

ACS 5.x: Esempio di configurazione dell'autenticazione TACACS+ e dell'autorizzazione dei comandi in base all'appartenenza al gruppo AD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Configurazione di ACS 5.x per l'autenticazione e l'autorizzazione](#)

[Configurare il dispositivo Cisco IOS per l'autenticazione e l'autorizzazione](#)

[Verifica](#)

[Informazioni correlate](#)

[Introduzione](#)

Questo documento offre un esempio di configurazione dell'autenticazione TACACS+ e dell'autorizzazione dei comandi in base all'appartenenza al gruppo AD di un utente con Cisco Secure Access Control System (ACS) 5.x e versioni successive. ACS utilizza Microsoft Active Directory (AD) come archivio identità esterno per archiviare risorse quali utenti, computer, gruppi e attributi.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- ACS 5.x è completamente integrato nel dominio AD desiderato. Se l'ACS non è integrato con il dominio AD desiderato, consultare [ACS 5.x e versioni successive: Integrazione con la configurazione di Microsoft Active Directory Esempio](#) per ulteriori informazioni sull'esecuzione dell'attività di integrazione.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Secure ACS 5.3
- Software Cisco IOS[®] versione 12.2(44)SE6.**Nota:** questa configurazione può essere eseguita su tutti i dispositivi Cisco IOS.
- Dominio di Microsoft Windows Server 2003

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

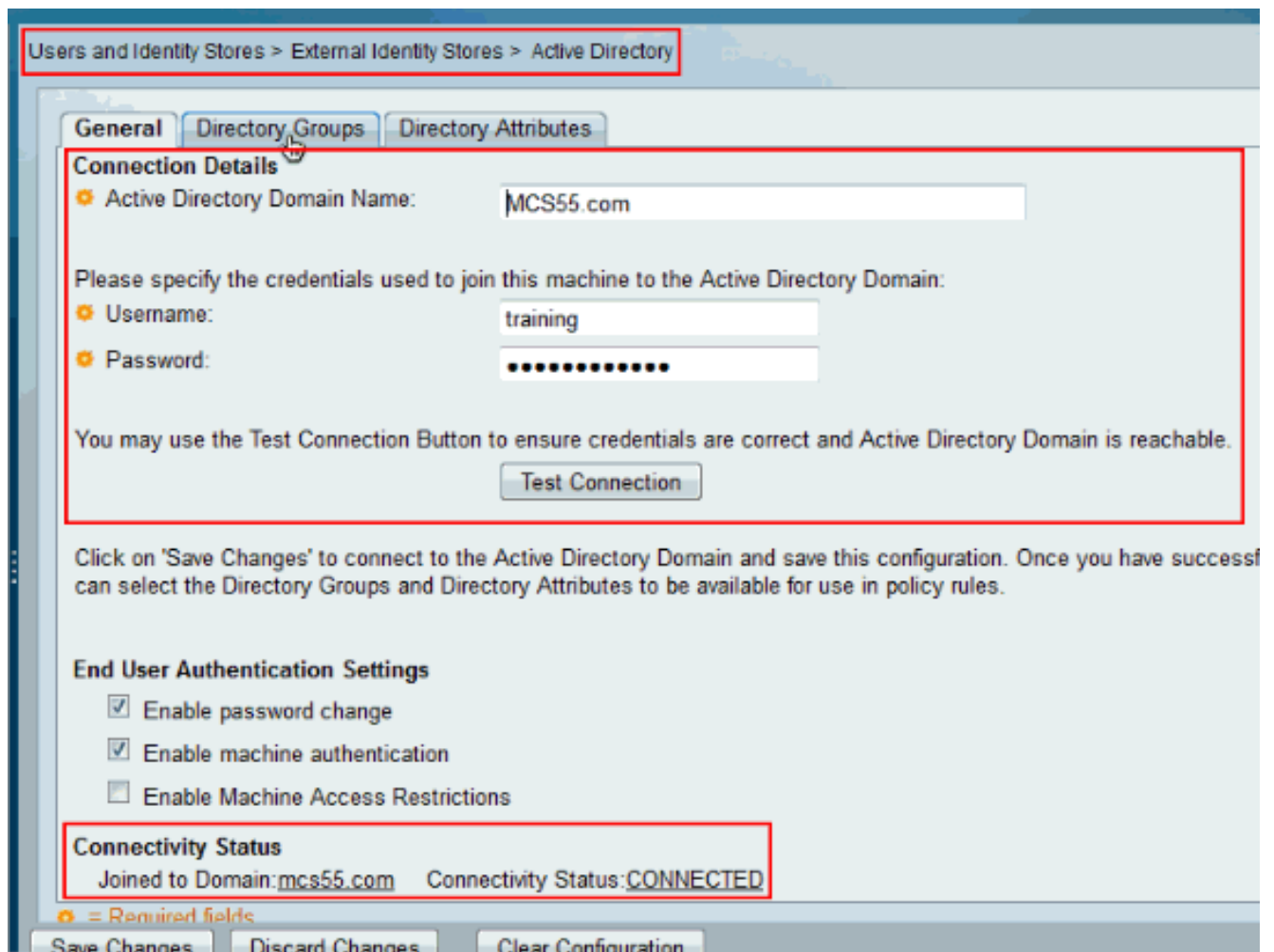
Configurazione

Configurazione di ACS 5.x per l'autenticazione e l'autorizzazione

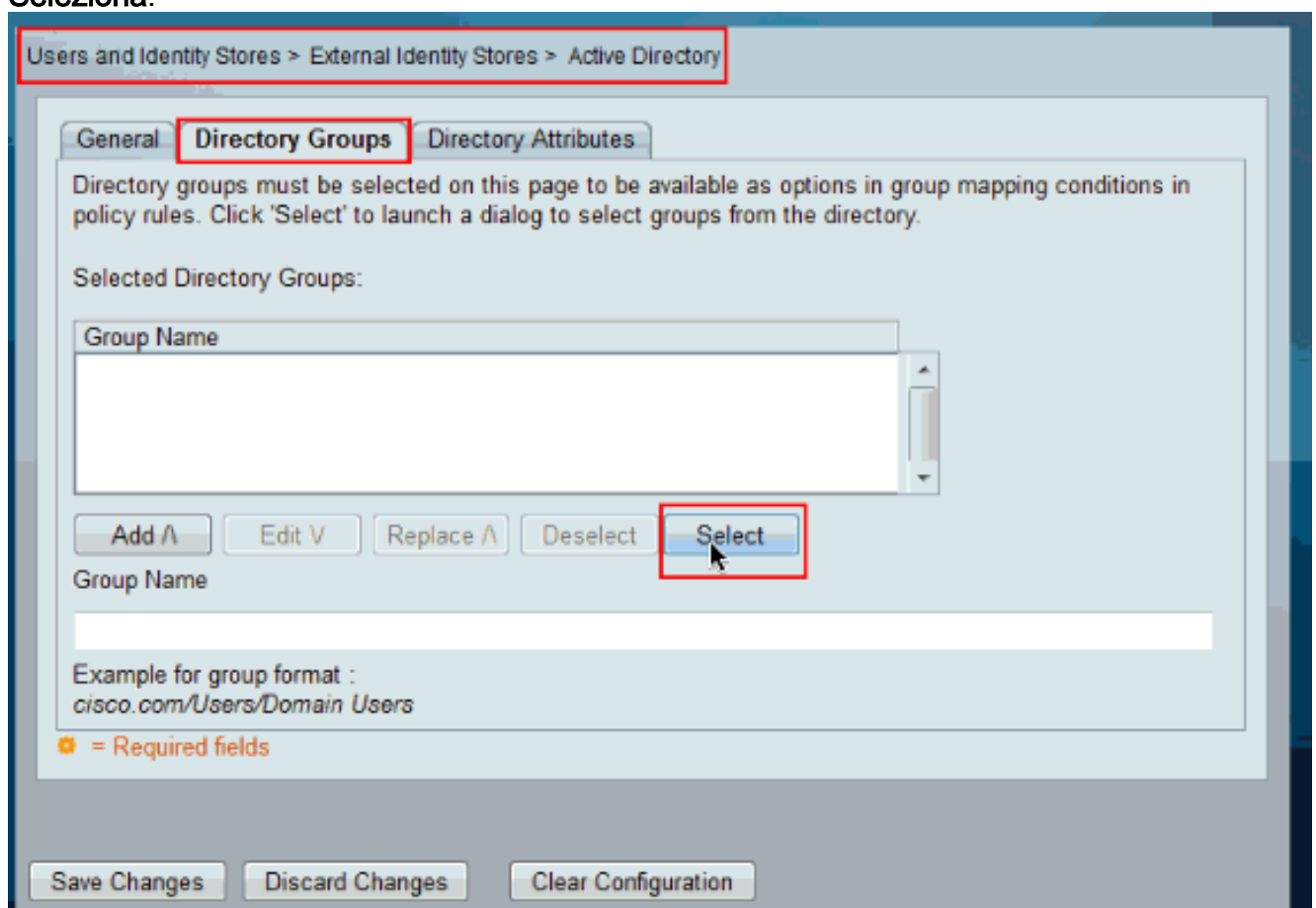
Prima di iniziare la configurazione di ACS 5.x per l'autenticazione e l'autorizzazione, ACS avrebbe dovuto essere integrato correttamente con Microsoft AD. Se l'ACS non è integrato con il dominio AD desiderato, consultare [ACS 5.x e versioni successive: Integrazione con la configurazione di Microsoft Active Directory Esempio](#) per ulteriori informazioni sull'esecuzione dell'attività di integrazione.

In questa sezione vengono mappati due gruppi AD a due set di comandi diversi e a due profili Shell, uno con accesso completo e l'altro con accesso limitato sui dispositivi Cisco IOS.

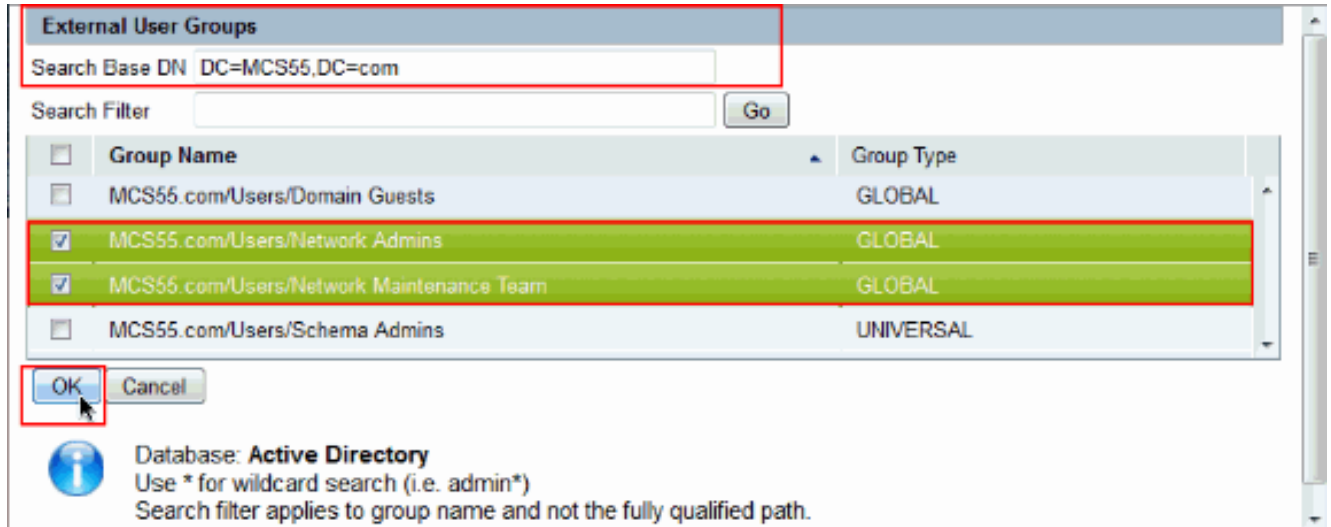
1. Accedere alla GUI di ACS utilizzando le credenziali di amministratore.
2. Scegliere **Utenti e archivi identità > Archivi identità esterni > Active Directory** e verificare che l'ACS sia stato aggiunto al dominio desiderato e che lo **stato della connettività** sia indicato come **connesso**. Fare clic sulla scheda **Gruppi di directory**.



