# ACS 5.x: مصادقة TACACS+ وتفويض الأوامر استنادا إلى مثال تكوين عضوية مجموعة الإعلانات

## المحتويات



## المقدمة

يقدم هذا المستند مثالا لتكوين مصادقة TACACS+ وتفويض الأوامر استنادا إلى عضوية مجموعة AD لمستخدم باستخدام نظام التحكم في الوصول الآمن (ACS) من Cisco الإصدار x.5 والإصدارات الأحدث. يستخدم ACS Active Directory (AD) من Microsoft كمخزن هوية خارجي لتخزين موارد مثل المستخدمين والأجهزة والمجموعات والسمات.

## المتطلبات الأساسية

### المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- ACS 5.x مدمج بالكامل في مجال AD المرغوب. إذا لم يتم دمج ACS مع مجال AD المرغوب، ارجع إلى ACS 5.x والإصدارات الأحدث: التكامل مع مثال تكوين Microsoft Active Directory للحصول على مزيد من المعلومات لتنفيذ مهمة التكامل.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Secure ACS 5.3
- برنامج IOS® الإصدار 12.2(44)SE6 من Cisco.**ملاحظة:** يمكن تنفيذ هذا التكوين على جميع أجهزة Cisco IOS.

- مجال Microsoft Windows Server 2003

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

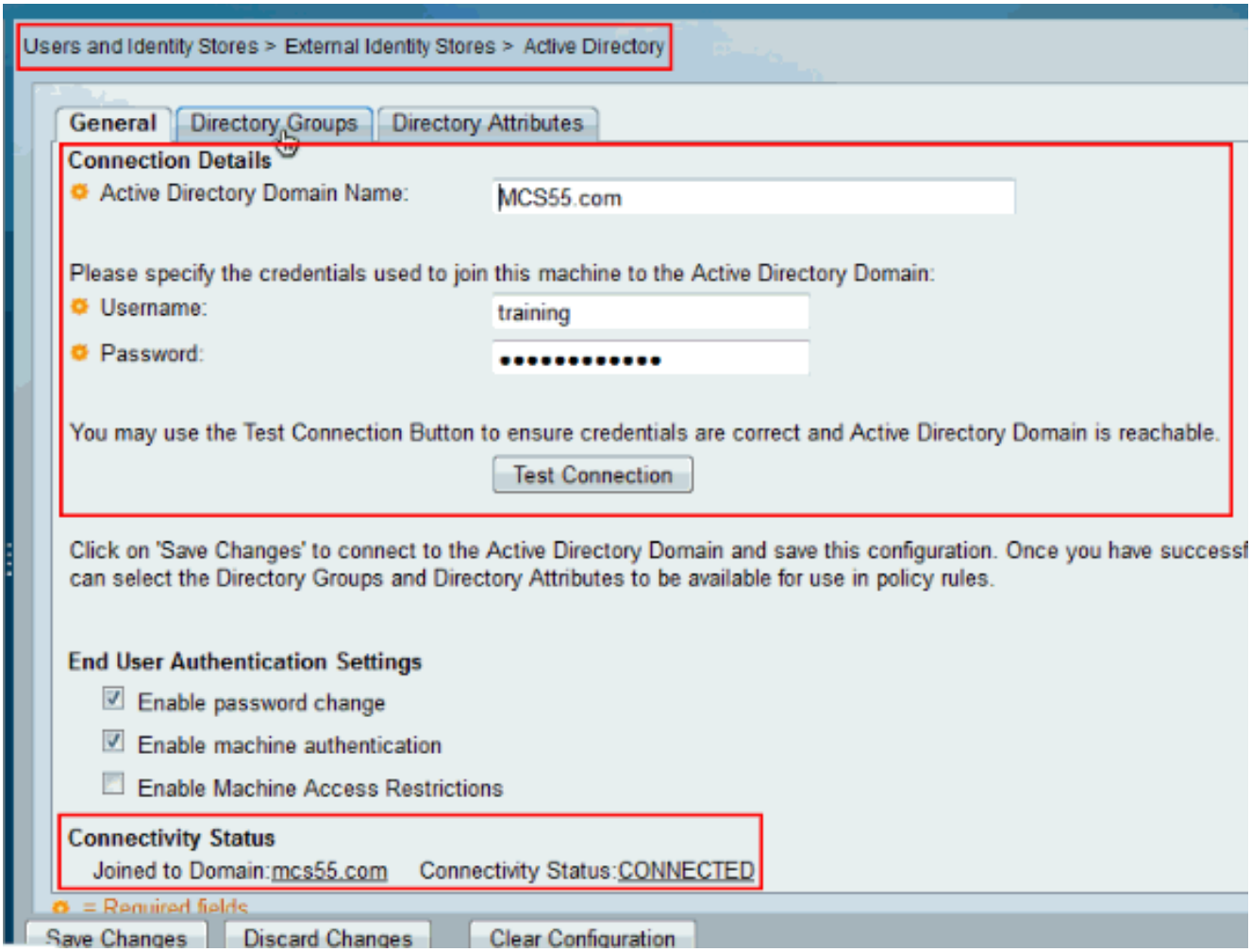
# التكوين

## تكوين ACS 5.x للمصادقة والتفويض

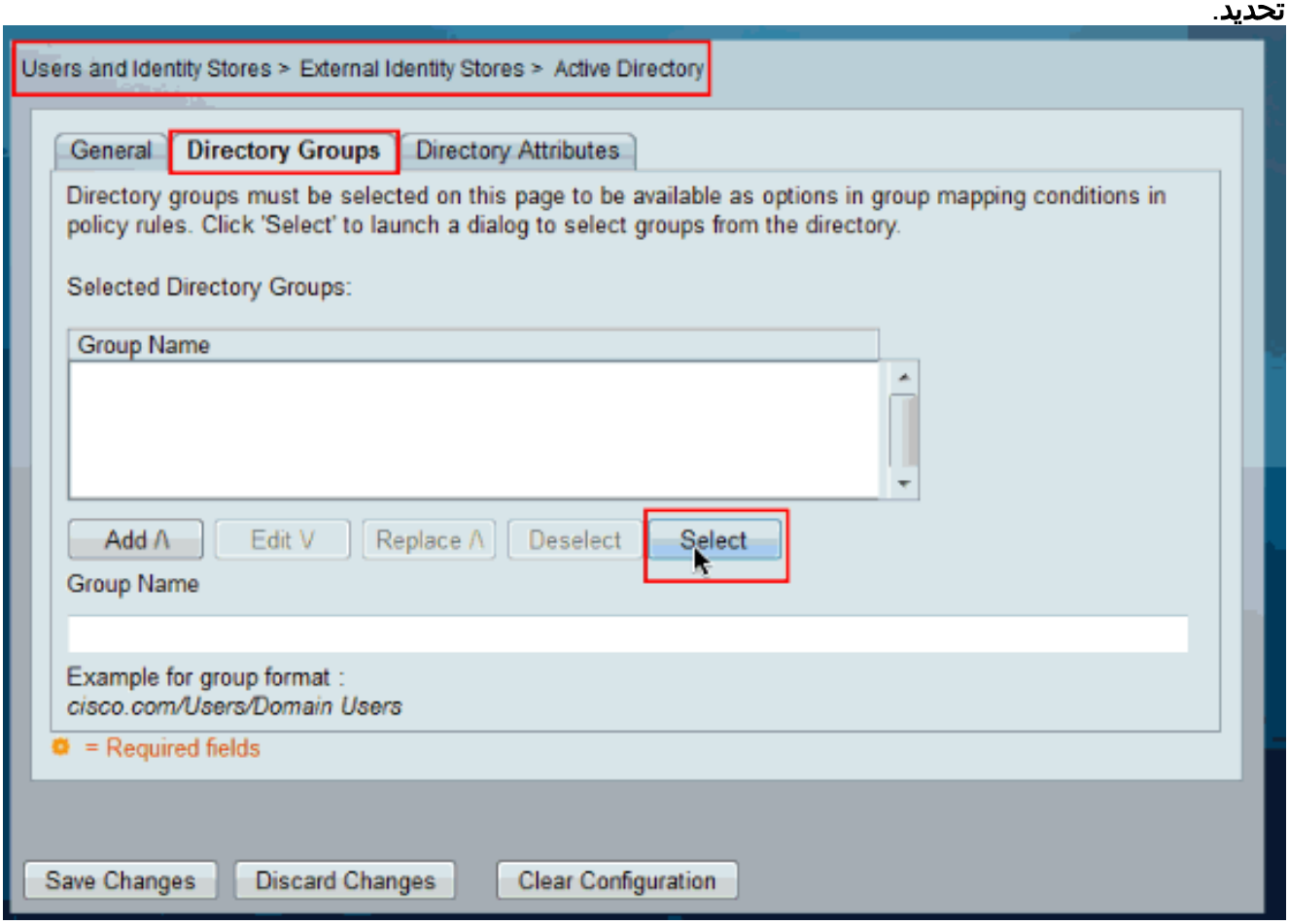
قبل البدء في تكوين ACS 5.x للمصادقة والتفويض، كان يجب دمج ACS بنجاح مع Microsoft AD. إذا لم يتم دمج ACS مع مجال AD المرغوب، ارجع إلى ACS 5.x والإصدارات الأحدث: التكامل مع مثال تكوين Microsoft Active Directory للحصول على مزيد من المعلومات لتنفيذ مهمة التكامل.

في هذا القسم، تقوم بترجمة مجموعتي إعلان إلى مجموعتي أوامر مختلفتين وتوصيفي Shell، إحداهما بالوصول الكامل والأخرى بالوصول المحدود على أجهزة Cisco IOS.

