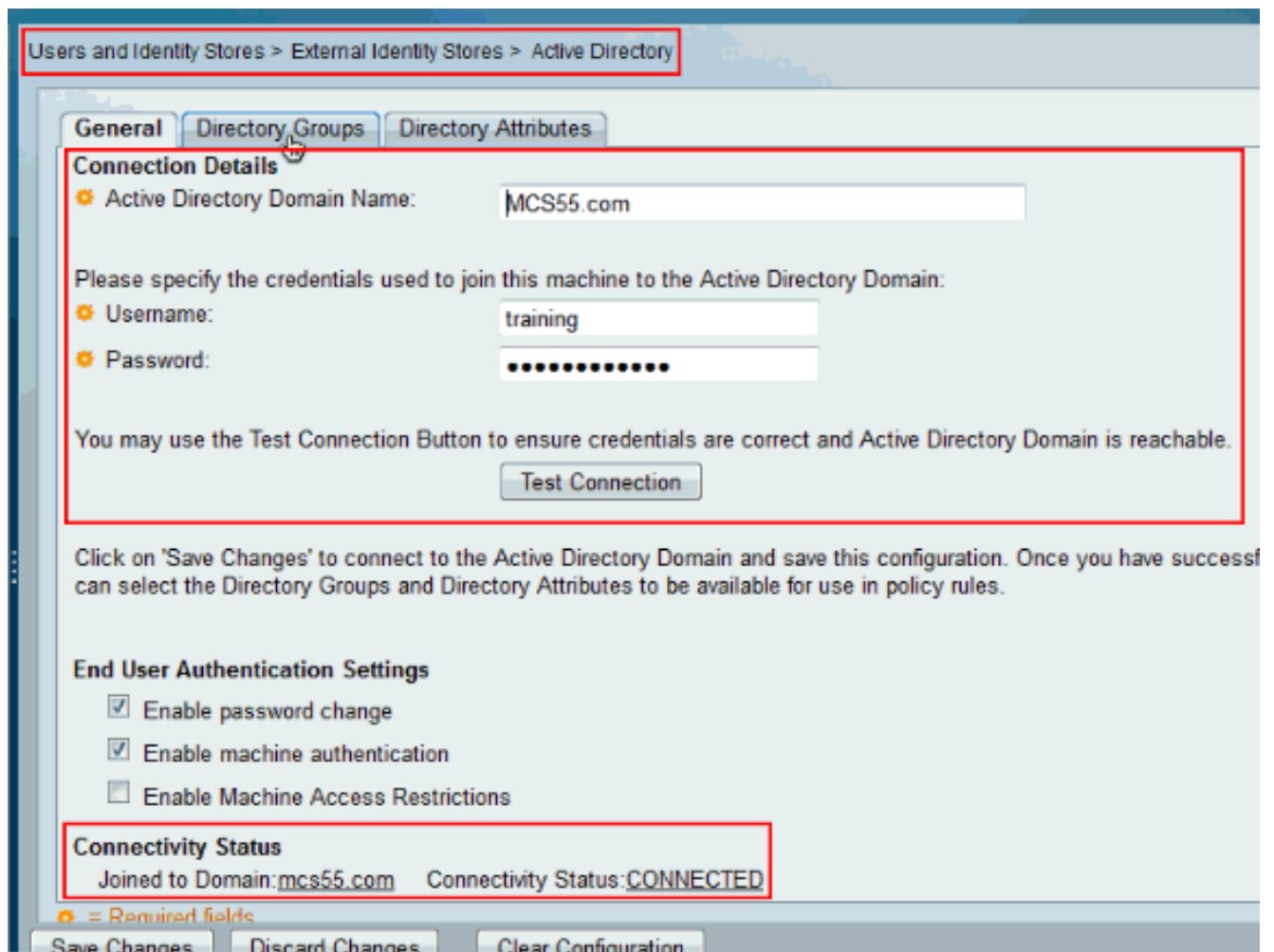
[Configuratie](#)

[ACS 5.x configureren voor verificatie en autorisatie](#)

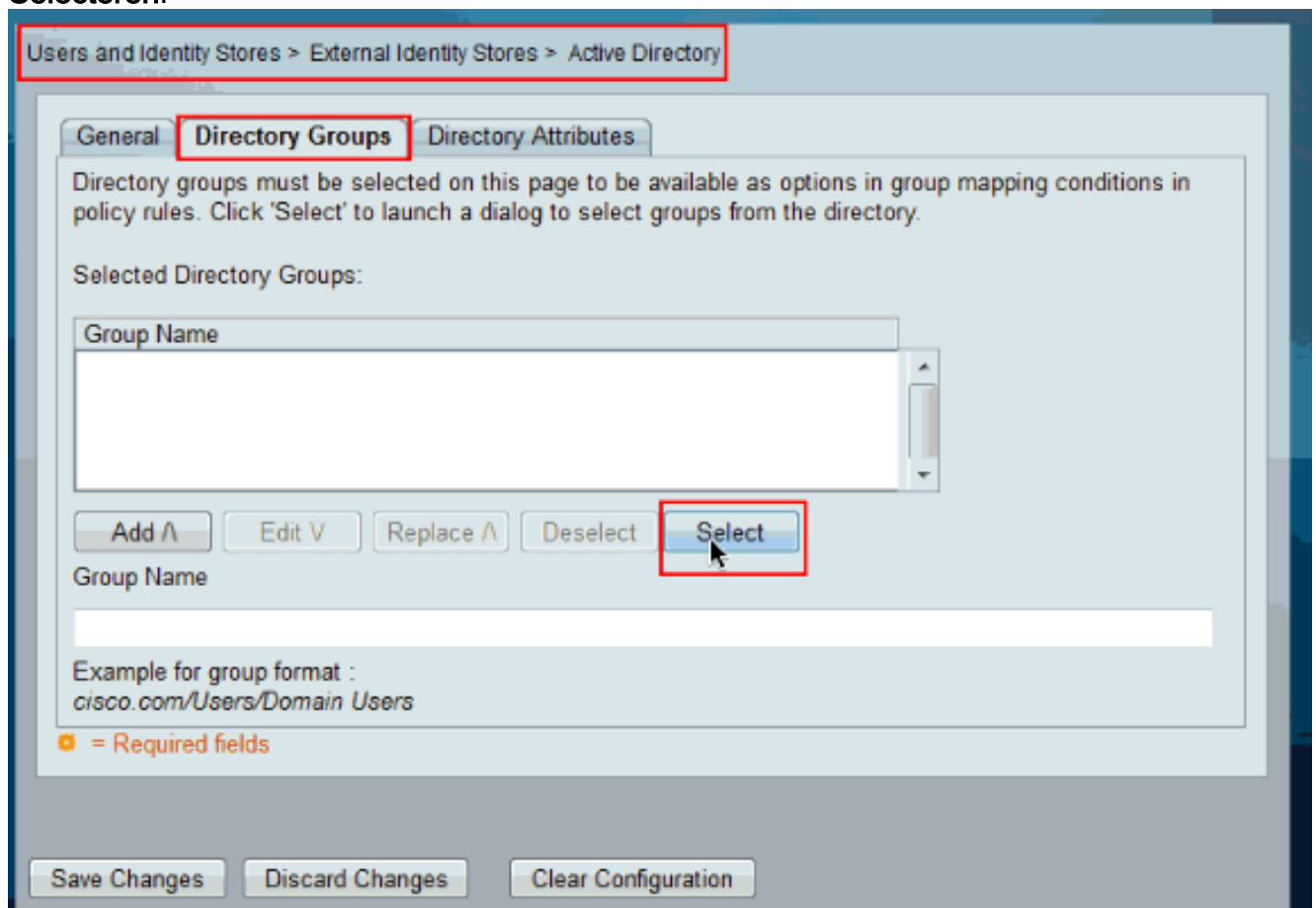
Voordat u begint met het configureren van de ACS 5.x voor verificatie en autorisatie, had ACS met succes geïntegreerd moeten zijn met Microsoft AD. Als ACS niet met het gewenste AD-domein is geïntegreerd, raadpleeg [ACS 5.x en hoger: Integratie met Microsoft Active Directory Configuration Voorbeeld](#) voor meer informatie om de integratietaak uit te voeren.

In deze sectie, kaart u twee AD groepen aan twee verschillende bevelreeksen en twee Shell profielen in, één met volledige toegang en de ander met beperkte toegang op de Cisco IOS apparaten.

1. Log in op de ACS GUI met Admin-referenties.
2. Kies **gebruikers en identiteitsopslag > Externe identiteitsopslag > Actieve map** en controleer of ACS zich bij het gewenste domein heeft aangesloten en ook of de **connectiviteit status** wordt weergegeven als **verbonden**. Klik op tabblad **Map groepen**.



3. Klik op
Selecteren.



4. Kies de groepen die aan de profielen van de Shell moeten worden toegewezen en de opdrachtsets in het latere deel van de configuratie. Klik op **OK**.

Group Name	Group Type
<input type="checkbox"/> MCS55.com/Users/Domain Guests	GLOBAL
<input checked="" type="checkbox"/> MCS55.com/Users/Network Admins	GLOBAL
<input checked="" type="checkbox"/> MCS55.com/Users/Network Maintenance Team	GLOBAL
<input type="checkbox"/> MCS55.com/Users/Schema Admins	UNIVERSAL

Database: **Active Directory**
Use * for wildcard search (i.e. admin*)
Search filter applies to group name and not the fully qualified path.

5. Klik op **Wijzigingen opslaan**.

Users and Identity Stores > External Identity Stores > Active Directory

General | **Directory Groups** | Directory Attributes

Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click 'Select' to launch a dialog to select groups from the directory.

