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以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

本文提供使用Cisco Secure Access Control System(ACS)5.x及更高版本根據使用者的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資源，例如使用者、電腦、組和屬性。

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整合配置示例以瞭解詳細資訊，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：**可以在所有Cisco IOS裝置上完成此配置。
- 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。

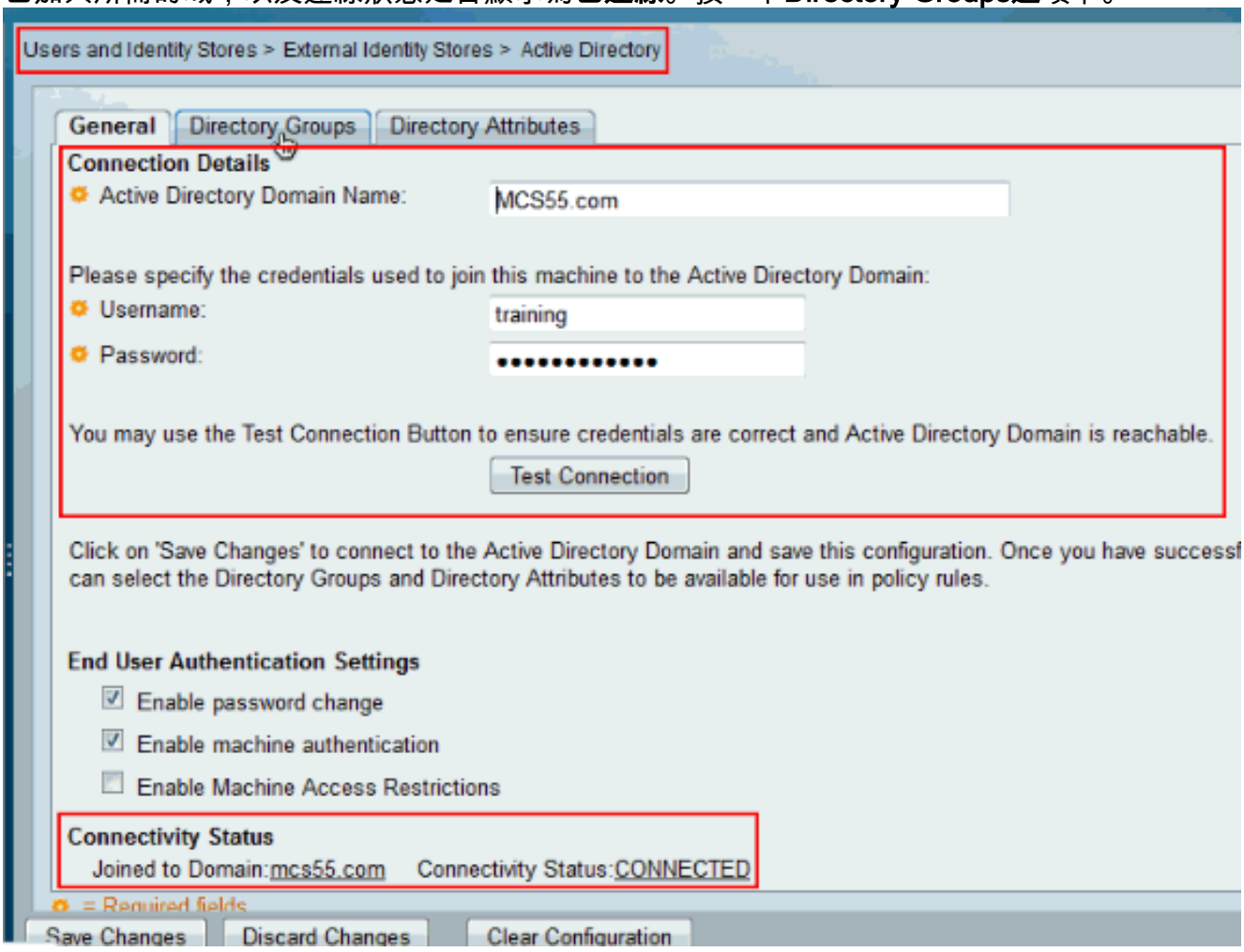
組態

配置ACS 5.x以進行身份驗證和授權

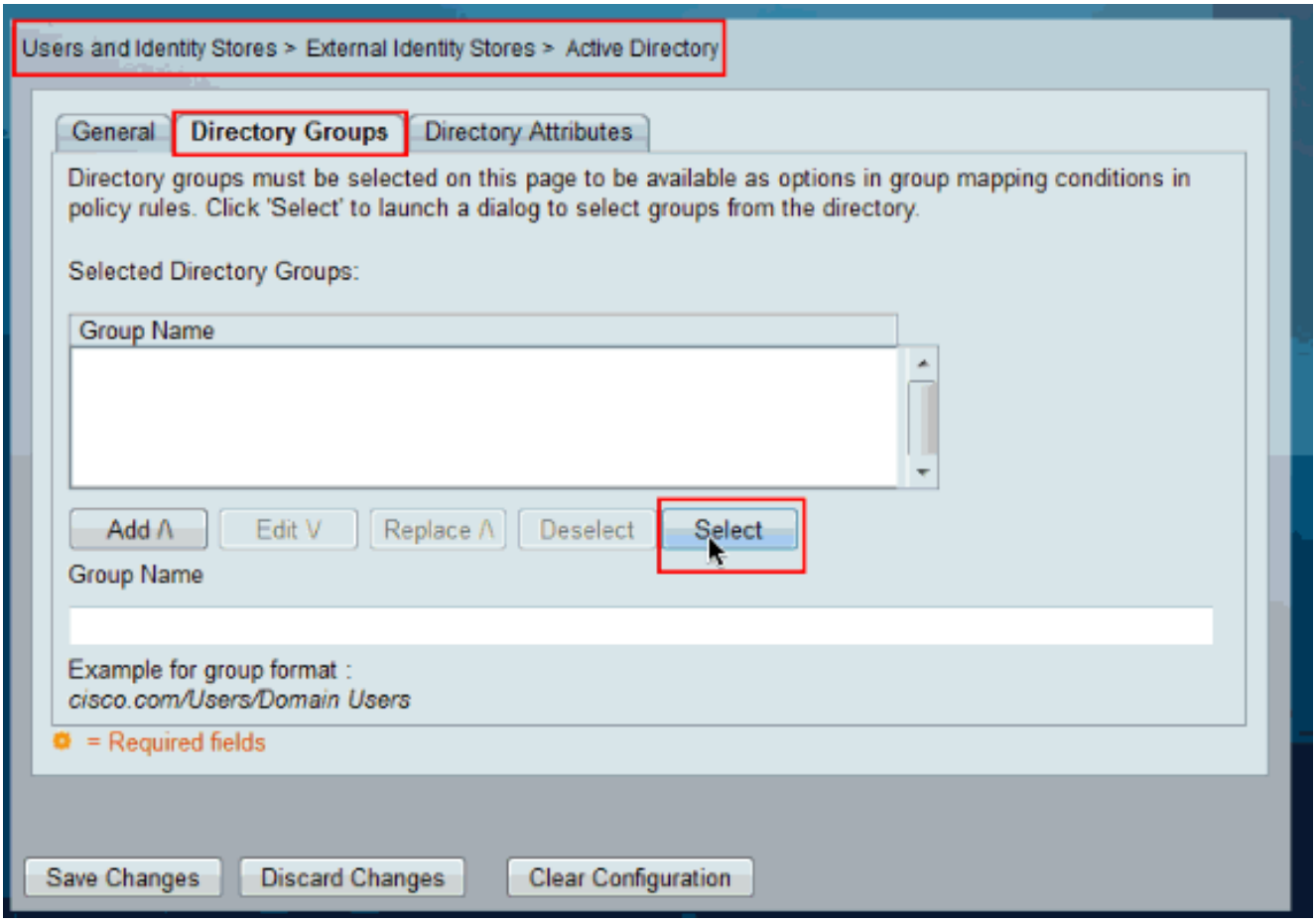
在開始配置ACS 5.x進行身份驗證和授權之前，應該已經將ACS成功與Microsoft AD整合。如果ACS未與所需的AD域整合，請參閱ACS 5.x及更高版本：與Microsoft Active Directory整合配置示例以瞭解詳細資訊，以便執行整合任務。

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。

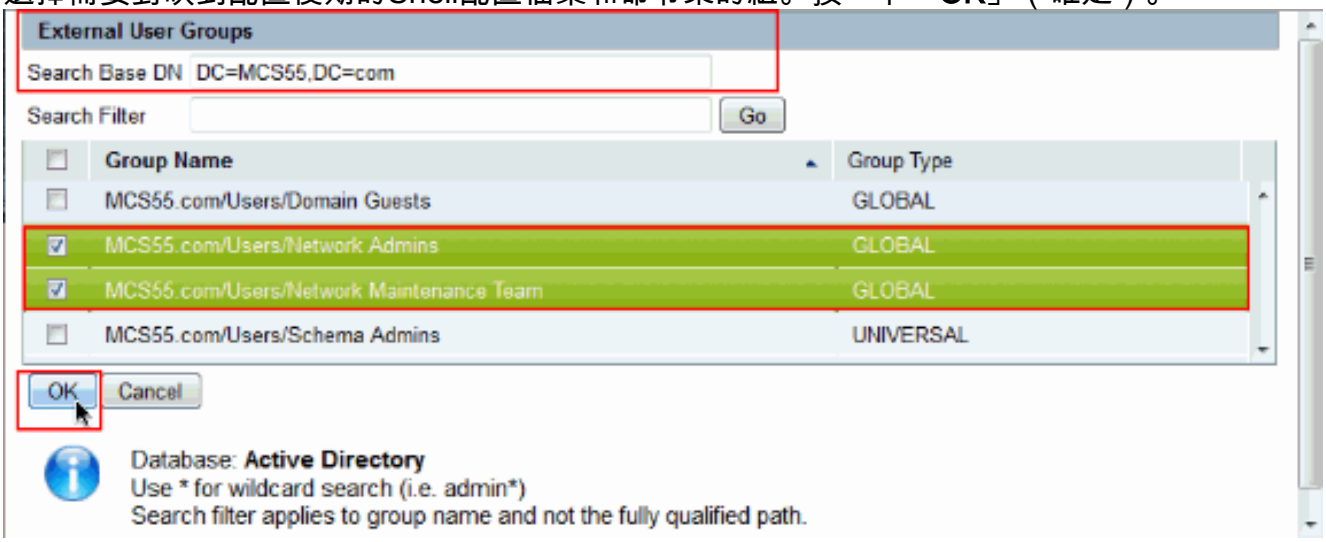
1. 使用管理員憑據登入ACS GUI。
2. 選擇**Users and Identity Stores > External Identity Stores > Active Directory**，並驗證ACS是否已加入所需的域，以及連線狀態是否顯示為**已連線**。按一下**Directory Groups**選項卡。



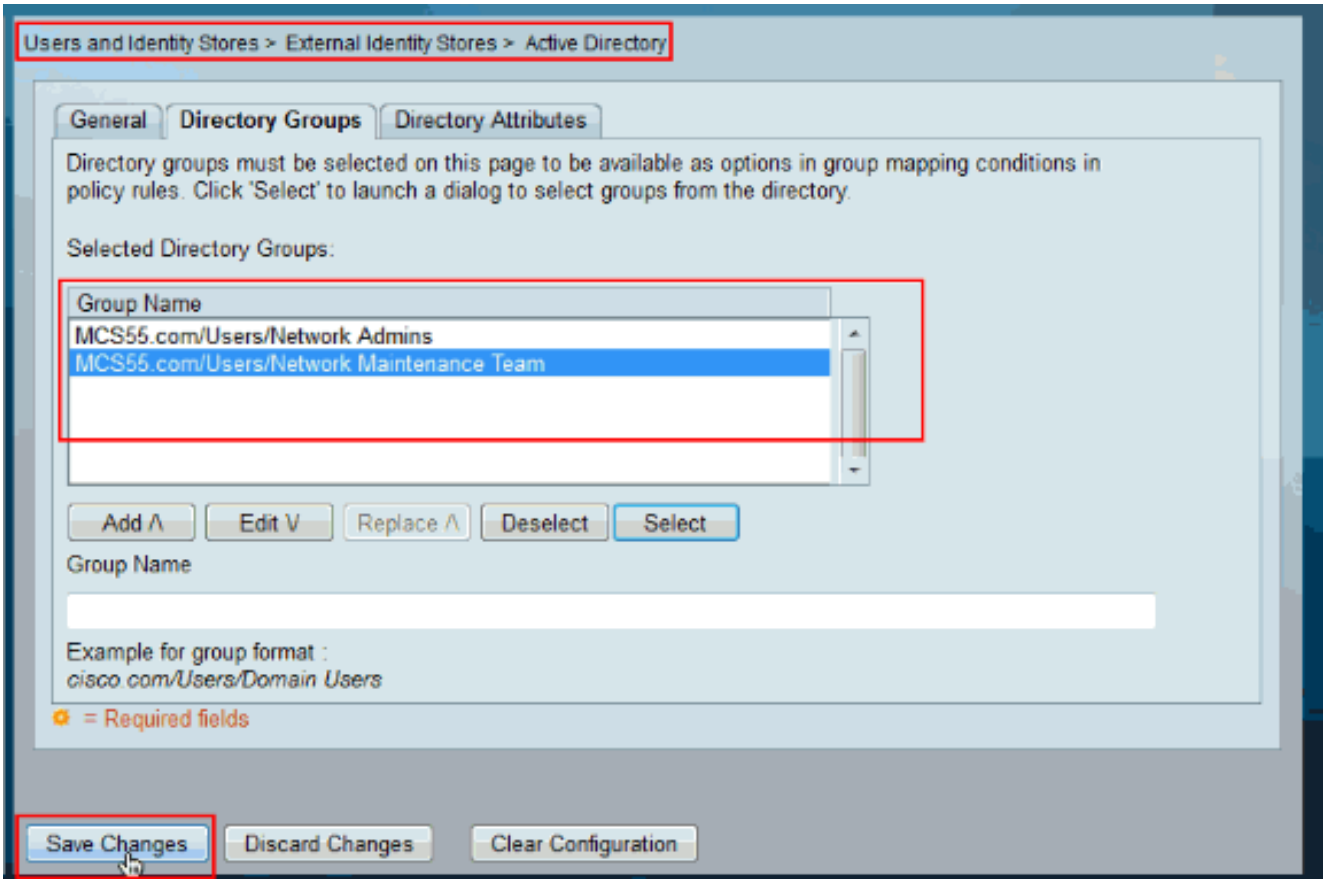
3. 按一下「**Select**」。



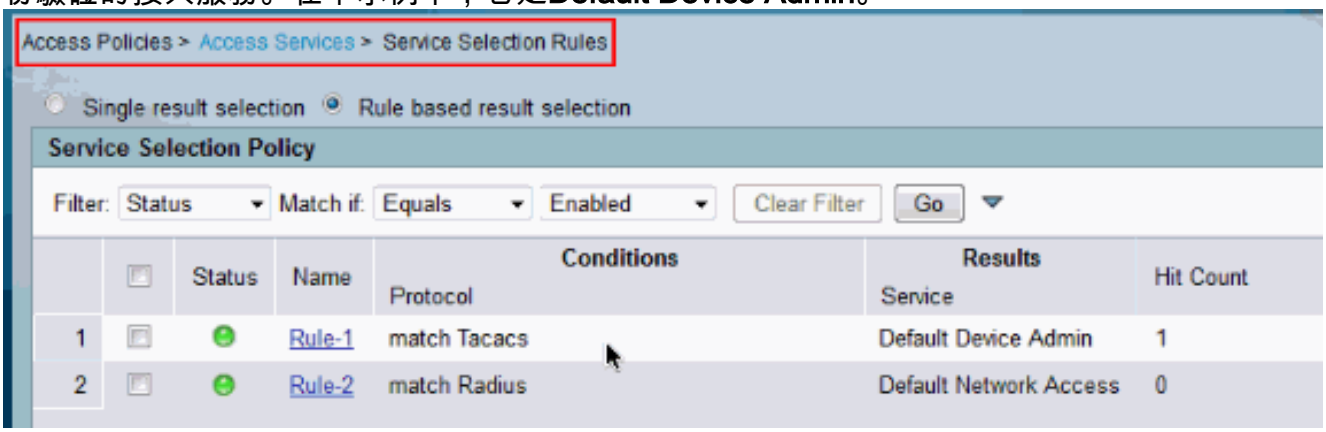
4. 選擇需要對映到配置後期的Shell配置檔案和命令集的組。按一下「**OK**」（確定）。