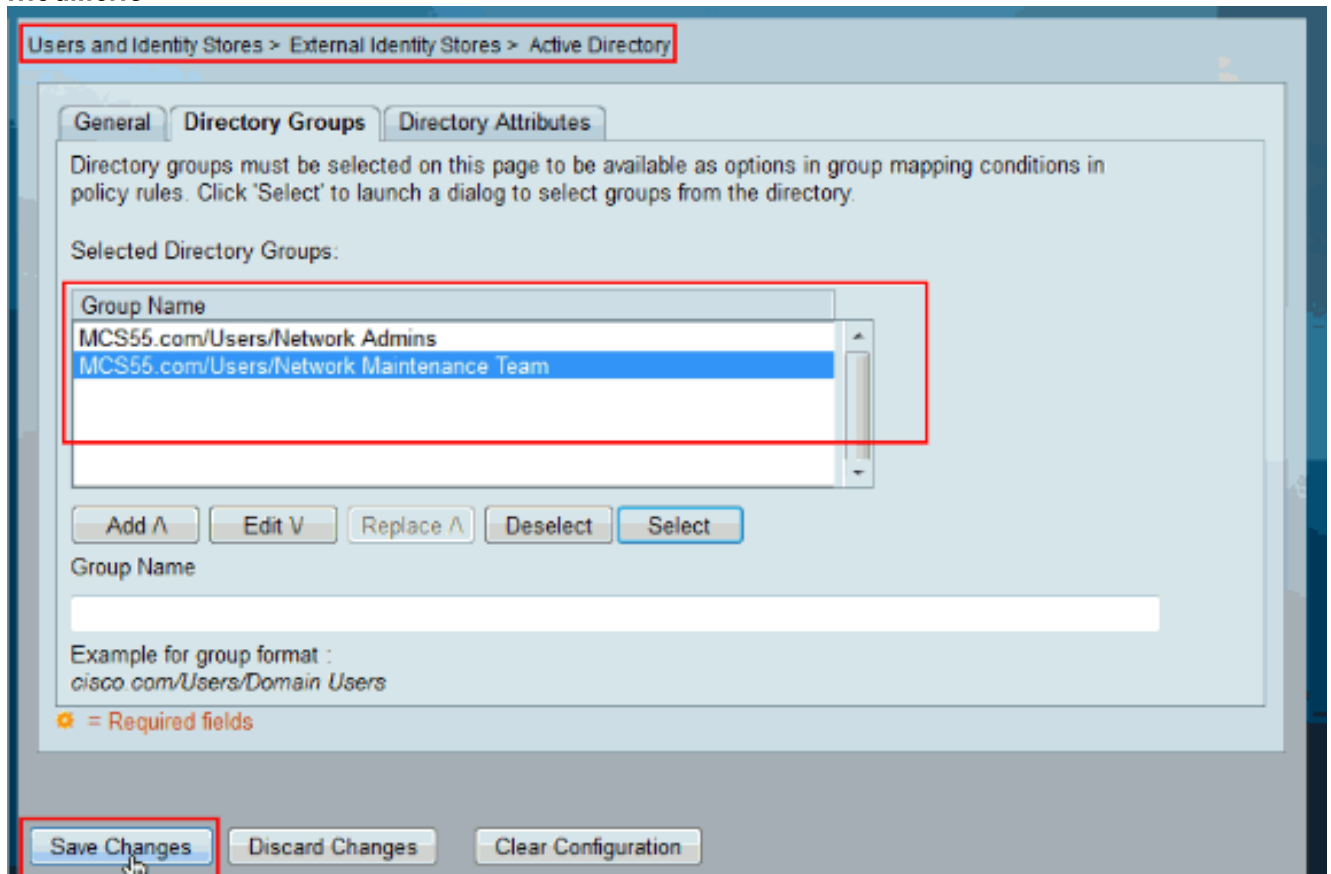
3. Fare clic su
Seleziona.



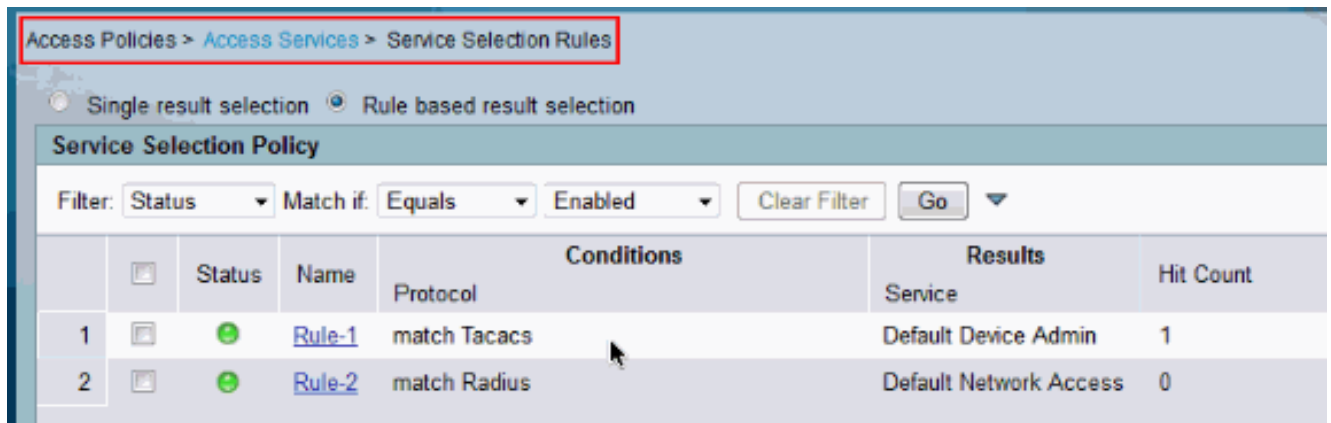
4. Scegliere i gruppi da mappare ai profili e ai set di comandi della shell nella parte successiva della configurazione. Fare clic su **OK**.



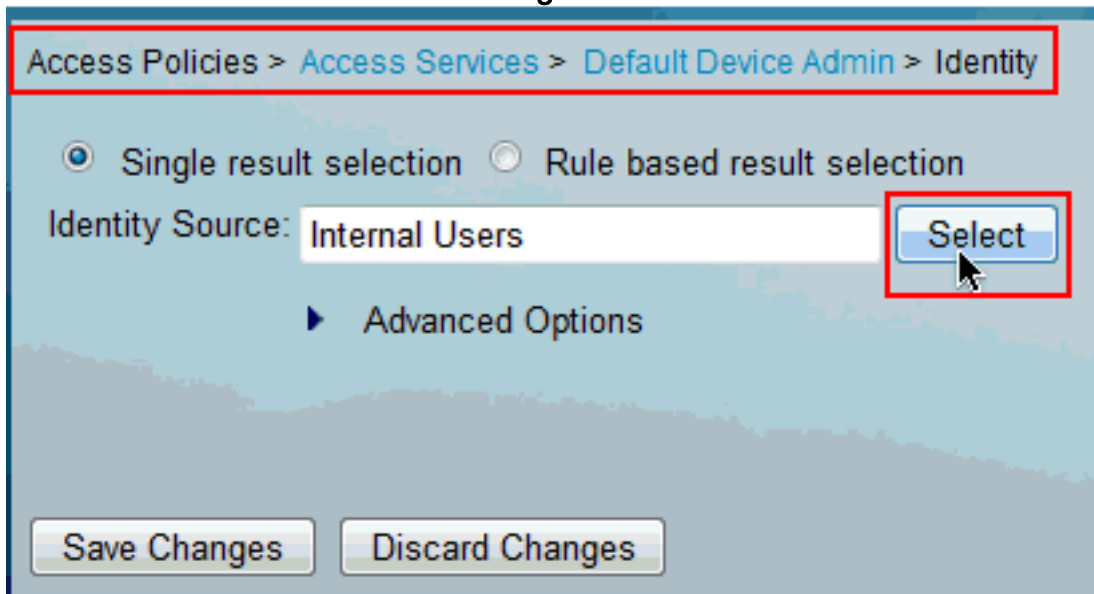
5. Fare clic su **Salva modifiche**.



6. Scegliere **Policy di accesso > Servizi di accesso > Regole di selezione dei servizi** e identificare il servizio di accesso che elabora l'autenticazione TACACS+. Nell'esempio, questo valore è **Default Device Admin**.