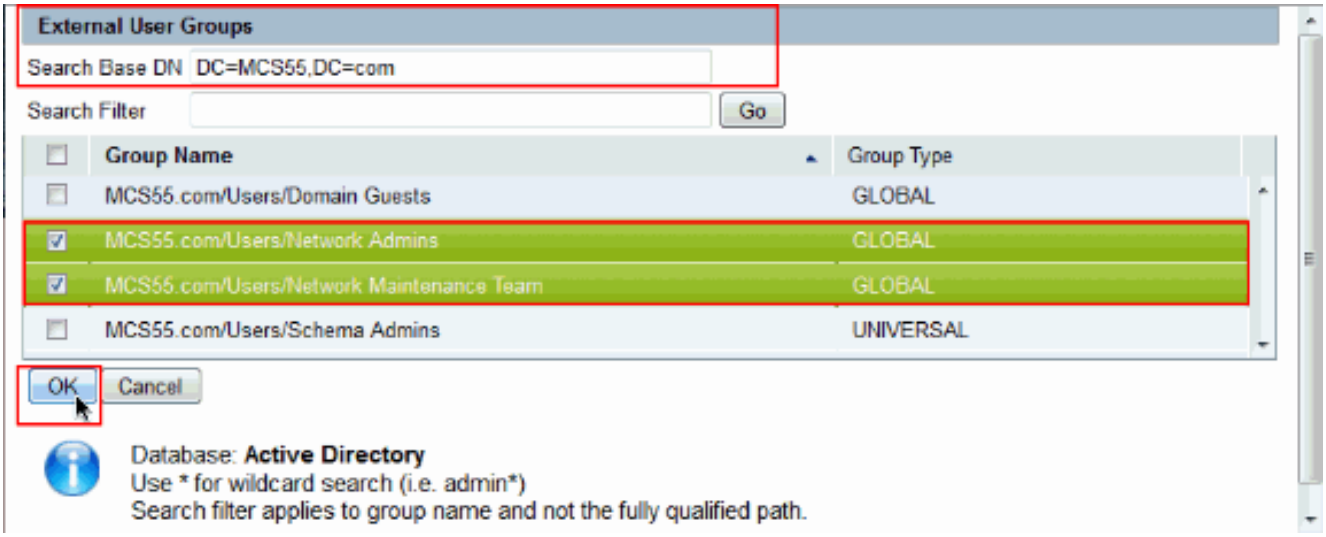
1. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (ACS) باستخدام بيانات اعتماد المسؤول.
2. أختر **Users and Identity Stores (المستخدمين ومتاجر الهوية) > External Identity Stores (مخازن الهوية الخارجية) > Active Directory (الدليل النشط)** وتحقق من انضمام ACS إلى المجال المطلوب وكذلك من إظهار **حالة الاتصال** على أنها **متصلة**.انقر فوق علامة التبويب **مجموعات الدلائل**".