Selected Directory Groups:

Group Name
MCS55.com/Users/Network Admins
MCS55.com/Users/Network Maintenance Team

Add ^ | Edit V | Replace ^ | Deselect | Select

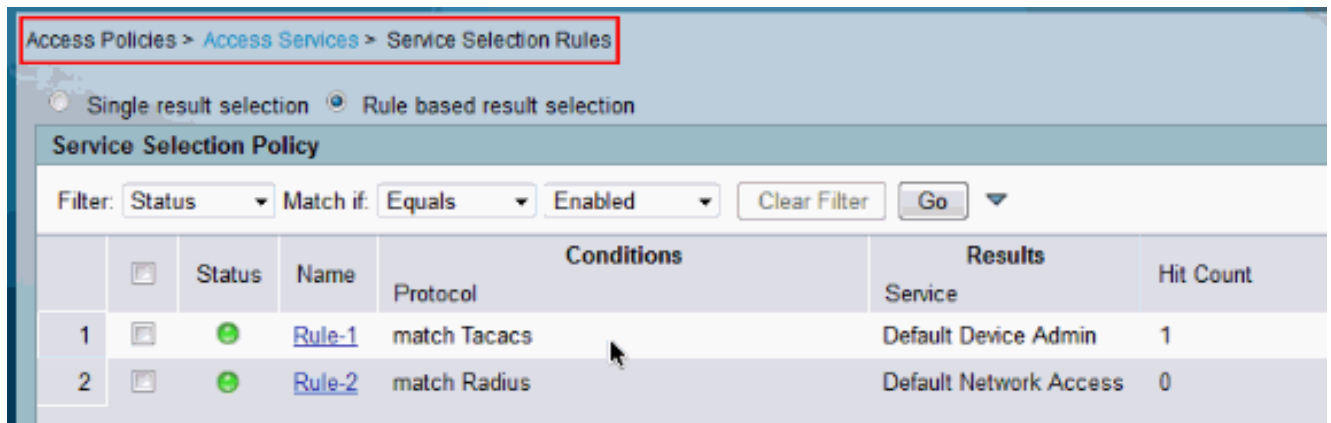
Group Name

Example for group format :
cisco.com/Users/Domain Users

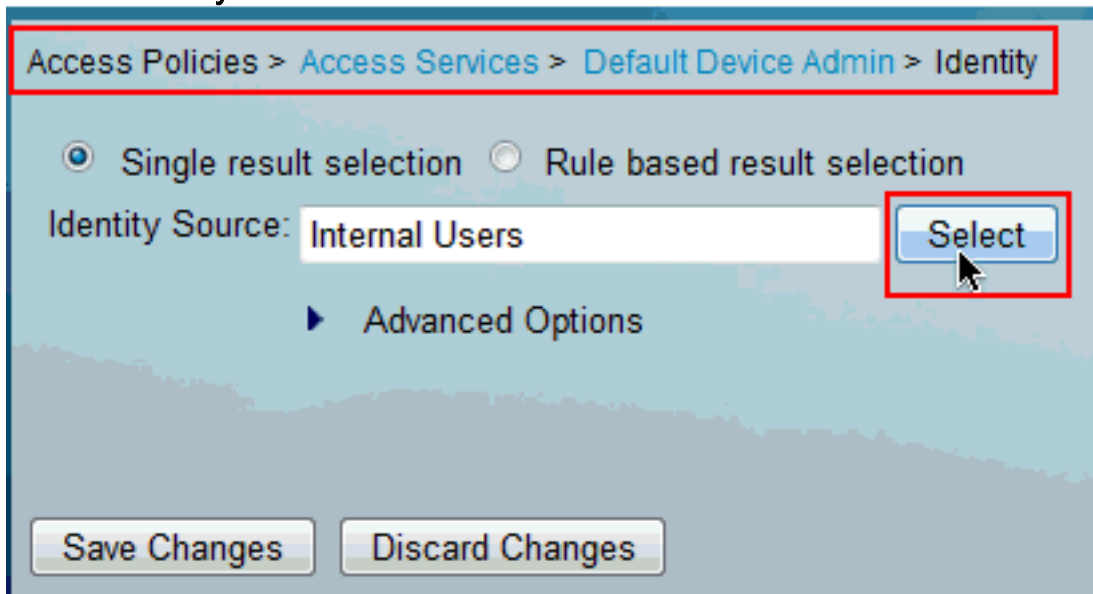
⚙ = Required fields

Save Changes | Discard Changes | Clear Configuration

6. Kies **Toegangsbeleid > Toegangsservices > Service selectieregels** en identificeer de toegangsservice die de TACACS+ verificatie verwerkt. In dit voorbeeld is het **standaard apparaatbeheer**.

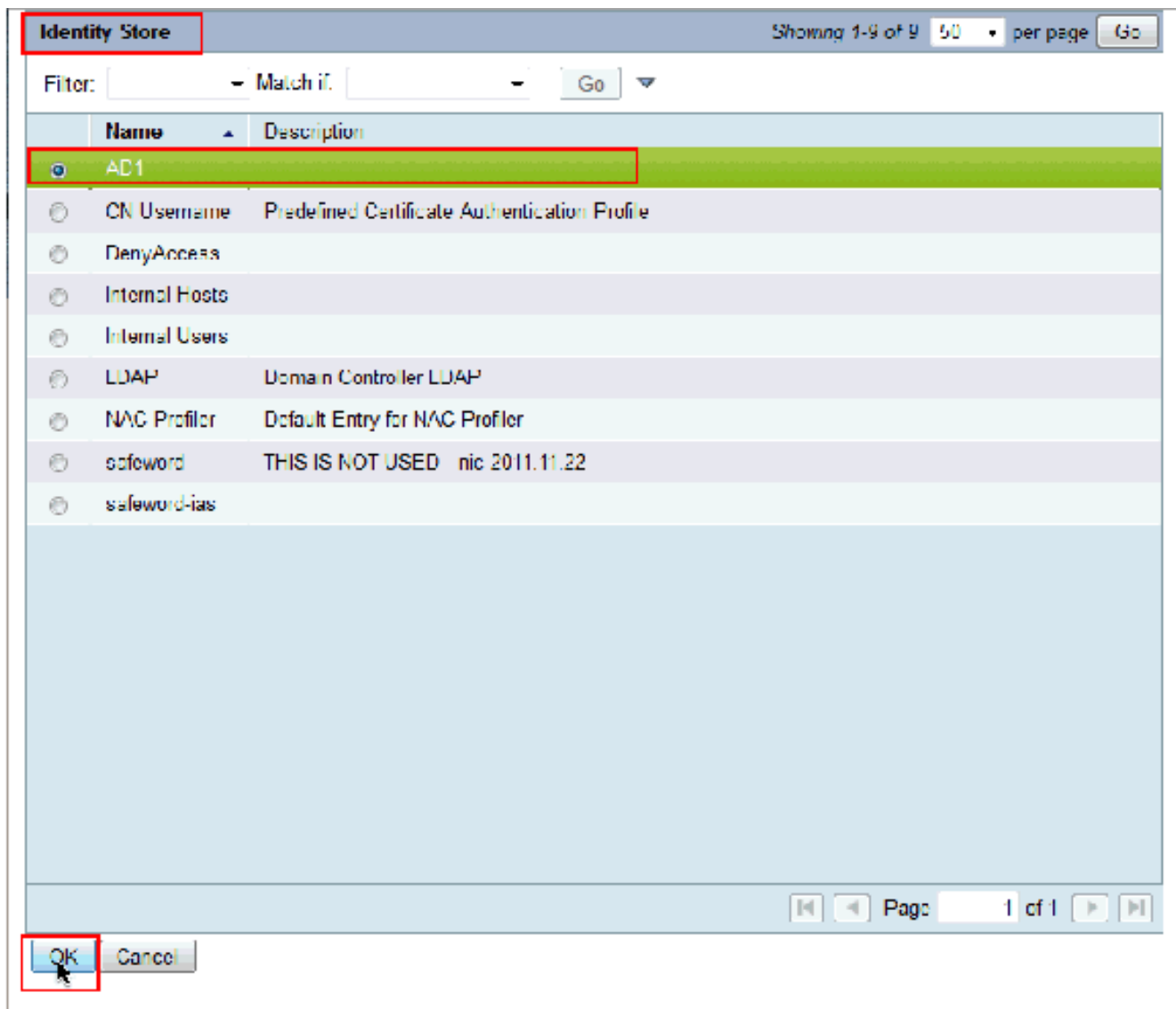


7. Kies Toegangsbeleid > Toegangsservices > Standaard Apparaatbeheer > Identity en klik op **Selecteer** naast Identity

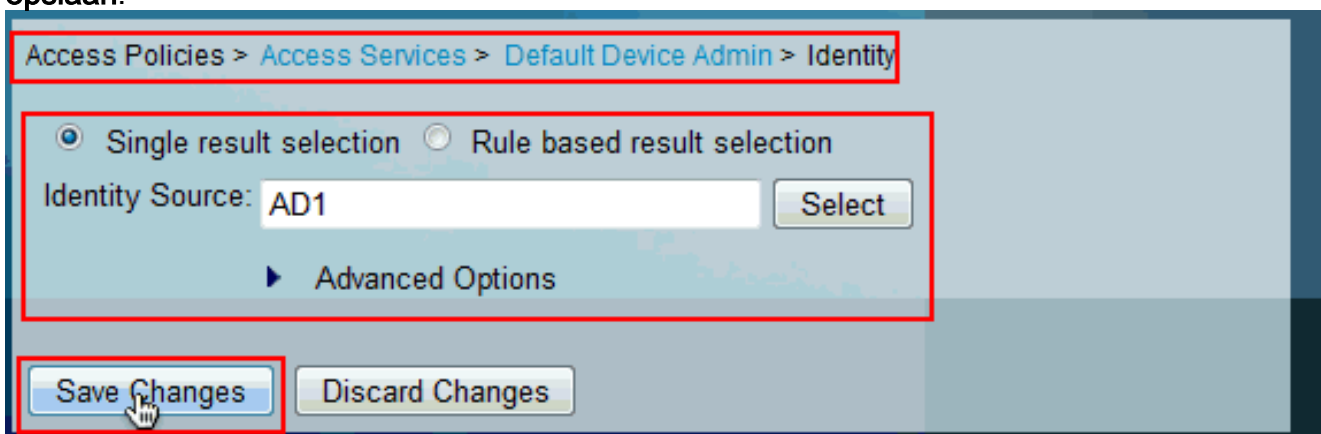


Source.