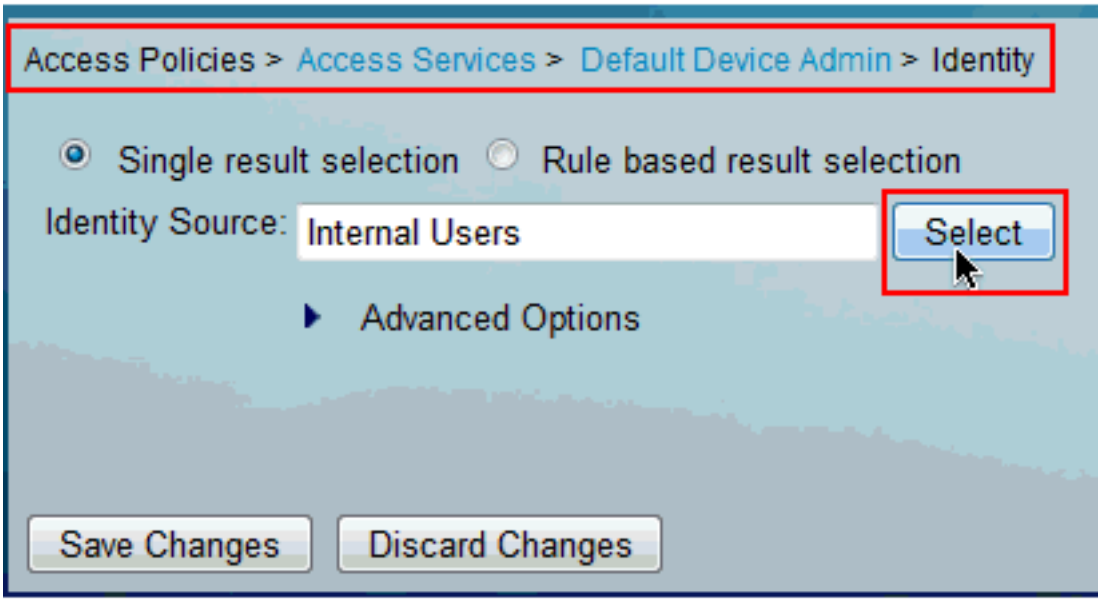
5. 按一下「**Save Changes**」。



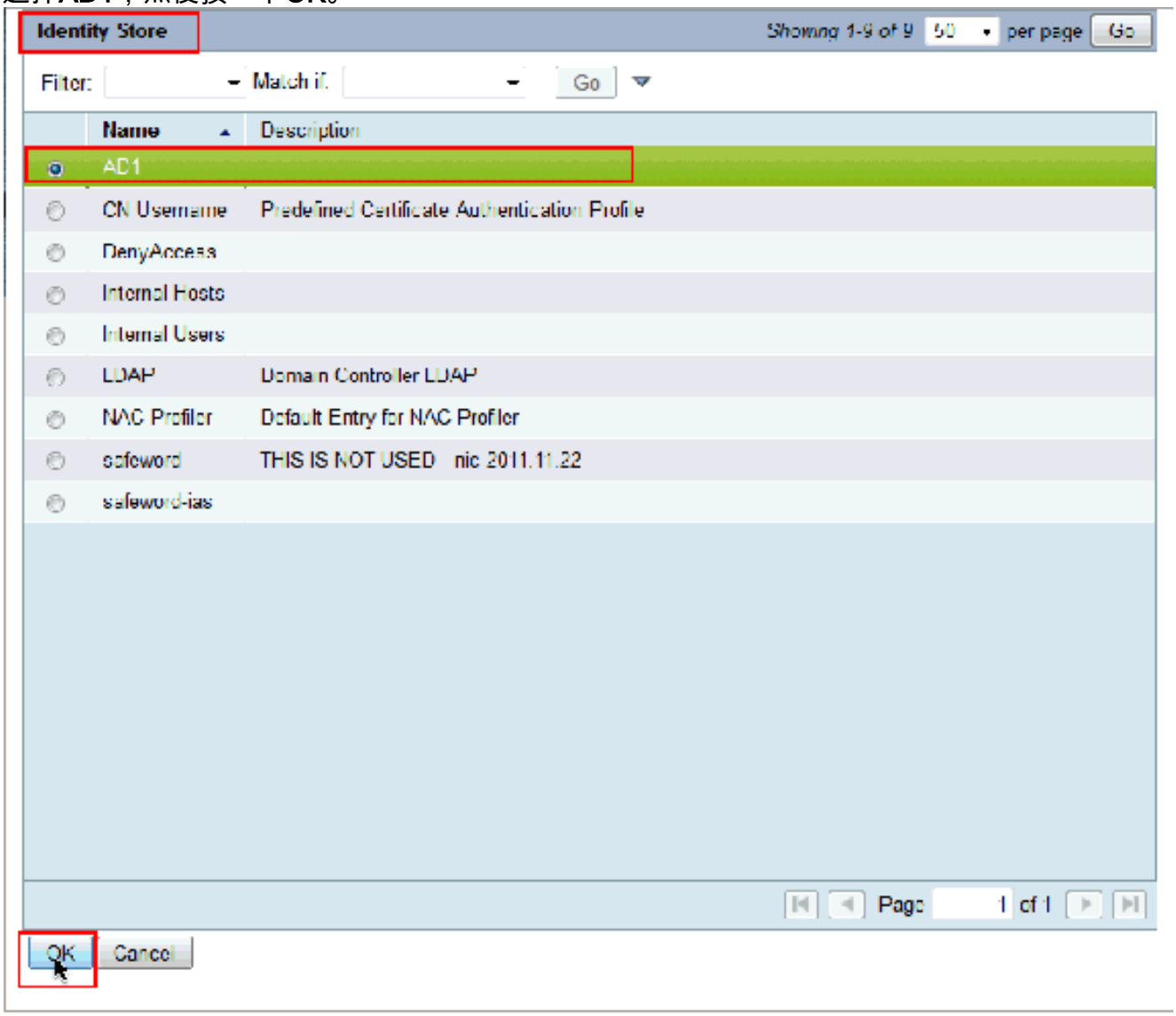
6. 選擇**Access Policies > Access Services > Service Selection Rules**，並確定處理TACACS+身份驗證的接入服務。在本示例中，它是**Default Device Admin**。



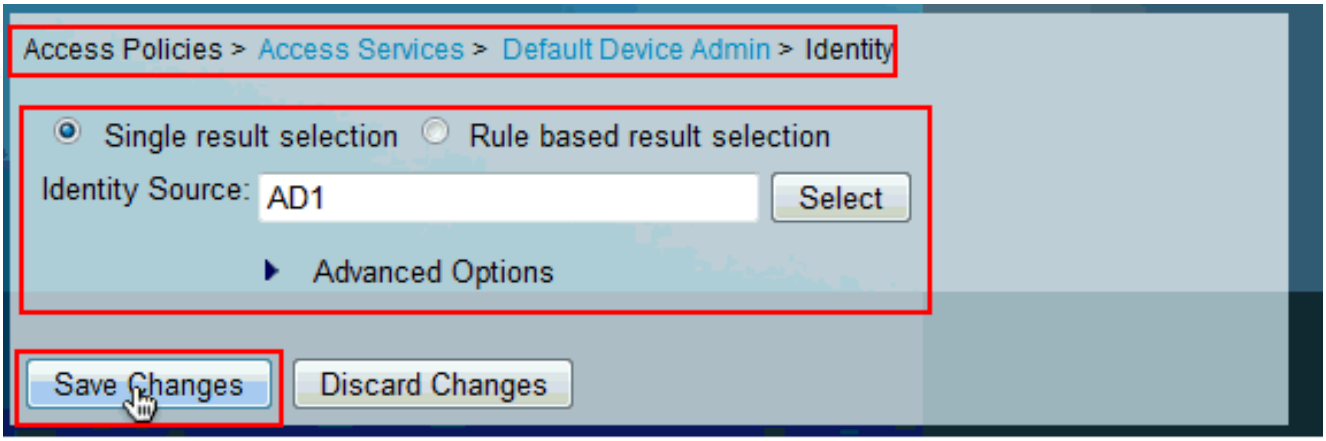
7. 選擇**Access Policies > Access Services > Default Device Admin > Identity**，然後按一下**Identity Source**旁邊的**Select**。



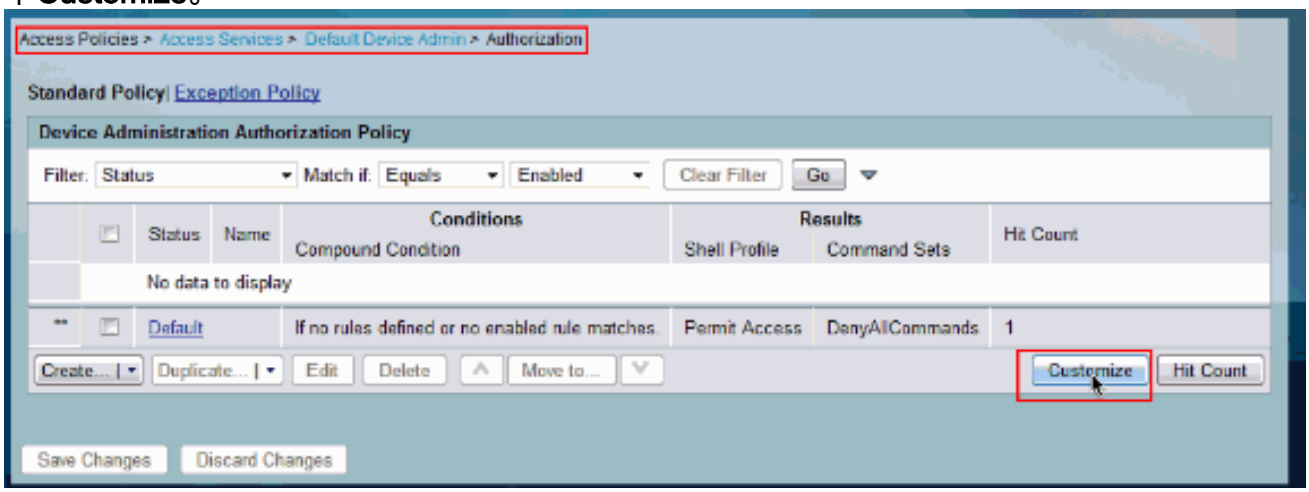
8. 選擇**AD1**，然後按一下**OK**。



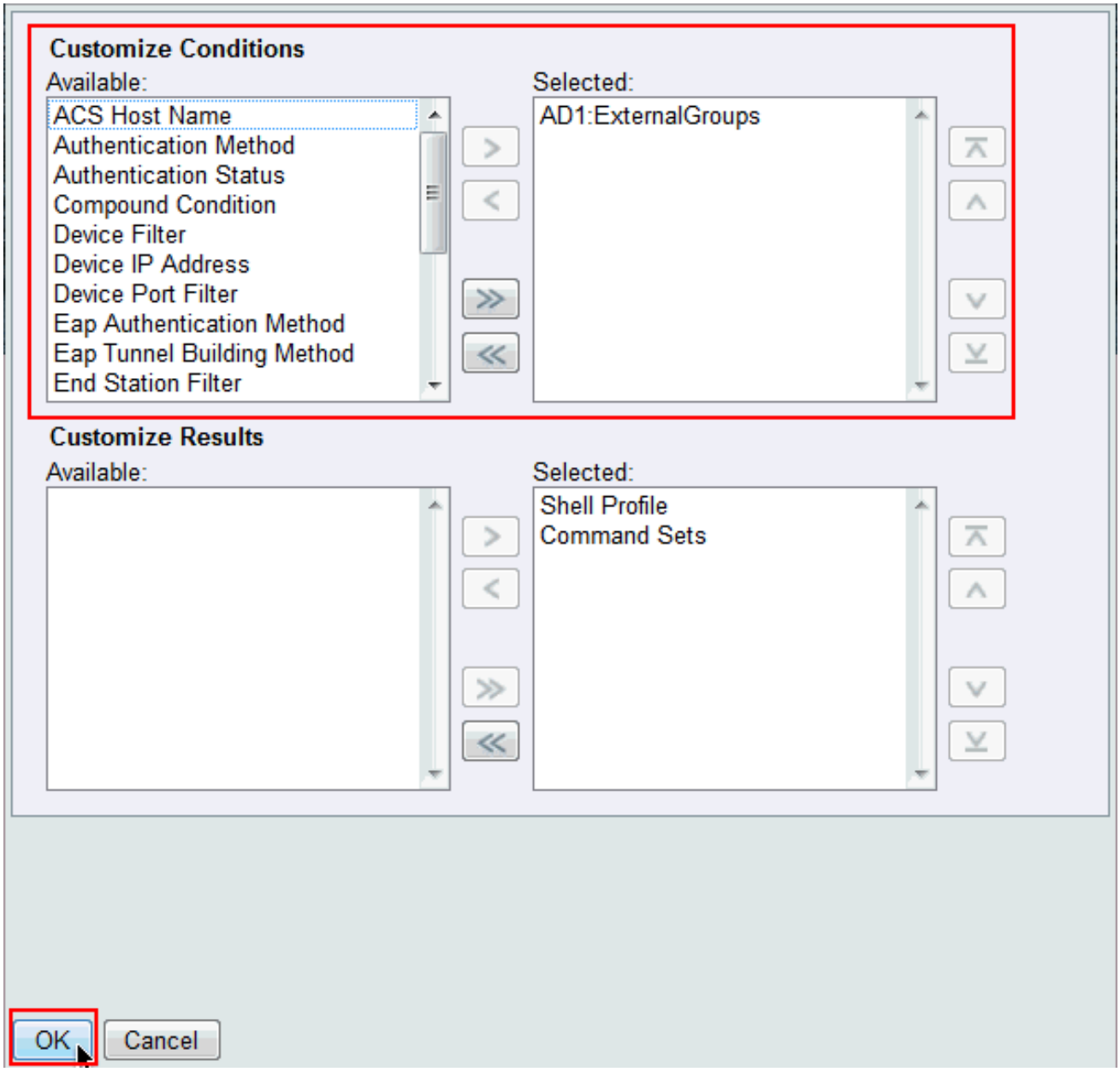
9. 按一下「**Save Changes**」。



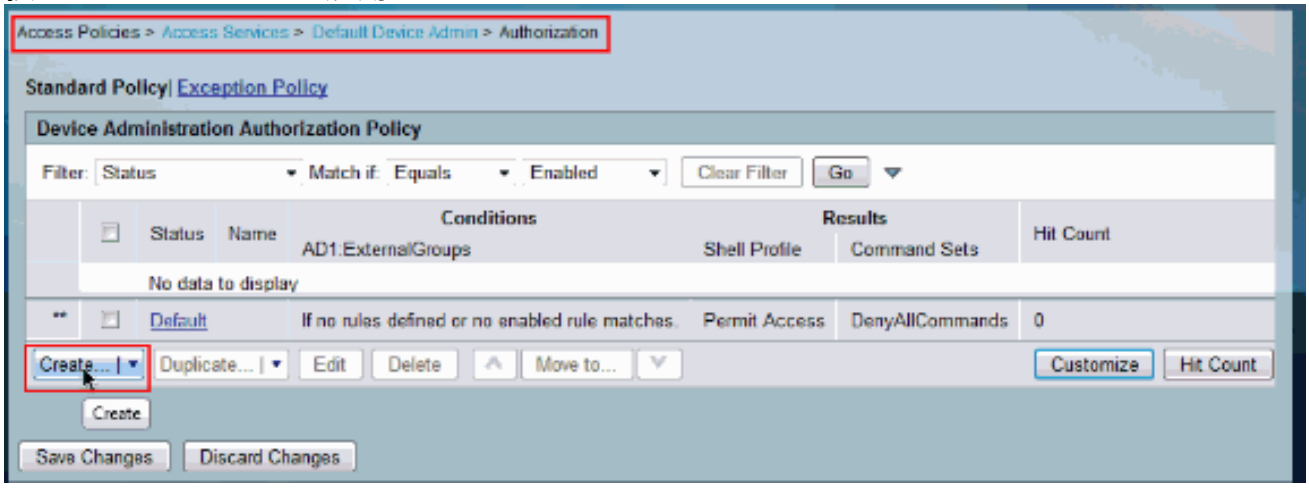
10. 選擇**Access Policies > Access Services > Default Device Admin > Authorization**，然後按一下**Customize**。



