

# ACS 5.x：基於AD組成員身份的TACACS+身份驗證和命令授權配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[組態](#)

[配置ACS 5.x進行身份驗證和授權](#)

[配置Cisco IOS裝置以進行身份驗證和授權](#)

[驗證](#)

[相關資訊](#)

## 簡介

本檔案將提供根據使用思科安全存取控制系統(ACS) 5.x和更新版本之使用者的AD群組成員身分設定TACACS+驗證和命令授權的範例。ACS使用Microsoft Active Directory (AD)作為外部身份庫來儲存使用者、電腦、組和屬性等資源。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- ACS 5.x已完全整合到所需的AD域。如果ACS未與所需的AD域整合，請參閱[ACS 5.x及更高版本：與Microsoft Active Directory整合配置示例](#)以獲取詳細資訊，以便執行整合任務。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全ACS 5.3
- Cisco IOS®軟體版本12.2(44)SE6。

注意：此配置可以在所有Cisco IOS裝置上完成。

- Microsoft Windows Server 2003域

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

## 組態

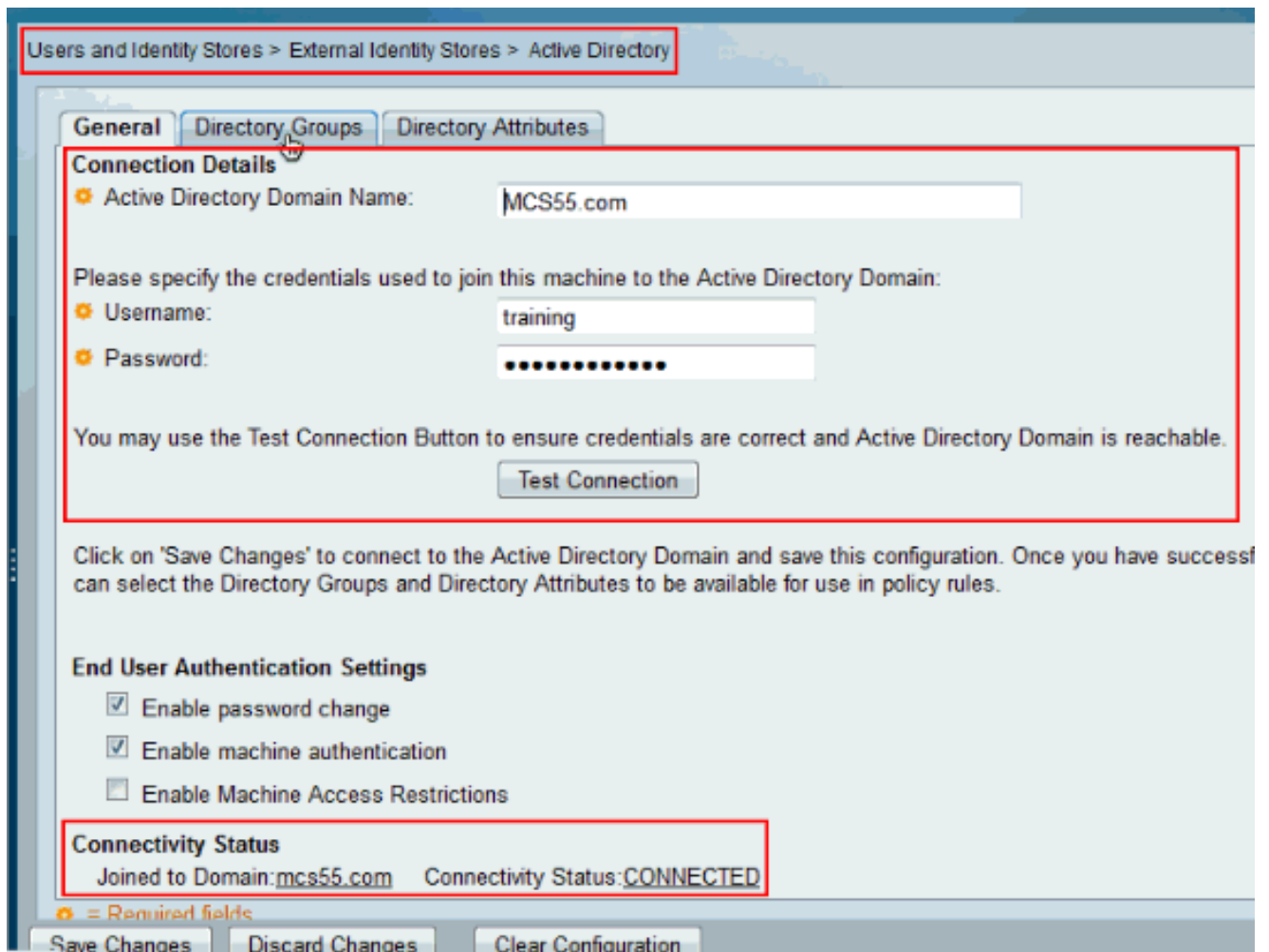
### 配置ACS 5.x進行身份驗證和授權

在開始配置ACS 5.x進行身份驗證和授權之前，ACS應已成功與Microsoft AD整合。如果ACS未與所需的AD域整合，請參閱[ACS 5.x及更高版本：與Microsoft Active Directory整合配置示例](#)以獲取詳細資訊，以便執行整合任務。

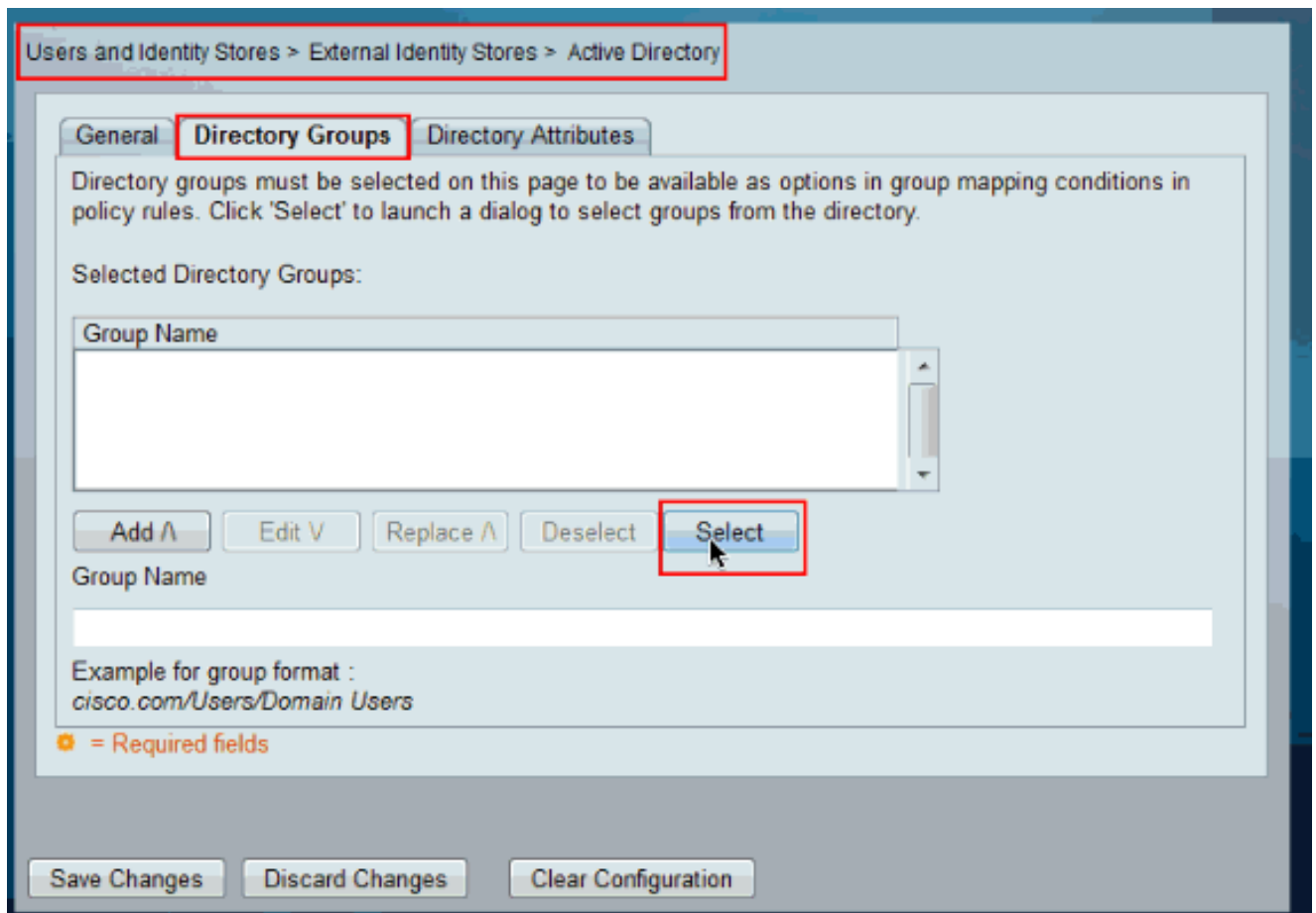
在本節中，您將兩個AD組對映到兩個不同的命令集和兩個Shell配置檔案，一個在Cisco IOS裝置上具有完全訪問許可權，另一個具有有限訪問許可權。

1. 使用管理員憑證登入到ACS GUI。
2. 選擇Users and Identity Stores > External Identity Stores > Active Directory，並驗證ACS是否已加入所需的域，以及連線狀態是否顯示為connected。