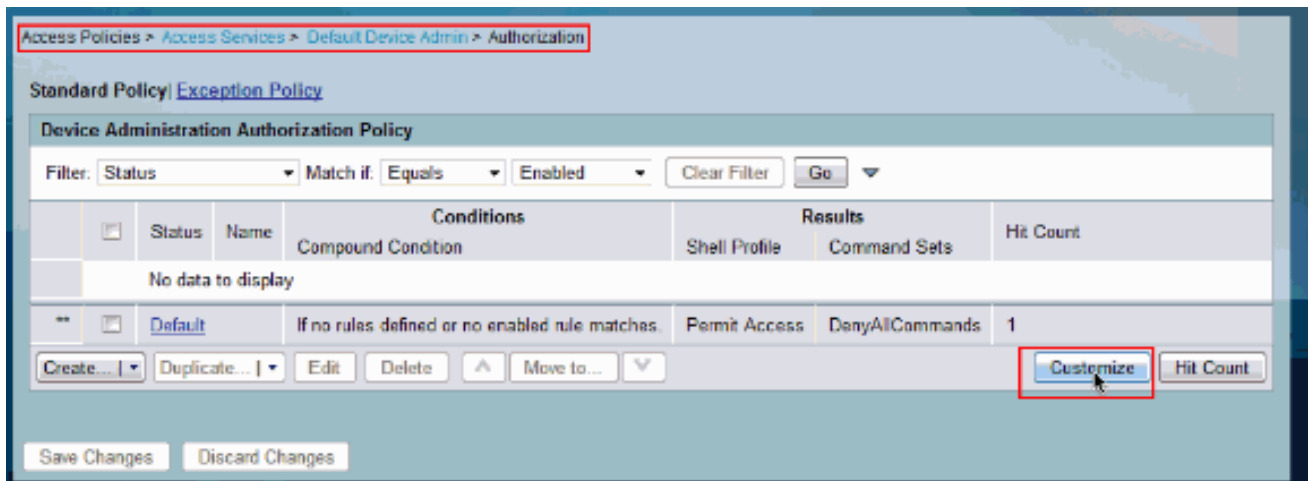
8. Kies **AD1** en klik op **OK**.



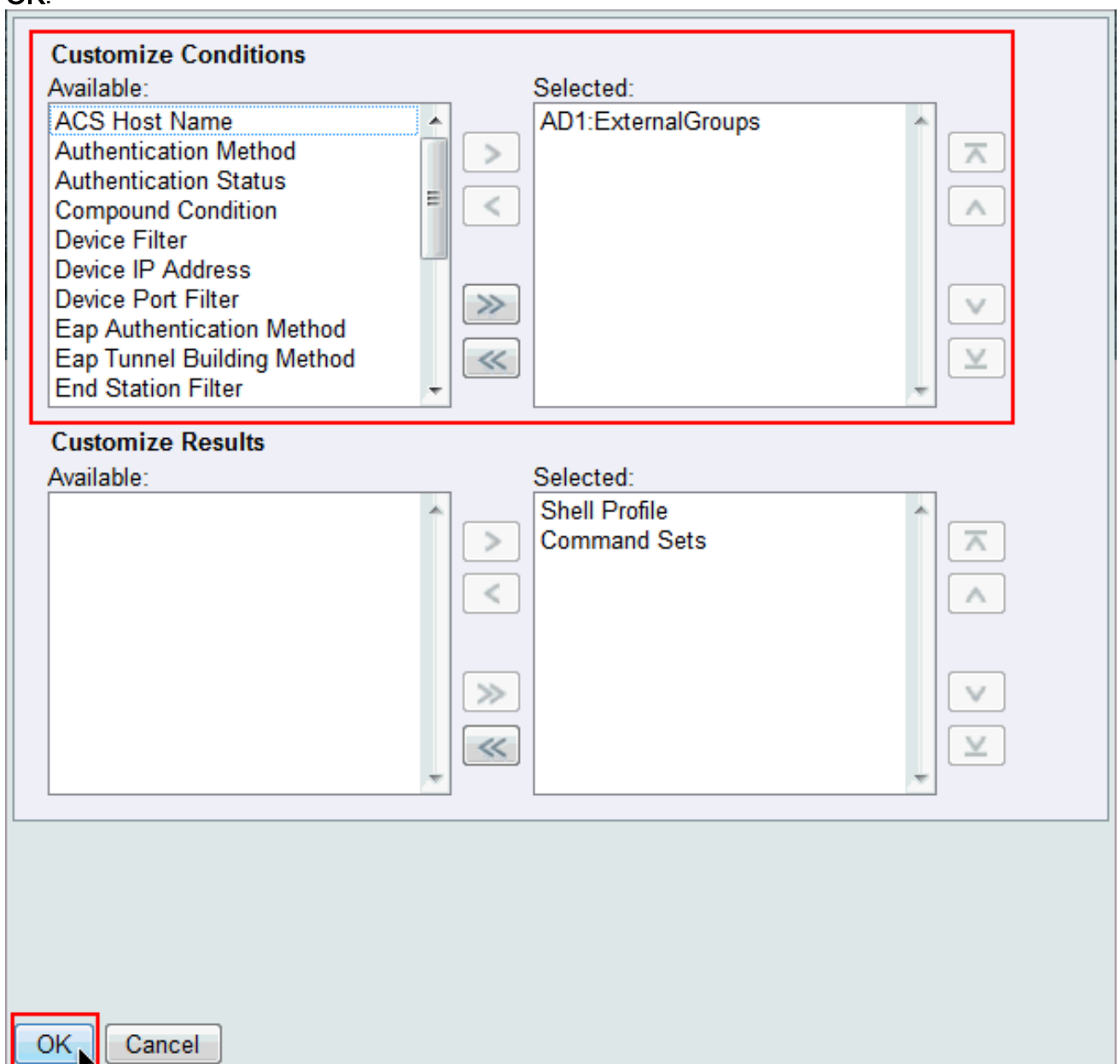
9. Klik op **Wijzigingen opslaan**.



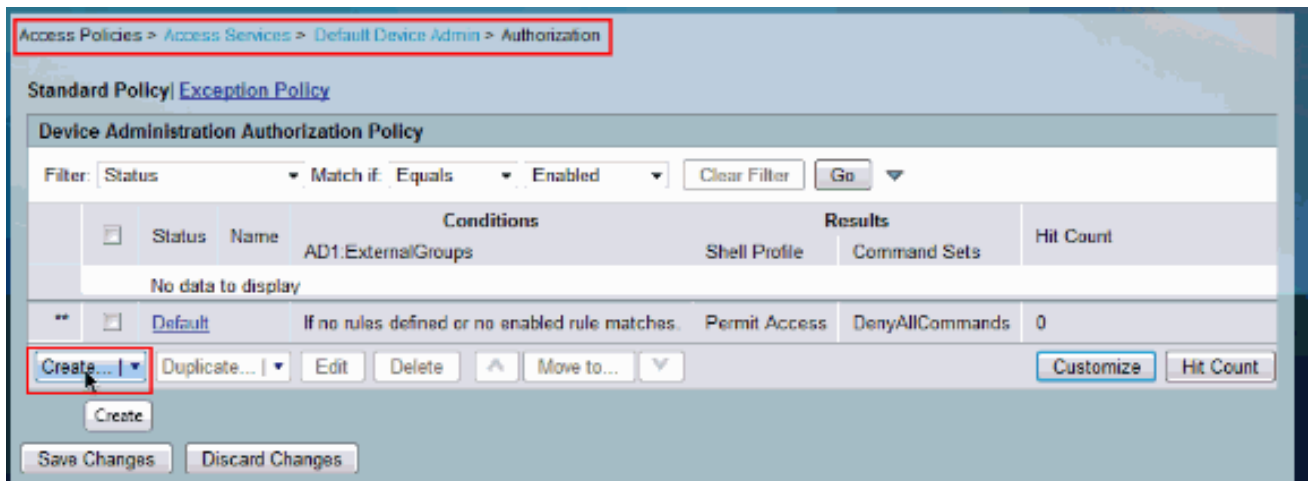
10. Kies **Toegangsbeleid > Toegangsservices > Standaard apparaatbeheer > autorisatie** en klik op **Aanpassen**.