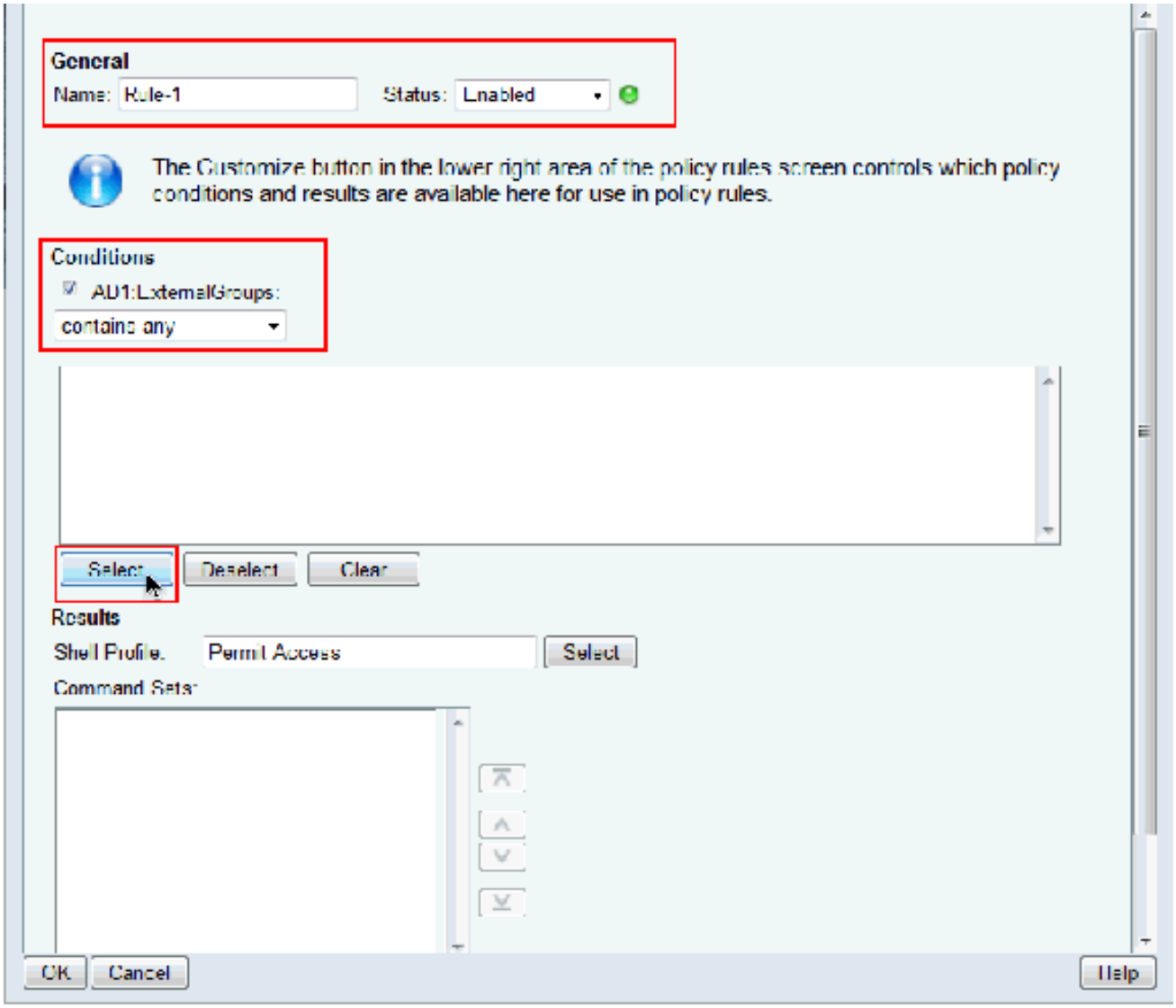
11. 將AD1:ExternalGroups從「可用」(Available)複製到「自定義條件」(Customize Conditions)的「選定」(Selected)部分，然後將「殼輪廓」(Shell Profile)和「命令集」(Command Sets)從「可用」(Available)移動到「自定義結果」(Customize Results)的「選定」部分。現在按一下**OK**。



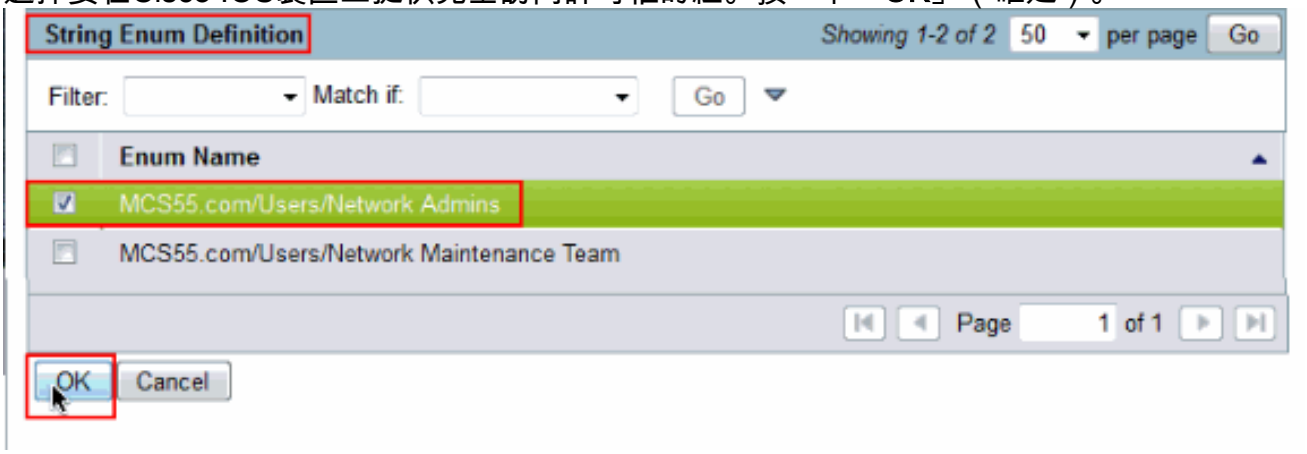
12. 按一下**Create**以建立新規則。



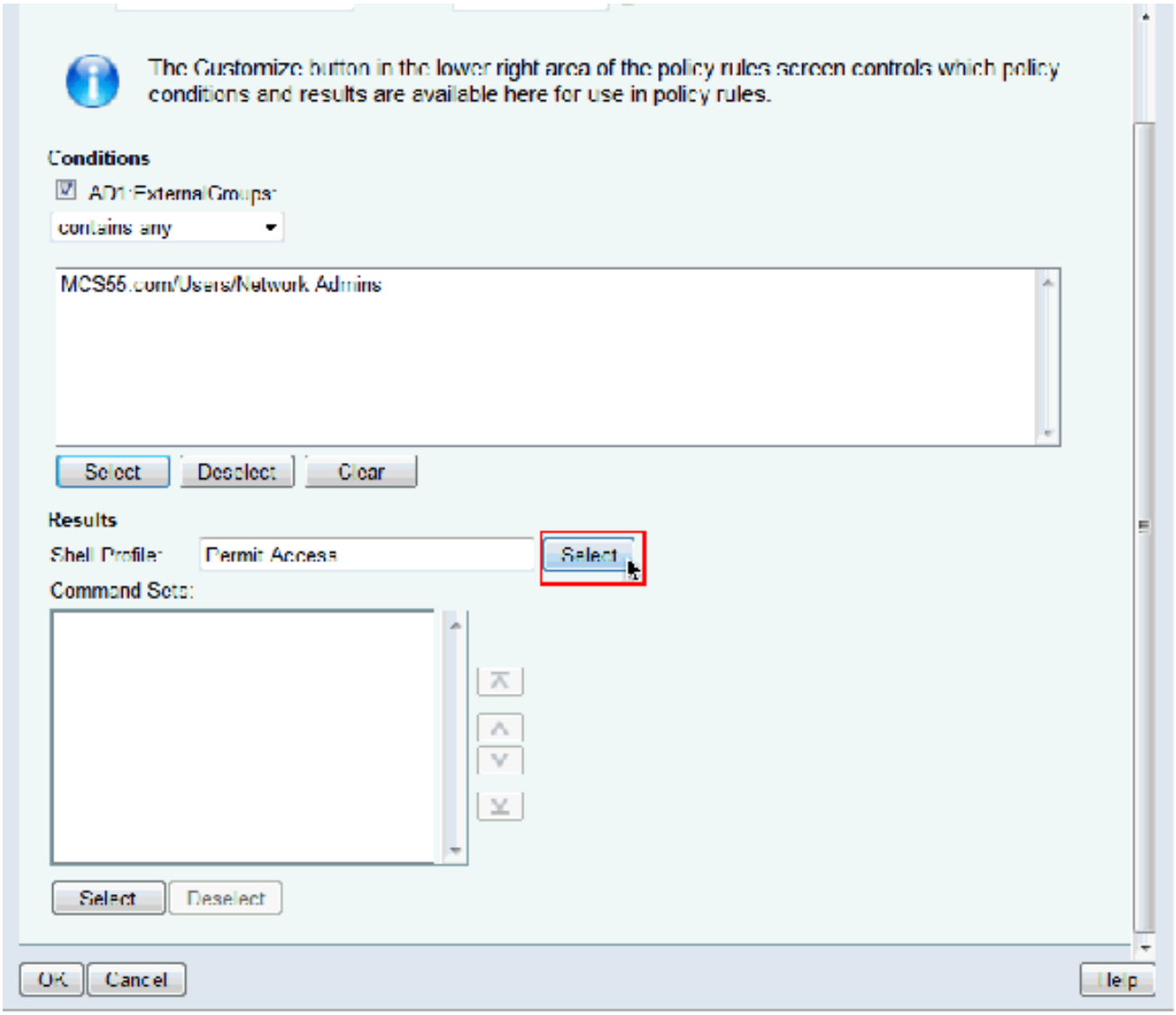
13. 在**AD1:ExternalGroups**條件中按一下**Select**。



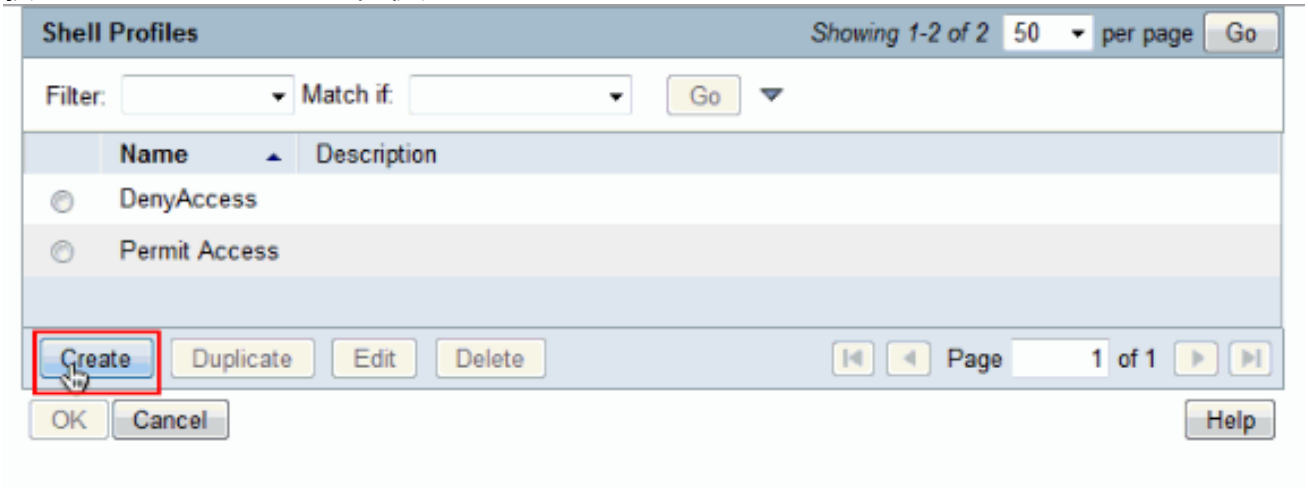
14. 選擇要在Cisco IOS裝置上提供完全訪問許可權的組。按一下「**OK**」（確定）。



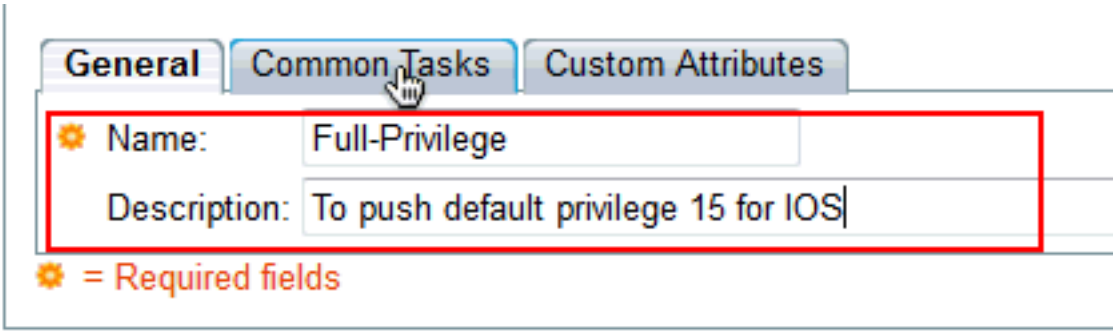
15. 在「外殼配置檔案」(Shell Profile)欄位中按一下**選擇**。