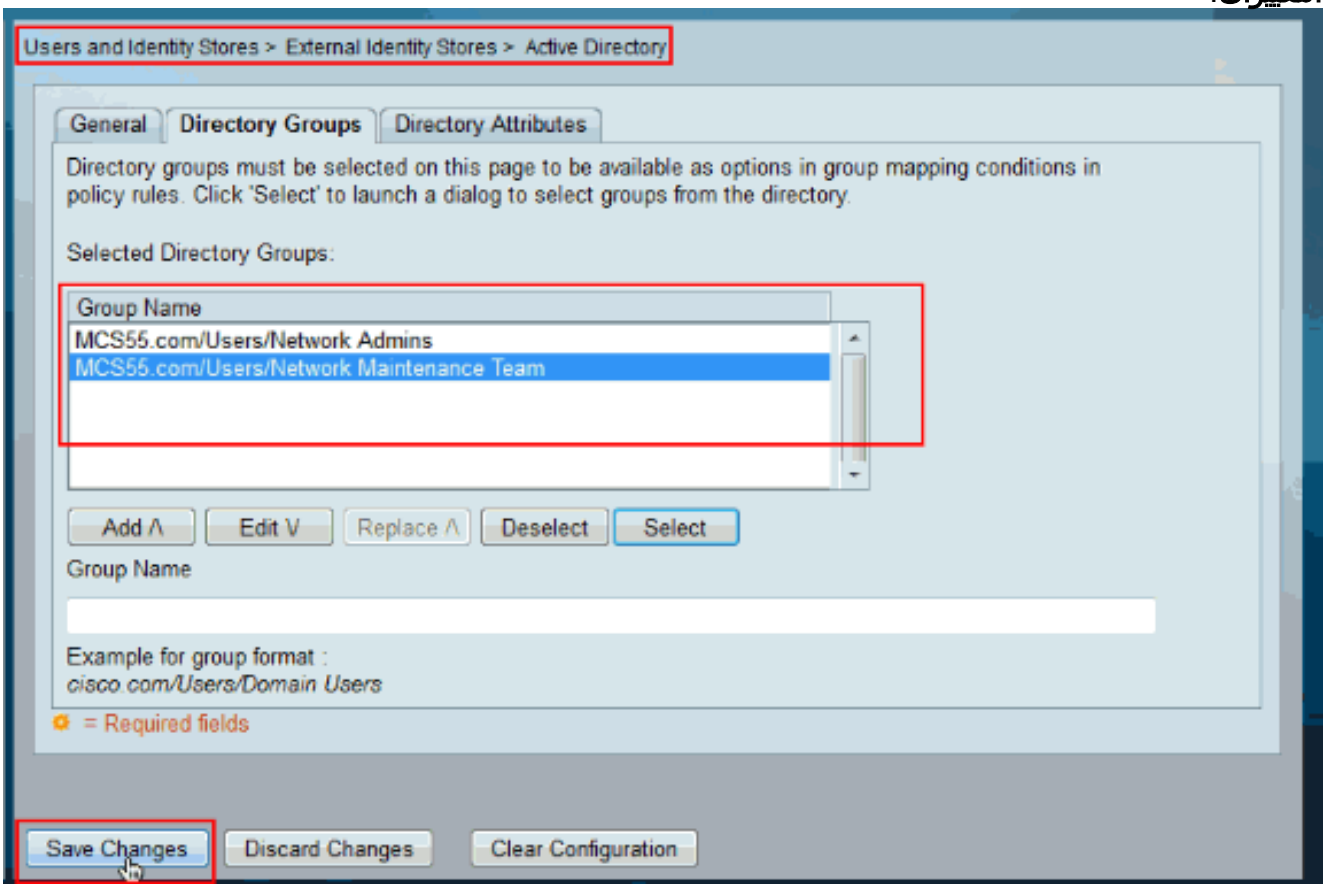

3. انقر فوق
**تحديد**.



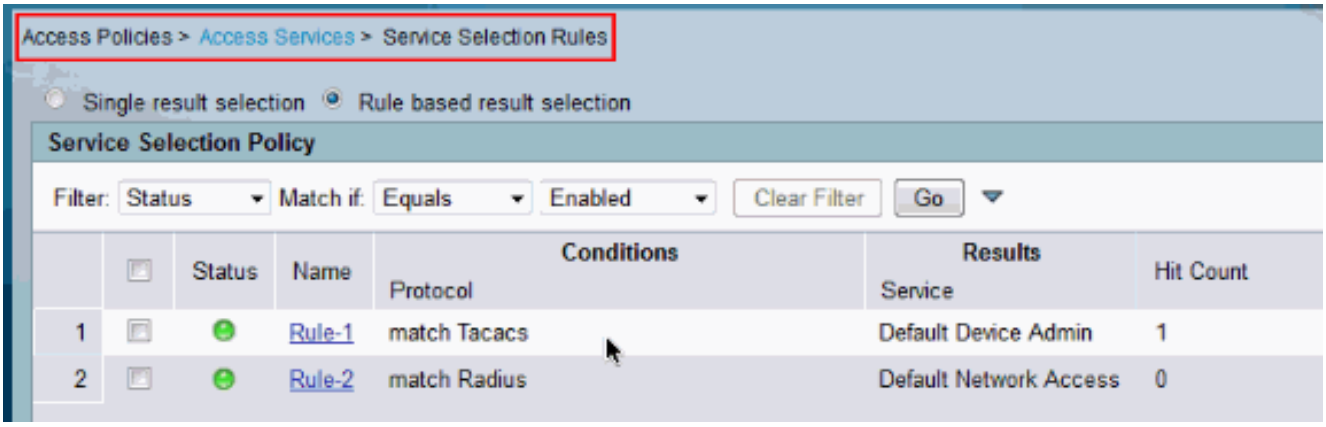
4. أختر المجموعات التي تحتاج أن تكون معينة إلى ملفات تخصيص Shell ومجموعات الأوامر في الجزء الأحدث من التكوين. وانقر فوق **OK**.



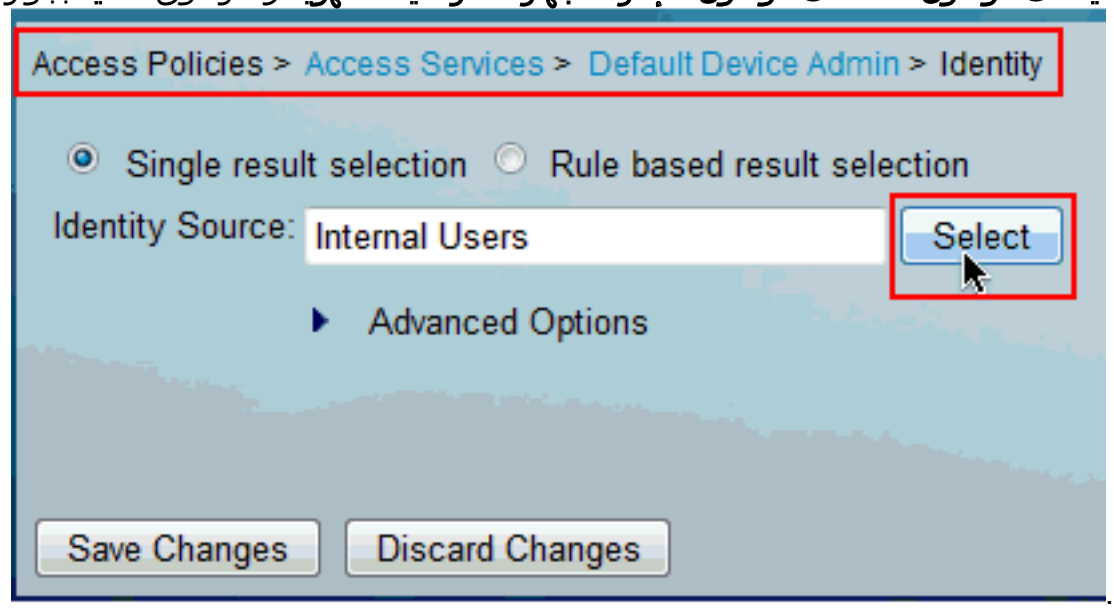

5. انقر فوق **حفظ التغييرات**.