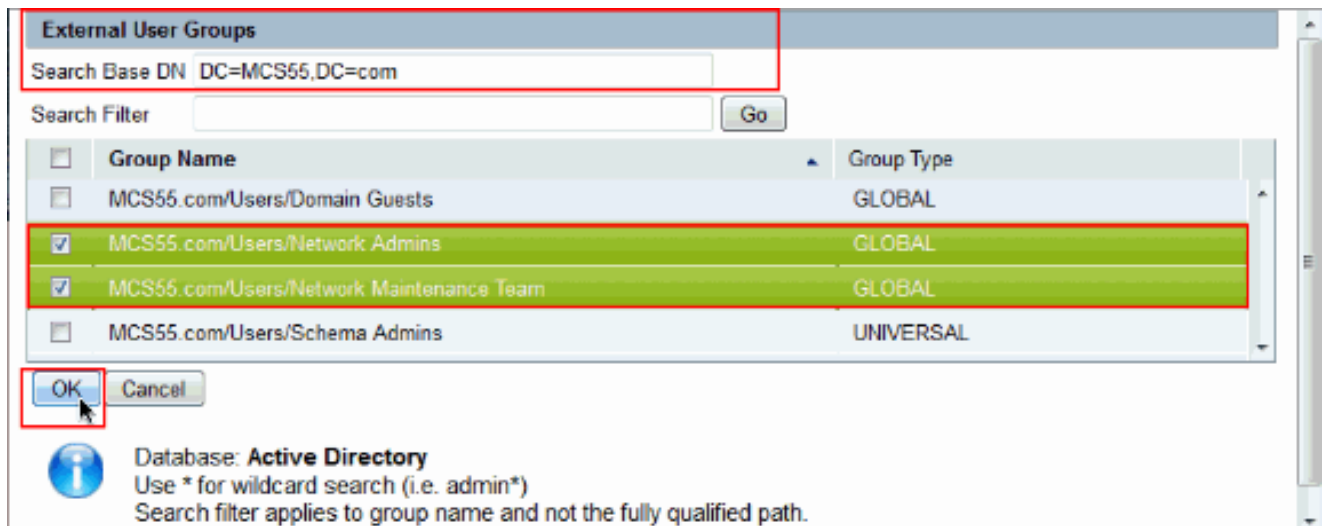
按一下Directory Groups頁籤。



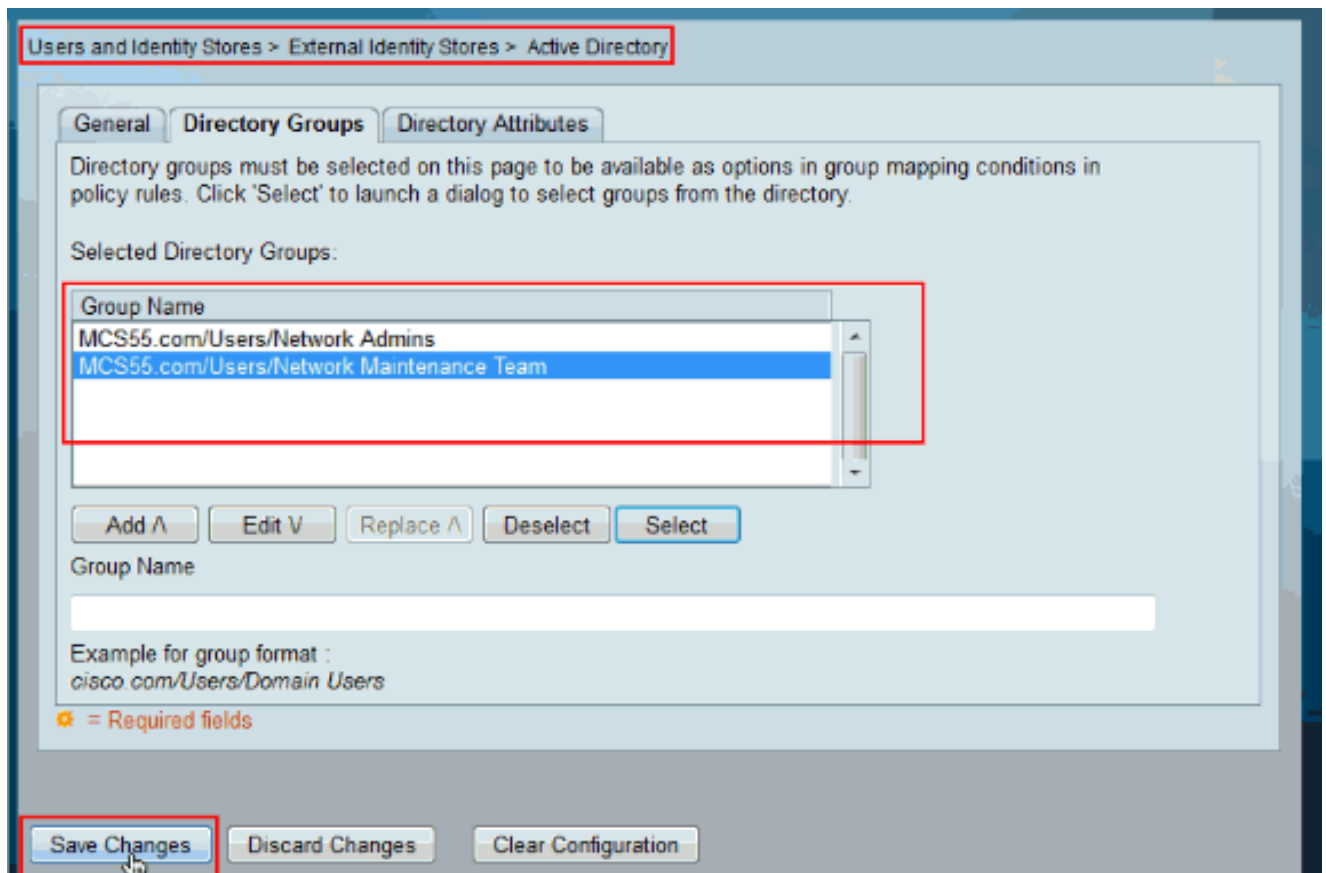
3. 按一下選擇。



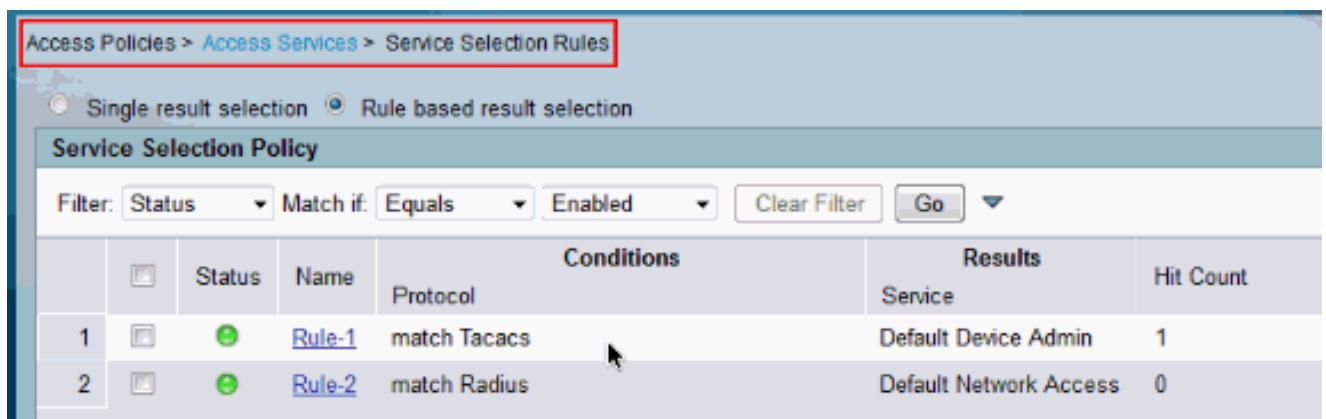
4. 選擇需要對映到配置後面部分的Shell配置檔案和命令集的組。按一下「OK」（確定）。



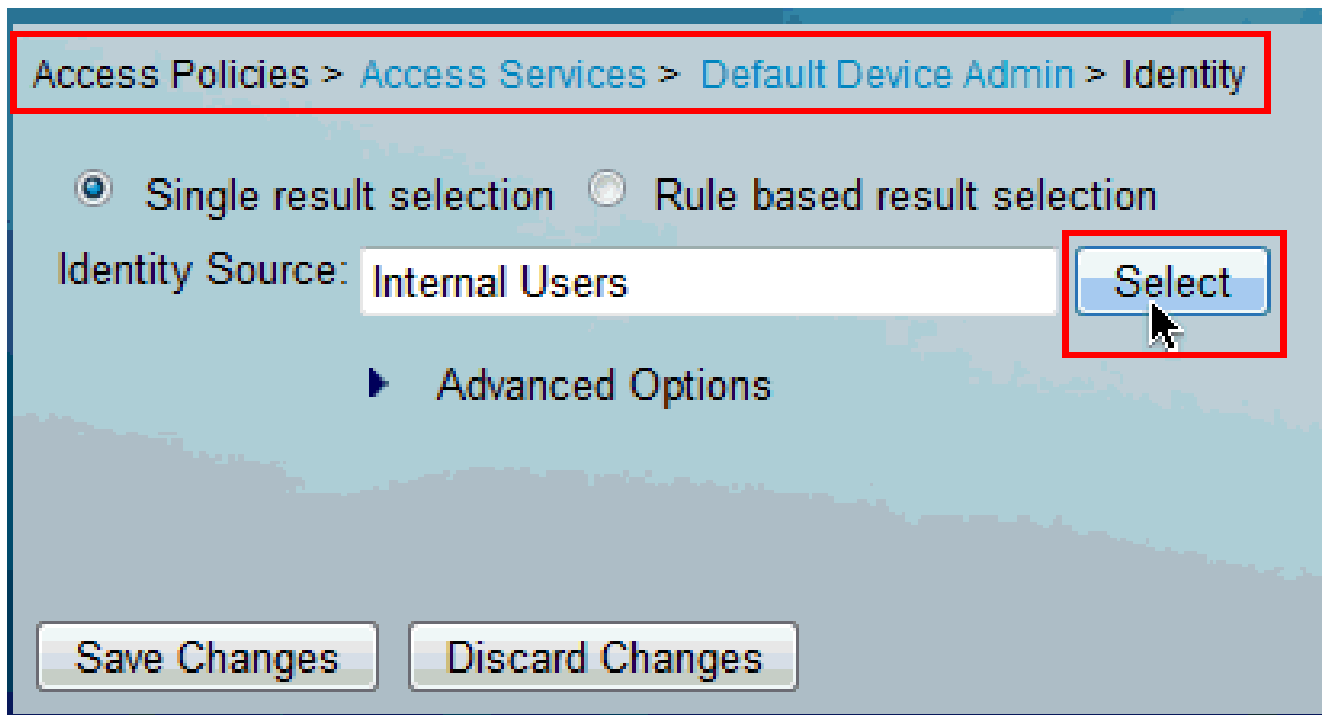
5. 按一下Save Changes。



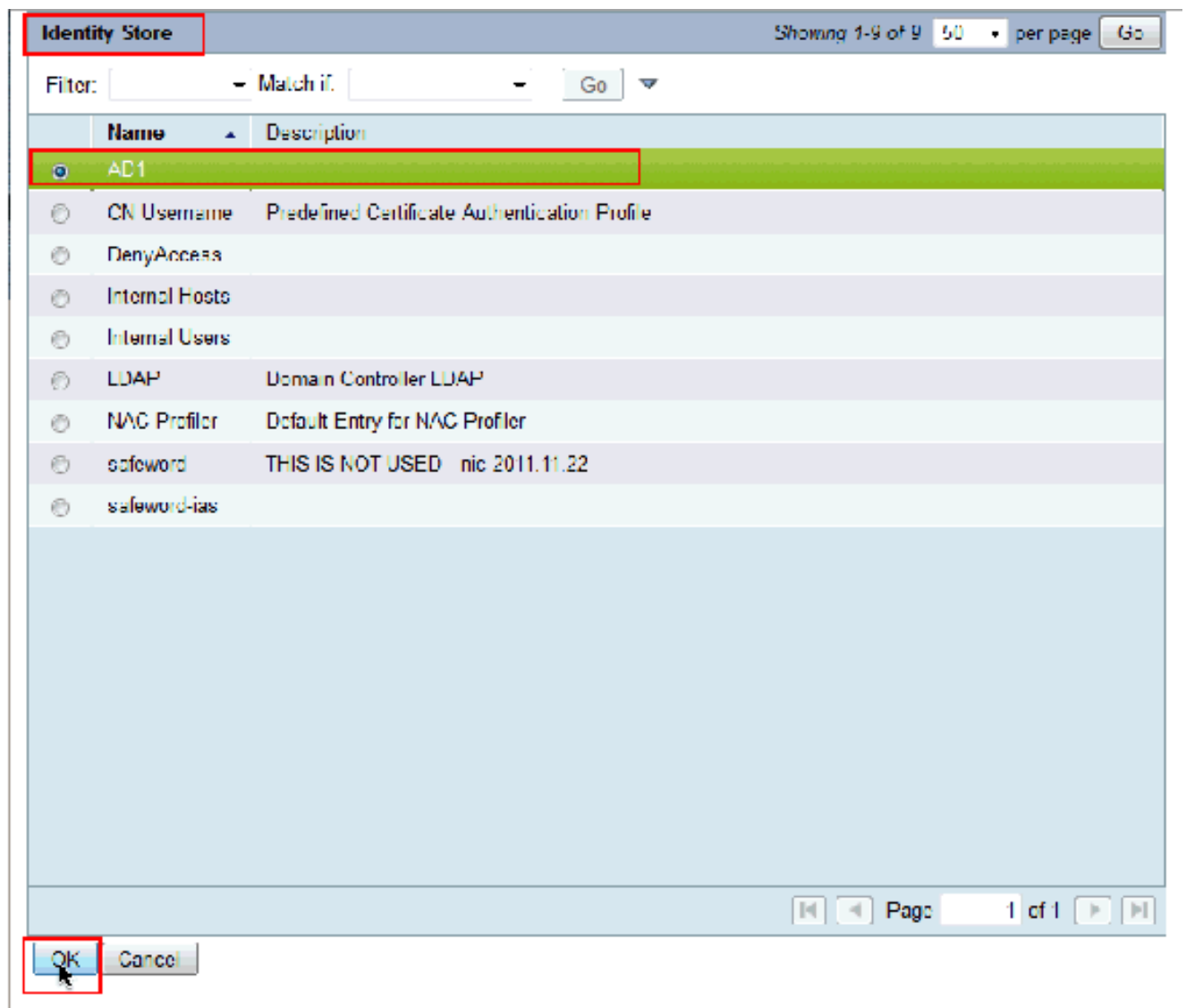
6. 選擇Access Policies > Access Services > Service Selection Rules並標識處理TACACS+身份驗證的訪問服務。在本示例中，它是Default Device Admin。