16. 按一下**Create**可為完全訪問使用者建立新的**Shell Profile**。

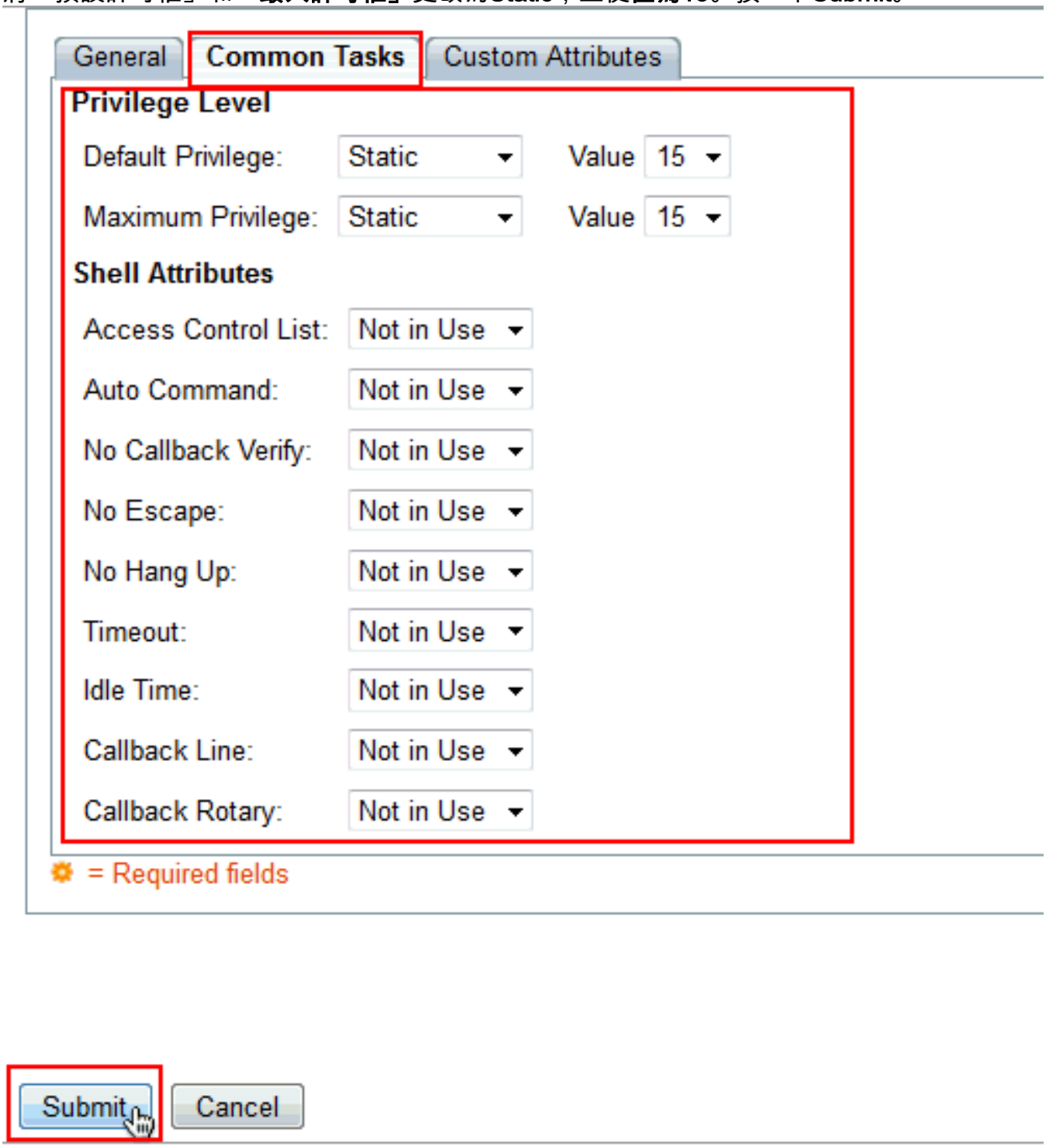


17. 在**General**索引標籤中提供**Name**和**Description**（可選），然後按一下**Common Tasks**索引標

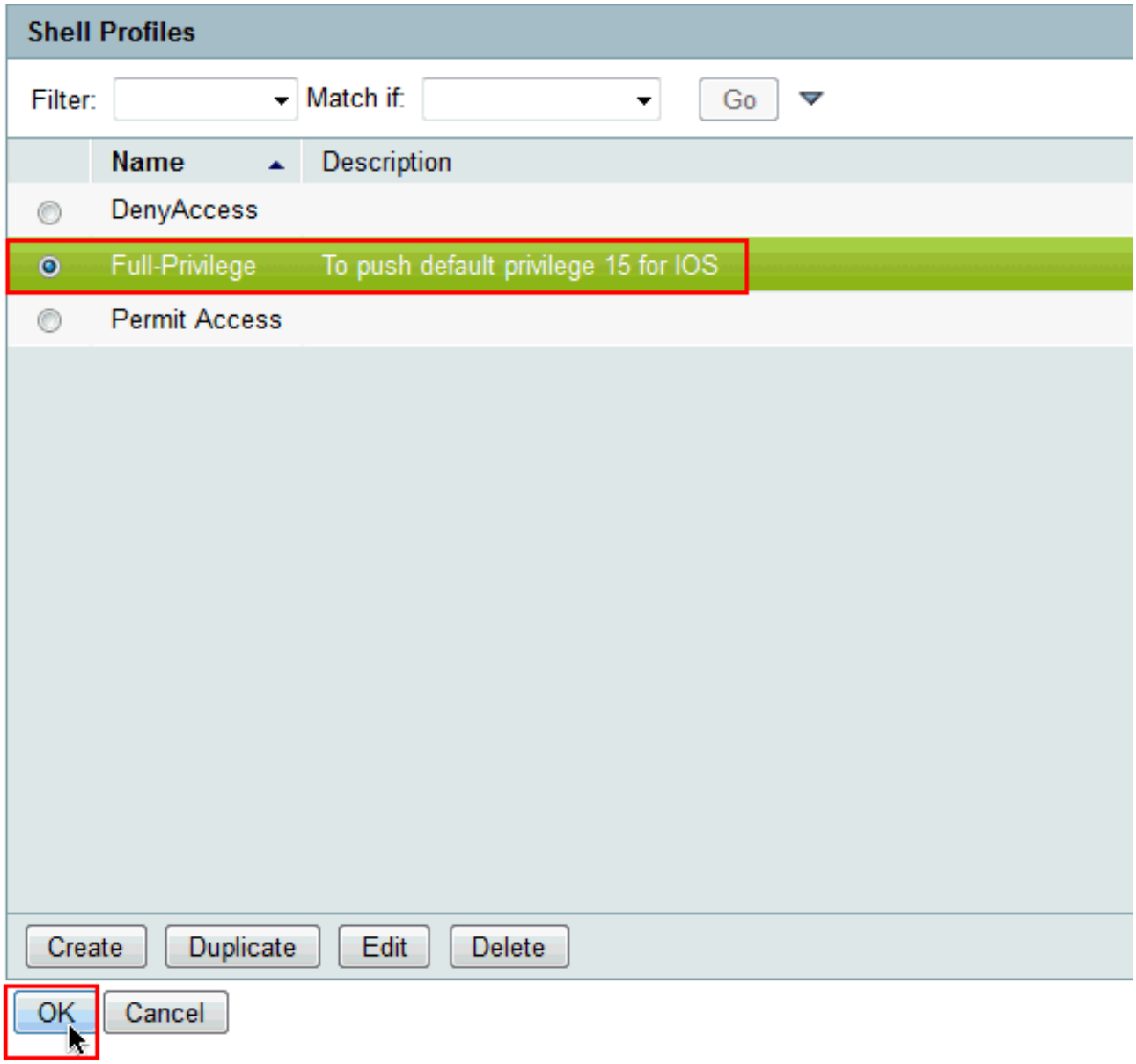


籤。

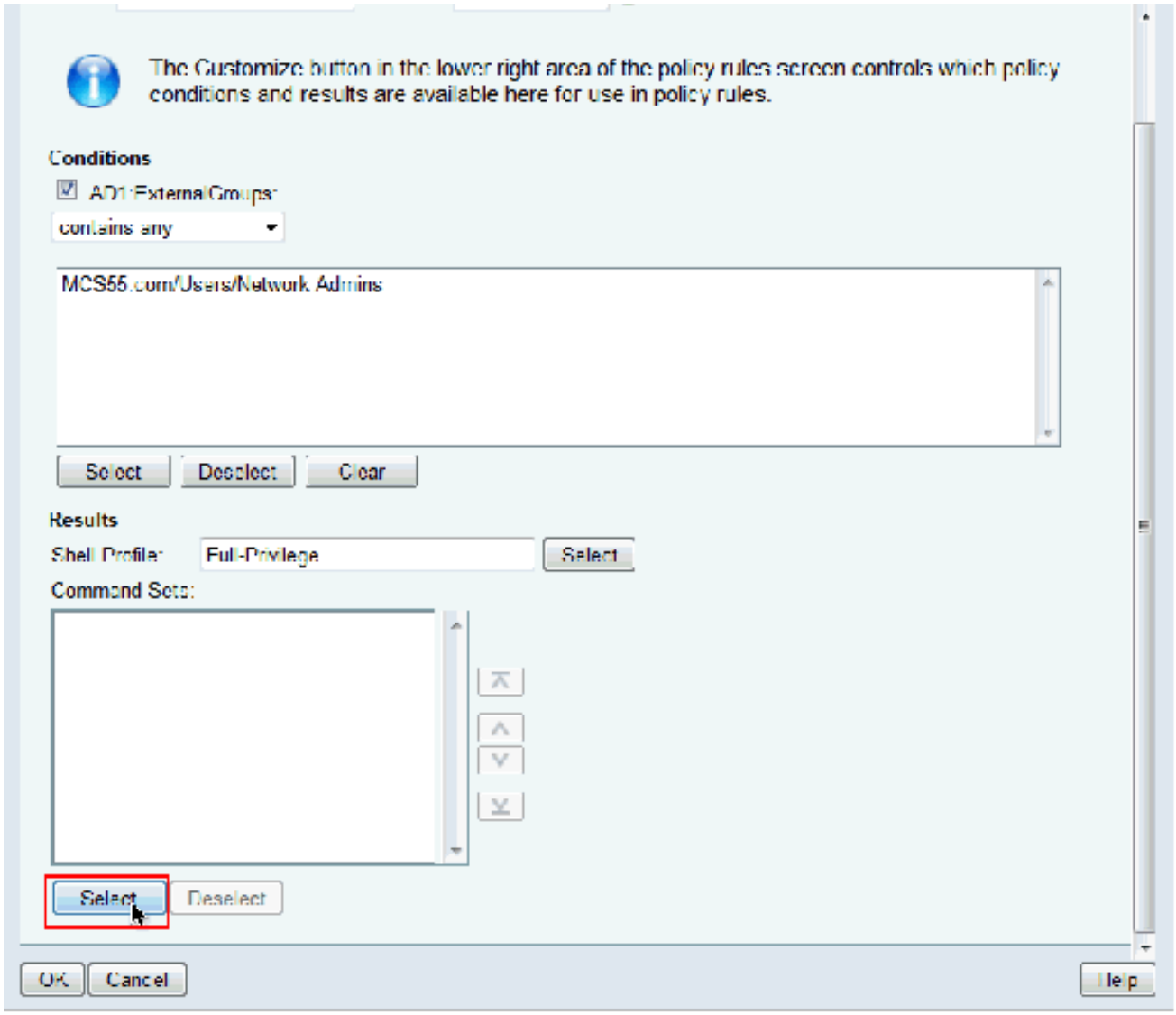
18. 將「預設許可權」和「**最大許可權**」更改為**Static**，並使**值為15**。按一下**Submit**。



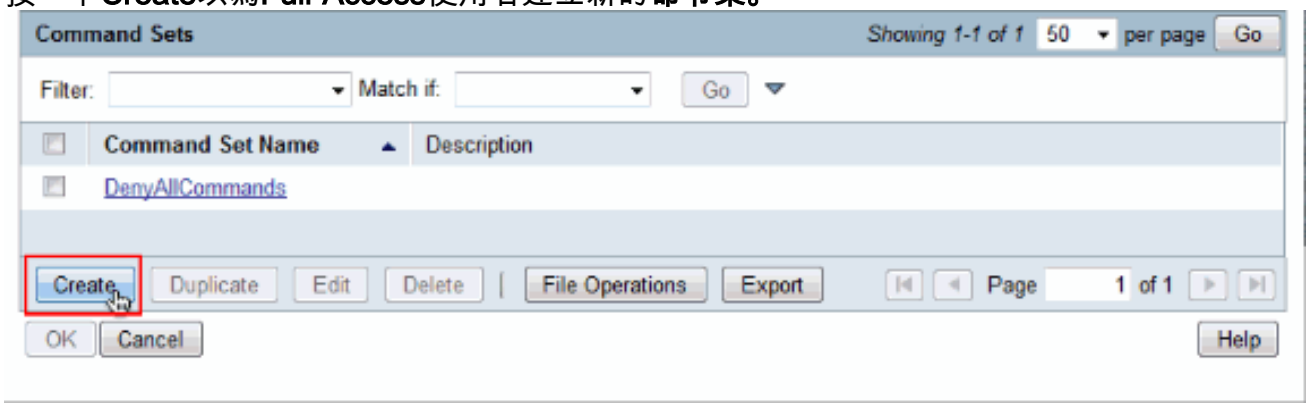
19. 現在，選擇新建立的完全訪問**外殼配置檔案**（在本示例中為「完全許可權」），然後按一下**OK**。



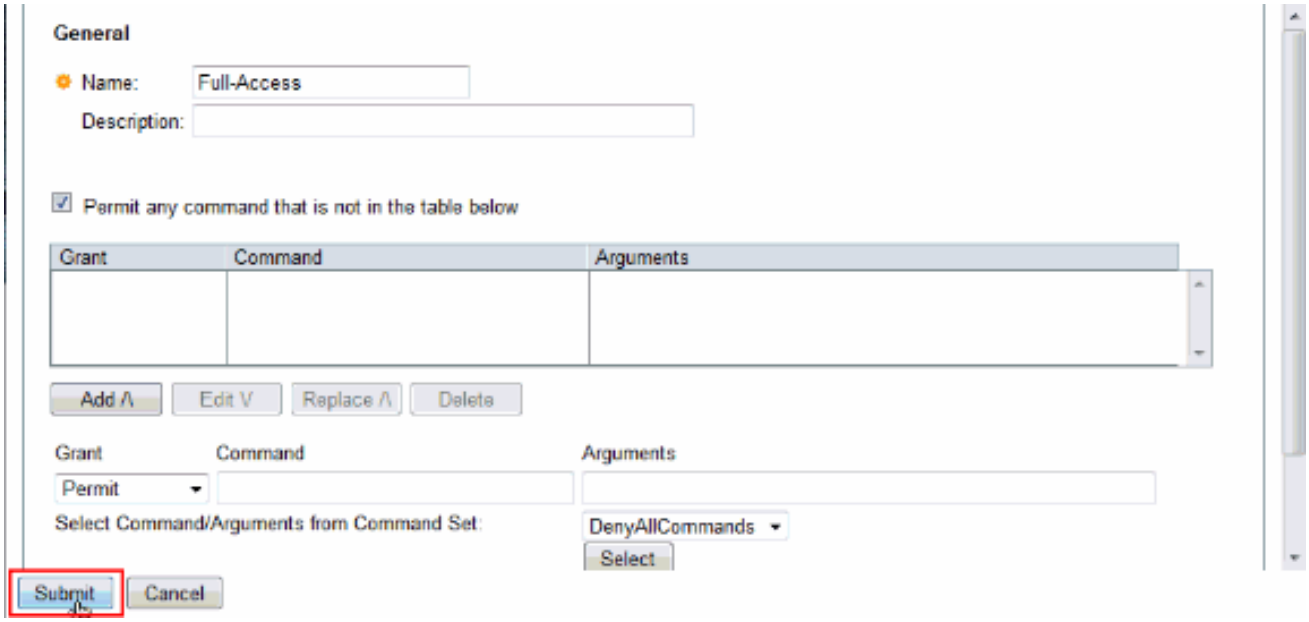
20. 在「命令集」欄位中按一下**選擇**。



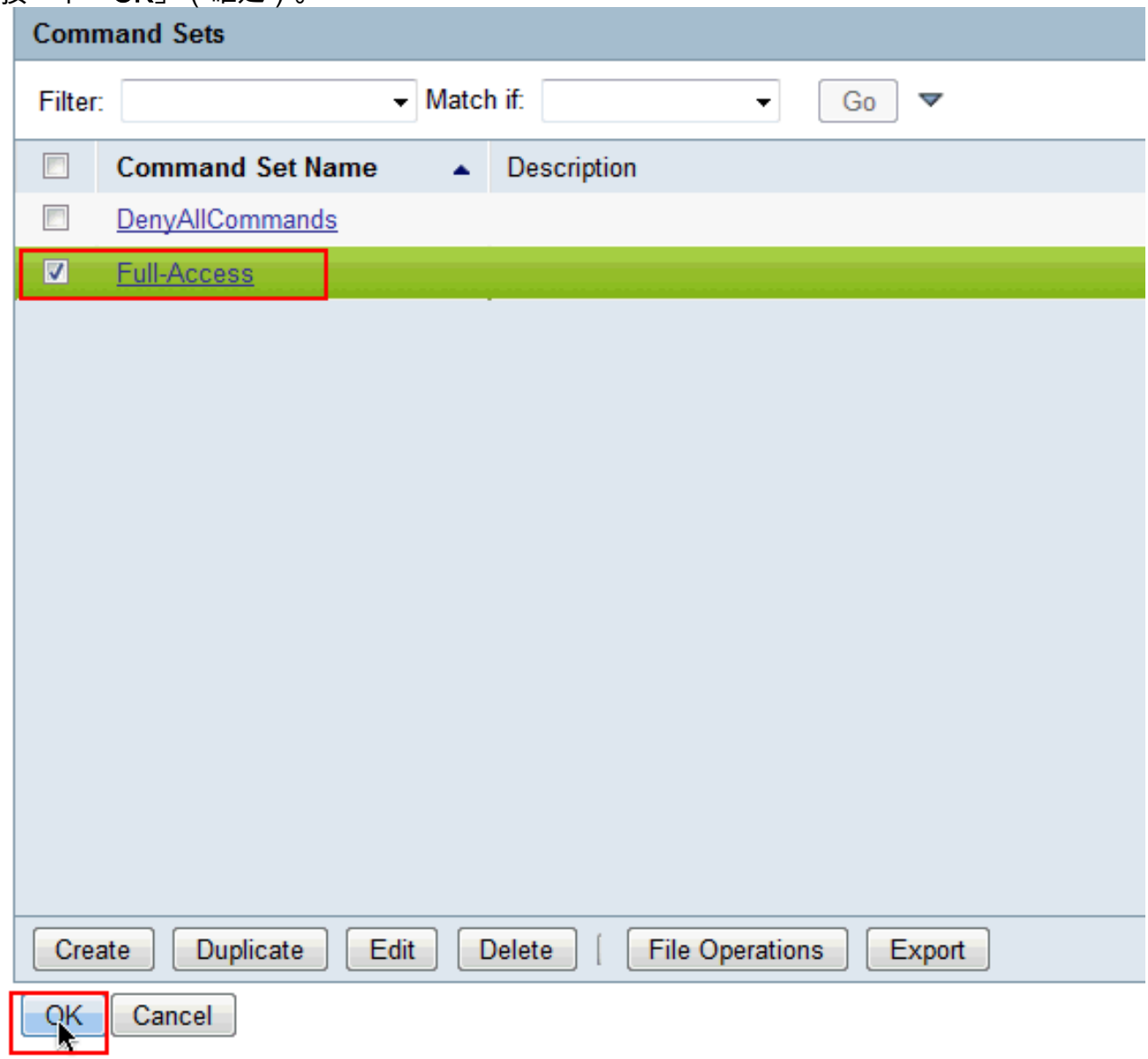
21. 按一下**Create**以為**Full-Access**使用者建立新的**命令集。**



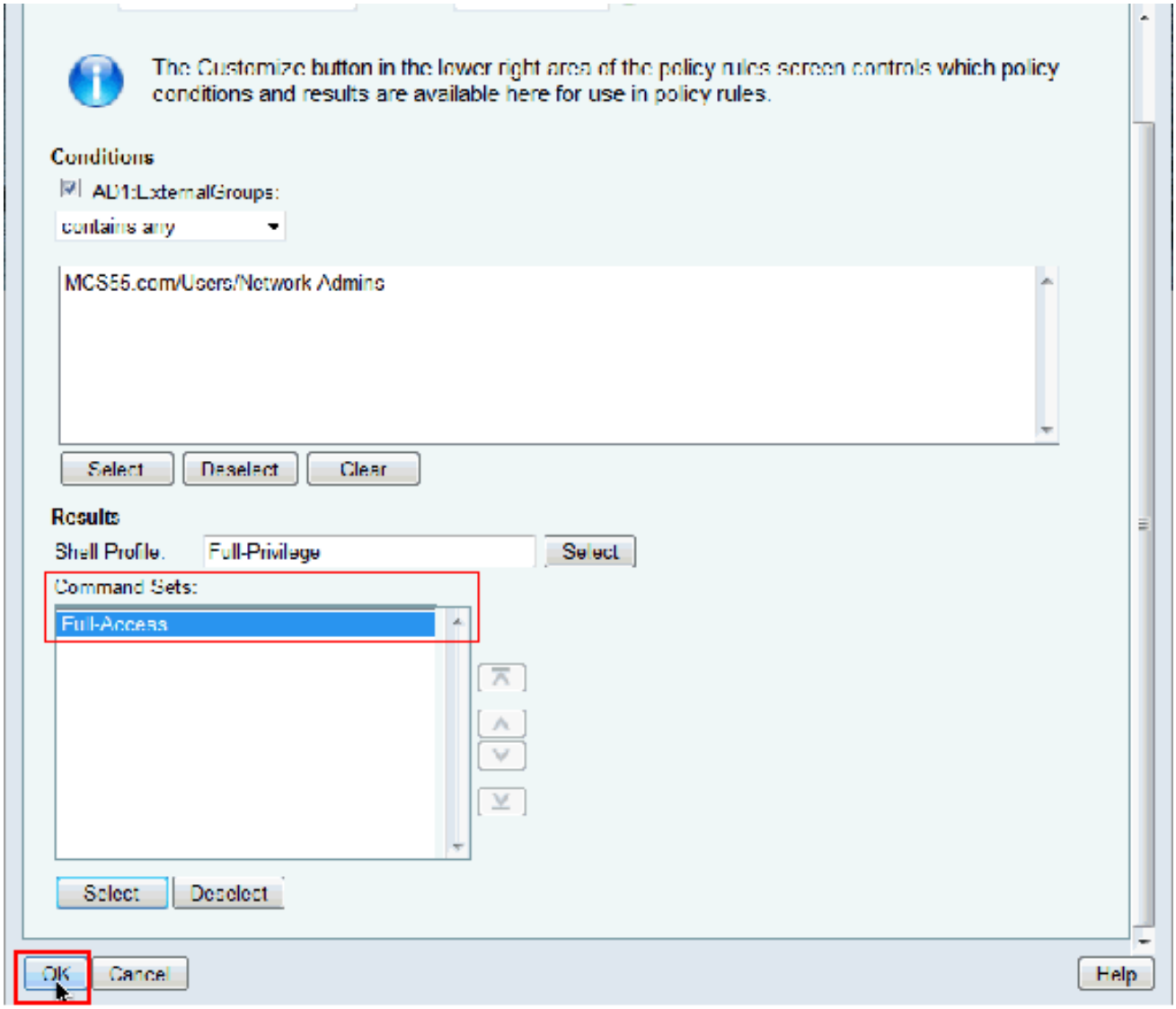
22. 提供**名稱**，並確保選中**Permit any command that is not in the table**旁邊的覈取方塊。按一下「**Submit**」。**註：有關**命令集的詳細[資訊，請參閱建立、複製和編輯](#)裝置管理的命令集。