6. أختر **سياسات الوصول > خدمات الوصول > قواعد تحديد الخدمة** وحدد خدمة الوصول، التي تعالج مصادقة TACACS+. في هذا المثال، ستكون **Default Device Admin**.

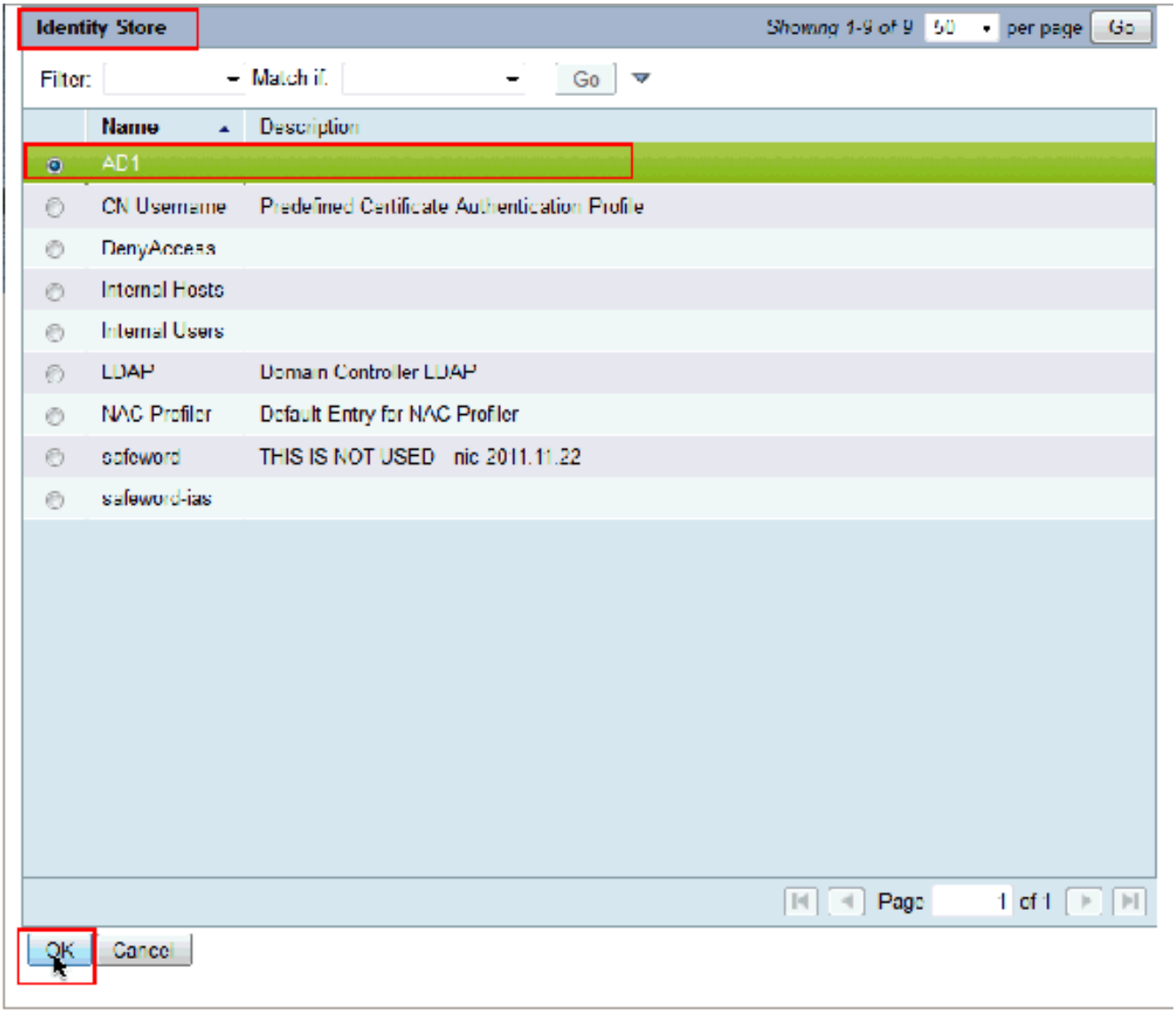



7. أختر **سياسات الوصول > خدمات الوصول > إدارة الجهاز الافتراضية > الهوية** وانقر فوق **تحديد** بجوار **مصدر**