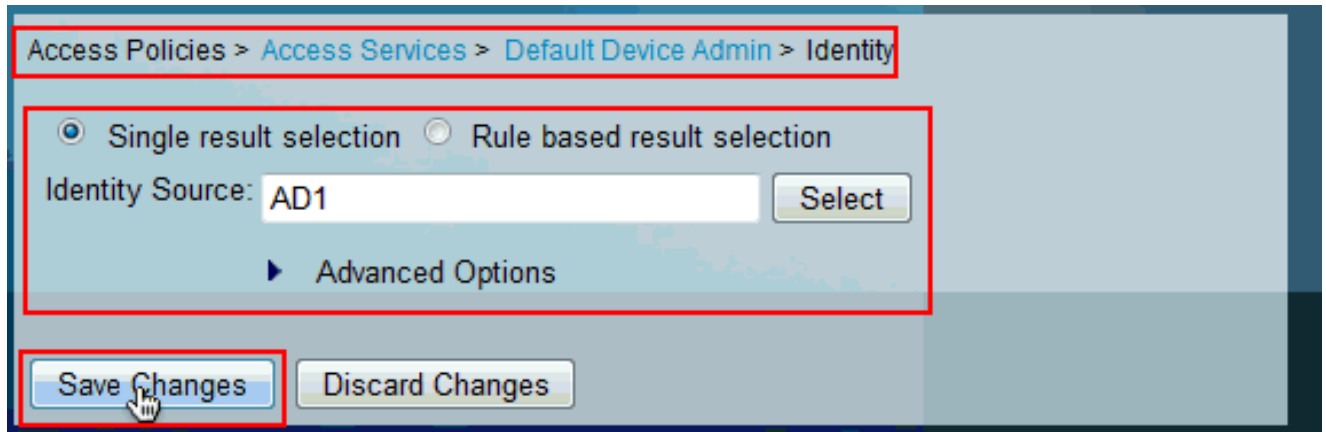
7. 選擇Access Policies > Access Services > Default Device Admin > Identity，然後按一下Identity Source旁邊的Select。



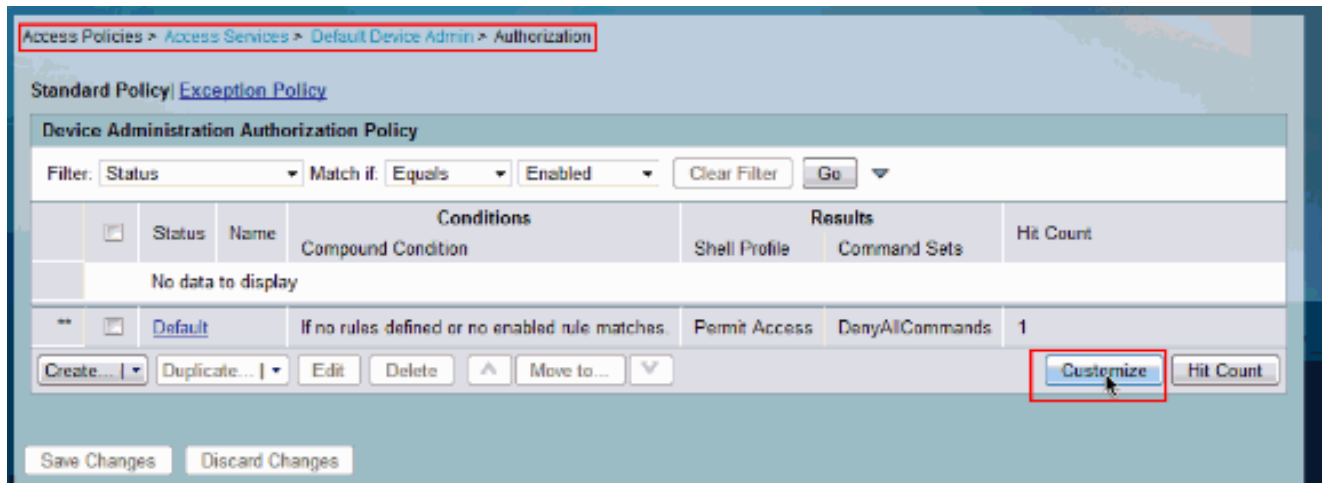
8. 選擇AD1並按一下OK。



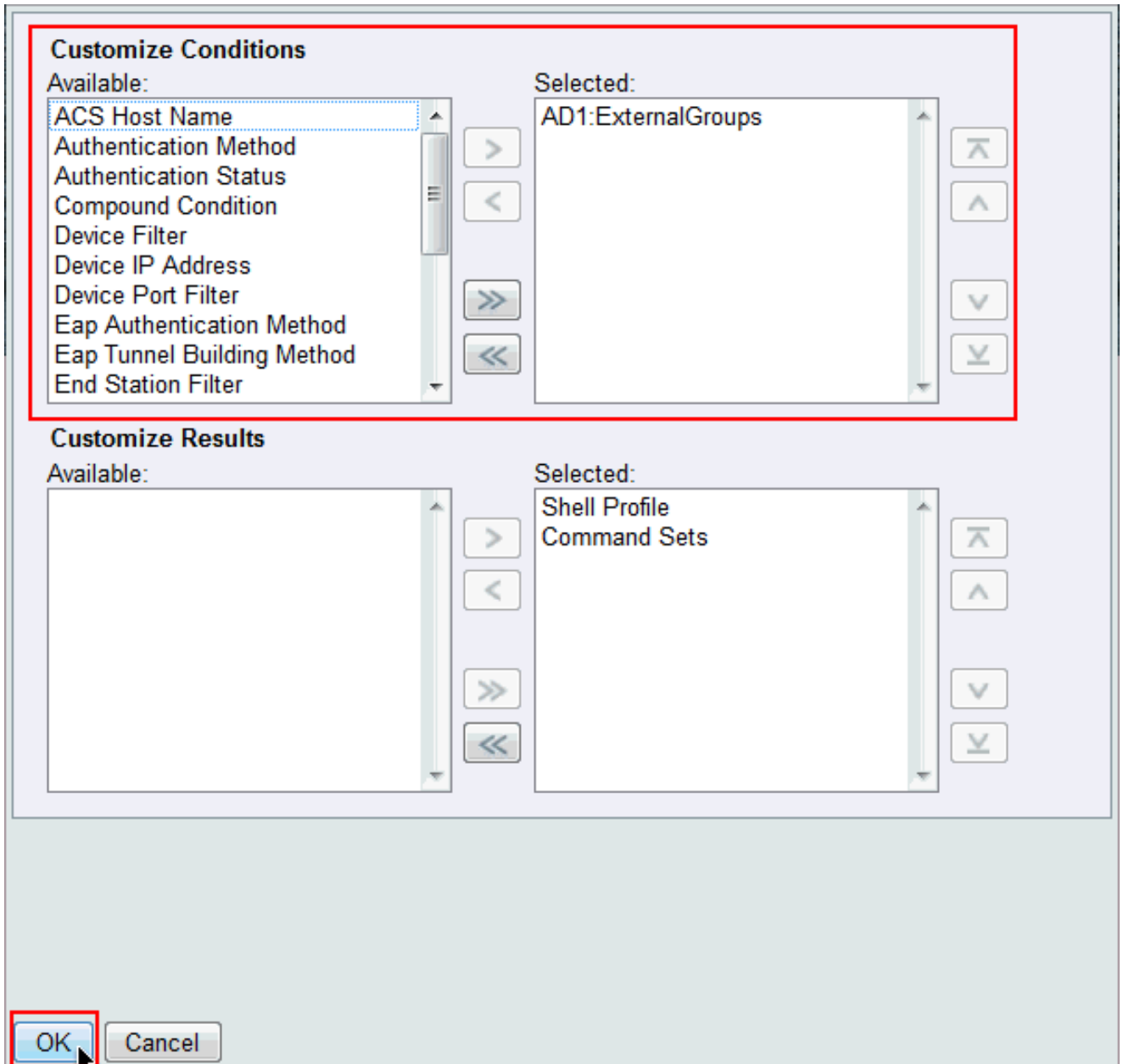
9. 按一下Save Changes。



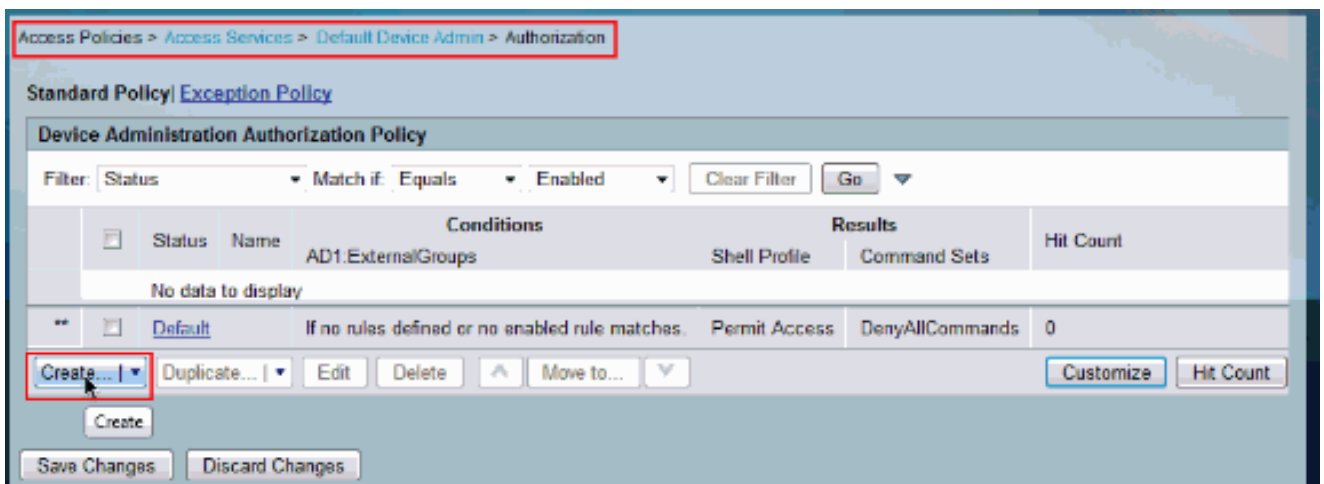
10. 選擇Access Policies > Access Services > Default Device Admin > Authorization，然後按一下Customize。



11. 將AD1 : ExternalGroups從可用複製到自訂條件的選取區段，然後將Shell設定檔和指令集從可用移動到自訂結果區段的選取區段中。現在請按一下OK。