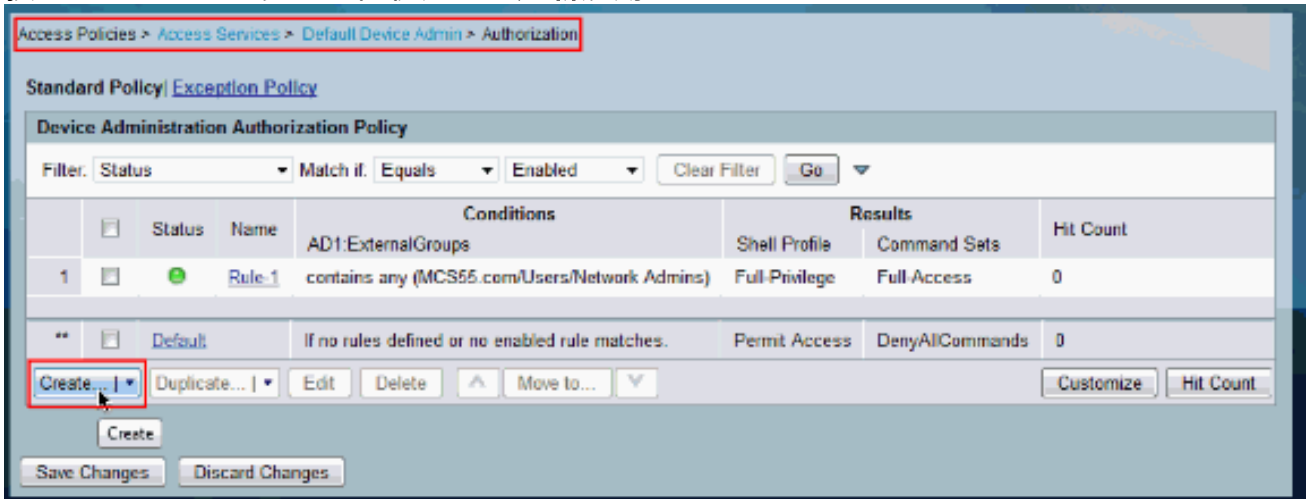
23. 按一下「**OK**」（確定）。



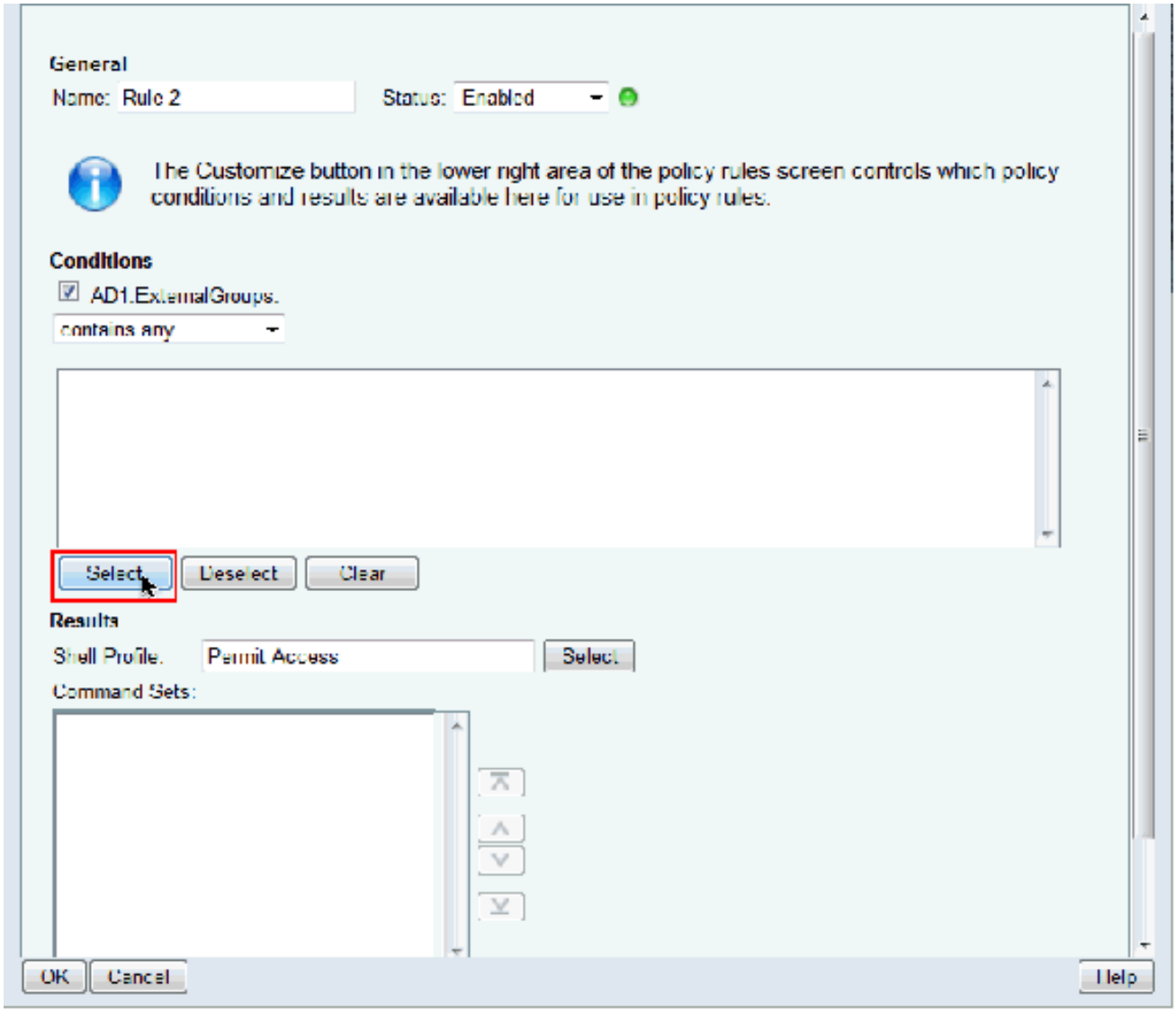
24. 按一下「**OK**」（確定）。這樣就完成了**Rule-1**的配置。



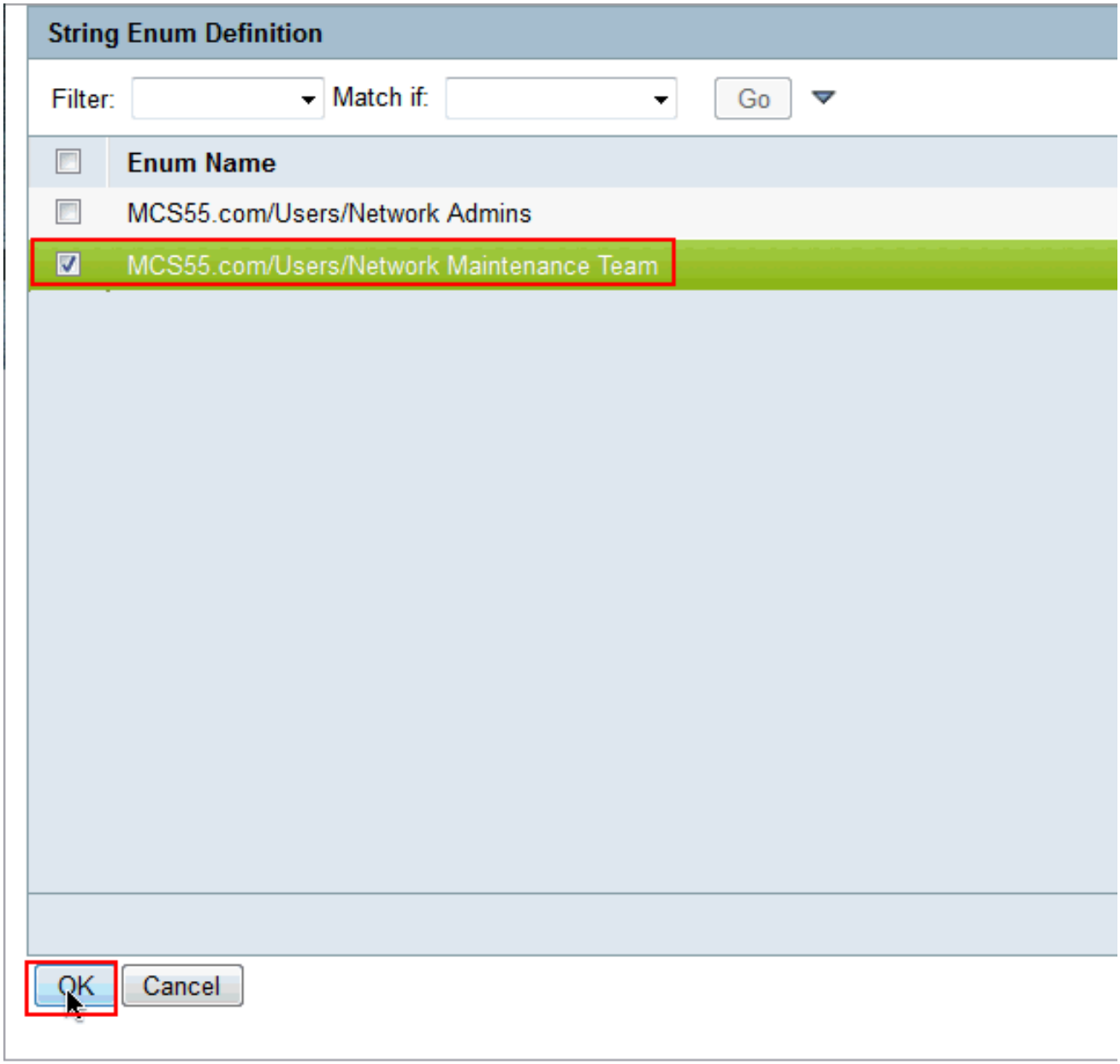
25. 按一下**Create**可為受限訪問使用者創**建新**規則。



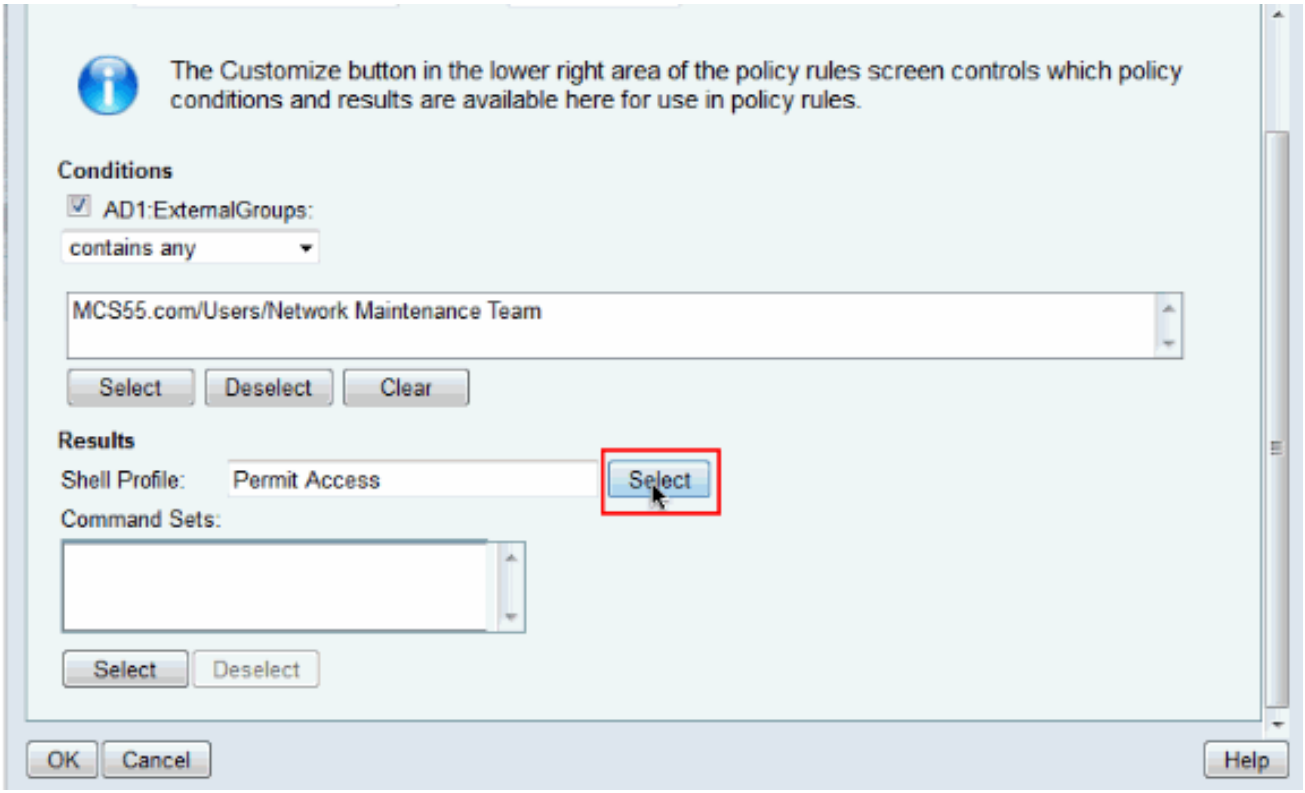
26. 選擇**AD1:ExternalGroups**，然後按一下**Select**。