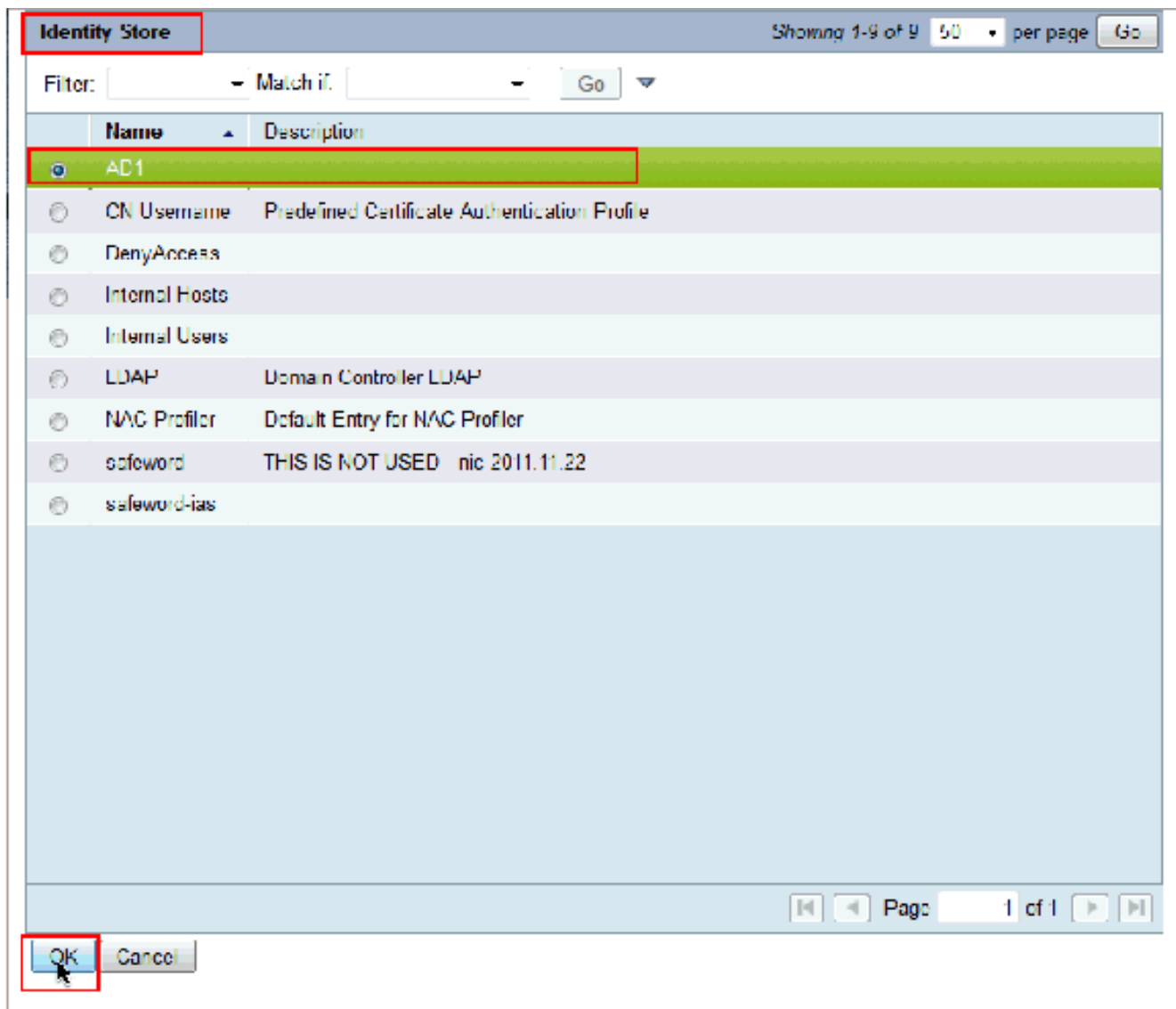


7. Scegliere **Criteri di accesso > Servizi di accesso > Amministrazione predefinita dispositivi > Identità** e fare clic su **Seleziona** accanto a **Origine**

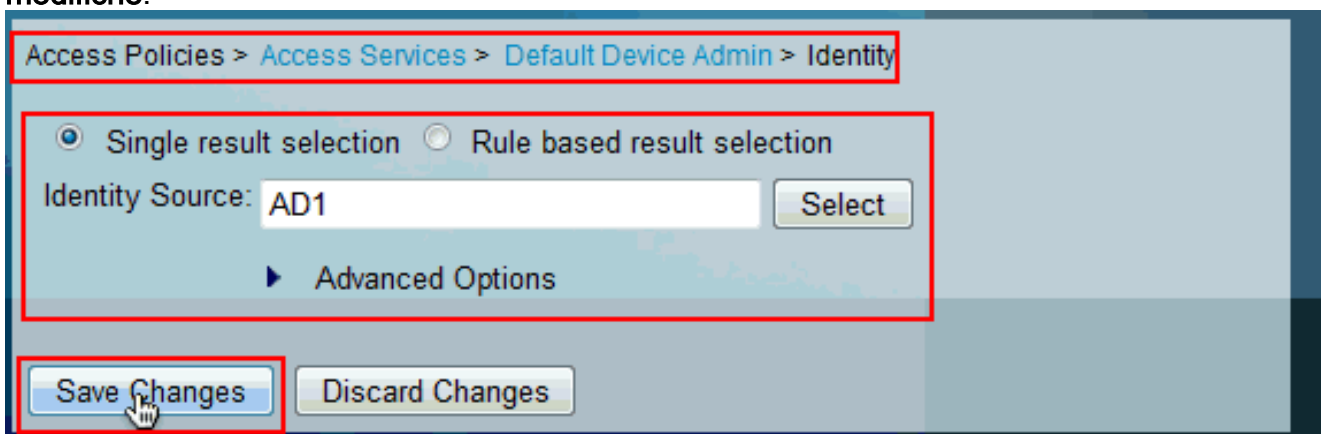


identità.

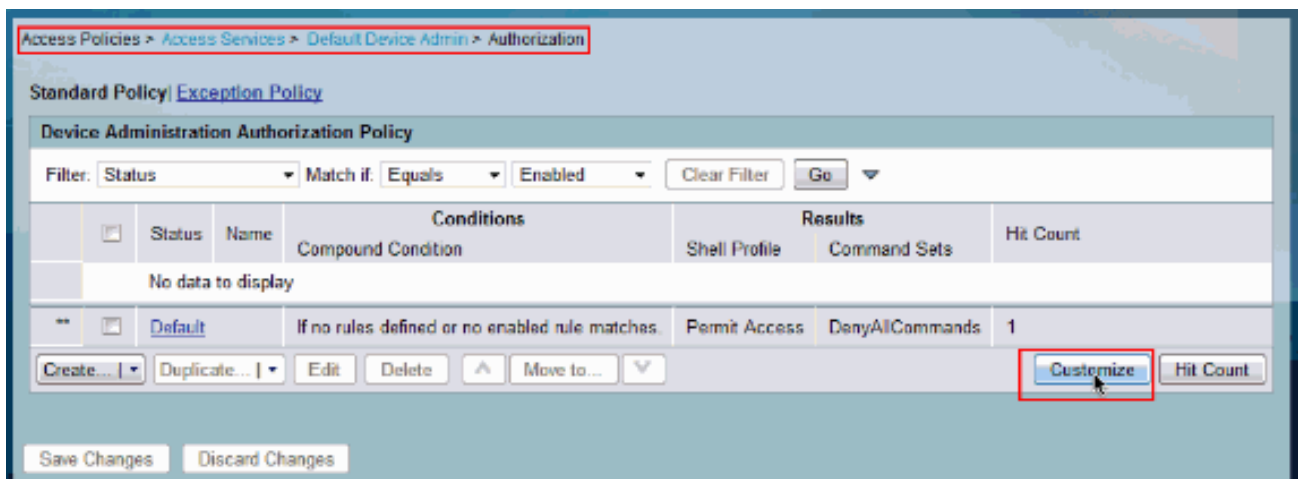
8. Scegliere **AD1** e fare clic su **OK**.



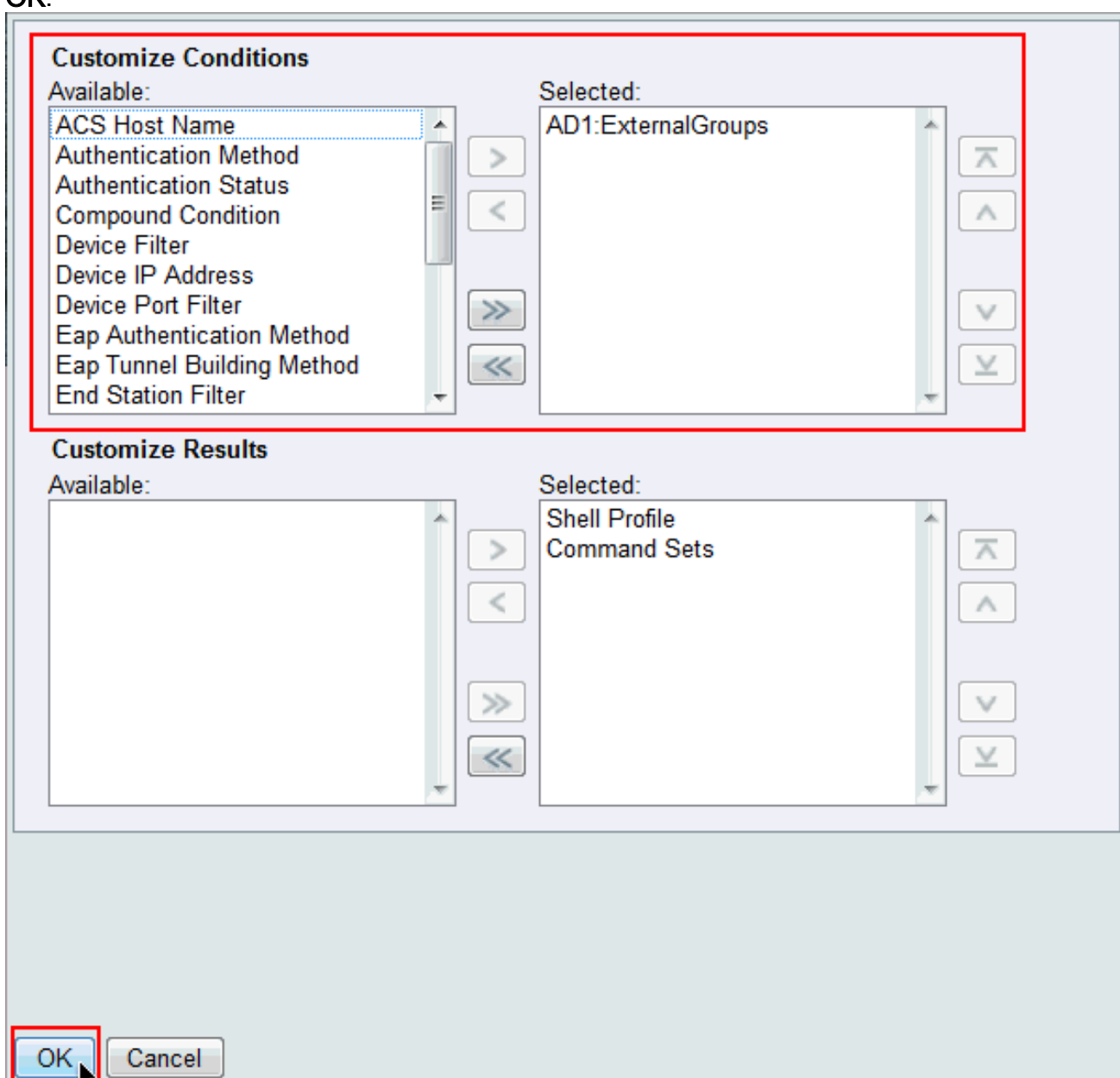
9. Fare clic su **Salva modifiche**.



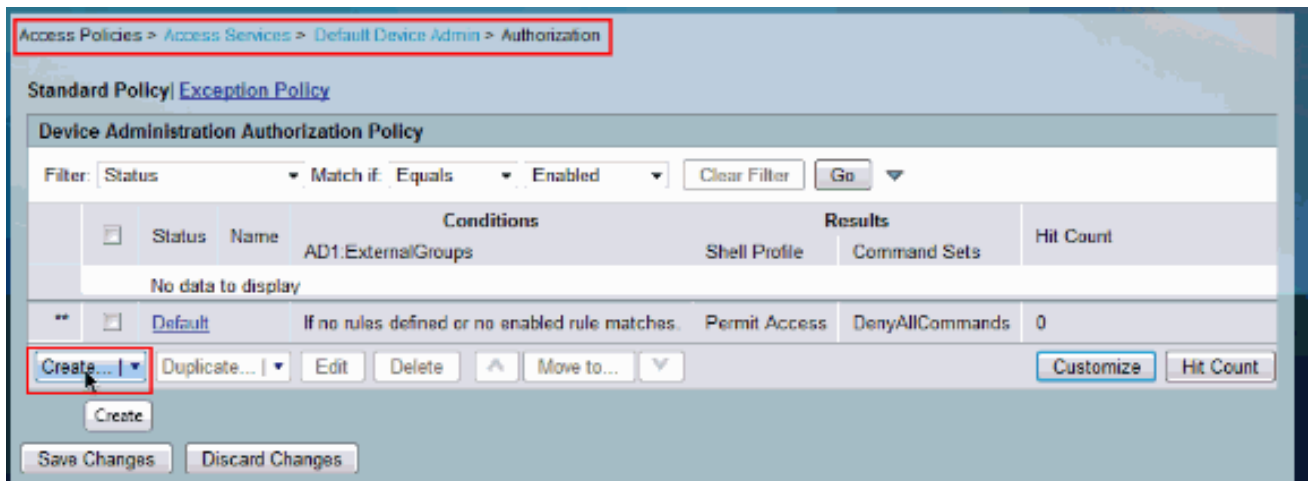
10. Scegliere **Criteria di accesso > Servizi di accesso > Amministrazione predefinita dispositivi > Autorizzazione** e fare clic su **Personalizza**.