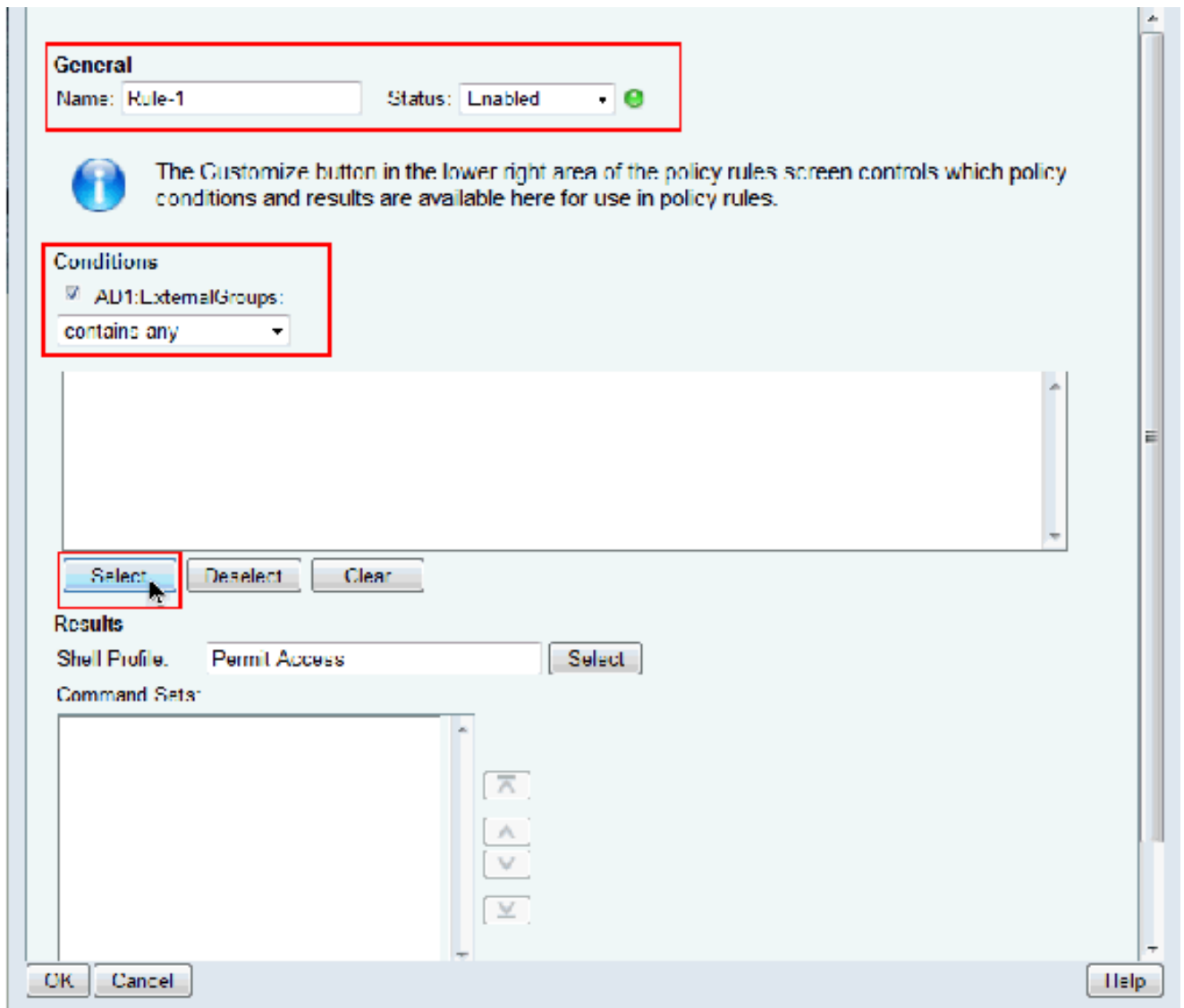


12. 按一下Create以建立新規則。

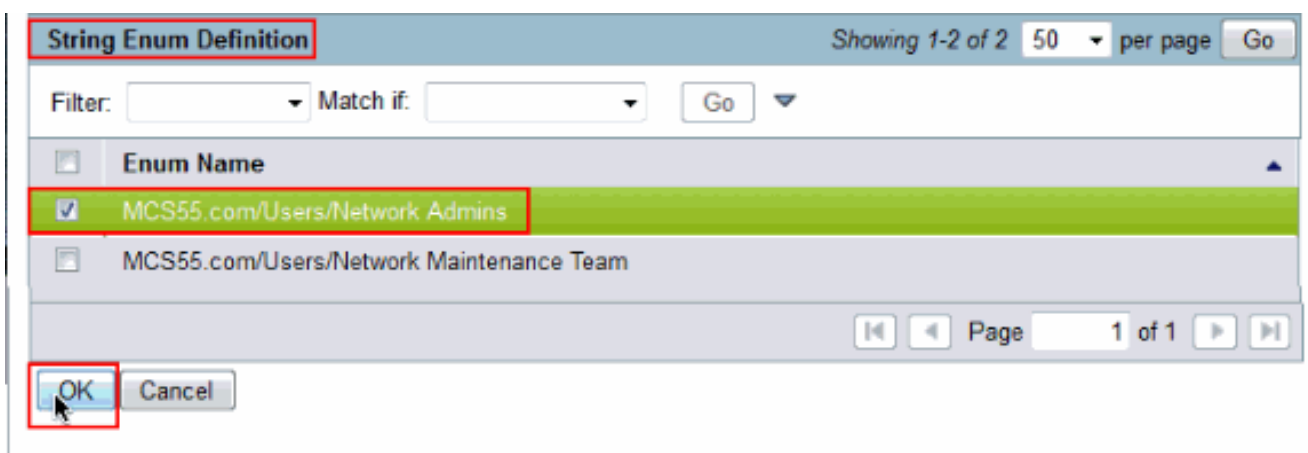


13. 在AD1 : ExternalGroups條件中按一下Select。

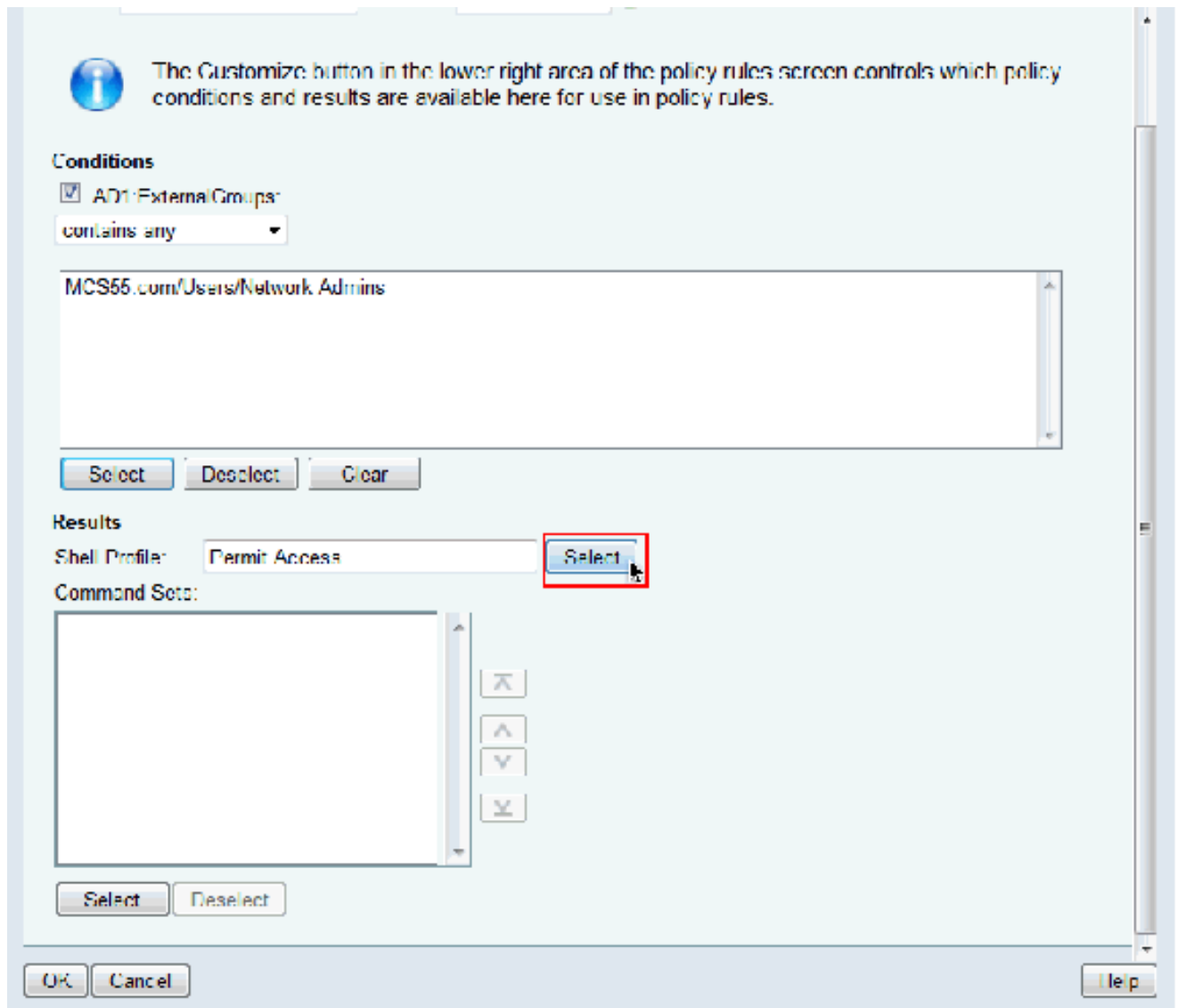




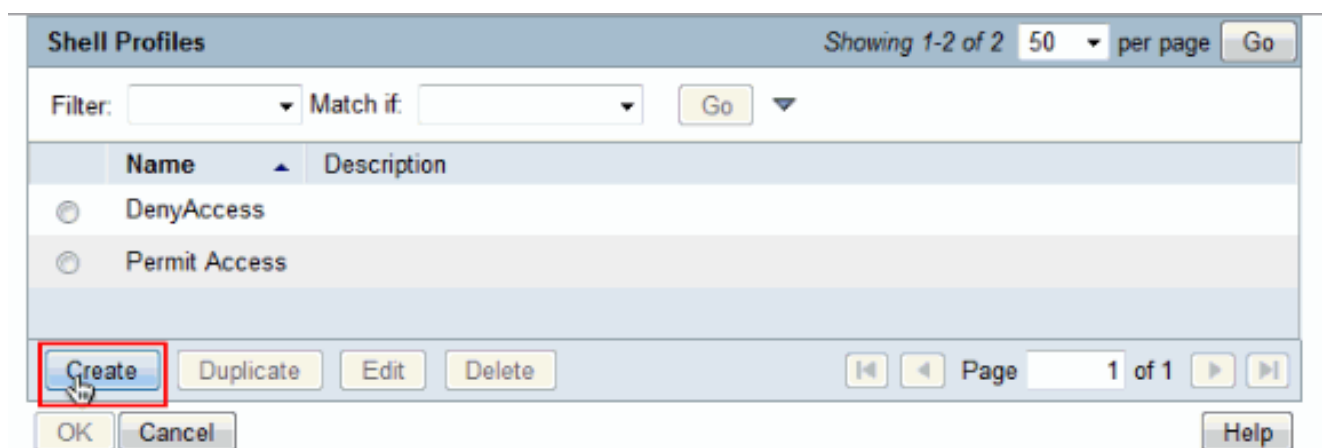
14. 選擇要在Cisco IOS裝置上提供完全訪問許可權的組。按一下「OK」（確定）。