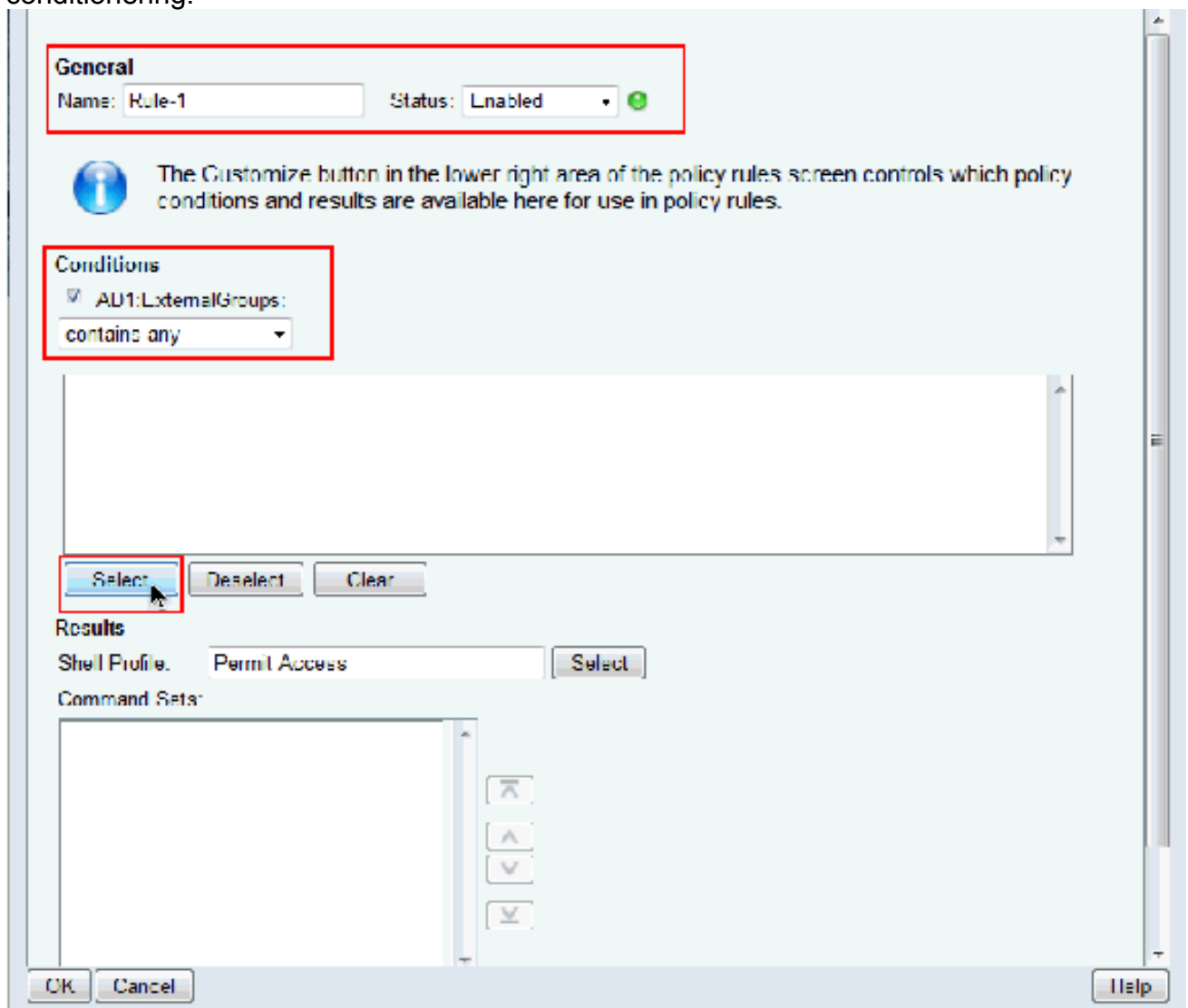
- Kopie AD1:Externe groepen van Beschikbaar tot geselecteerd gedeelte van Aangepaste condities en verplaats vervolgens Shell Profile en Commensets van Beschikbaar naar **Geselecteerd** gedeelte van Pas Resultaten aan. Klik nu op **OK**.



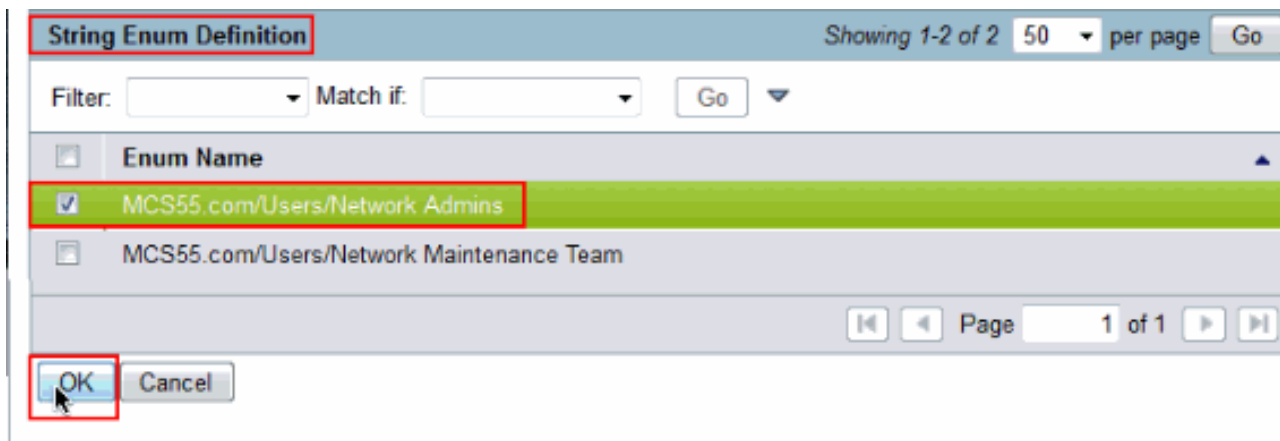
- Klik op **Maken** om een nieuwe Regel te maken.



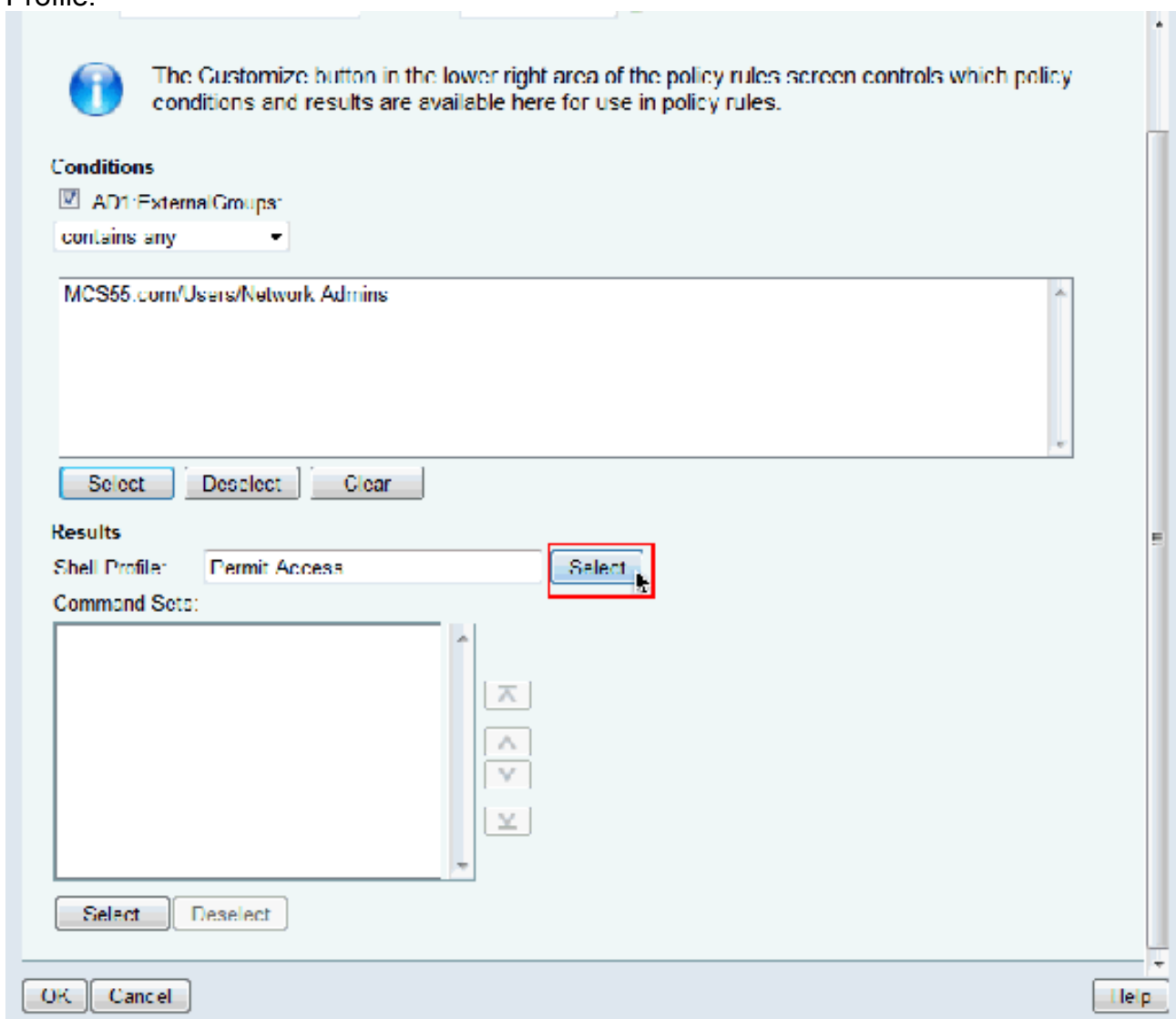
13. Klik op **Selecteren** in de **AD1:Externe Groepen** conditionering.