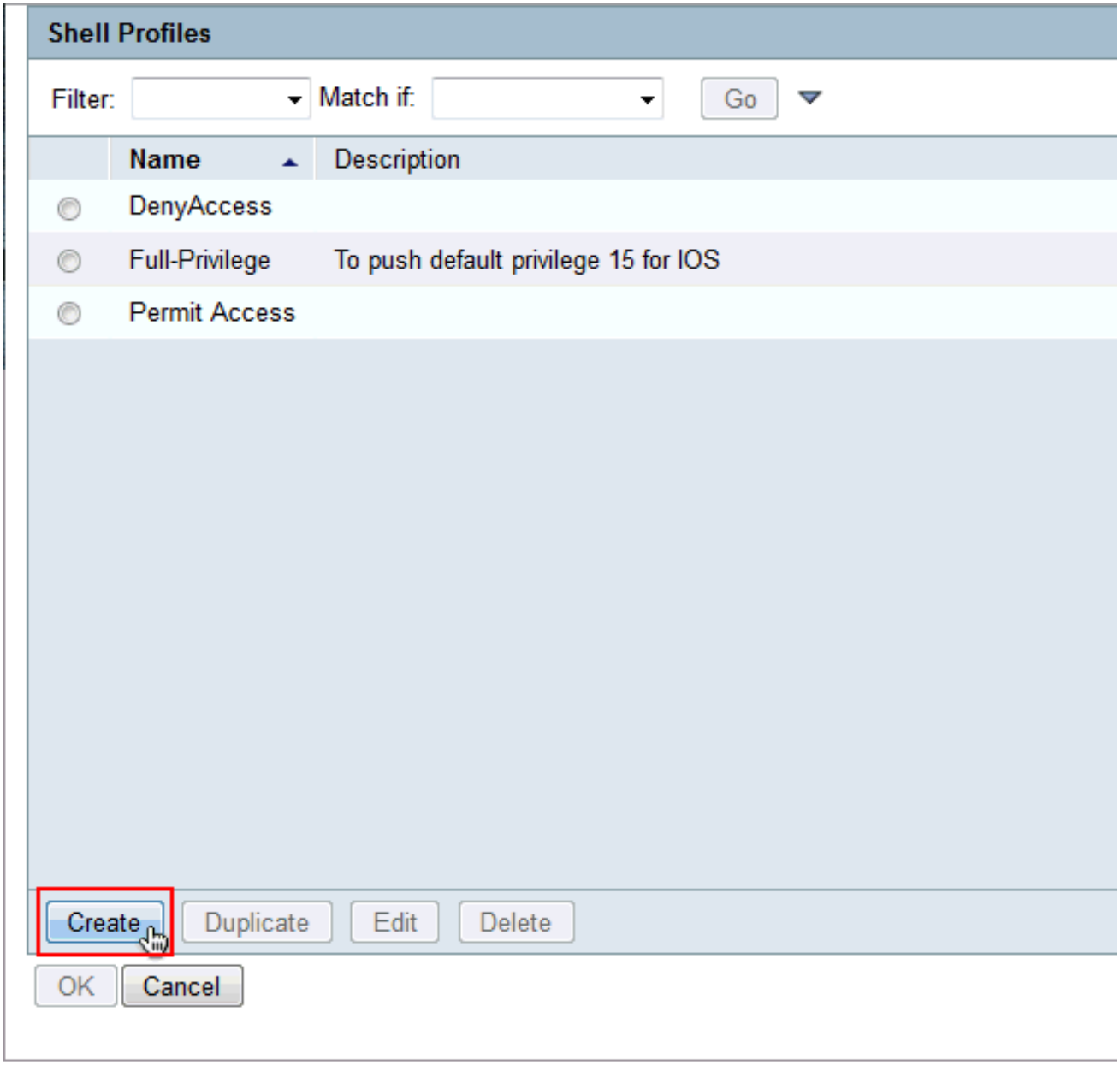
27. 選擇要提供有限訪問許可權的組（或）組，然後按一下**確定**。



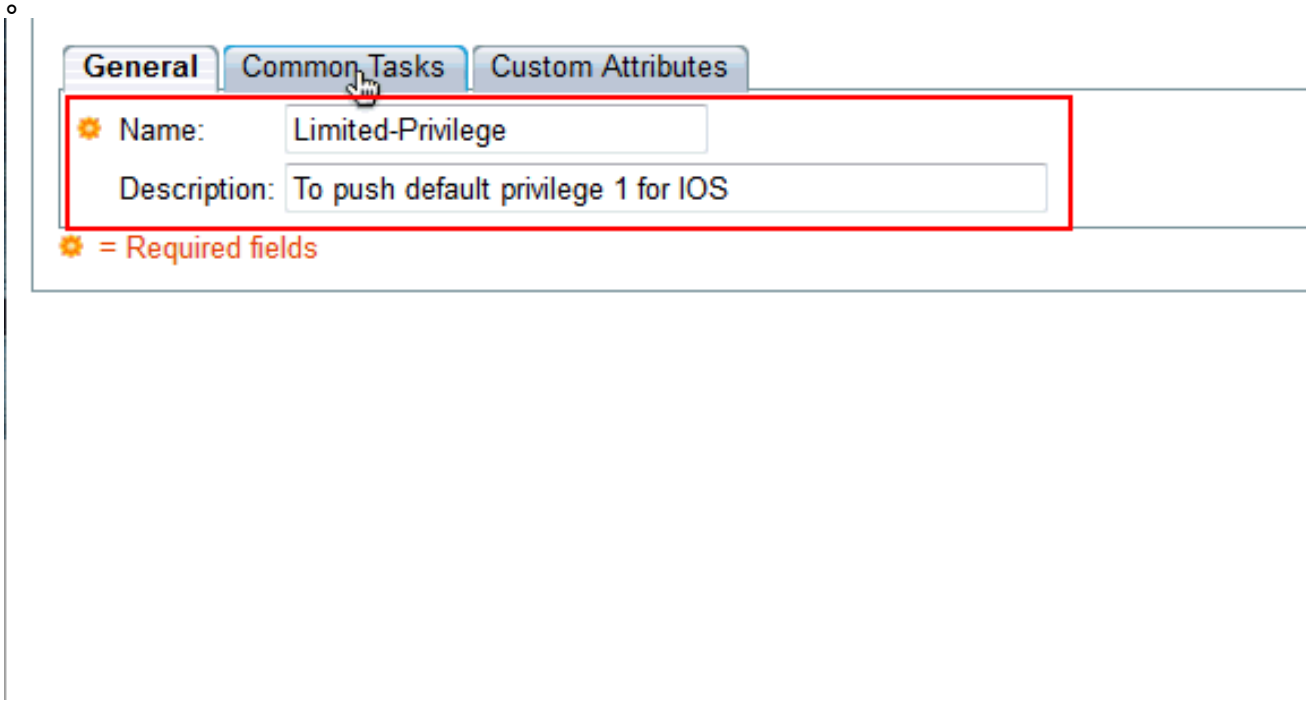
28. 在「外殼配置檔案」(Shell Profile)欄位中按一下**選擇**。



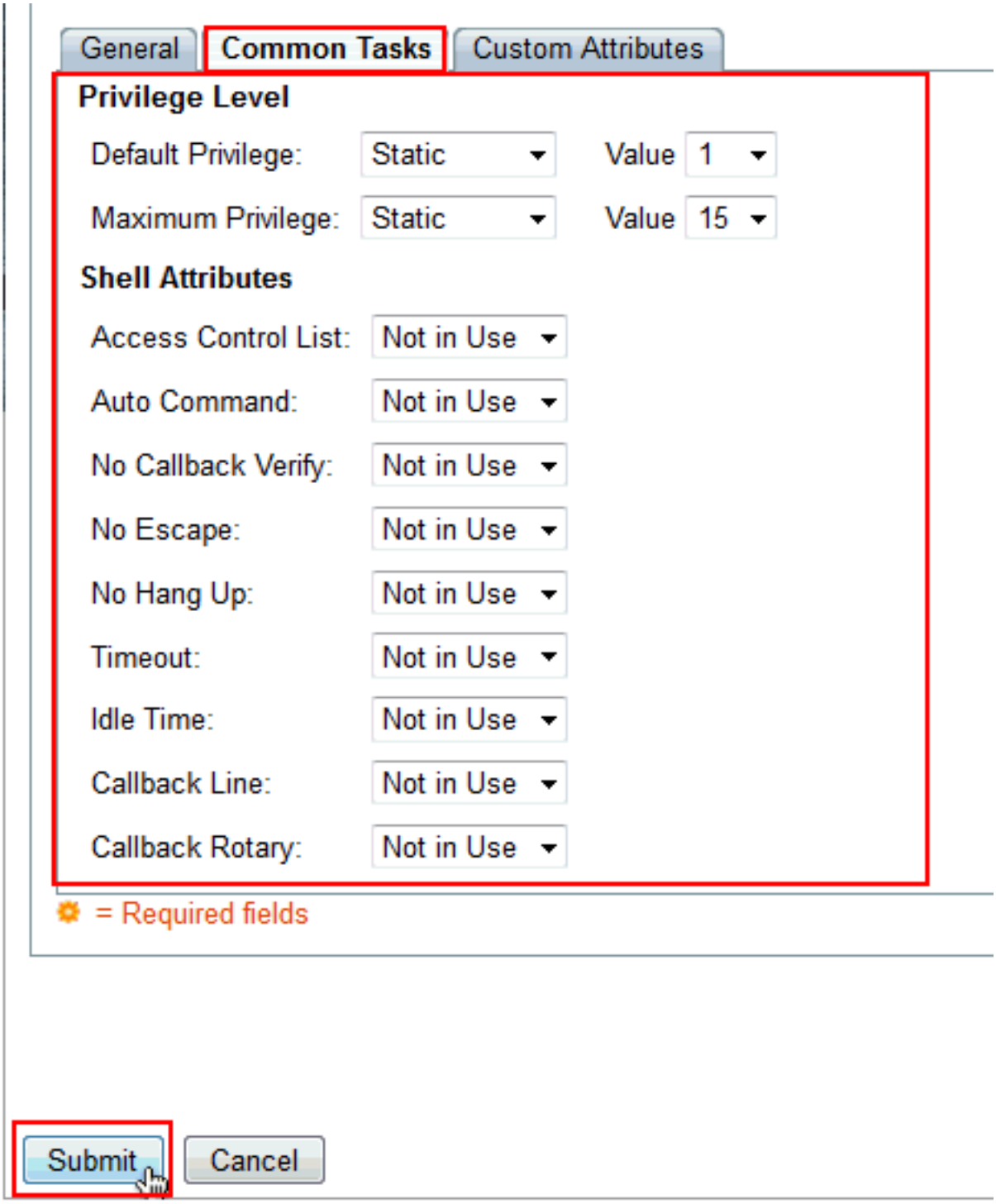
29. 按一下**Create**以建立新的**Shell Profile**以進行受限訪問。



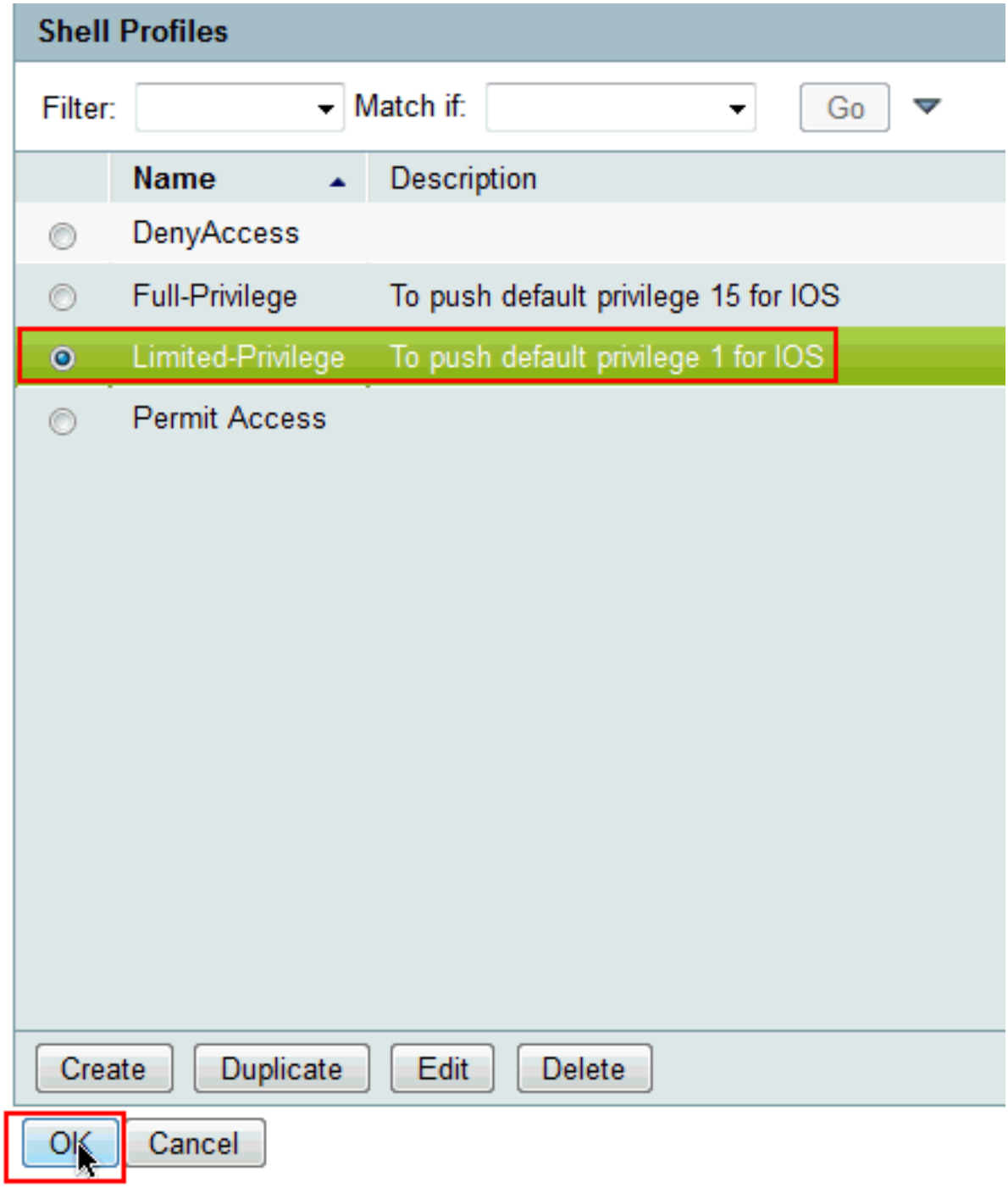
30. 在**General** 索引標籤中提供**Name**和**Description**（可選），然後點選**Common Tasks**索引標籤。



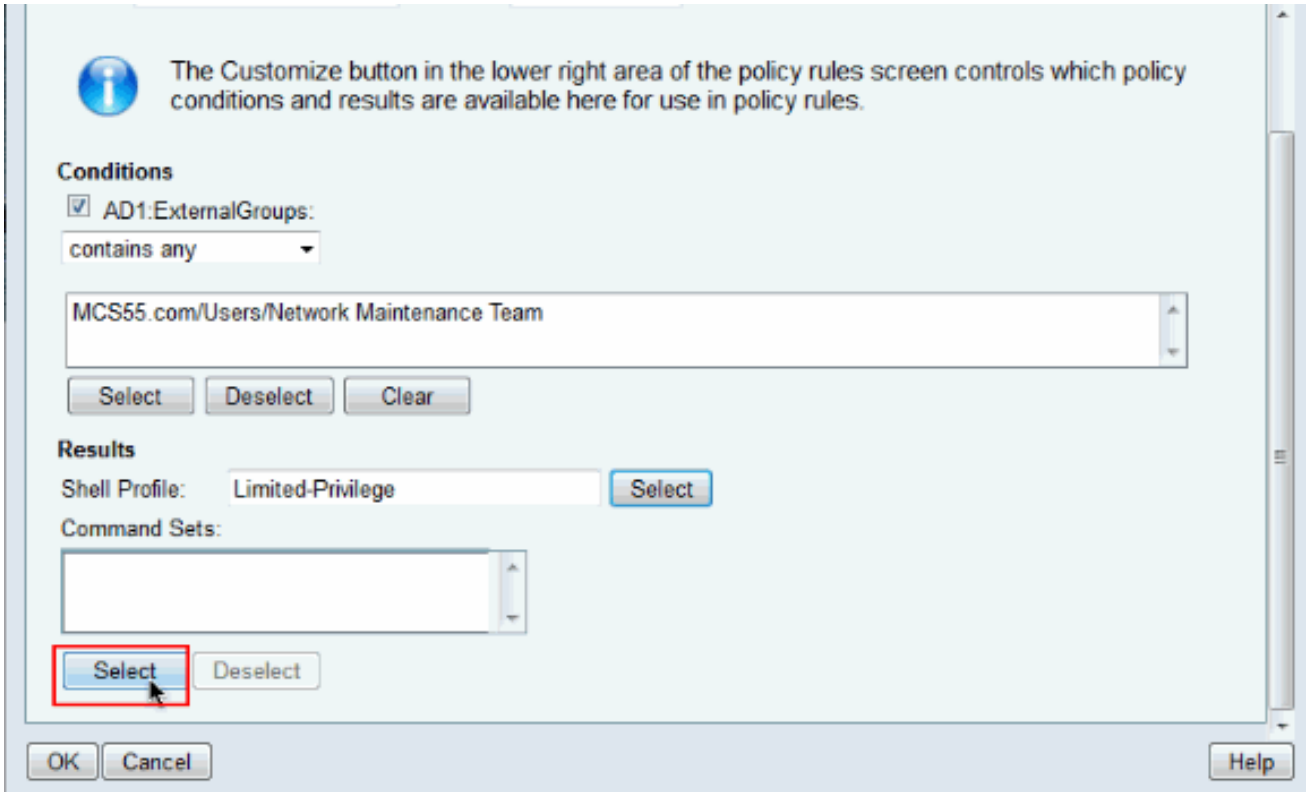
31. 將Default Privilege和**Maximum Privilege**更改為**Static**，分別使用值1和**15**。按一下「**Submit**」。