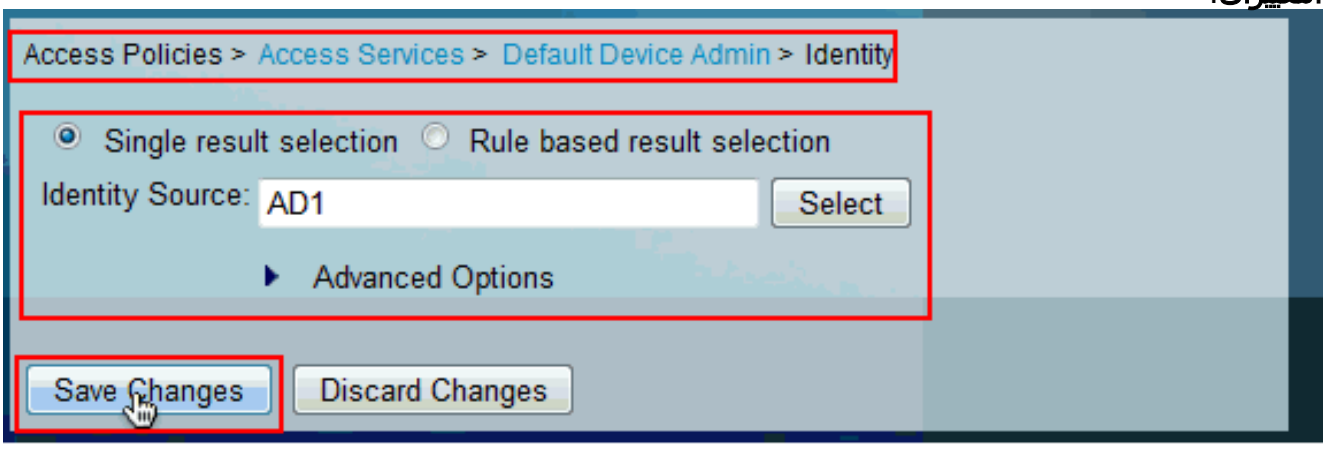



**الهوية.**

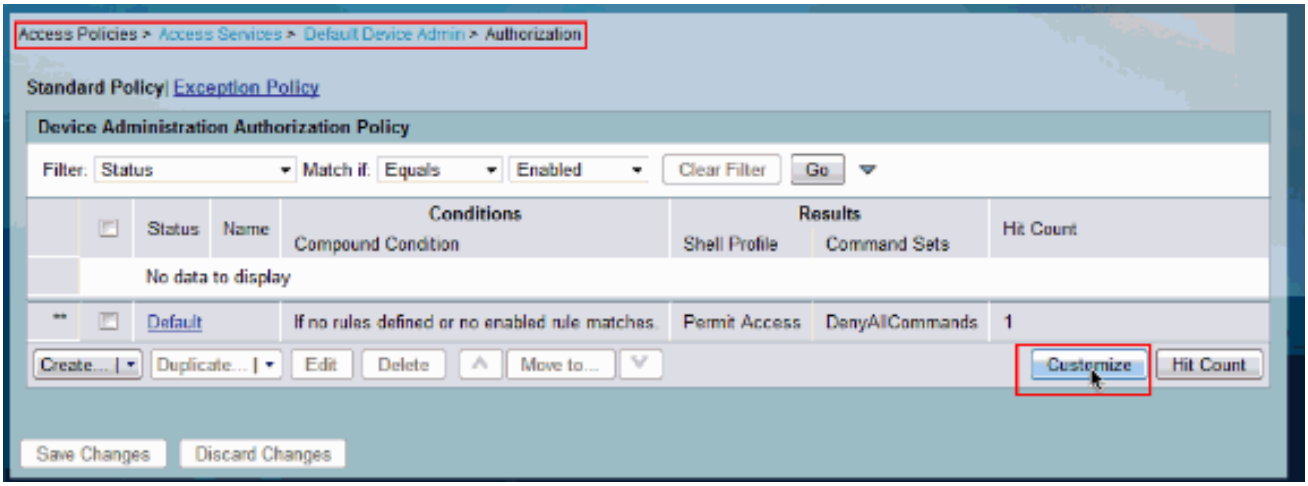
8. أخترت **AD1** وطقطقة **ok**.