14. Kies de groep die u volledige toegang op het Cisco IOS apparaat wilt verlenen. Klik op **OK**.



15. Klik op **Selecteren** in het veld Shell Profile.



16. Klik op **Maken** om een nieuw **Shell-profiel** voor gebruikers van volledige toegang te maken.

General **Common Tasks** Custom Attributes

Privilege Level

Default Privilege: Static Value 15

Maximum Privilege: Static Value 15

Shell Attributes

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use

No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

Callback Line: Not in Use

Callback Rotary: Not in Use

⚙ = Required fields

Submit Cancel

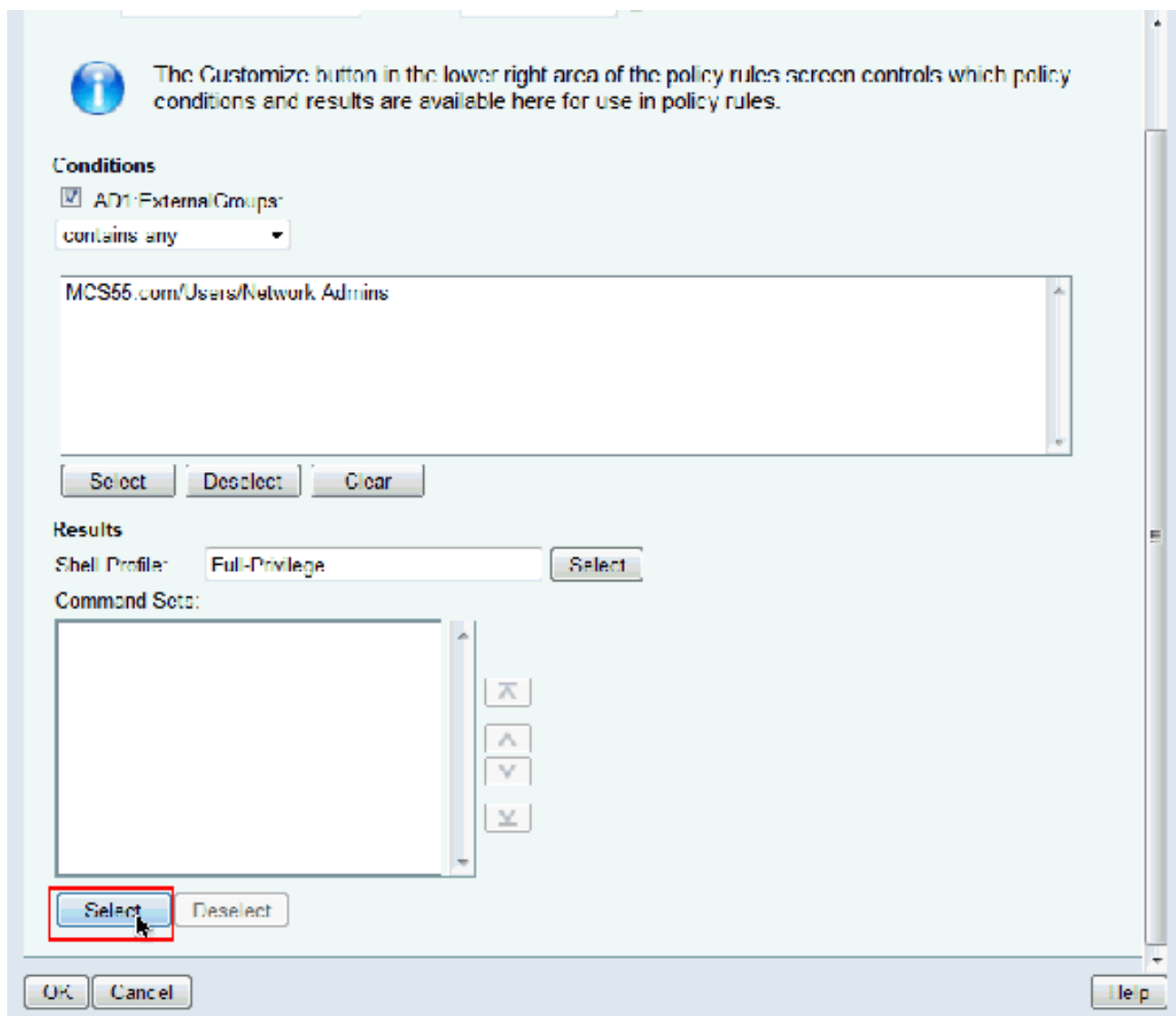
19. Kies nu het nieuwe gemaakte volledige **Shell Profile** van de toegang (Full-Priviool in dit voorbeeld) en klik **OK**.

Shell Profiles

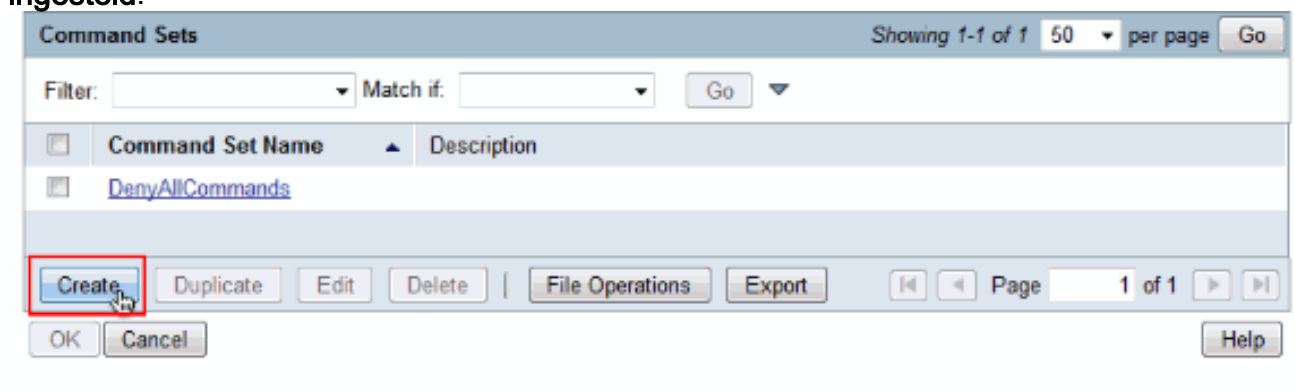
Filter: Match if:

	Name	Description
<input type="radio"/>	DenyAccess	
<input checked="" type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input type="radio"/>	Permit Access	

20. Klik op **Selecteren** in het veld
Opdrachten.



21. Klik op **Maken** om een nieuwe **Opdracht** te maken die voor gebruikers van de volledige Toegang is ingesteld.



22. Typ een naam en zorg ervoor dat het aanvinkvakje naast **Geef toe** dat een opdracht die niet in de onderstaande tabel staat, is ingeschakeld. Klik op **Inzenden**. N.B.: Raadpleeg [Opdrachtsets maken, kopiëren en bewerken voor apparaatbeheer](#) voor meer informatie over opdrachtsets.

General

Name:
Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

23. Klik op
OK.

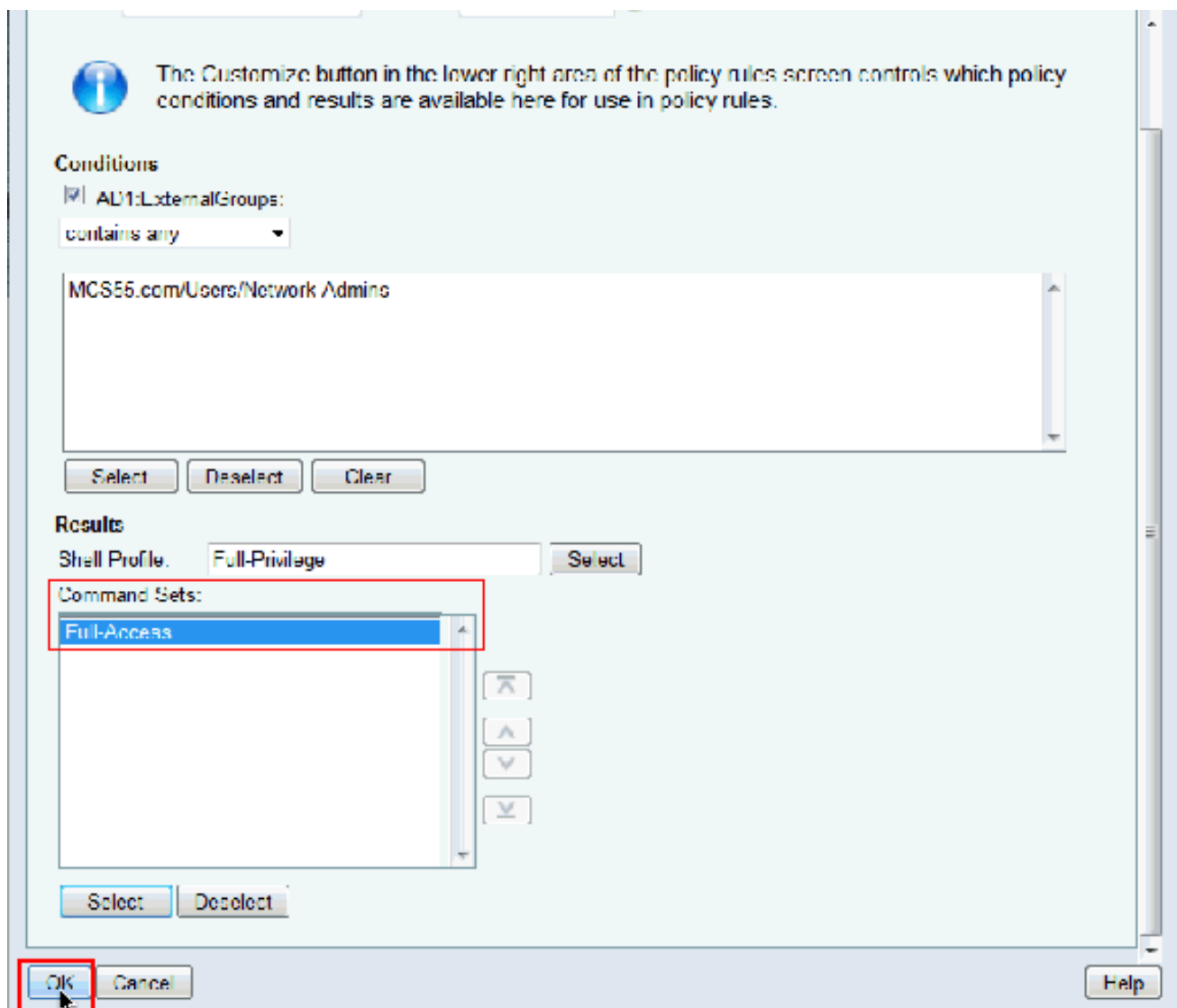
Command Sets

Filter: Match if:

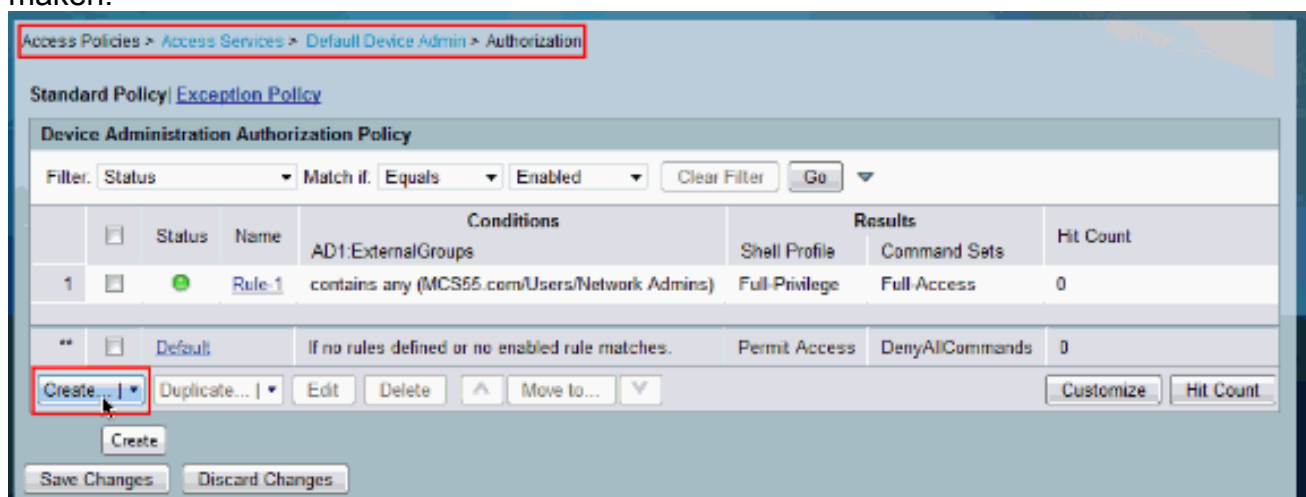
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

|

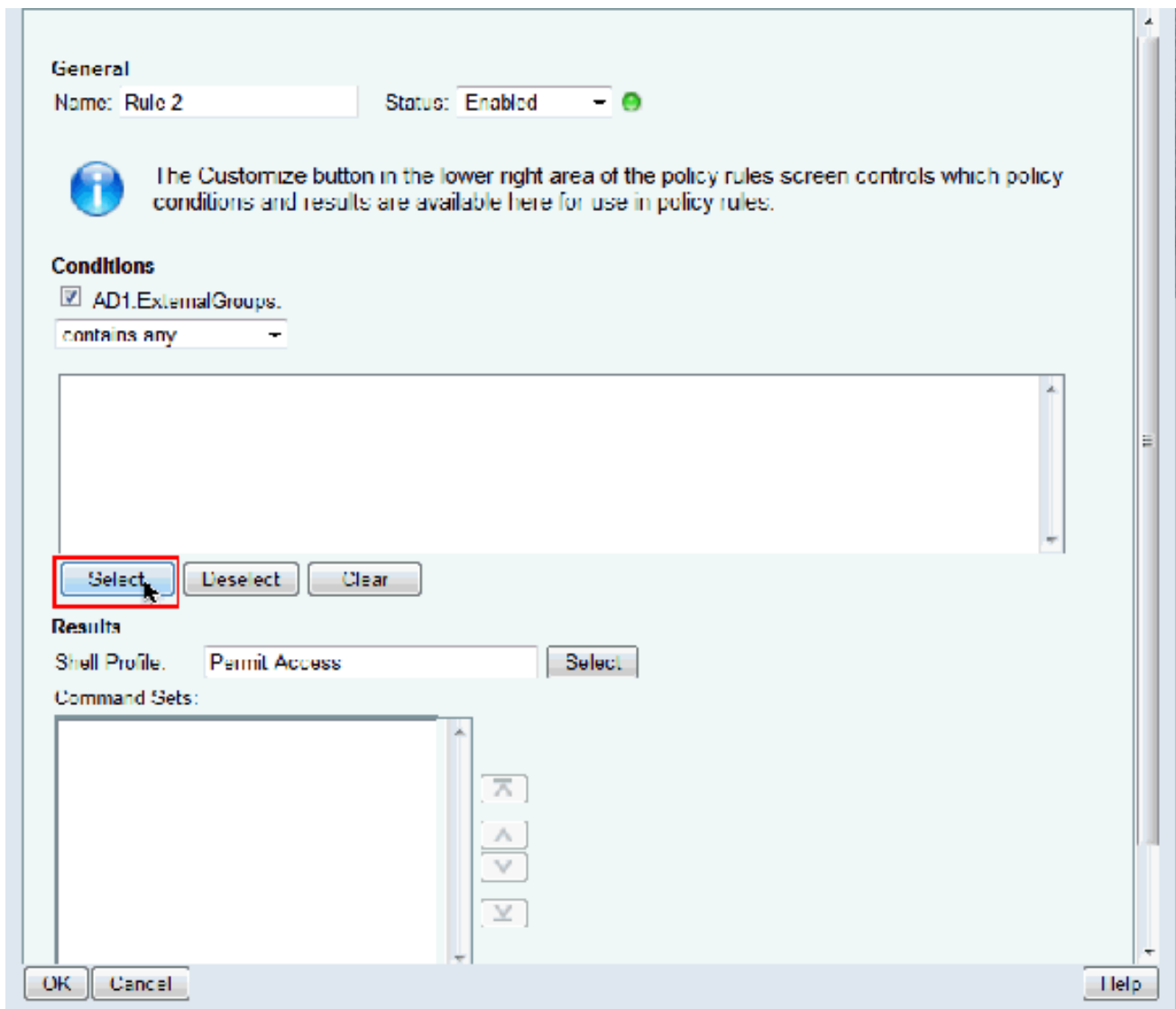
24. Klik op **OK**. Dit voltooit de configuratie van **regel 1**.



25. Klik op **Maken** om een nieuwe Regel voor **bepaalde** gebruikers te maken.



26. Kies **AD1:Externe groepen** en klik op **Selecteren**.



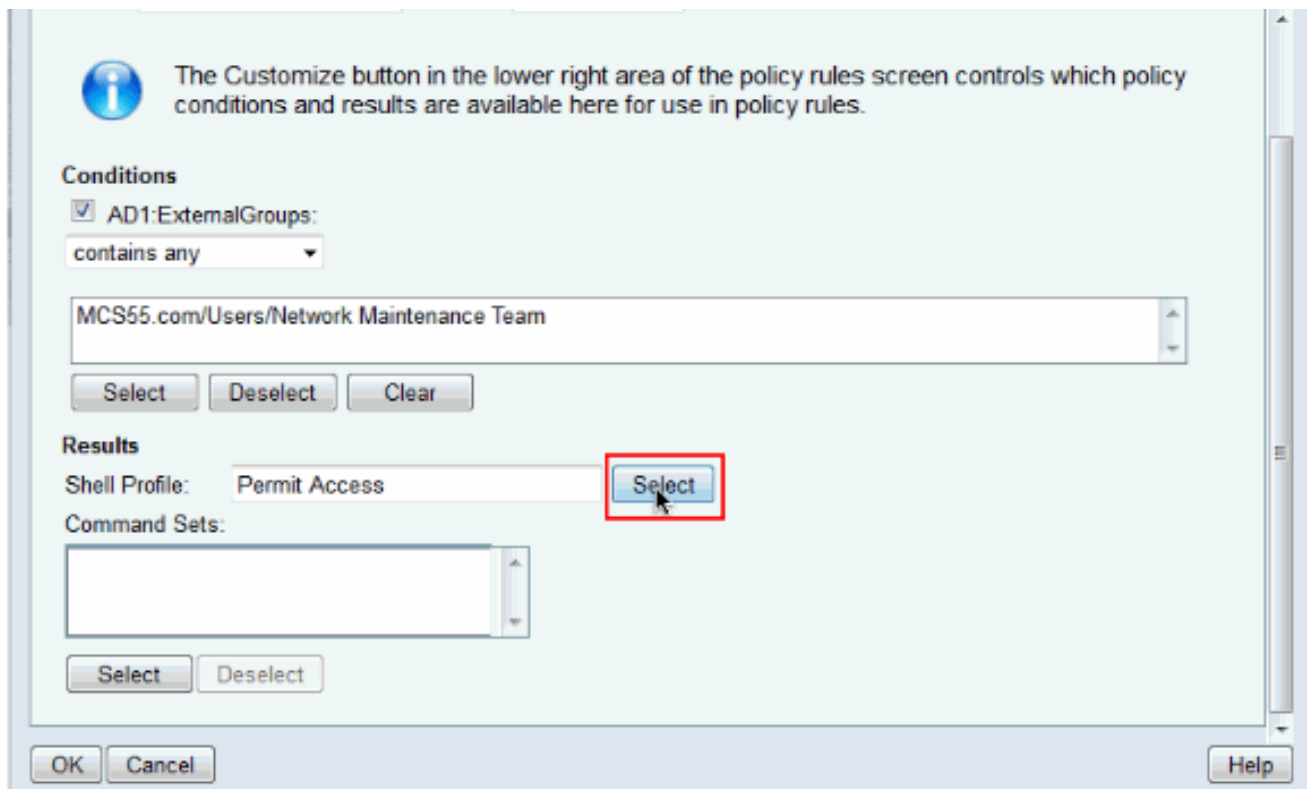
27. Kies de groep (of) groepen waartoe u beperkte toegang wilt verlenen en klik op OK.