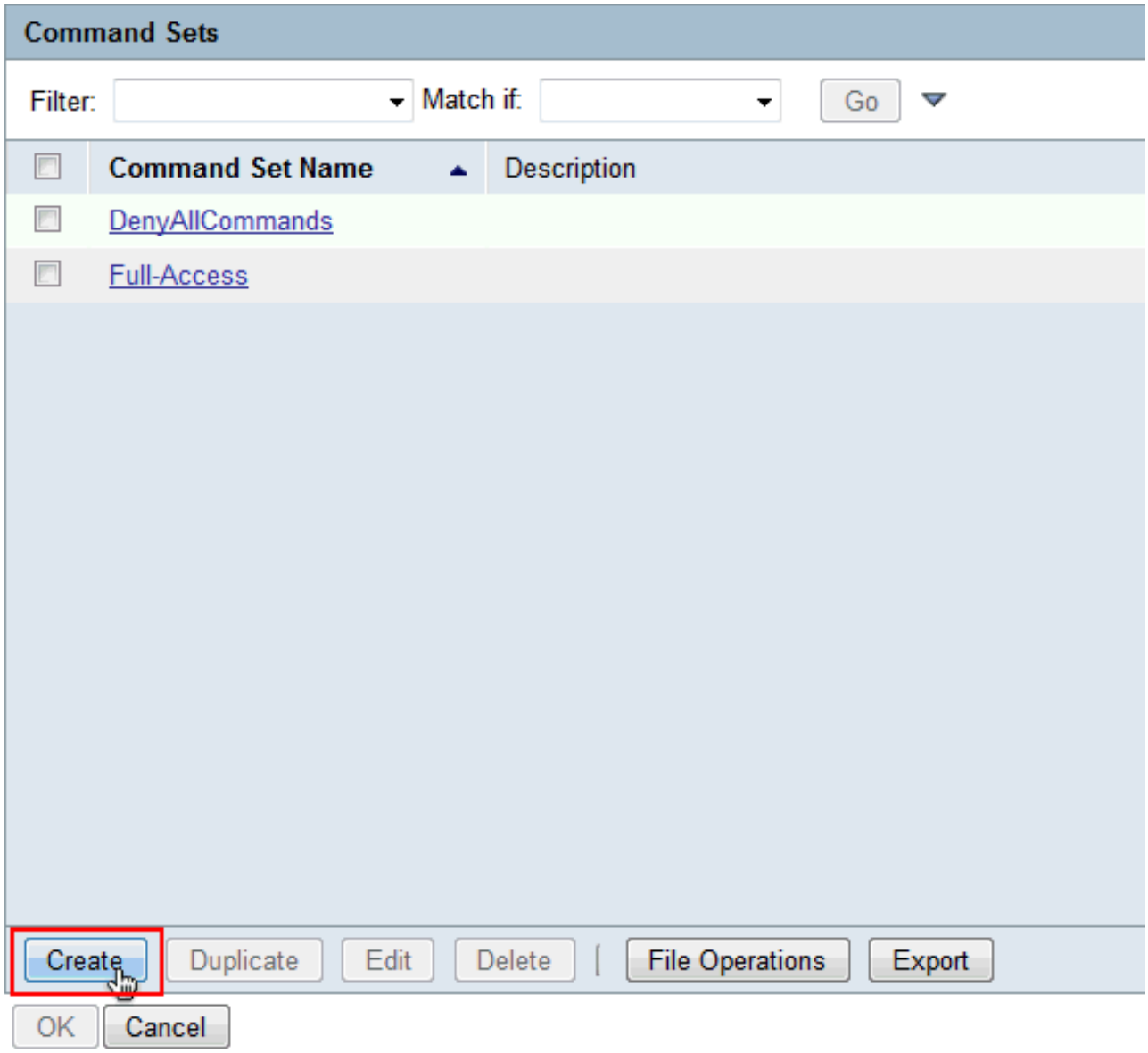
32. 按一下「**OK**」（確定）。



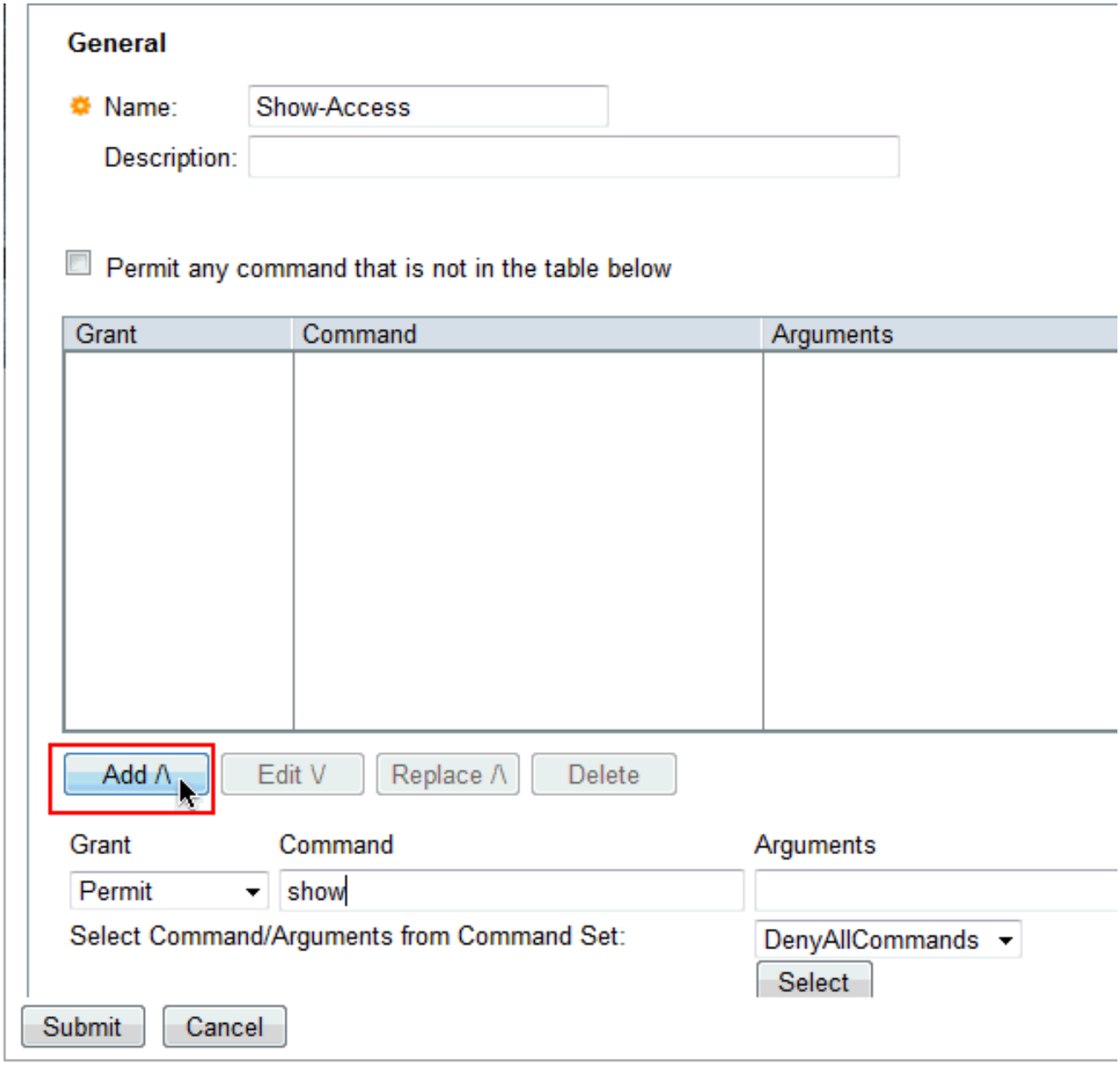
33. 在「命令集」欄位中按一下**選擇**。



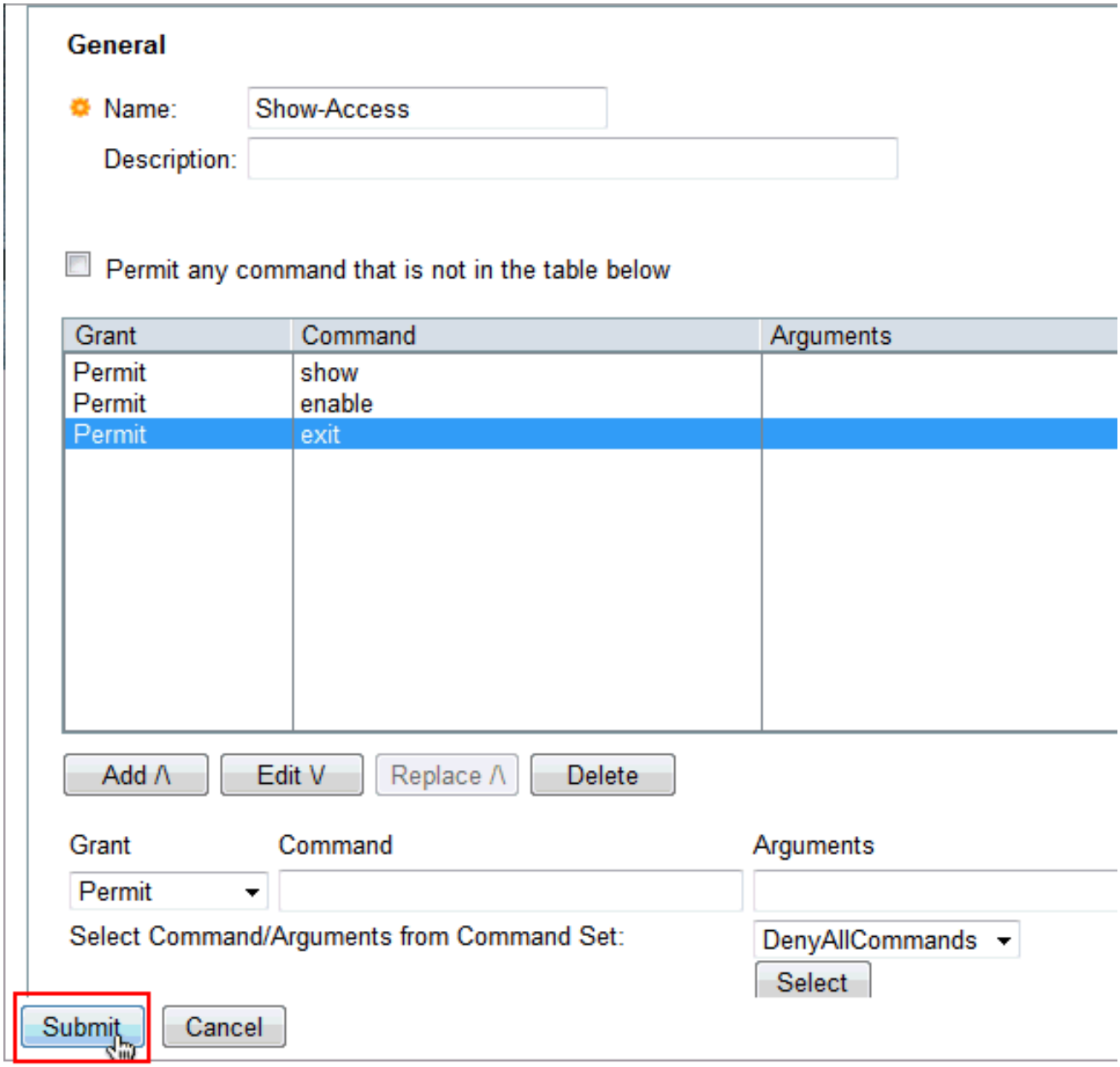
34. 按一下**Create**為受限訪問組建立新的**命令集**。



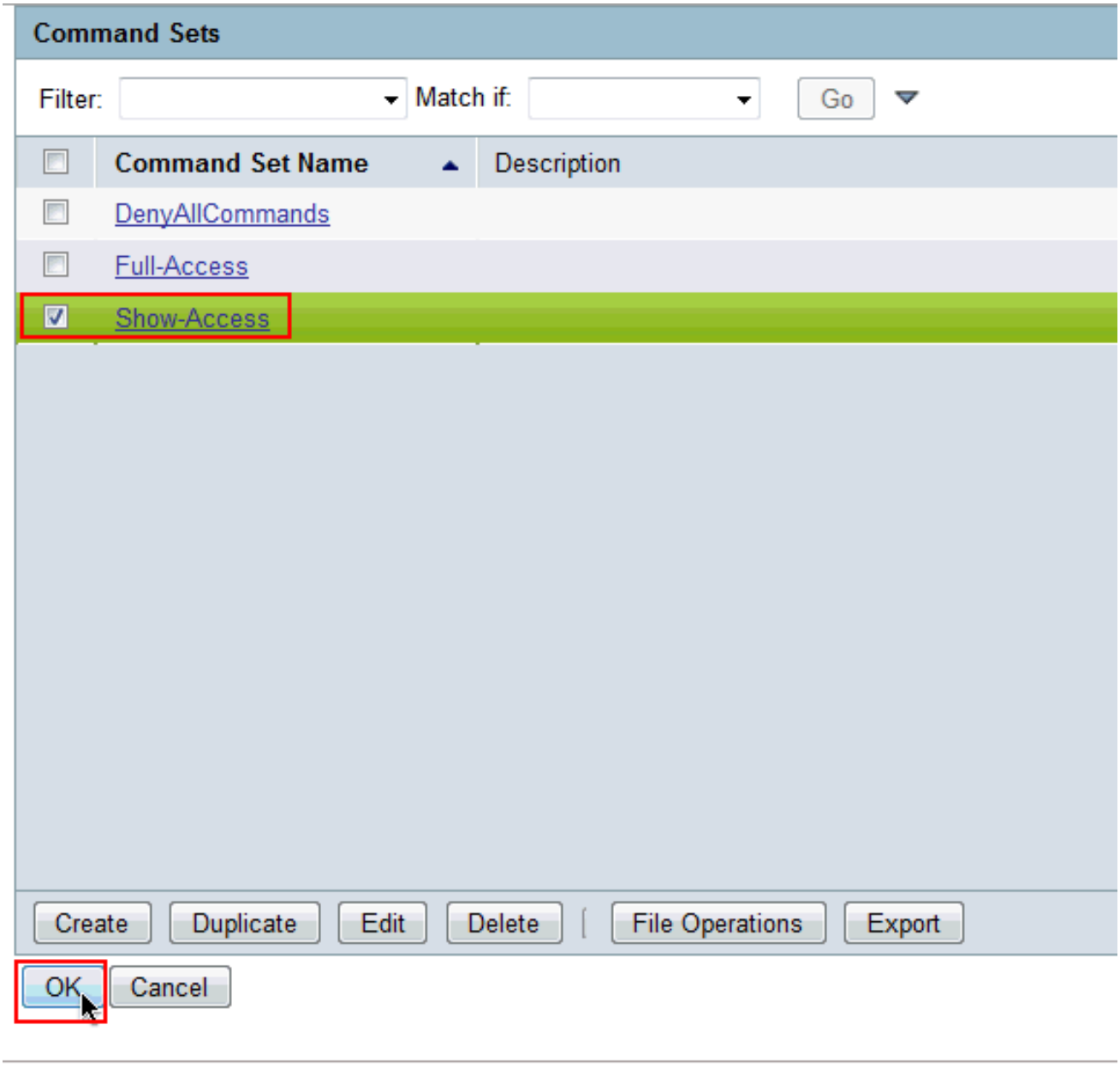
35. 提供**名稱**，並確保未選中**Permit any command that is not in the table**旁邊的覈取方塊。在**命令**部分提供的空白處鍵入**show**後，單擊Add，然後在**Grant**部分中選擇**Permit**，以便僅允許有限訪問組中的使用者使用show命令。



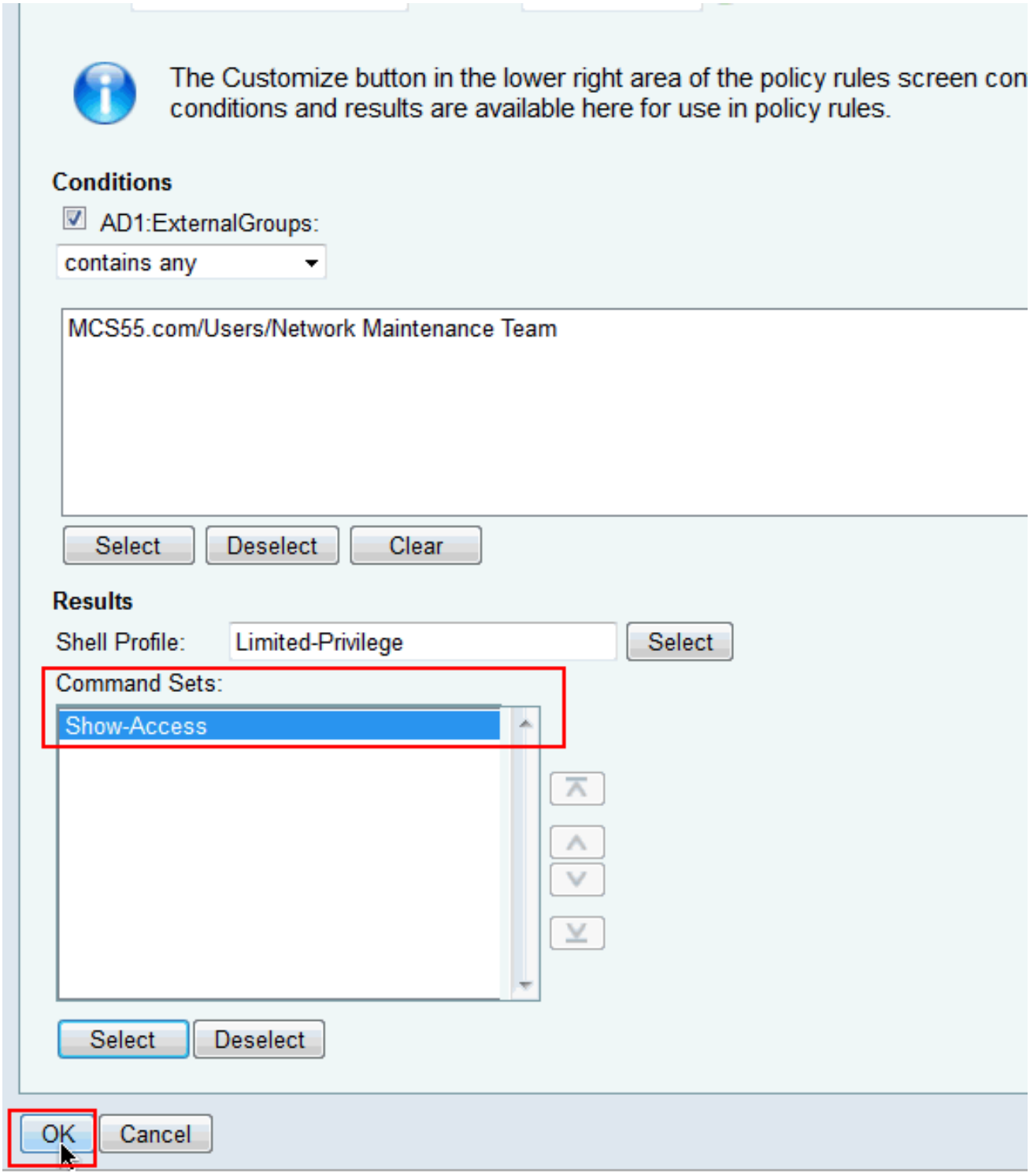
36. 類似地，使用**Add**為有限訪問組中的使用者新增任何其他允許使用的命令。按一下「**Submit**」。**註：有關**命令集的詳細資訊，請參閱建立、複製和編輯裝置管理的命令集。