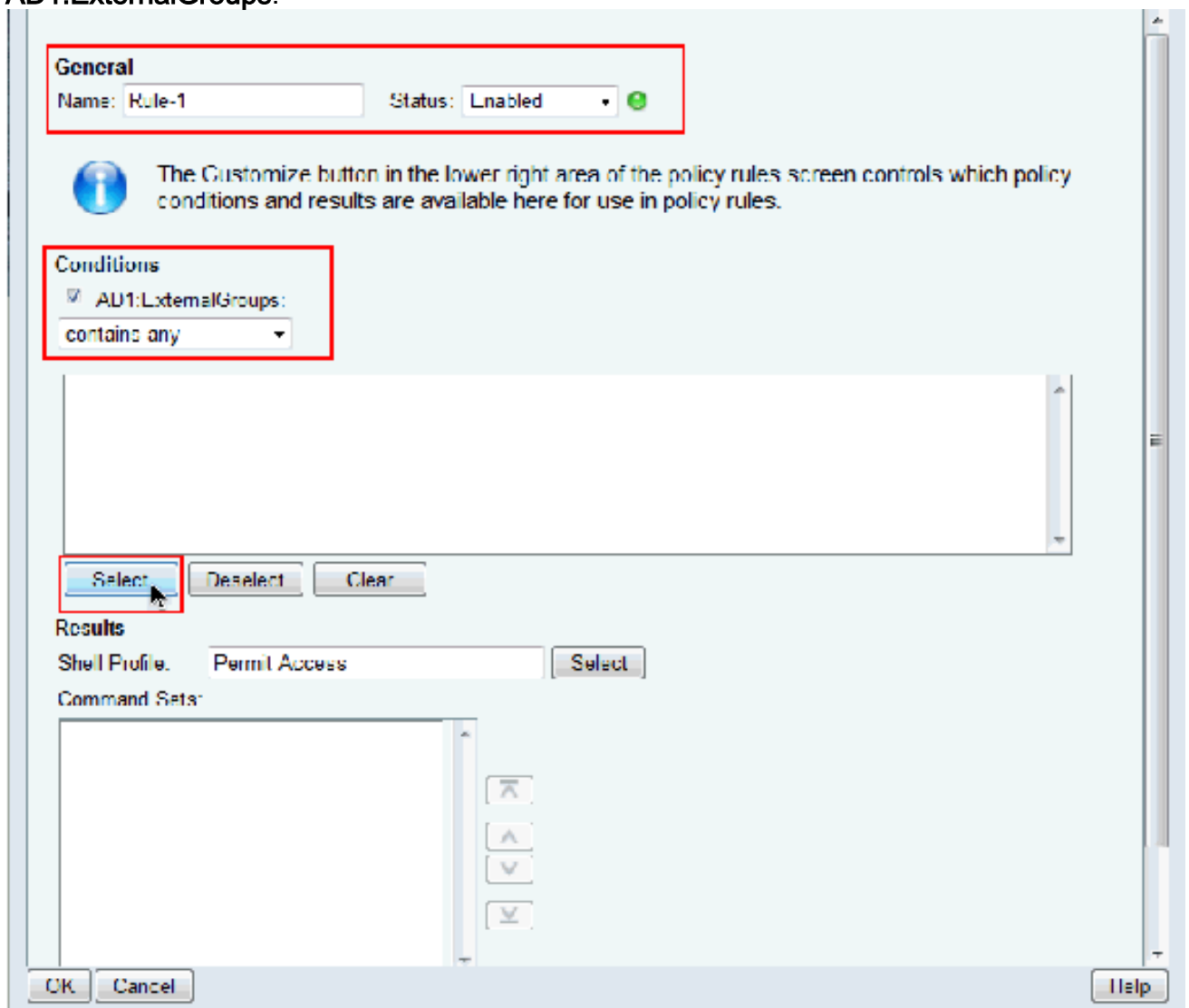
- Copiare AD1:ExternalGroups dalla sezione Disponibile a Selezionato di Personalizza condizioni e quindi spostare il profilo della shell e i set di comandi dalla sezione Disponibile a Selezionato di Personalizza risultati. Fare clic su **OK**.



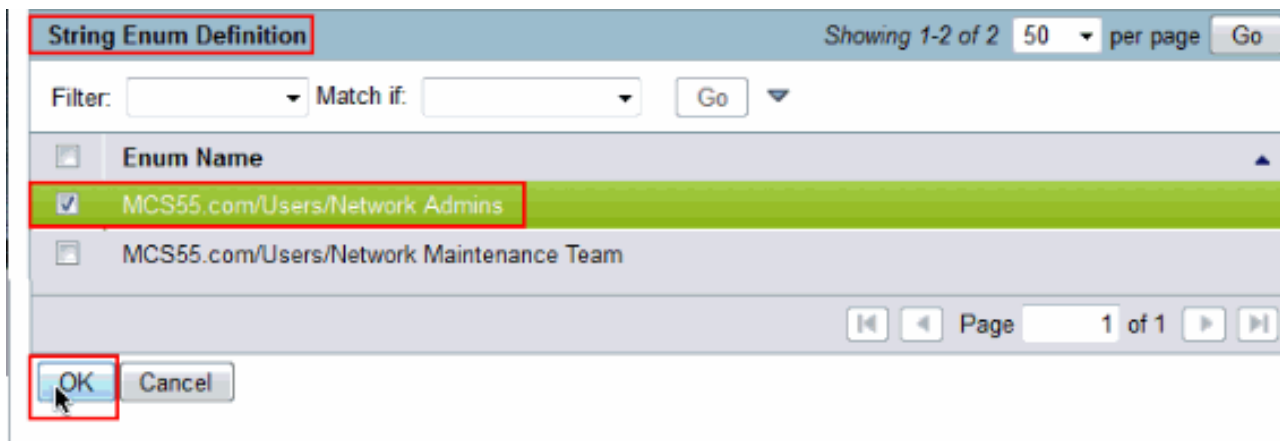
- Per creare una nuova regola, fare clic su **Create** (Crea).



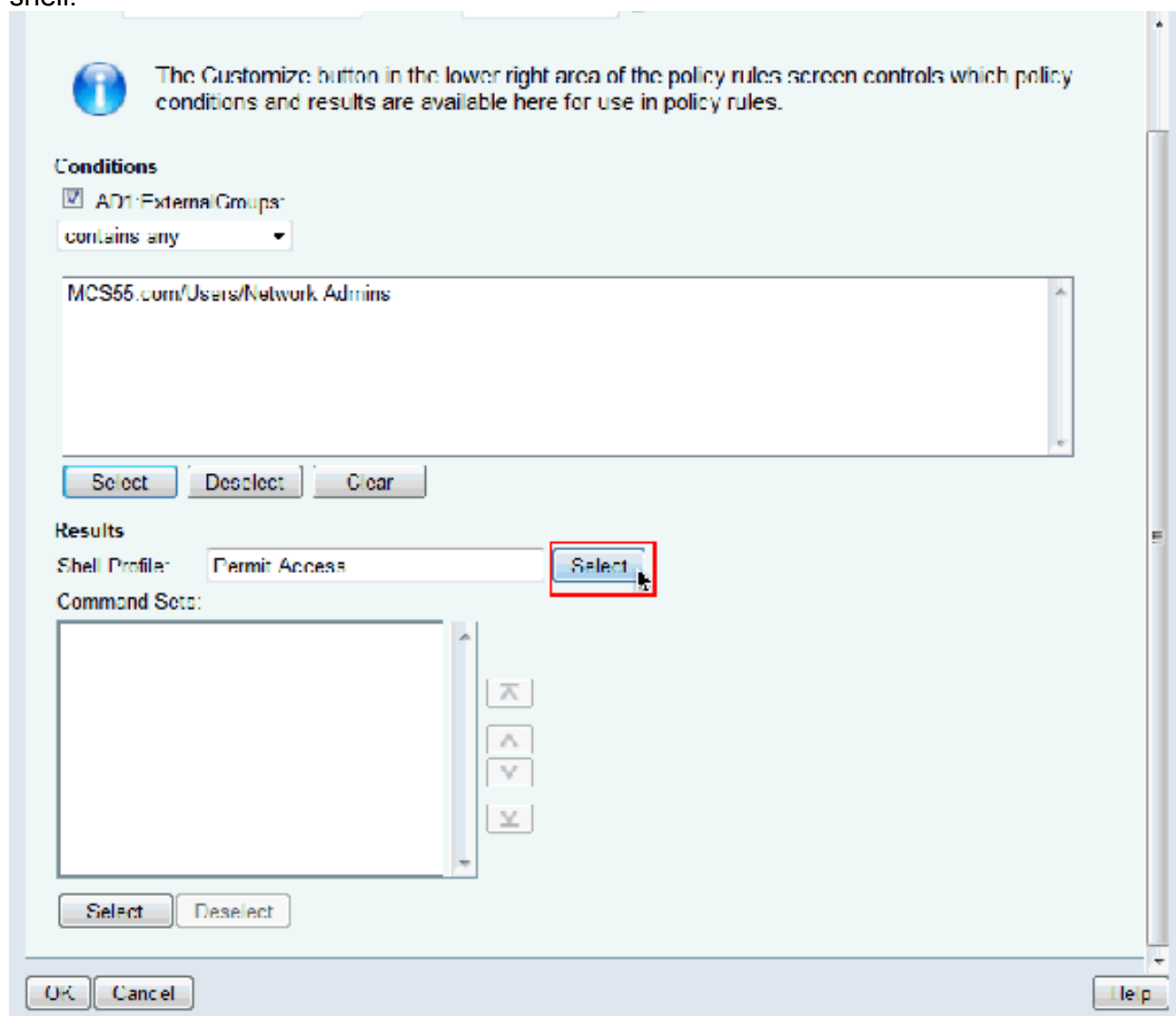
13. Fare clic su **Seleziona** nella condizione **AD1:ExternalGroups**.