String Enum Definition

Filter: Match if: Go

<input type="checkbox"/>	Enum Name
<input type="checkbox"/>	MCS55.com/Users/Network Admins
<input checked="" type="checkbox"/>	MCS55.com/Users/Network Maintenance Team

28. Klik op **Selecteren** in het veld Shell Profile.



29. Klik op **Create** om een nieuw **Shell-profiel** te maken voor beperkte toegang.

Shell Profiles

Filter: Match if:

	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input type="radio"/>	Permit Access	

30. Typ een **naam** en **omschrijving** (optioneel) in het **tabblad Algemeen** en klik op het tabblad **Gemeenschappelijk Taken**.

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

⚙ = Required fields

31. Verander de **standaard** en de **maximale** prioriteit in **Statisch** met respectievelijk **1** en **15**. Klik op **Inzenden**.

General

Common Tasks

Custom Attributes

Privilege Level

Default Privilege: Static Value 1

Maximum Privilege: Static Value 15

Shell Attributes

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use

No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

Callback Line: Not in Use

Callback Rotary: Not in Use

 = Required fields

Submit

Cancel

32. Klik op

Shell Profiles

Filter: Match if: Go

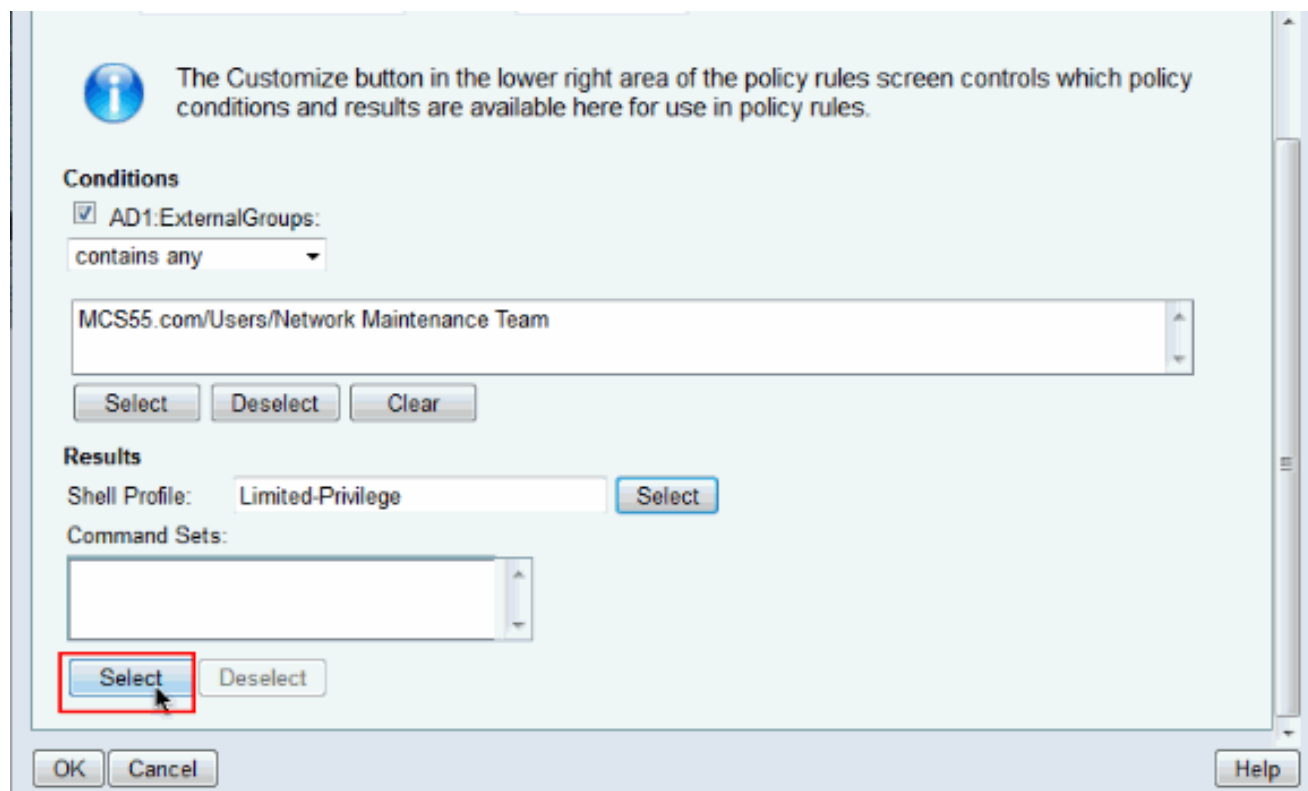
	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input checked="" type="radio"/>	Limited-Privilege	To push default privilege 1 for IOS
<input type="radio"/>	Permit Access	

Create Duplicate Edit Delete

OK Cancel

OK.

33. Klik op **Selecteren** in het veld
Opdrachten.



34. Klik op **Maken** om een nieuwe **Opdracht** te maken **die** voor de beperkte toegangsgroep is ingesteld.

Command Sets

Filter: Match if:

<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input type="checkbox"/>	Full-Access	

|

35. Geef een **naam op** en controleer of het selectieteken naast **Toestaan dat een opdracht die niet in de onderstaande tabel staat**, niet is geselecteerd. Klik op **Add** na het typen van **show** in de ruimte in het opdrachtgedeelte en kies **Toestemming** in het vak **Grant** zodat alleen de **showopdrachten** voor de gebruikers in het vak **beperkte toegang** zijn toegestaan.

General

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

36. Voeg ook andere opdrachten toe die voor de gebruikers in de groep met beperkte toegang moeten worden toegestaan met het gebruik van **Add**. Klik op **Inzenden**. **N.B.:** Raadpleeg [Opdrachtsets maken, kopiëren en bewerken voor apparaatbeheer](#) voor meer informatie over opdrachtsets.

General

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command:

Arguments:

Select Command/Arguments from Command Set:

37. Klik op
OK.

Command Sets

Filter: Match if:

<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input type="checkbox"/>	Full-Access	
<input checked="" type="checkbox"/>	Show-Access	

|

38. Klik op
OK.



The Customize button in the lower right area of the policy rules screen conditions and results are available here for use in policy rules.

Conditions

AD1:ExternalGroups:

contains any

MCS55.com/Users/Network Maintenance Team

Select

Deselect

Clear

Results

Shell Profile: Limited-Privilege

Select

Command Sets:

Show-Access

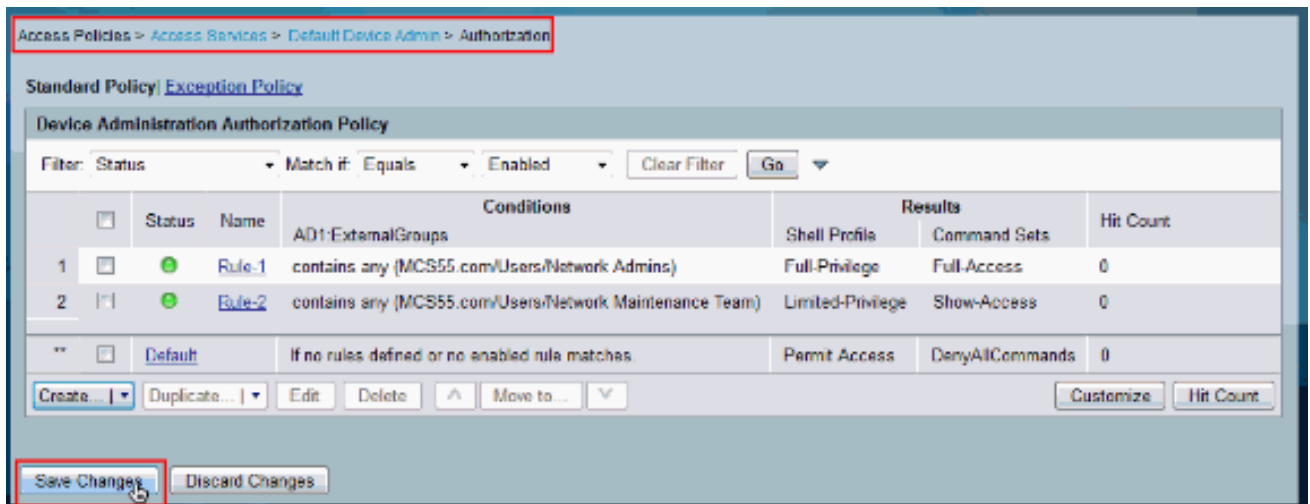
Select

Deselect

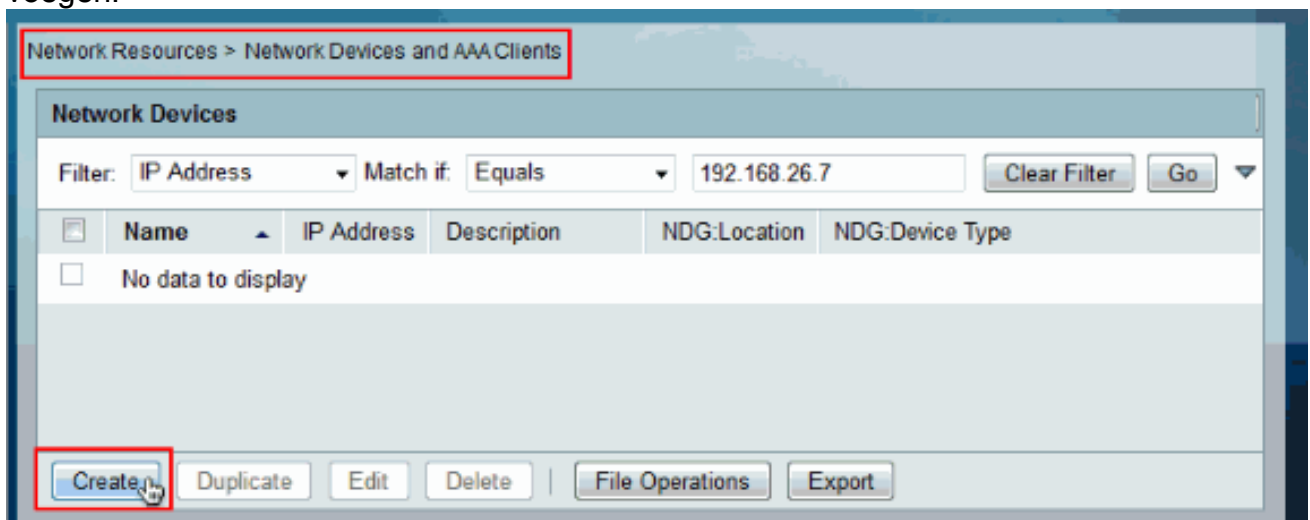
OK

Cancel

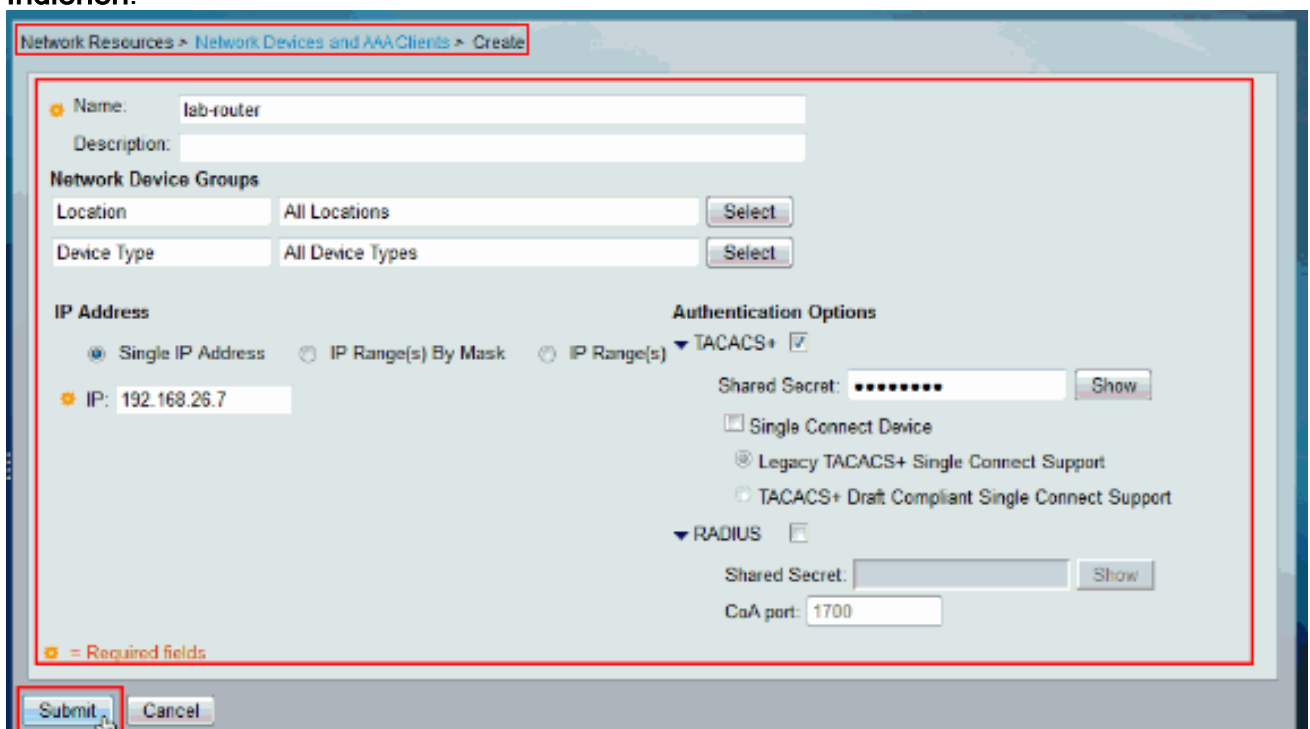
39. Klik op **Wijzigingen opslaan**.



40. Klik op **Create** om het **Cisco IOS**-apparaat als **AAA-client** aan de ACS toe te voegen.



41. Geef een naam, IP-adres, gedeeld geheim voor TACACS+ en klik op **Indienen**.



[Configureer het Cisco IOS-apparaat voor verificatie en autorisatie](#)

Voltooi deze stappen om Cisco IOS apparaat en ACS voor verificatie en autorisatie te configureren.

1. Maak een lokale gebruiker met volledig privilege voor back-up met de opdracht **gebruikersnaam** zoals hier wordt getoond:

```
username admin privilege 15 password 0 cisco123!
```

2. Geef het IP-adres van de ACS op om AAA in te schakelen en ACS 5.x als TACACS-server toe te voegen.

```
aaa new-model  
tacacs-server host 192.168.26.51 key cisco123
```

Opmerking: de toets moet overeenkomen met het gedeelde geheim dat op het ACS voor dit Cisco IOS-apparaat is meegeleverd.

3. Test de bereikbaarheid van de TACACS-server met de opdracht **testgebied** zoals getoond.

```
test aaa group tacacs+ user1 xxxxx legacy  
Attempting authentication test to server-group tacacs+ using tacacs+  
User was successfully authenticated.
```

De uitvoer van de vorige opdracht toont aan dat de TACACS-server bereikbaar is en dat de gebruiker geauthentiseerd is. **Opmerking:** Gebruiker1 en wachtwoord xxx behoren tot AD. Als de test mislukt, zorg er dan voor dat het gedeelde geheim in de vorige stap juist is.

4. Configureer de inlognaam en voer authenticaties in en gebruik vervolgens de EXEC- en opdrachtautorisaties zoals hier wordt getoond:

```
aaa authentication login default group tacacs+ local  
aaa authentication enable default group tacacs+ enable  
aaa authorization exec default group tacacs+ local  
aaa authorization commands 0 default group tacacs+ local  
aaa authorization commands 1 default group tacacs+ local  
aaa authorization commands 15 default group tacacs+ local  
aaa authorization config-commands
```

Opmerking: De lokale en Enable sleutelwoorden worden gebruikt voor back-up naar de lokale gebruiker van Cisco IOS en maken geheim als de TACACS-server onbereikbaar is.

Verifiëren

Om verificatie van verificatie en autorisatie kunt u inloggen op het Cisco IOS-apparaat door telnet.

1. Telnet aan het Cisco IOS apparaat als gebruiker1 die tot de volledige toegangsgroep in AD behoort. De groep Network Admins is de groep in AD die in kaart wordt gebracht aan het Full-Priviool Shell Profile en Full-Access Commision dat op de ACS is ingesteld. Probeer elke opdracht uit te voeren om er zeker van te zijn dat u volledige toegang hebt.

```
username: user1
password:

router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#router rip
router1(config-router)#version 2
router1(config-router)#exit
router1(config)#exit
router1#
```

2. Telnet aan het Cisco IOS apparaat als gebruiker2 die tot de groep van de beperkte toegang in AD. (de groep van het **Team van het Netwerk** is de groep in AD die aan het **Beperkte** van de **Shell** van het **Priverecht** en van de **show** van de Toegang in kaart wordt gebracht). Als u een opdracht anders probeert uit te voeren dan de opdrachten die in de opdrachtset voor Show-Access worden genoemd, krijgt u een fout voor `Opdrachtautorisatie`, die aantoont dat user2 beperkte toegang heeft.

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

AAA Protocol > TACACS+ Authorization

Authorization Status : Pass or Fail
Date : June 08, 2012

Generated on June 8, 2012 11:57:34 AM IST

Reload

✔=Pass ✖=Fail 🔍=Click for details

ACS View Timestamp	ACS Timestamp	Status	Details	Failure Reason	User Name	Command Set	Shell Profile	Network Device
Jun 8,12 6:21:19.410 AM	Jun 8,12 6:21:19.393 AM	✔			user2	[CmdA]write		lab-cosmos
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.793 AM	✖		11025 Command failed to match a Permit rule	user2	[CmdA]write memory		lab-cosmos
Jun 8,12 6:20:59.999 AM	Jun 8,12 6:20:59.830 AM	✖		11024 Command failed to match a Permit rule	user2	[CmdA]configure terminal		lab-cosmos
Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50.056 AM	✔			user2	[CmdA]show version		lab-cosmos
Jun 8,12 6:20:38.506 AM	Jun 8,12 6:20:38.490 AM	✔			user2	[CmdA]enable		lab-cosmos
Jun 8,12 6:20:34.426 AM	Jun 8,12 6:20:34.406 AM	✔			user2	[CmdA]=	Limited-Privilege	lab-cosmos
				Commands run by user 2				
Jun 8,12 6:20:02.616 AM	Jun 8,12 6:20:02.596 AM	✔			user1	[CmdA]write		lab-cosmos
Jun 8,12 6:20:00.265 AM	Jun 8,12 6:20:00.246 AM	✔			user1	[CmdA]version 2		lab-cosmos
Jun 8,12 6:19:57.203 AM	Jun 8,12 6:19:57.200 AM	✔			user1	[CmdA]router rip		lab-cosmos
Jun 8,12 6:19:55.103 AM	Jun 8,12 6:19:55.076 AM	✔			user1	[CmdA]configure terminal		lab-cosmos
Jun 8,12 6:19:52.743 AM	Jun 8,12 6:19:52.740 AM	✔			user1	[CmdA]=	Full-Privilege	lab-cosmos
				Commands run by user1				

Gerelateerde informatie

- [Cisco Secure Access Control-system](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)