General
Name:
Show-Access
Description:
Permit any command that is not in the table below
Grant
Command
Arguments
Permit
show
Permit
enable
Permit
exit
Add /\
Edit V
Replace /\
Delete
Grant
Command
Arguments
Permit
Select Command/Arguments from Command Set:
DenyAllCommands
Select
Submit
Cancel

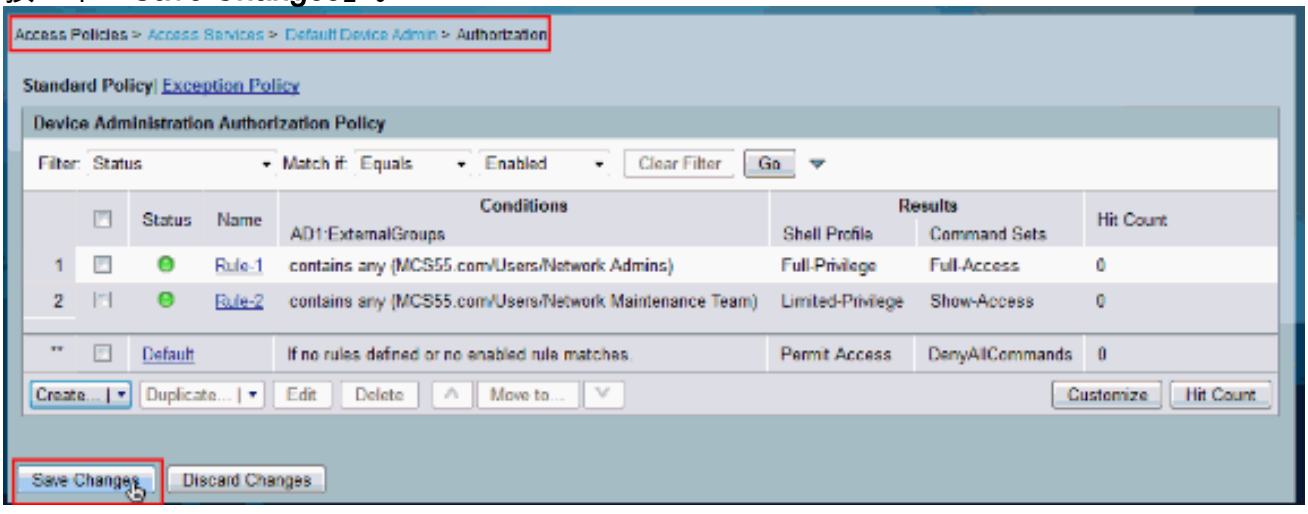
37. 按一下「OK」（確定）。


Command Sets
Filter:
Match if:
Go
Command Set Name
Description
DenyAllCommands
Full-Access
Show-Access
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel

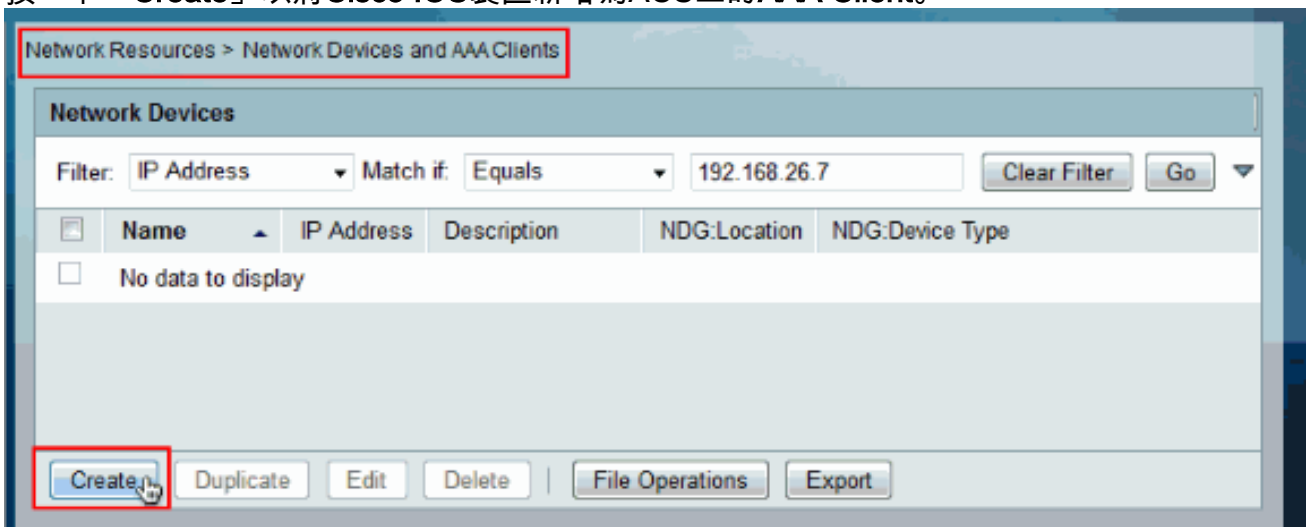
38. 按一下「**OK**」（確定）。



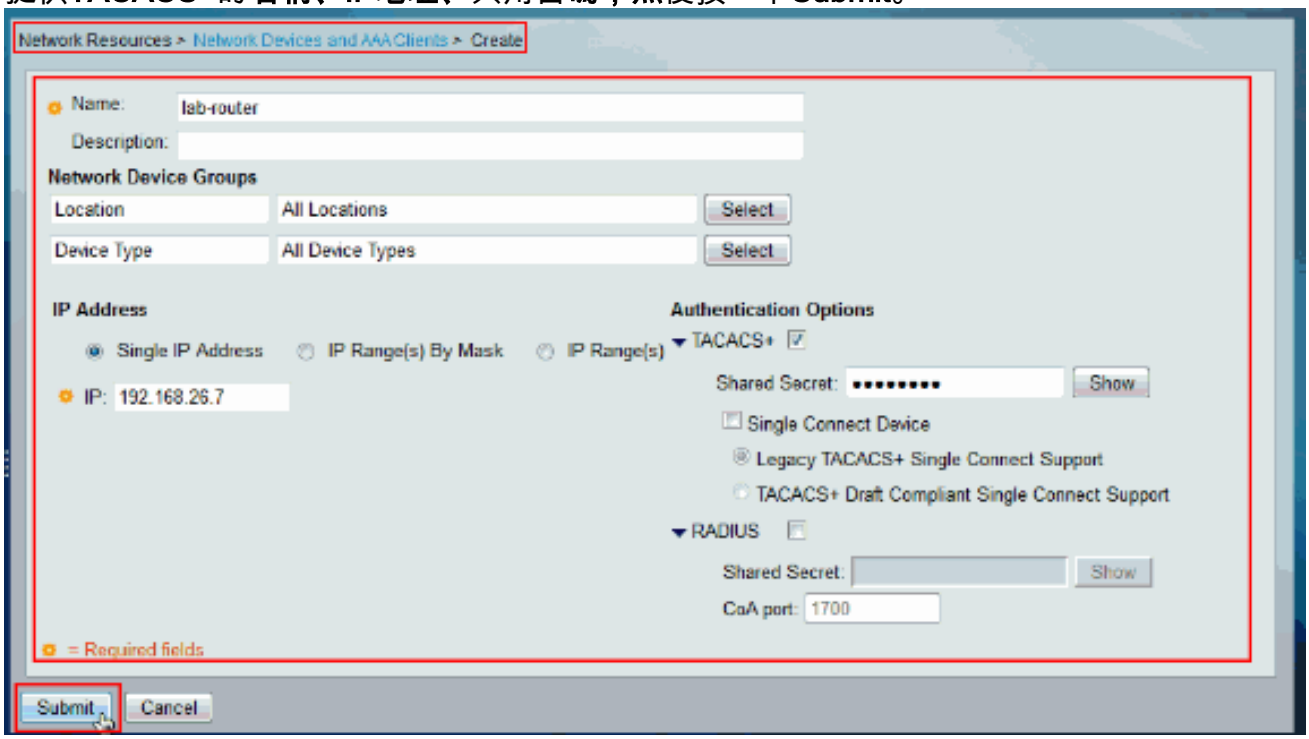
39. 按一下「**Save Changes**」。



40. 按一下「**Create**」以將**Cisco IOS**裝置新增為ACS上的**AAA Client**。



41. 提供**TACACS+**的**名稱、IP地址**、共用密**碼，然**後按一下**Submit**。



配置Cisco IOS裝置以進行身份驗證和授權

完成這些步驟，以設定Cisco IOS裝置和ACS以進行驗證和授權。

1. 使用**username**命令建立對回退具有完全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並新增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伺服器的可達性，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伺服器可訪問且使用者已成功通過身份驗證。**注意：**使用者1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enable secret。

驗證

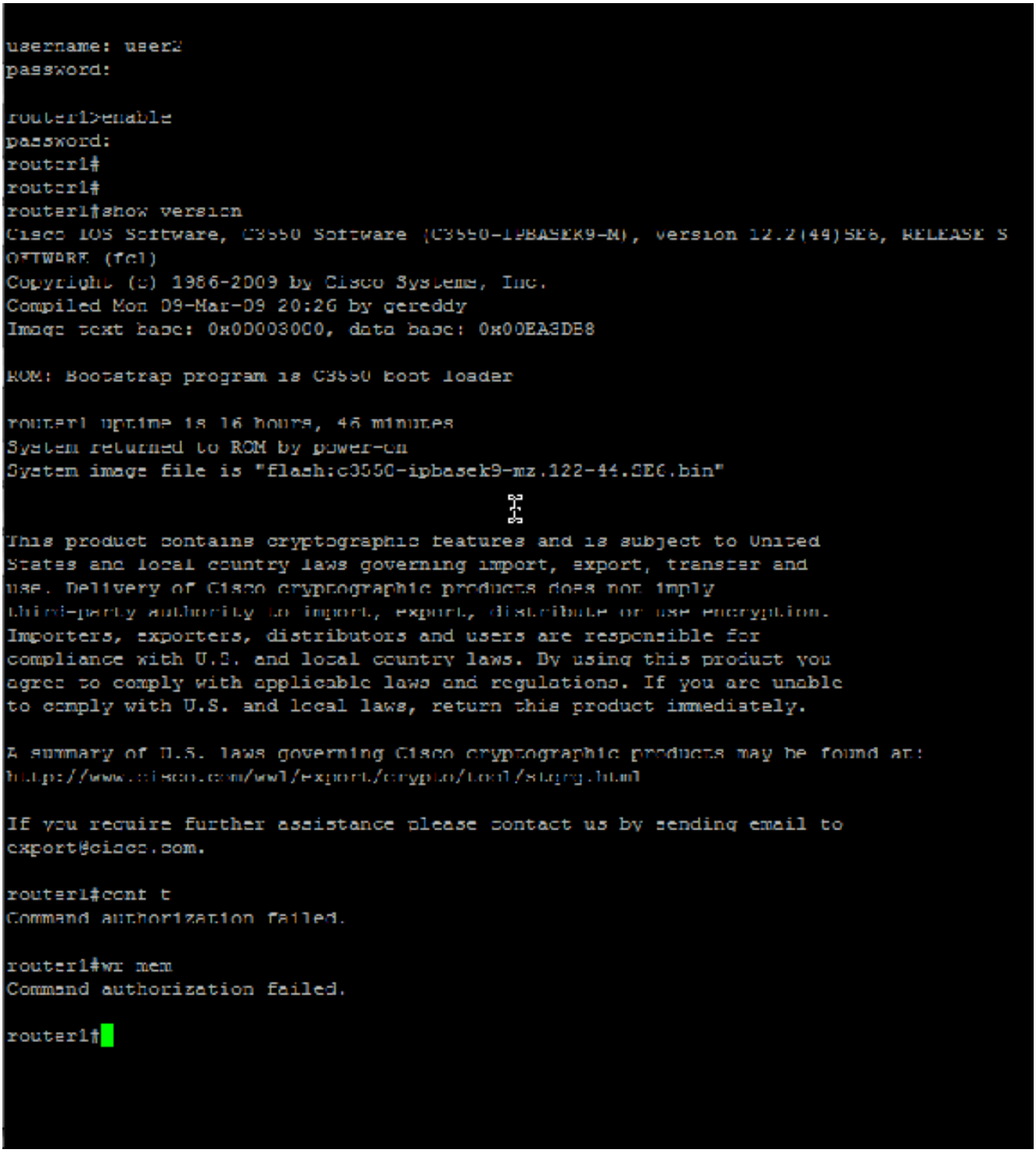
驗證透過Telnet登入Cisco IOS裝置的驗證和授權。

1. 以user1的身份通過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上設定的完全特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。

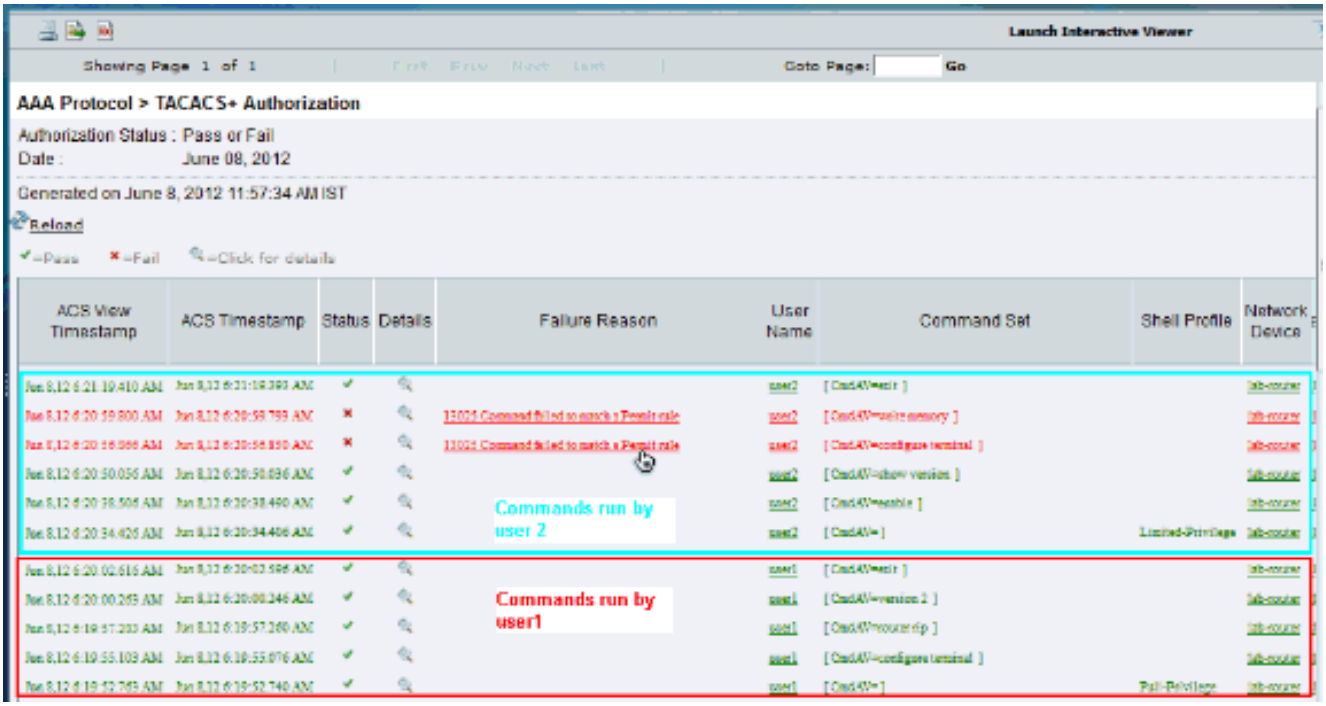
```
username: user1
password:

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身份通過Telnet連線到Cisco IOS裝置，該使用者在AD中屬於受限訪問組。(**Network Maintenance Team**組是AD中對映到在ACS上設定**Limited-Privilege Shell Profile**和**Show-Access Command**的組)。 如果您嘗試運行除Show-Access命令集中提到的命令以外的任何命令，您應該會收到`Command Authorization Failed`錯誤，其中顯示user2具有有限的訪問許可權。



3. 登入到ACS GUI並啟動**監控和報告檢視器**。選擇**AAA Protocol > TACACS+Authorization**以驗證user1和user2執行的活動。



相關資訊

- 思科安全存取控制系統
- 技術支援與文件 - Cisco Systems