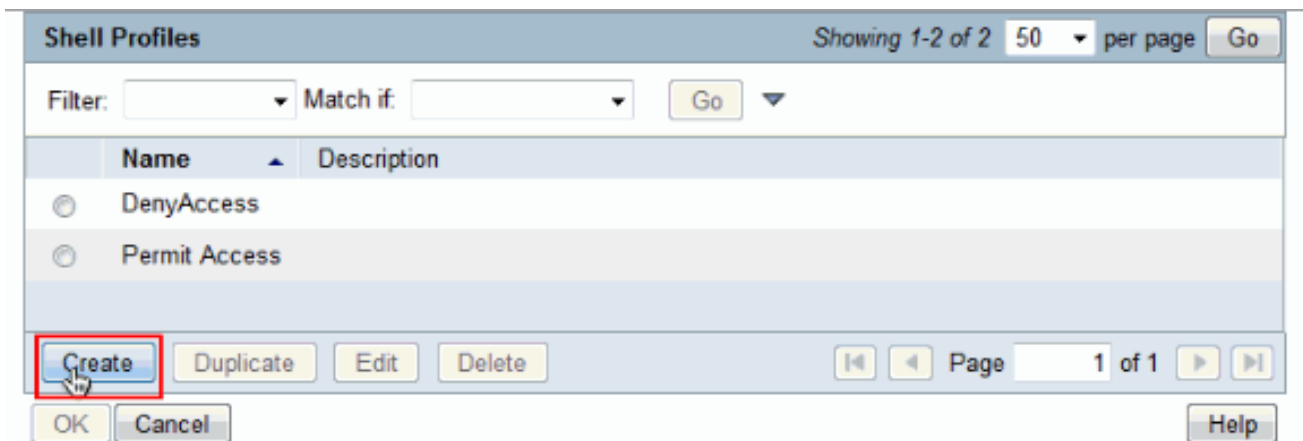
14. Selezionare il gruppo a cui si desidera concedere l'accesso completo sul dispositivo Cisco IOS. Fare clic su **OK**.



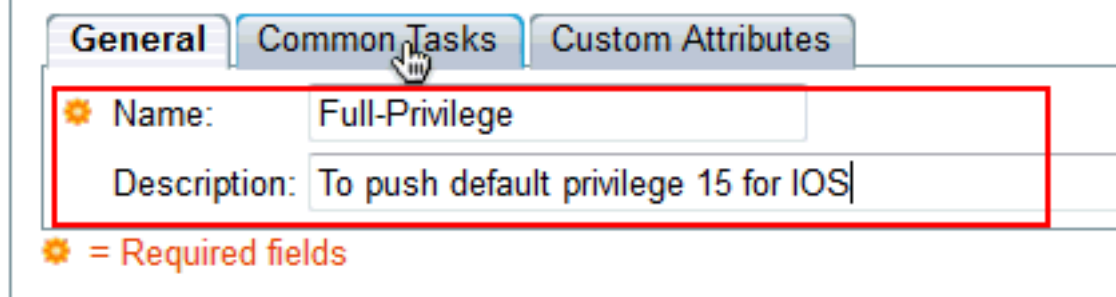
15. Fare clic su **Seleziona** nel campo Profilo shell.



16. Per creare un nuovo **profilo** di **shell** per gli utenti con accesso completo, fare clic su **Crea**.



17. Specificare **Name** and **Description** (facoltativo) nella scheda **General** e fare clic sulla scheda **Common**



Tasks. _____

18. Modificare Privilegio predefinito e **Privilegio massimo** in **Statico** con **valore 15**. Fare clic su **Sottometti**.

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

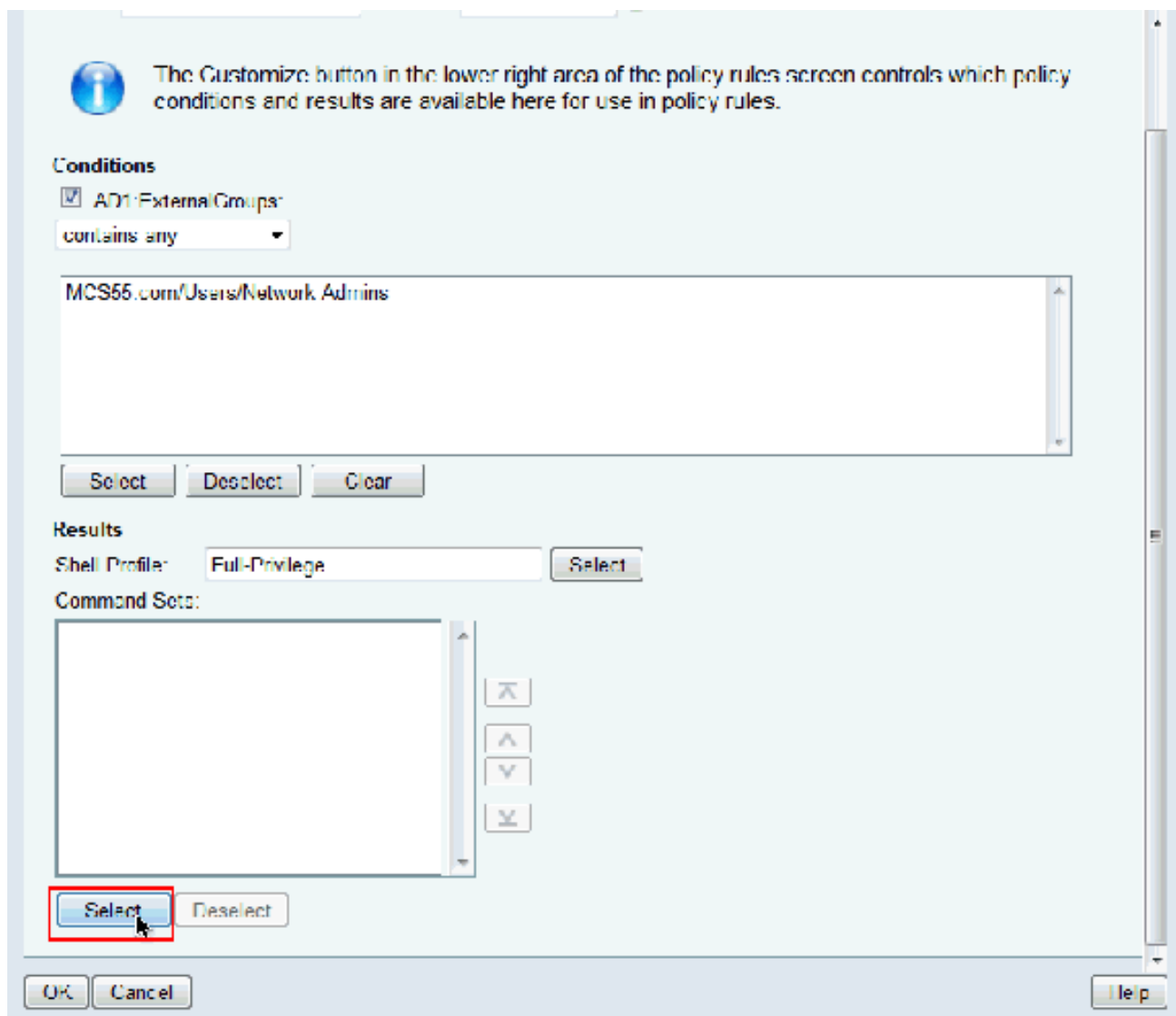
19. Scegliere il nuovo **profilo di shell ad** accesso completo (in questo esempio Privilegio completo) e fare clic su **OK**.

Shell Profiles

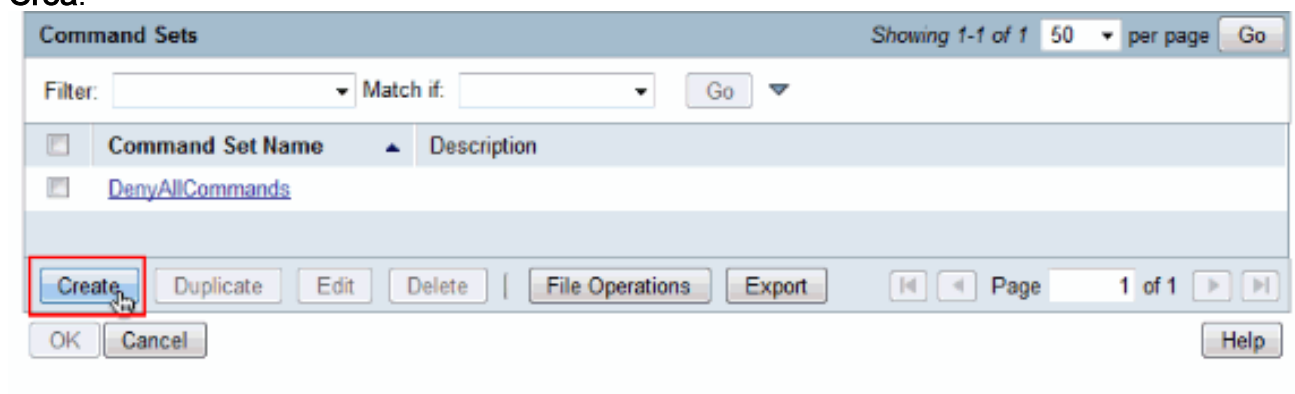
Filter: Match if:

	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. Fare clic su **Seleziona** nel campo Set comandi.



21. Per creare un nuovo **set di comandi** per gli utenti **ad accesso completo**, fare clic su **Crea**.



22. Specificare un **Nome** e verificare che la casella di controllo accanto a **Consenti comandi** non presenti nella tabella seguente sia selezionata. Fare clic su **Invia**. **Nota:** per ulteriori informazioni sui set di comandi, consultare il documento sulla [creazione, la duplicazione e la modifica dei set di comandi per l'amministrazione dei dispositivi](#).

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:

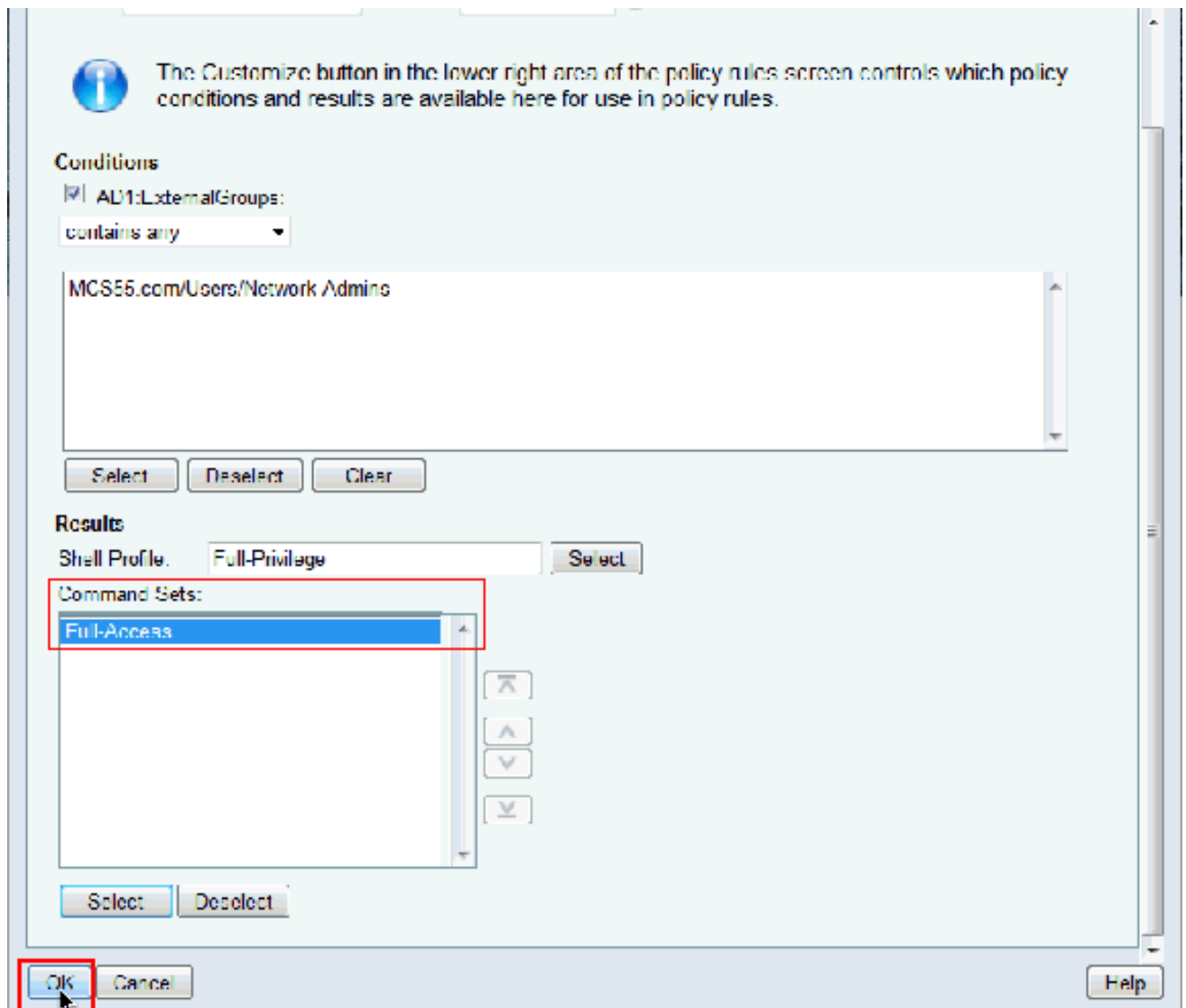
23. Fare clic su
OK.