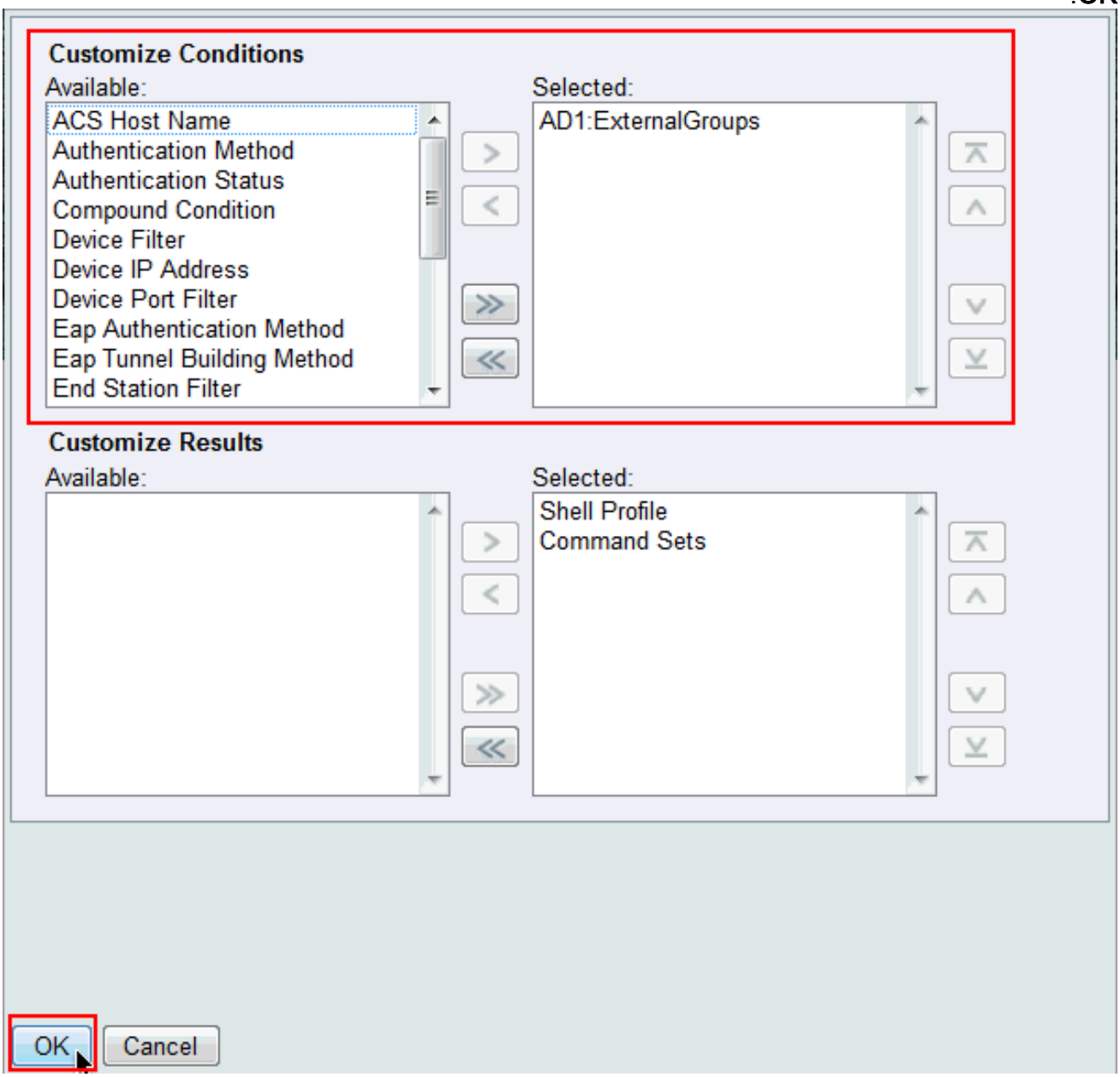

9. انقر فوق **حفظ التغييرات**.



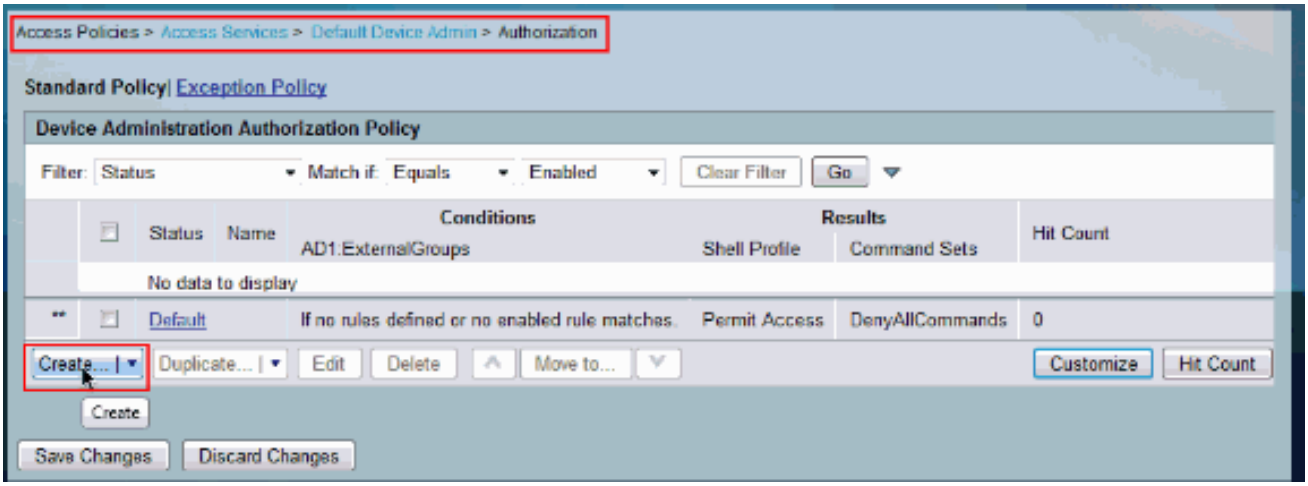

10. أختر **سياسات الوصول > خدمات الوصول > إدارة الجهاز الافتراضية > التفويض** وانقر فوق **تخصيص**.