15. 在「Shell Profile」欄位中按一下Select。



16. 按一下Create為擁有完全訪問許可權的使用者建立新的Shell配置檔案。



17. 在常規頁籤中提供名稱和說明（可選），然後按一下常見任務頁籤。

General Common Tasks Custom Attributes

⚙ Name: Full-Privilege

Description: To push default privilege 15 for IOS

⚙ = Required fields

18. 將Default Privilege和Maximum Privilege更改為Static，值15。按一下Submit。

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

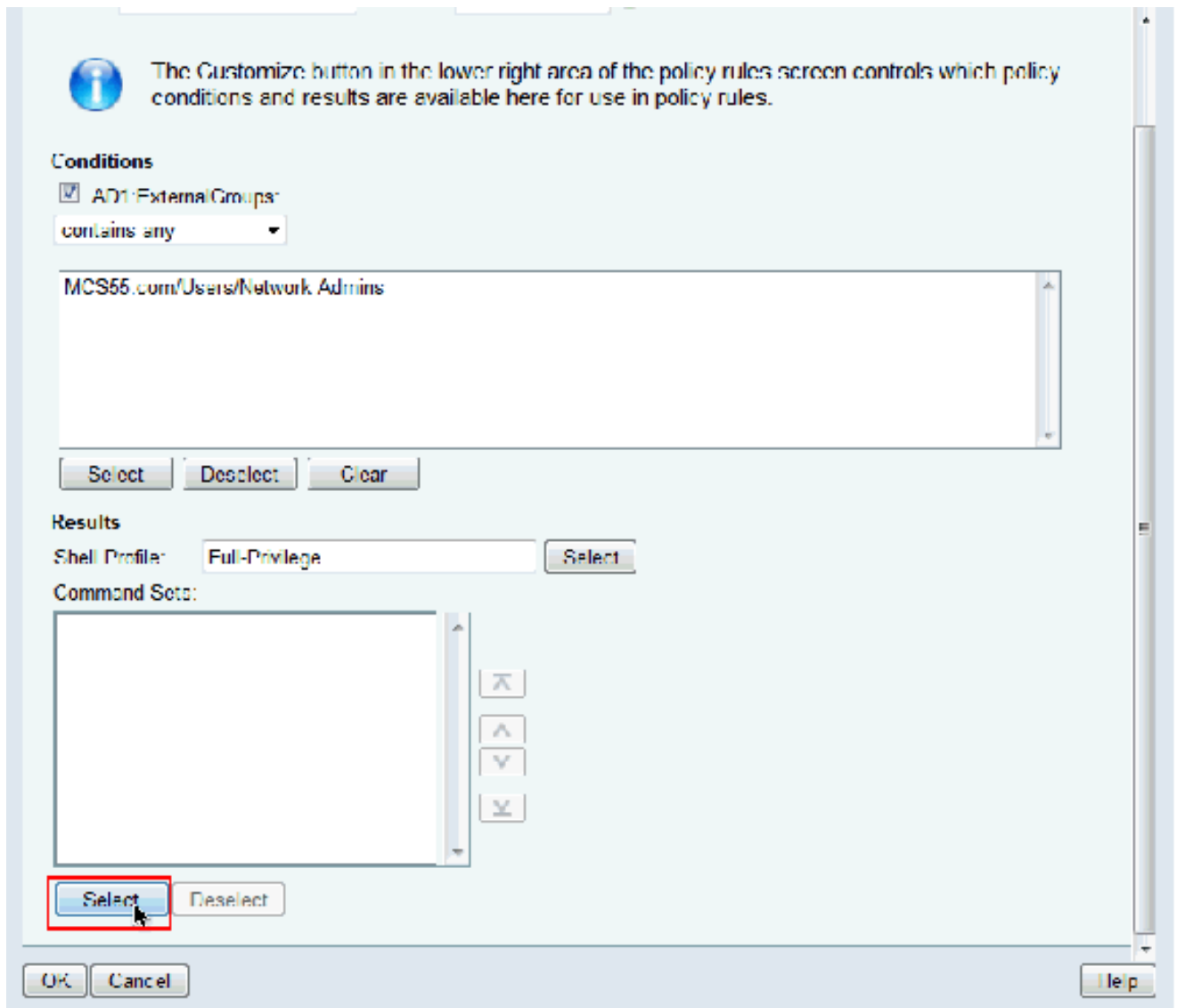
19. 現在選擇新建立的完全訪問Shell配置檔案（在本示例中為Full-Privilege），然後按一下OK。

**Shell Profiles**

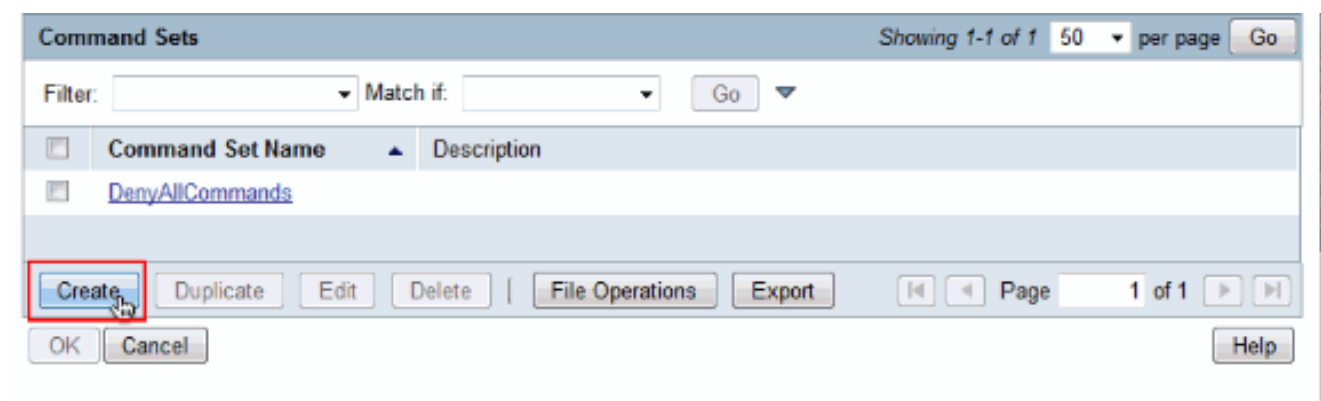
Filter:  Match if:

	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. 在Command Sets欄位中按一下Select。



21. 按一下Create為Full-Access使用者建立一個新的命令集。



22. 提供名稱，並確保選中Permit any command that is not in the table below釁取方塊。按一下Submit。

註：有關命令集的詳細資訊，請參閱[建立、複製和編輯用於裝置管理的命令集](#)。

**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. 按一下「OK」(確定)。

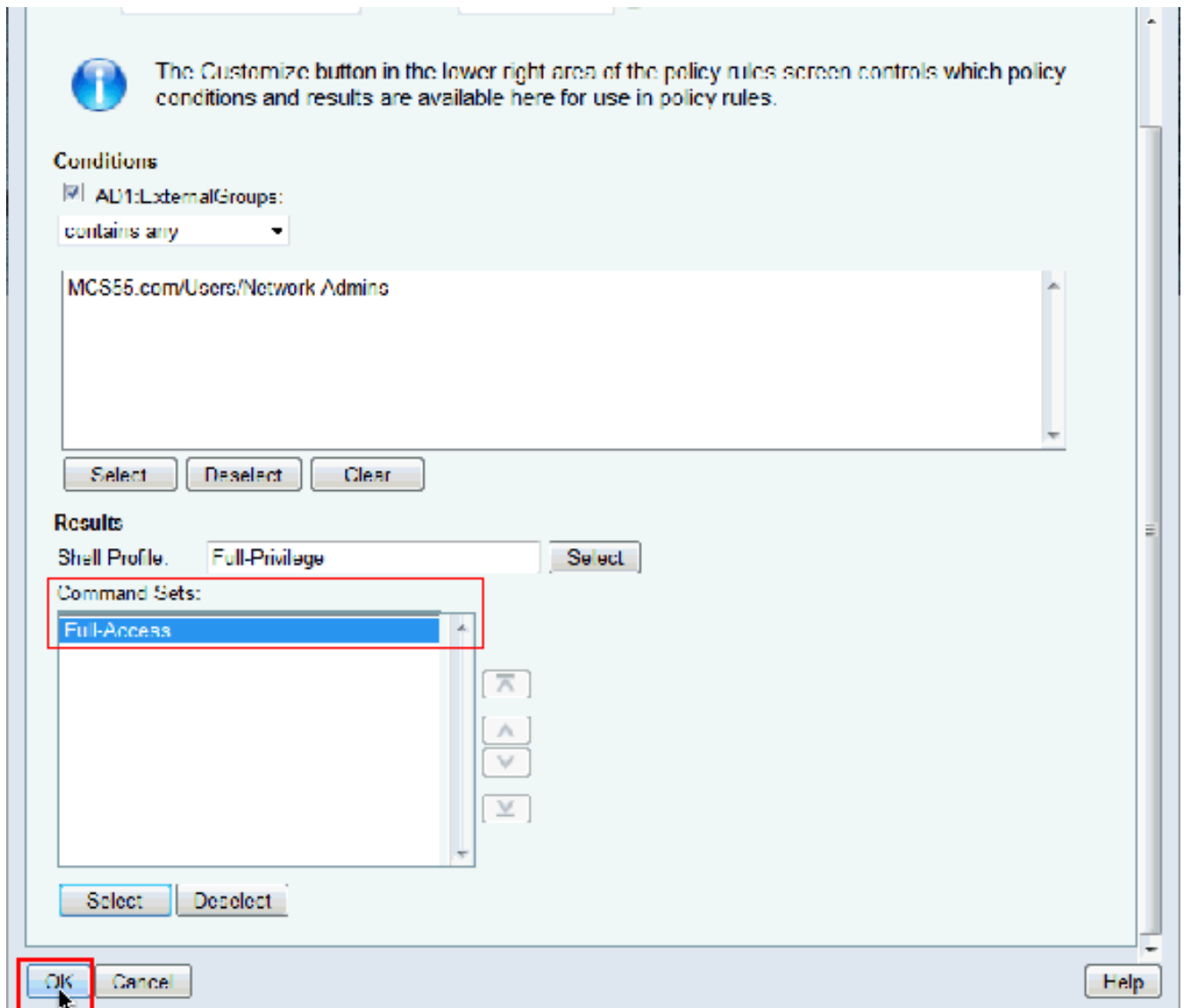
**Command Sets**

Filter:  Match if:

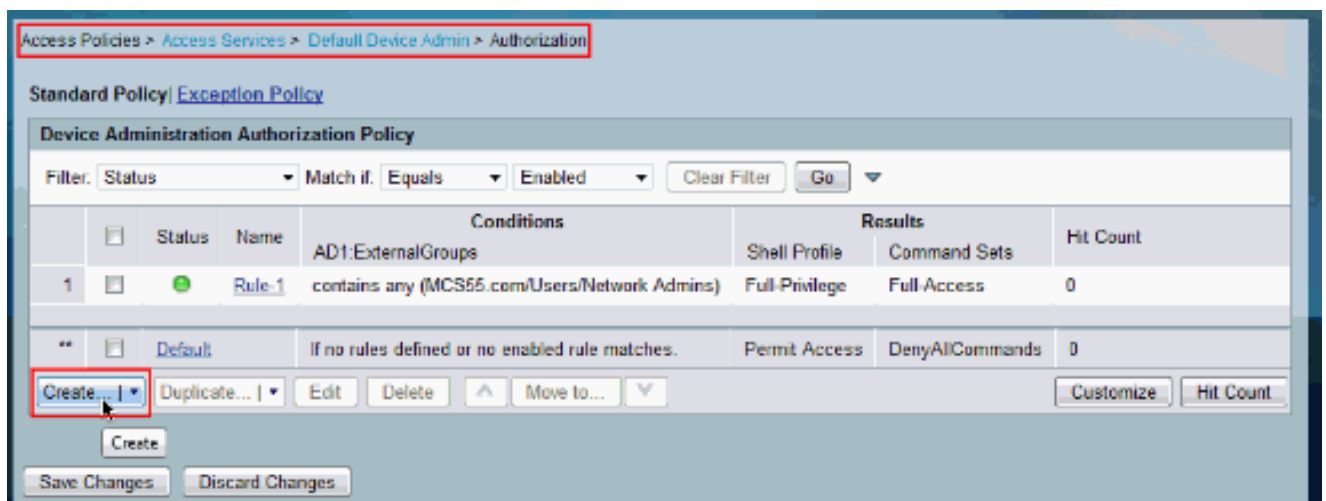
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	<a href="#">DenyAllCommands</a>	
<input checked="" type="checkbox"/>	<a href="#">Full-Access</a>	