Command Sets

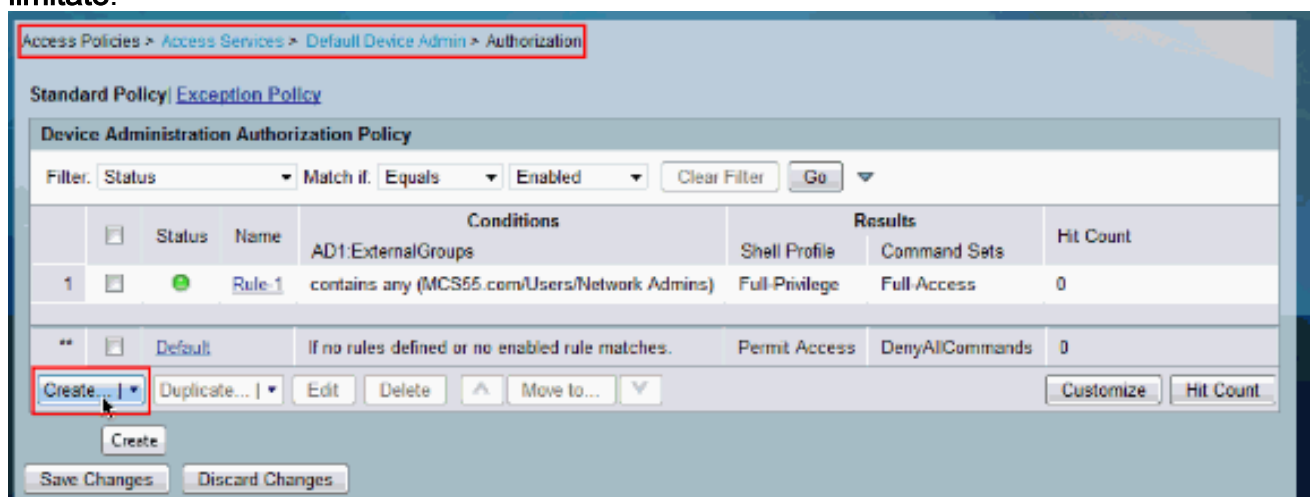
Filter: Match if:

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

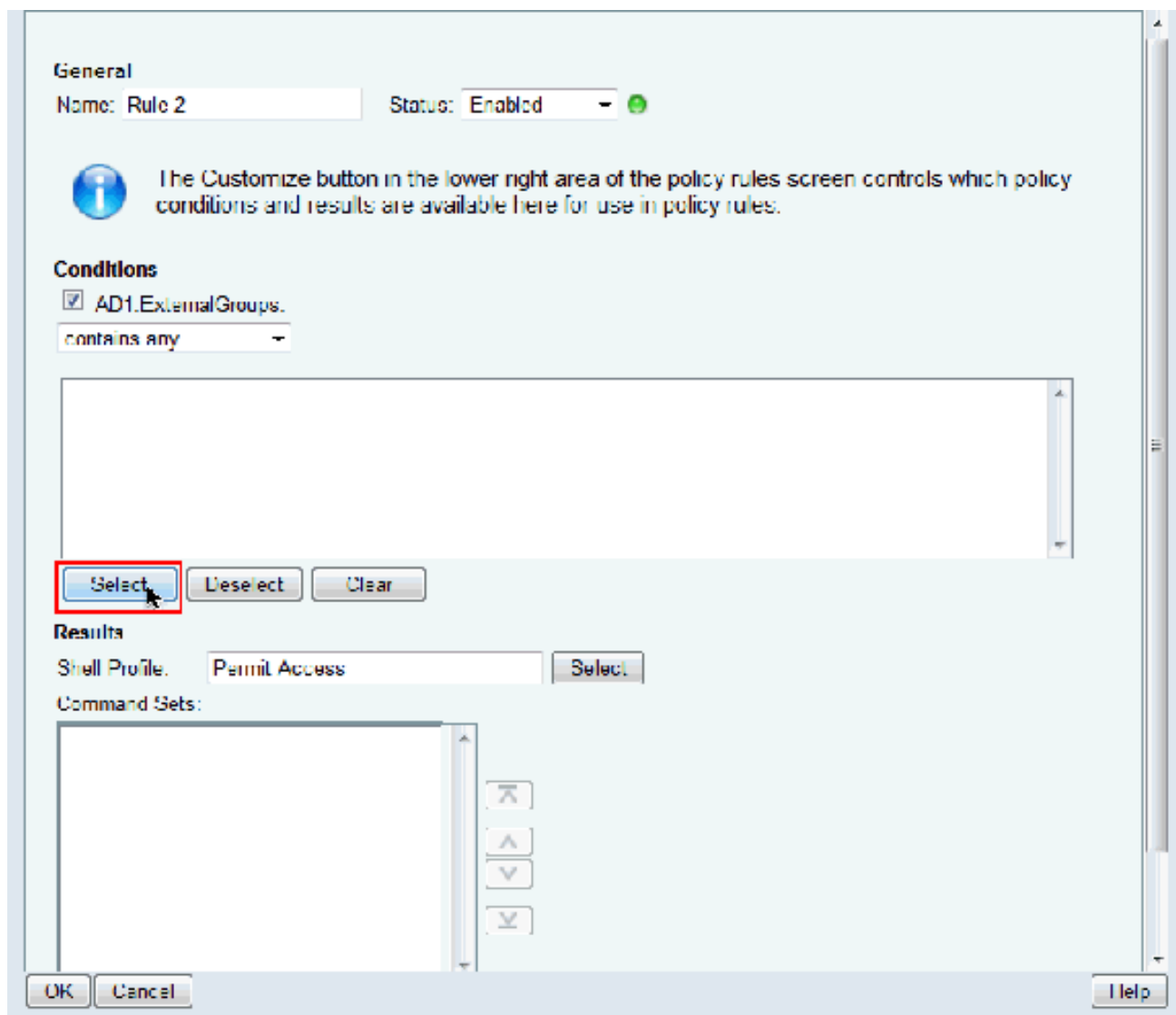
24. Fare clic su **OK**. La configurazione della **regola 1** è stata completata.



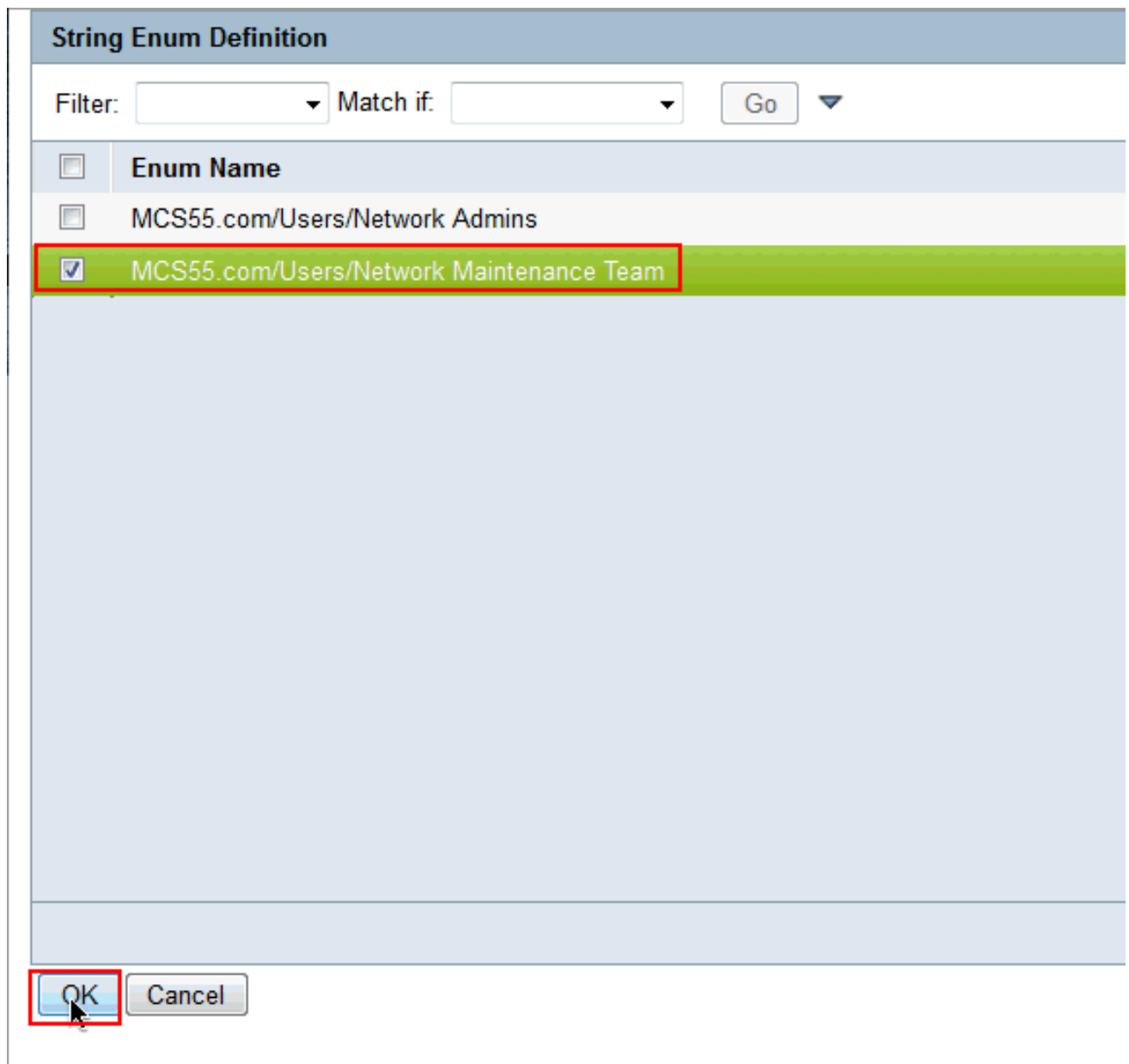
25. Fare clic su **Create** (Crea) per creare una nuova regola per gli utenti con **accesso limitato**.



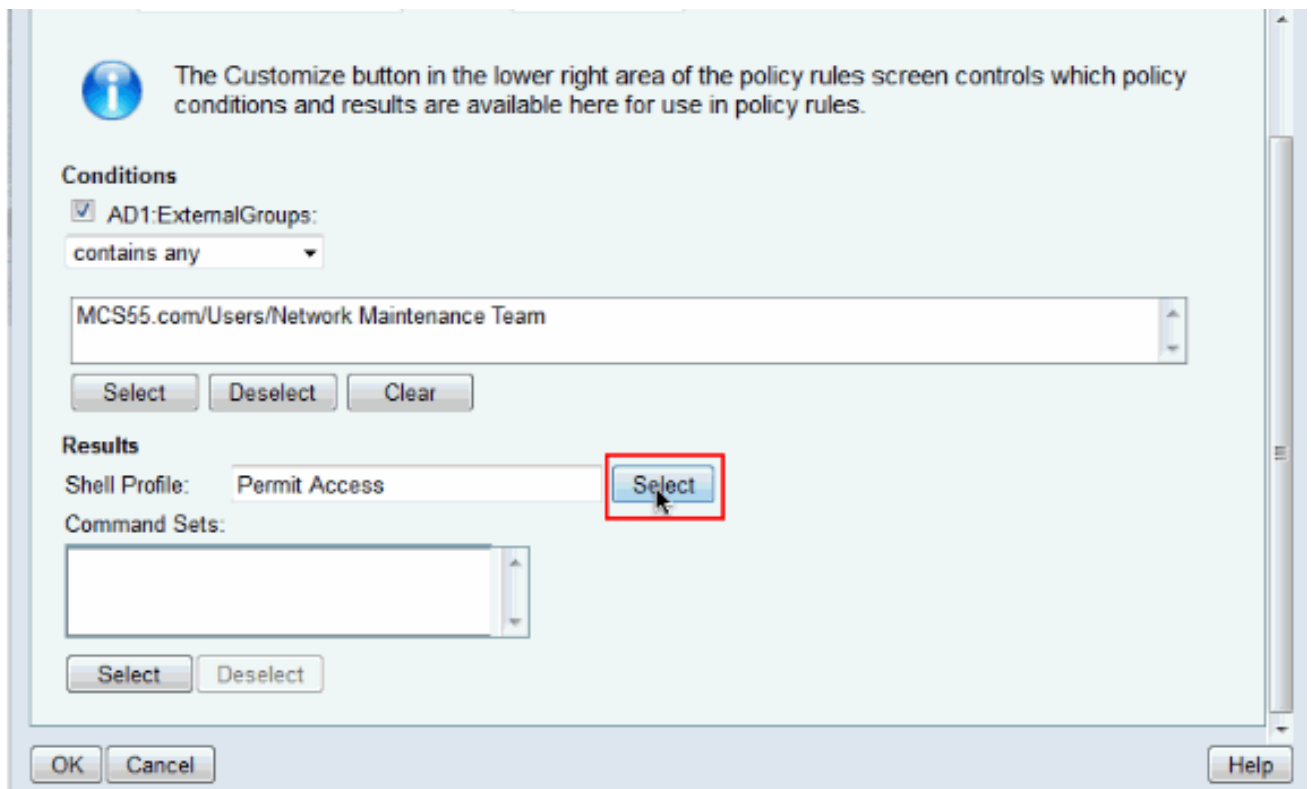
26. Scegliere **AD1:ExternalGroups** e fare clic su **Seleziona**.



27. Scegliere il gruppo o i gruppi a cui si desidera concedere l'accesso limitato e fare clic su OK.



28. Fare clic su **Seleziona** nel campo Profilo shell.



29. Per creare un nuovo **profilo** di **shell** per l'accesso limitato, fare clic su **Crea**.

Shell Profiles

Filter: Match if:

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

30. Specificare **Nome** e **Descrizione** (facoltativo) nella scheda **Generale** e fare clic sulla scheda **Attività comuni**.

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

⚙ = Required fields

31. Modificare Privilegio predefinito e **Privilegio massimo** in **Statico** con i valori **1** e **15** rispettivamente. Fare clic su

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

Invia.

32. Fare clic su

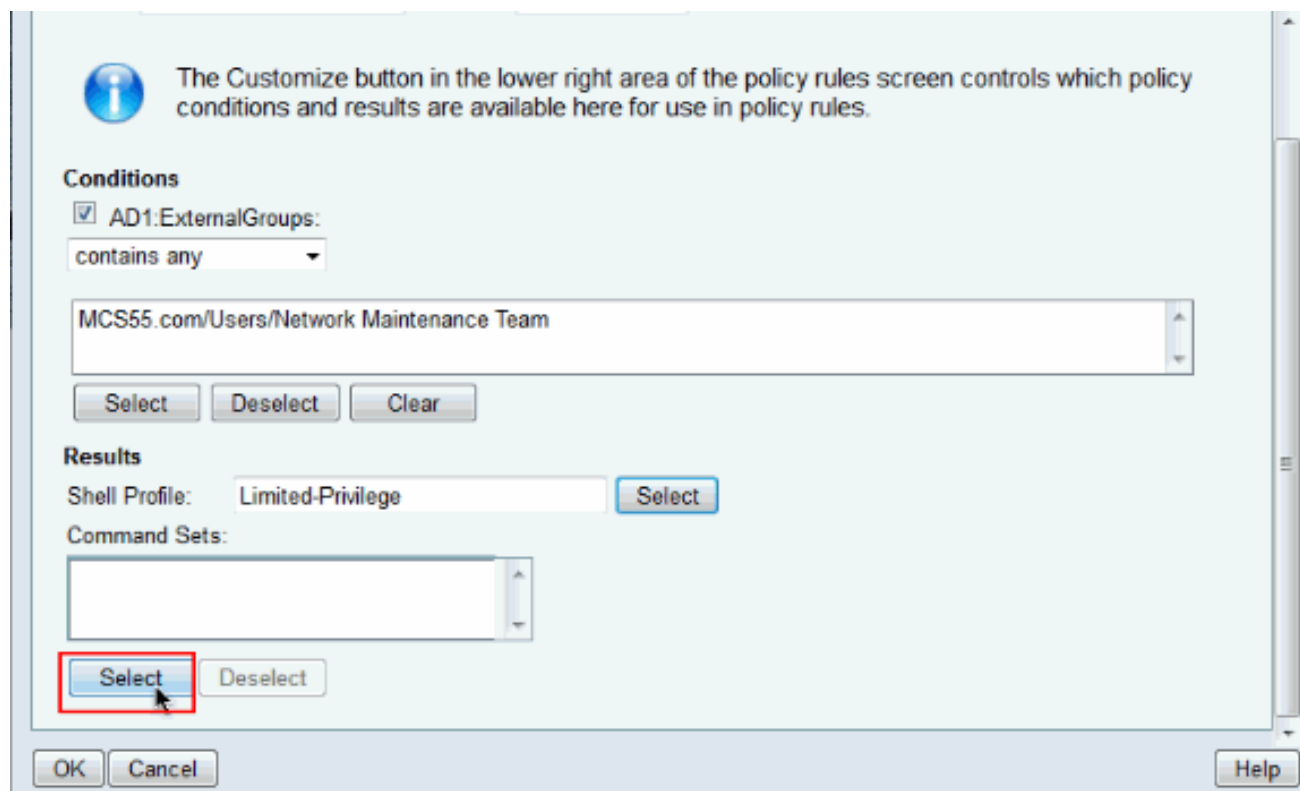
Shell Profiles

Filter: Match if: Go

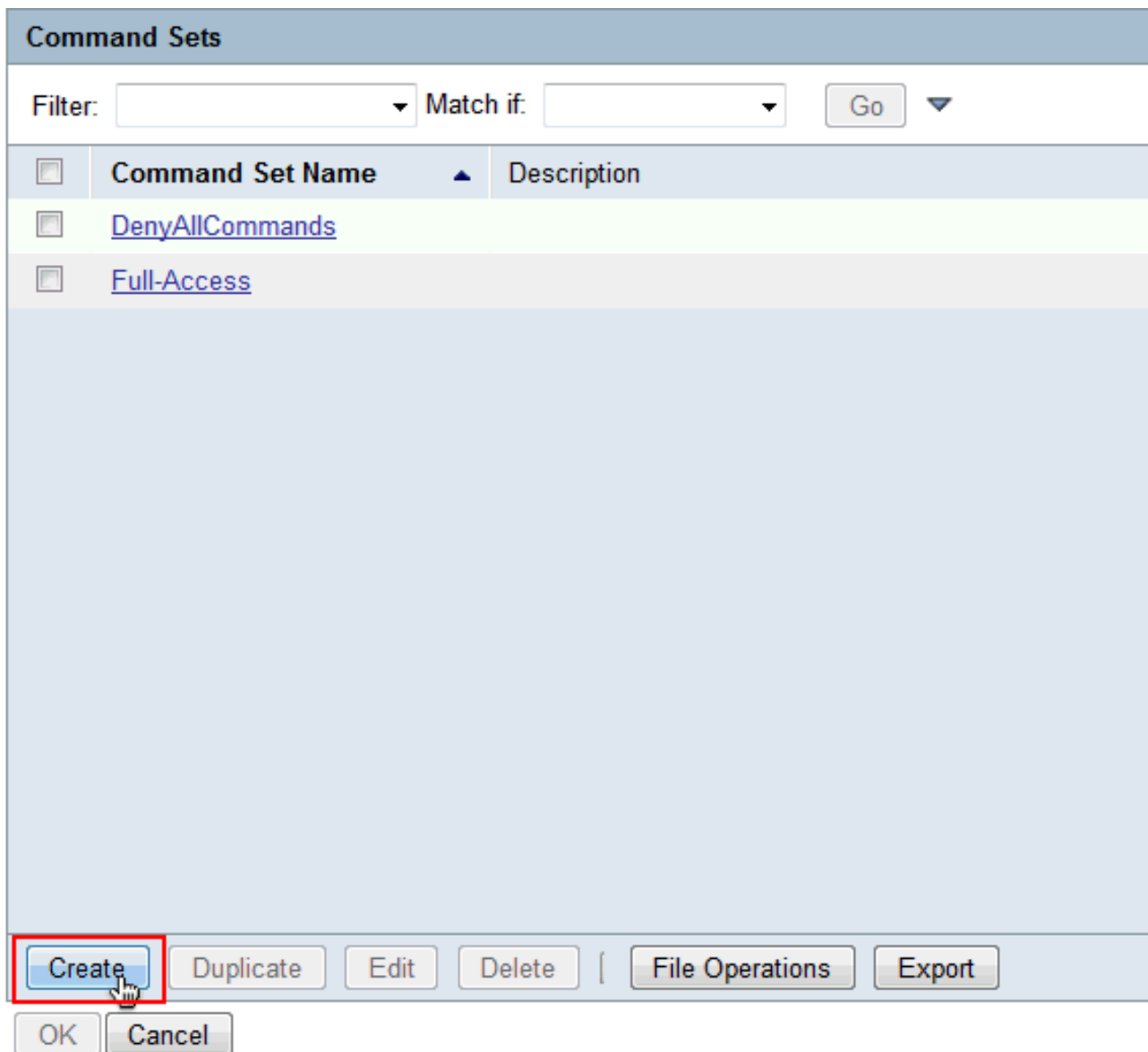
	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input checked="" type="radio"/>	Limited-Privilege	To push default privilege 1 for IOS
<input type="radio"/>	Permit Access	

OK.