|

24. 按一下「OK」(確定)。這將完成Rule-1的配置。

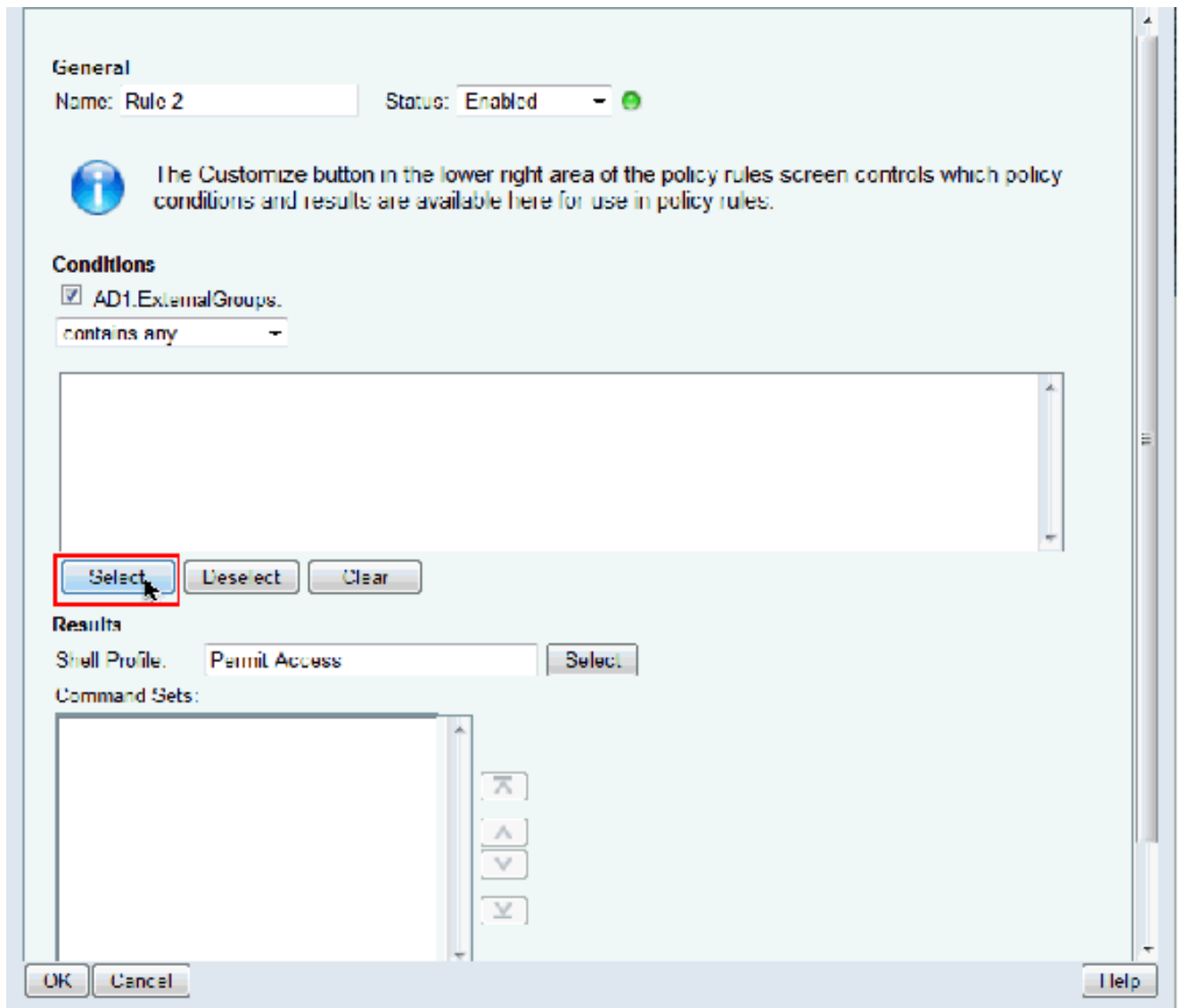


25. 點選建立為有限訪問使用者建立新規則。

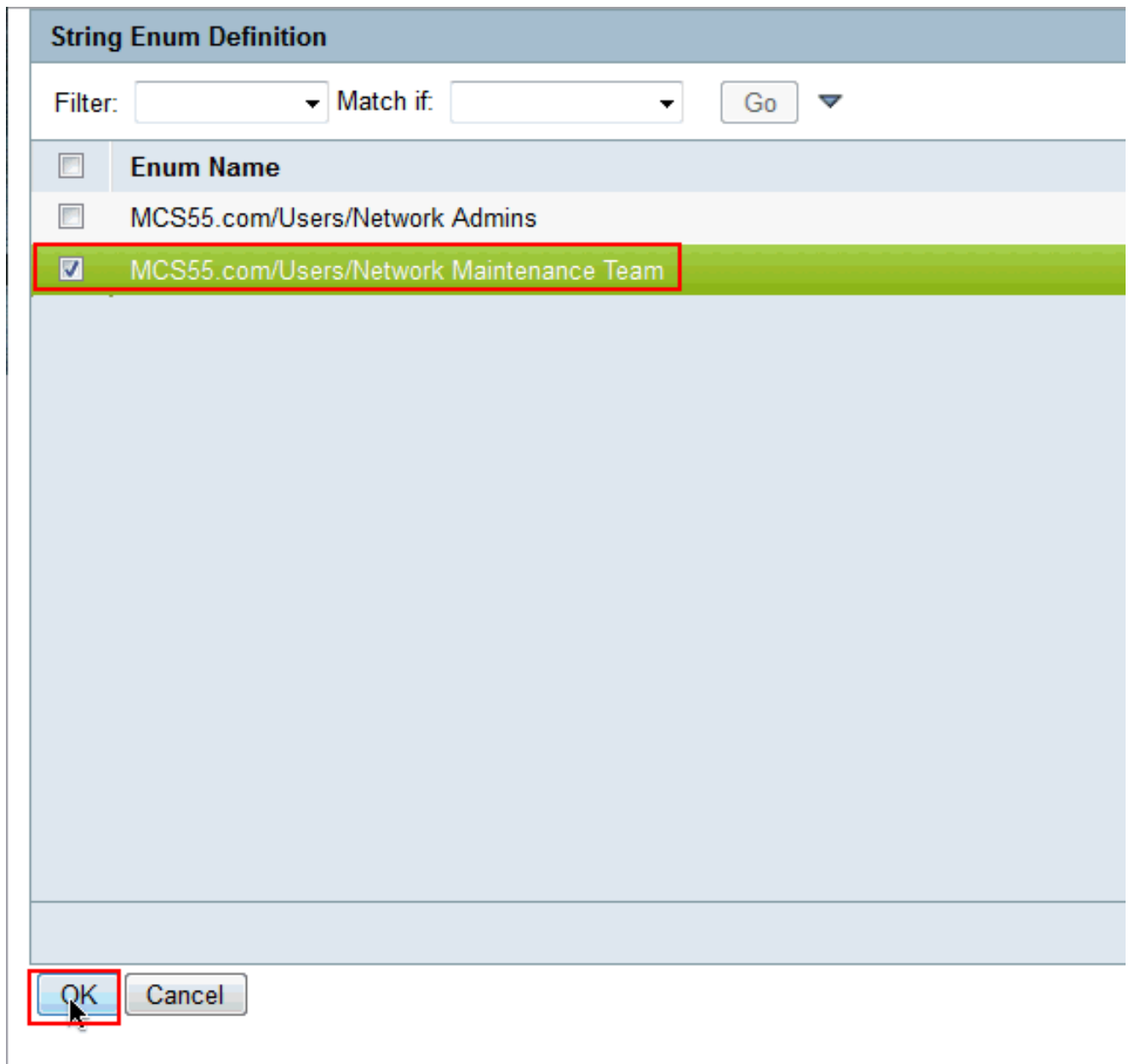


26. 選擇AD1 : ExternalGroups , 然後按一下Select。

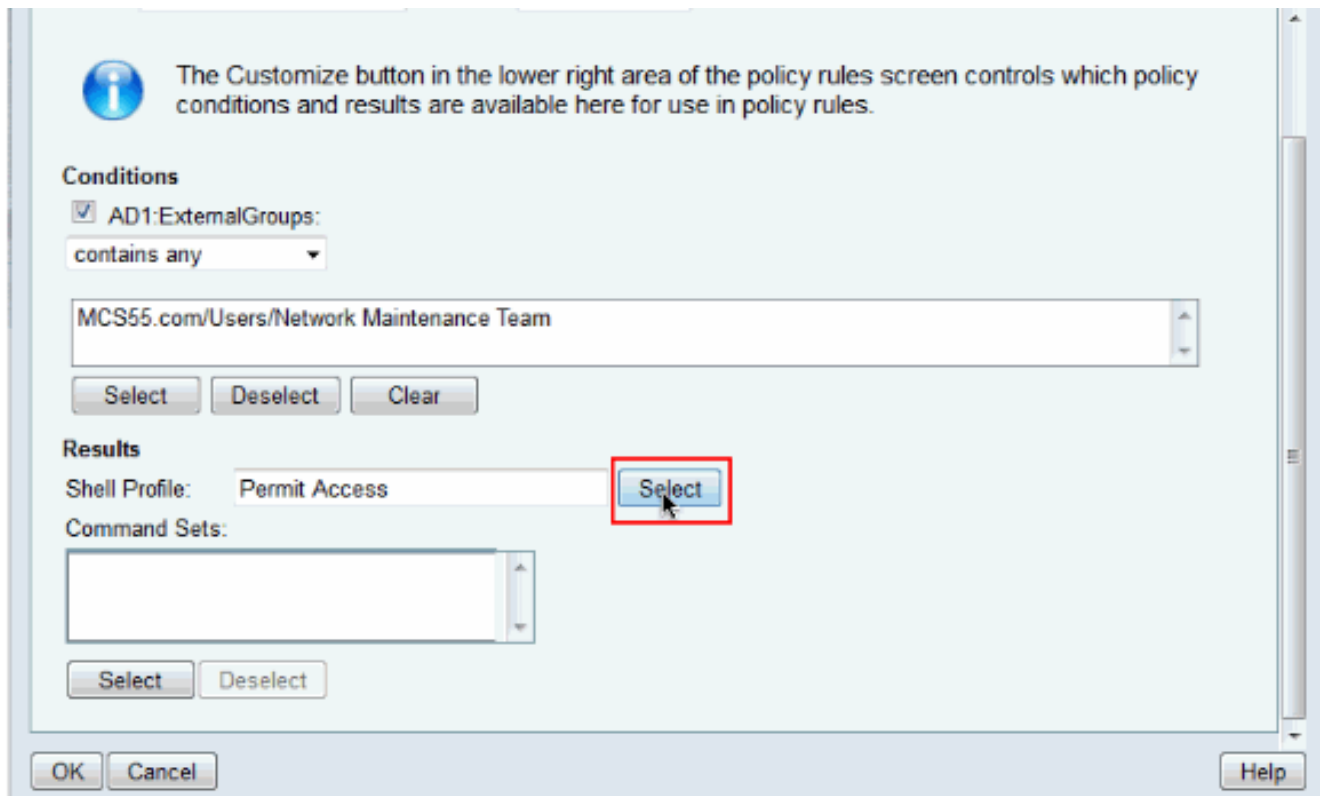




27. 選擇要提供有限訪問許可權的組（或）組，然後按一下OK。



28. 在「Shell Profile」欄位中按一下Select。



29. 按一下Create為受限訪問建立新的Shell配置檔案。

**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. 在常規頁籤中提供名稱和說明（可選），然後按一下常見任務頁籤。

General Common Tasks Custom Attributes

Name: Limited-Privilege  
Description: To push default privilege 1 for IOS

☛ = Required fields

31. 分別將預設許可權和最大許可權更改為靜態，值為1和15。按一下Submit。

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

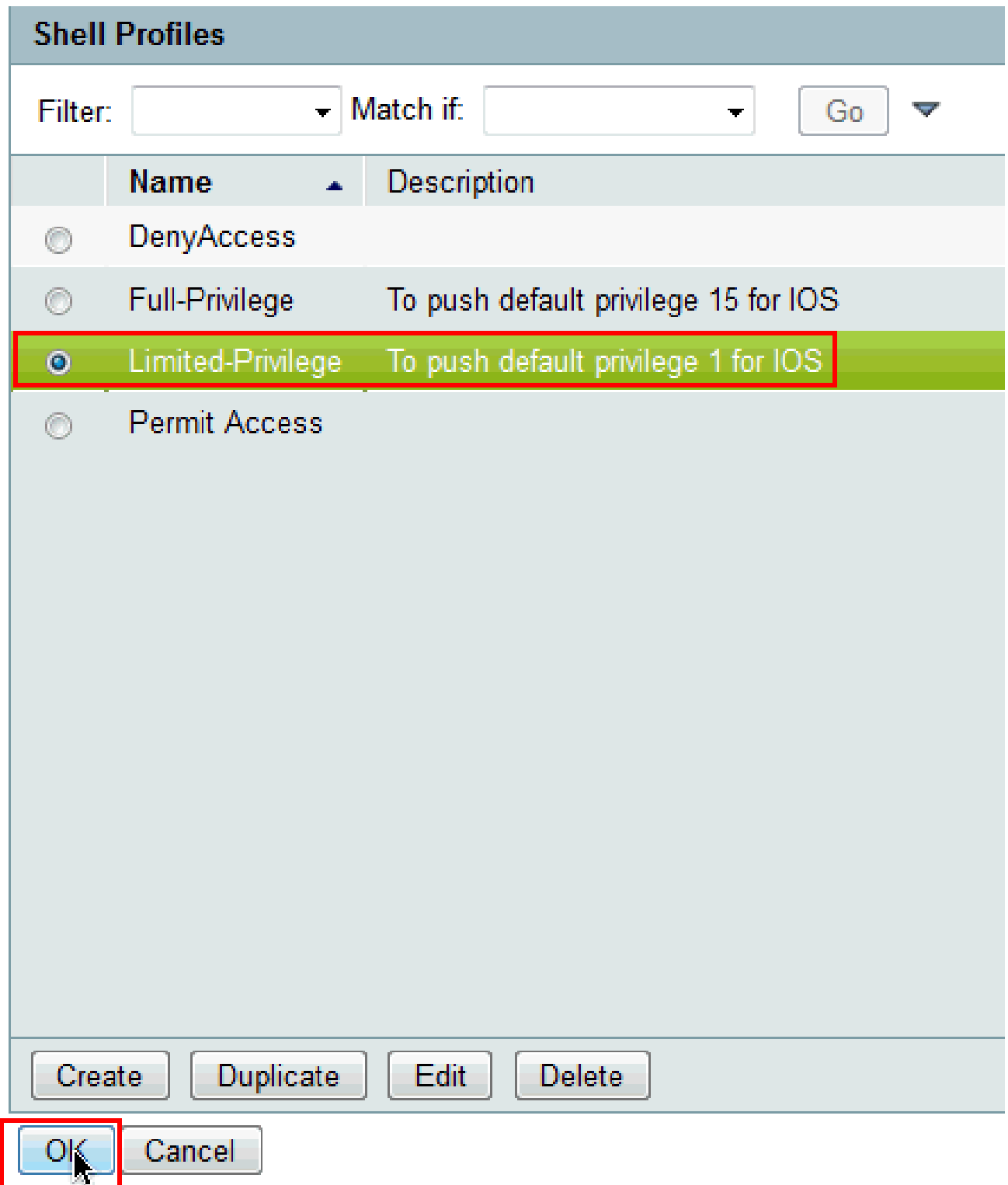
Callback Line: Not in Use

Callback Rotary: Not in Use

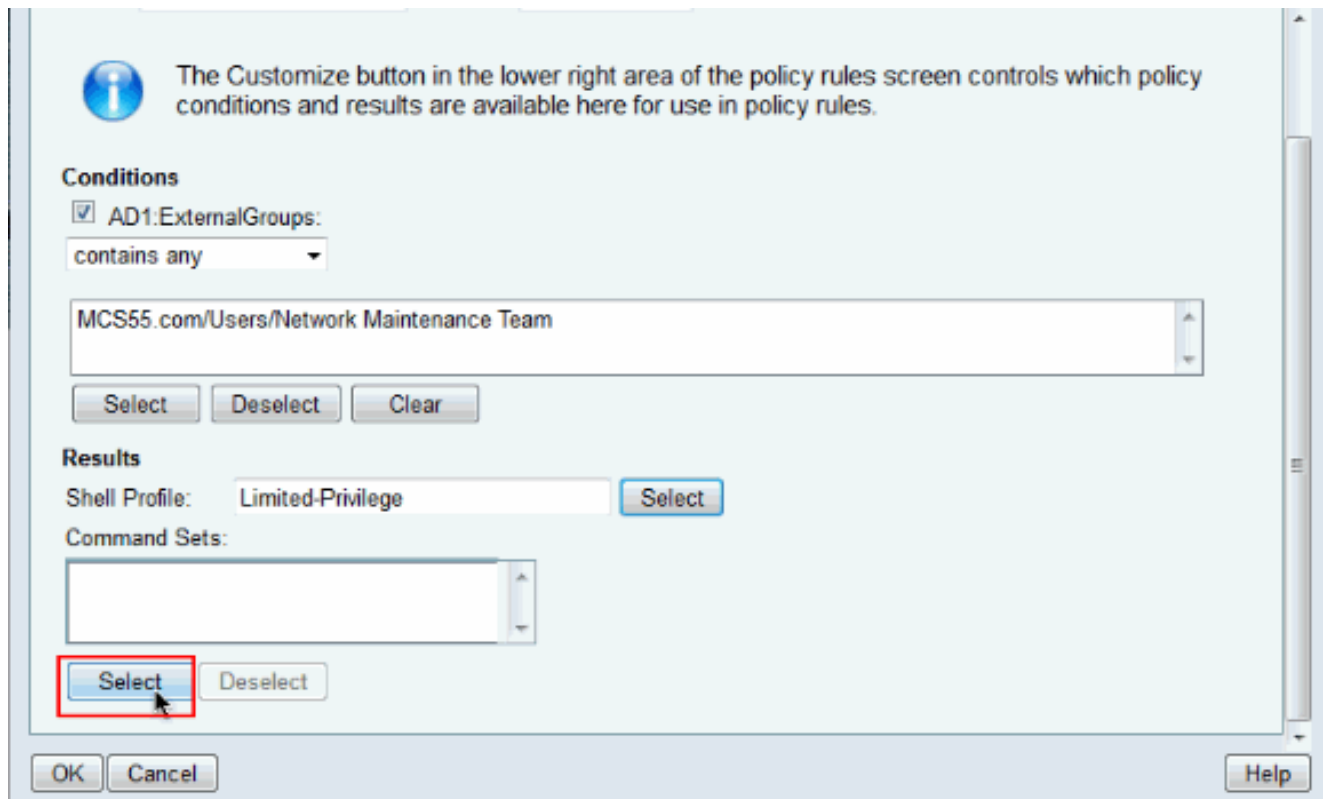
 = Required fields

Submit Cancel

32. 按一下「OK」(確定)。

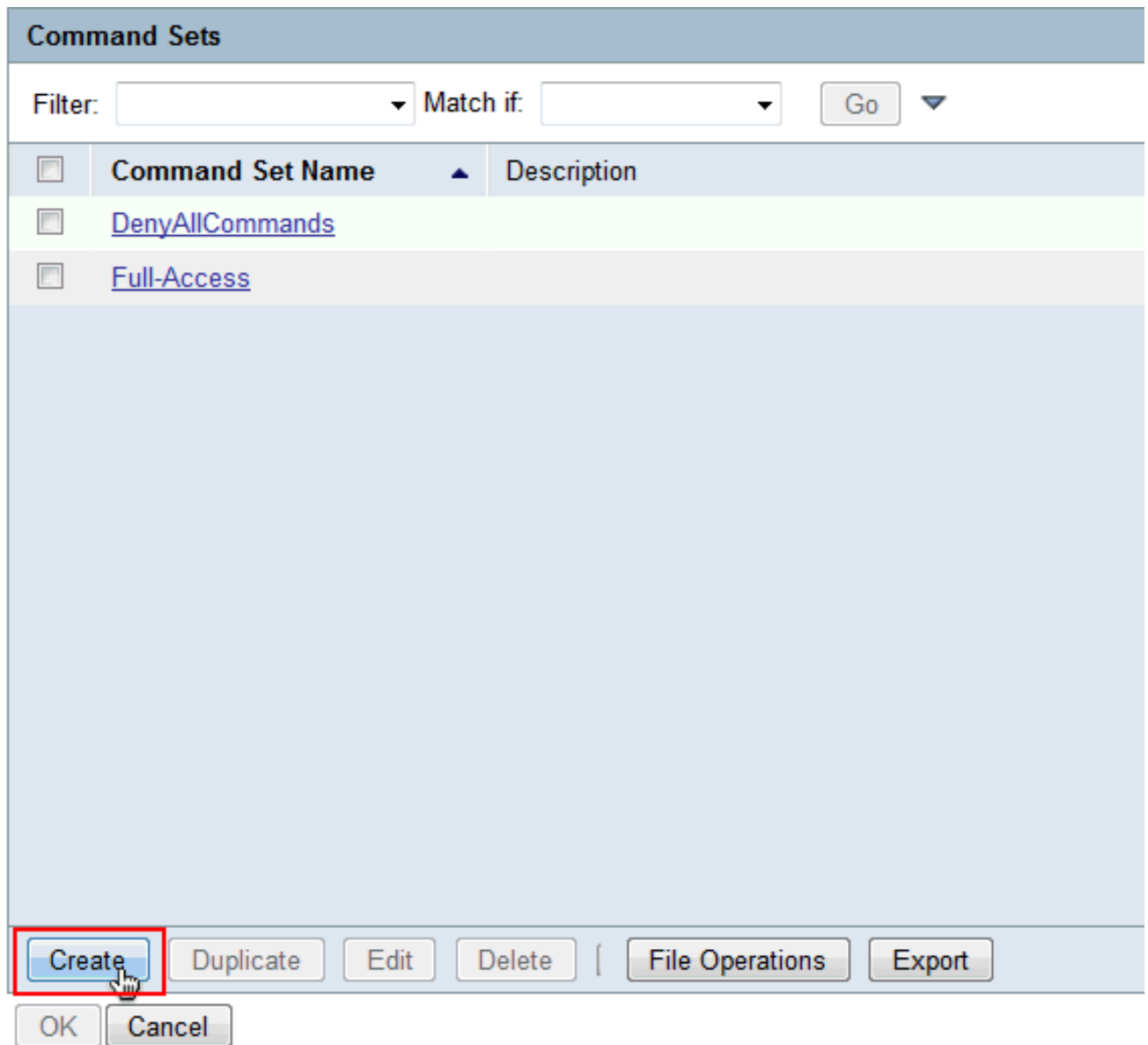


33. 在Command Sets欄位中按一下Select。



34. 按一下Create為受限訪問組建立新的命令集。





35. 提供名稱，並確保未選中Permit any command that not in the table旁邊的覈取方塊。在命令部分提供的空白處鍵入show後，按一下Add，然後在Grant部分中選擇Permit，以便僅允許有限訪問組中的使用者使用show命令。

**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. 類似地，使用Add增加任何其他要允許有限訪問組內的使用者使用的命令。按一下Submit。

註：有關命令集的詳細資訊，請參閱[建立、複製和編輯用於裝置管理的命令集](#)。

**General**

Name:

Description:

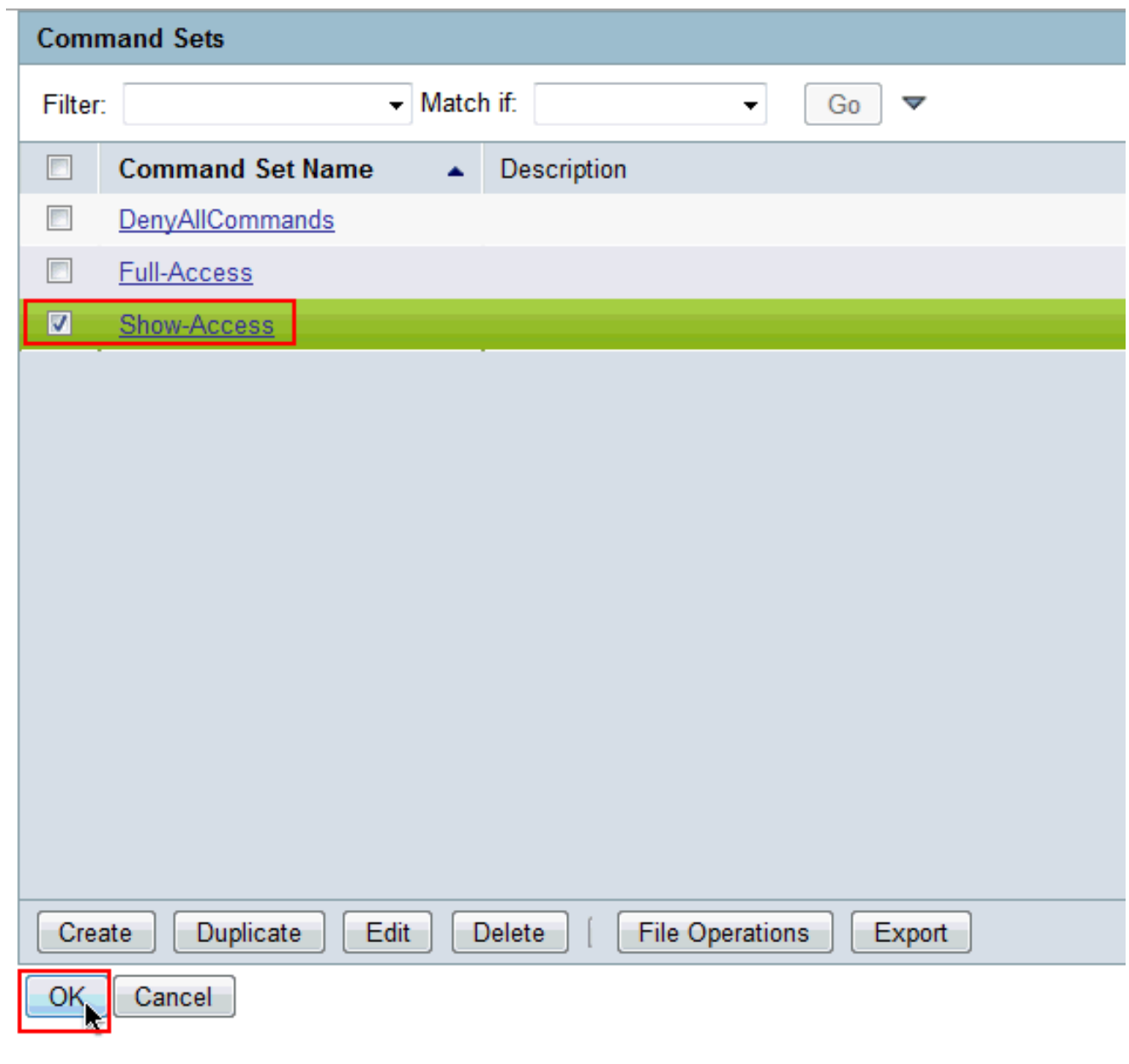
Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant:  Command:  Arguments:

Select Command/Arguments from Command Set:

37. 按一下「OK」(確定)。



38. 按一下「OK」(確定)。



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

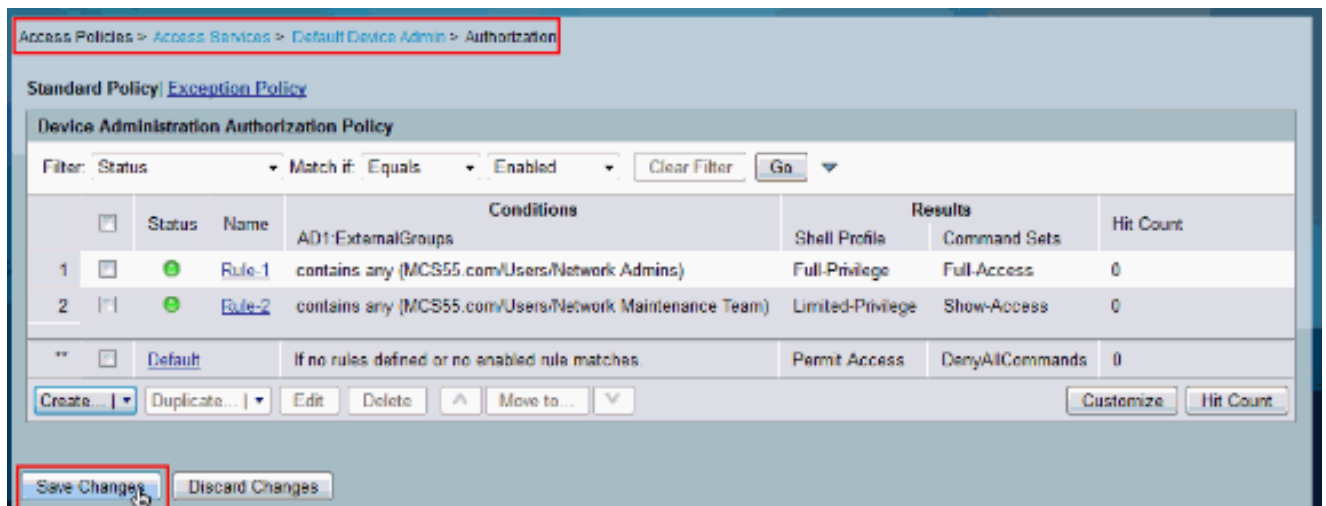
Select

Deselect

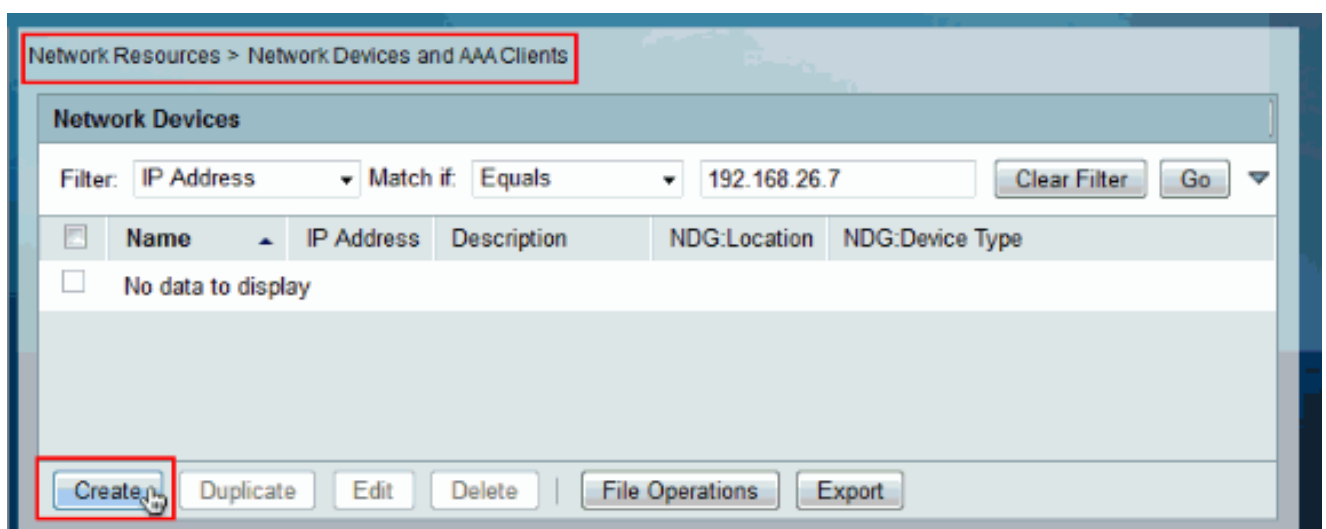
OK

Cancel

39. 按一下Save Changes。



40. 按一下Create以將Cisco IOS裝置增加為ACS上的AAA Client。



41. 為TACACS+提供名稱、IP地址、共用金鑰，然後按一下提交。

## 配置Cisco IOS裝置以進行身份驗證和授權

完成以下步驟以配置Cisco IOS裝置和ACS以進行身份驗證和授權。

1. 使用username命令建立一個具有完全回退許可權的本地使用者，如下所示：

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

2. 提供ACS的IP地址以啟用AAA並增加ACS 5.x作為TACACS伺服器。

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

注意：金鑰應與ACS上為此Cisco IOS裝置提供的共用金鑰匹配。

3. 使用[test aaa](#)命令測試TACACS伺服器可接通性，如下所示。

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

上一個命令的輸出顯示，TACACS伺服器可訪問，並且使用者已成功透過身份驗證。

注意：User1和密碼xxx屬於AD。如果測試失敗，請確保上一步中提供的共用金鑰正確。

4. 配置登入並啟用身份驗證，然後使用Exec和命令授權，如下所示：

```
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
```

注意：如果TACACS伺服器無法訪問，則Local和Enable關鍵字分別用於回退到Cisco IOS本地使用者和啟用金鑰。

## 驗證

為了驗證身份驗證和授權，請透過Telnet登入到Cisco IOS裝置。

1. 以user1的身份透過Telnet連線到Cisco IOS裝置，該使用者屬於AD中的完全訪問組。Network Admins組是AD中對映到ACS上設定的完全許可權外殼配置檔案和完全訪問命令的組。嘗試運行任何命令以確保您具有完全訪問許可權。

```
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. 以user2身份透過Telnet連線到Cisco IOS裝置，該使用者屬於AD中的有限訪問組。(網路維護團隊組是AD中對映到ACS上有限許可權外殼配置檔案和Show-Access命令集的組)。如果您嘗試運行Show-Access命令集中提到的命令以外的任何命令，您應該收到Command Authorization Failed錯誤，其中顯示user2具有有限的訪問許可權。



```

username: user2
password:

router1>enable
password:
router1#
router1#
router1#show version
Cisco IOS Software, C3550 Software (C3550-IPBASEK9-M), version 12.2(44)SE6, RELEASE S
FTWARE (fc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text base: 0x00003000, data base: 0x00EA3DE8

ROM: Bootstrap program is C3550 boot loader

router1 uptime is 16 hours, 46 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-44.SE6.bin"

                    55
                    55

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/export/crypto/qa/slsrpt.html

If you require further assistance please contact us by sending email to
export@cisco.com.

router1#conf t
Command authorization failed.

router1#wr mem
Command authorization failed.

router1#

```

- 登入到ACS GUI並啟動Monitoring and Reports viewer。選擇AAA Protocol > TACACS+Authorization以驗證user1和user2所執行的活動。

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 6:21:18.393 AM	✓			user2	[CmdAV=exec ]		lab-router
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:58.793 AM	✗		11021 Command failed to match a Permit rule	user2	[CmdAV=write memory ]		lab-router
Jun 8,12 6:20:58.986 AM	Jun 8,12 6:20:58.810 AM	✗		11021 Command failed to match a Permit rule	user2	[CmdAV=configure terminal ]		lab-router
Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50.036 AM	✓			user2	[CmdAV=show version ]		lab-router
Jun 8,12 6:20:38.506 AM	Jun 8,12 6:20:38.490 AM	✓			user2	[CmdAV=enable ]		lab-router
Jun 8,12 6:20:34.426 AM	Jun 8,12 6:20:34.406 AM	✓			user2	[CmdAV=]	Limited-Privilege	lab-router
Jun 8,12 6:20:02.616 AM	Jun 8,12 6:20:02.596 AM	✓			user1	[CmdAV=exec ]		lab-router
Jun 8,12 6:20:00.246 AM	Jun 8,12 6:20:00.246 AM	✓			user1	[CmdAV=version 2 ]		lab-router
Jun 8,12 6:19:57.203 AM	Jun 8,12 6:19:57.200 AM	✓			user1	[CmdAV=router rip ]		lab-router
Jun 8,12 6:19:55.103 AM	Jun 8,12 6:19:55.076 AM	✓			user1	[CmdAV=configure terminal ]		lab-router
Jun 8,12 6:19:52.743 AM	Jun 8,12 6:19:52.740 AM	✓			user1	[CmdAV=]	Full-Privilege	lab-router

## 相關資訊

- [思科安全存取控制系統](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。