33. Fare clic su **Seleziona** nel campo Set comandi.



34. Fare clic su **Crea** per creare un nuovo **set di comandi** per il gruppo di accesso limitato.



35. Specificare un **Nome** e verificare che la casella di controllo accanto a **Consenti comandi non presenti nella tabella seguente** non sia selezionata. Fare clic su Add dopo aver digitato **show** nello spazio disponibile nella sezione **command** e scegliere **Permit** nella sezione **Grant** in modo che solo i comandi show siano consentiti per gli utenti nel gruppo di accesso limitato.

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. Analogamente, aggiungere altri comandi da consentire agli utenti del gruppo ad accesso limitato con l'uso di **Add**. Fare clic su **Invia**. **Nota:** per ulteriori informazioni sui set di comandi, consultare il documento sulla [creazione, la duplicazione e la modifica dei set di comandi per l'amministrazione dei dispositivi](#).

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. Fare clic su
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. Fare clic su
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

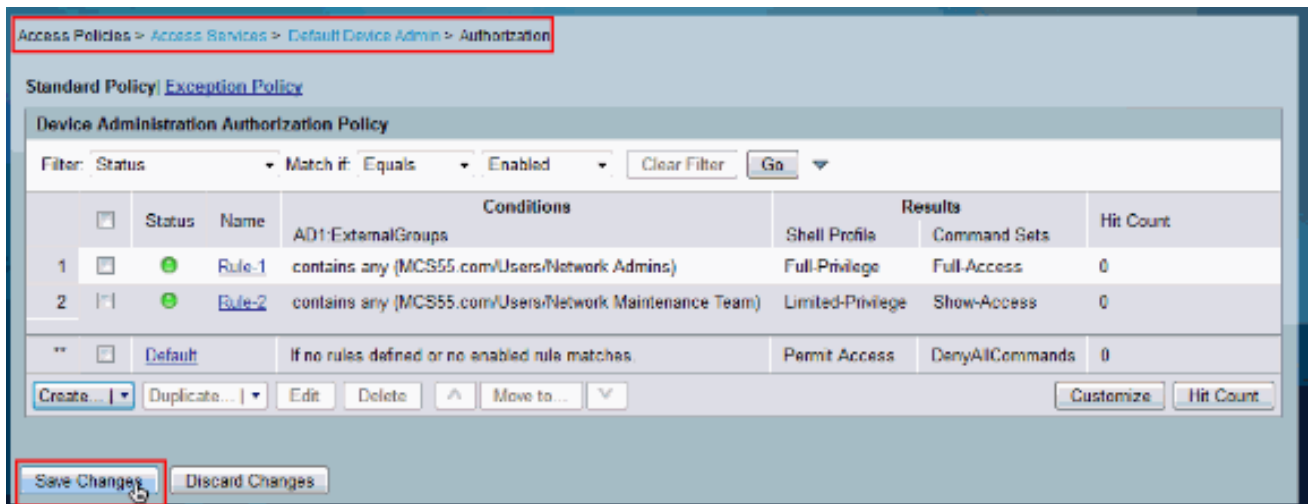
Select

Deselect

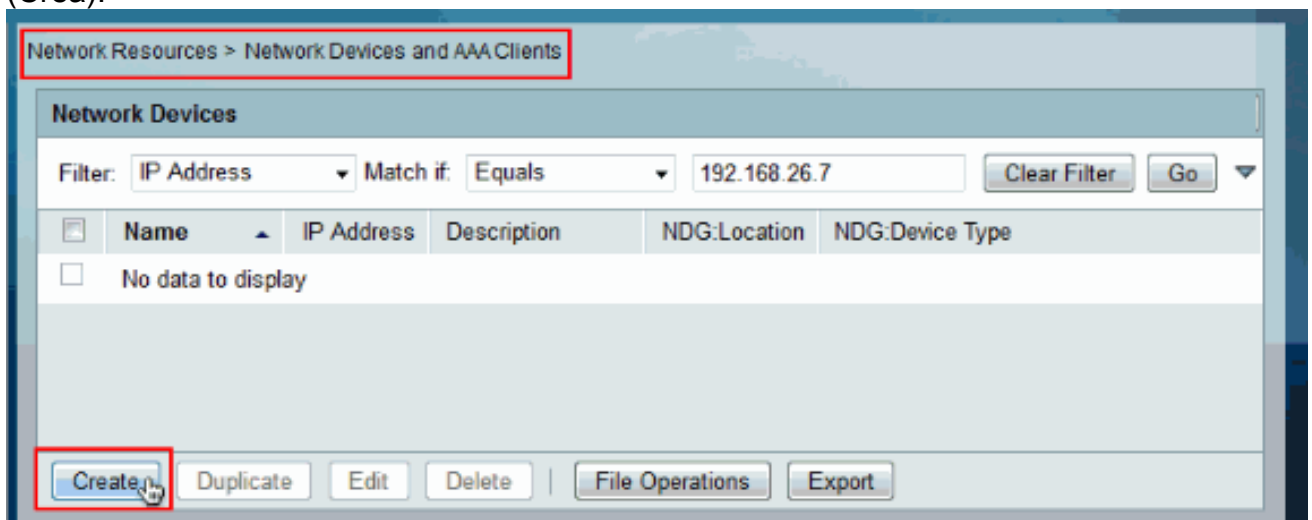
OK

Cancel

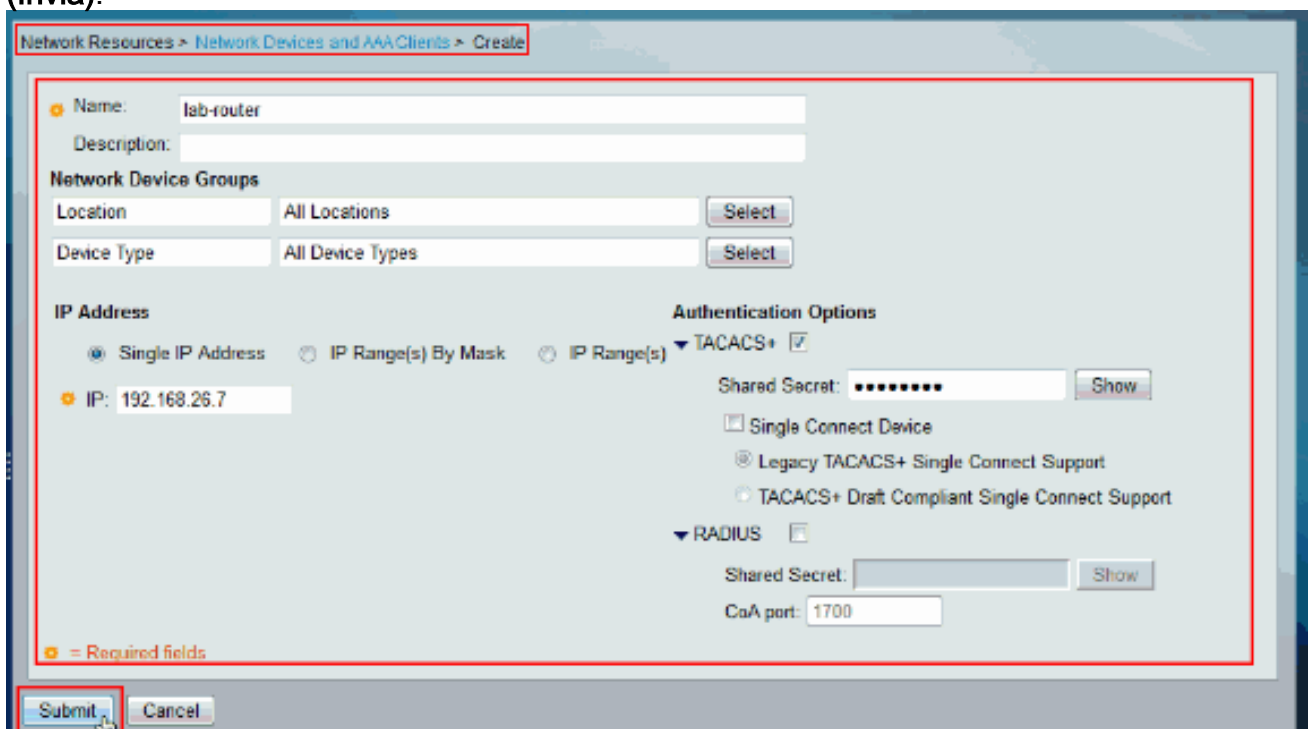
39. Fare clic su **Salva** modifiche.



40. Per aggiungere il dispositivo **Cisco IOS** come **client AAA** sull'ACS, fare clic su **Create** (Crea).



41. Specificare nome, indirizzo IP e segreto condiviso per TACACS+ e fare clic su **Submit** (Invia).



[Configurare il dispositivo Cisco IOS per l'autenticazione e l'autorizzazione](#)

Completare questa procedura per configurare il dispositivo Cisco IOS e l'ACS per l'autenticazione e l'autorizzazione.

1. Creare un utente locale con privilegi completi per il fallback utilizzando il comando **username**, come mostrato di seguito:

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

2. Specificare l'indirizzo IP del server ACS per abilitare il server AAA e aggiungere ACS 5.x come server TACACS.

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

Nota: la chiave deve corrispondere al segreto condiviso fornito sull'ACS per questo dispositivo Cisco IOS.

3. Verificare la raggiungibilità del server TACACS con il comando **test aaa**, come mostrato.

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

L'output del comando precedente mostra che il server TACACS è raggiungibile e che l'utente è stato autenticato correttamente. **Nota:** l'utente 1 e la password xxx appartengono ad AD. Se il test non riesce, verificare che il valore di Shared-Secret fornito nel passaggio precedente sia corretto.

4. Configurare l'accesso e abilitare le autenticazioni, quindi utilizzare le autorizzazioni di esecuzione e di comando come mostrato di seguito:

```
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
```

Nota: le parole chiave Local e Enable vengono usate per il fallback all'utente locale Cisco IOS e per abilitare il segreto rispettivamente se il server TACACS non è raggiungibile.

Verifica

Per verificare l'autenticazione e l'autorizzazione, accedere al dispositivo Cisco IOS tramite Telnet.

1. Telnet su dispositivo Cisco IOS come utente1 appartenente al gruppo ad accesso completo in Active Directory. Il gruppo Network Admins è il gruppo in Active Directory mappato al profilo della shell con privilegi completi e al comando ad accesso completo impostato su ACS. Provare a eseguire qualsiasi comando per assicurarsi di disporre dell'accesso completo.

```
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 per il dispositivo Cisco IOS come utente2 che appartiene al gruppo ad accesso limitato in Active Directory. (Il gruppo del **team di manutenzione della rete** è il gruppo in Active Directory mappato al **profilo della shell con privilegi limitati** e al **set di comandi Show-Access** su ACS). Se si tenta di eseguire un comando diverso da quelli indicati nel set di comandi Show-Access, viene visualizzato il messaggio di errore `Command Authorization Failed` (Autorizzazione comando non riuscita), che indica che l'utente 2 dispone di accesso limitato.

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 6:21:19.399 AM	✓			user2	[CmdA]write		lab-cosmos
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.799 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 6:20:59.899 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 6:20:38.499 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				

Informazioni correlate

- [Cisco Secure Access Control System](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)