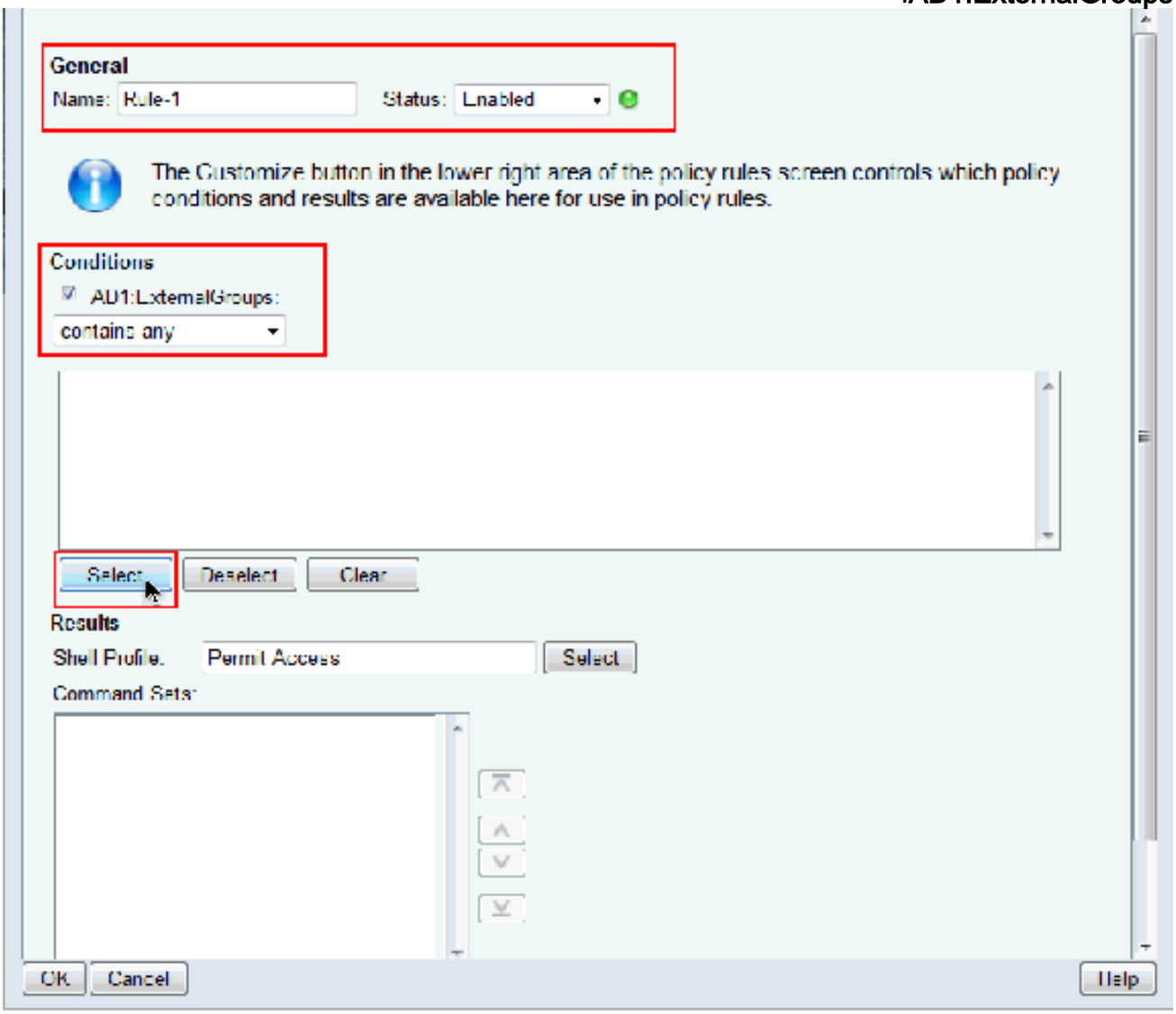

11. انسخ AD1:ExternalGroups من متاح إلى قسم محدد من شروط التخصيص ثم نقل ملف تعريف Shell ومجموعات الأوامر من متاح إلى قسم تخصيص النتائج. وانقر الآن فوق OK.



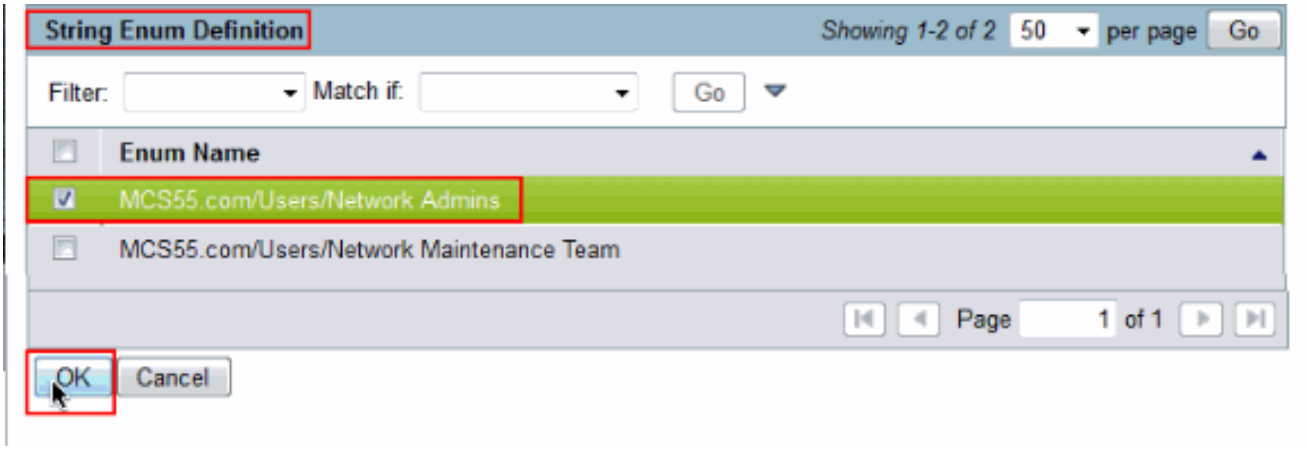

12. انقر فوق **إنشاء** لإنشاء قاعدة جديدة.



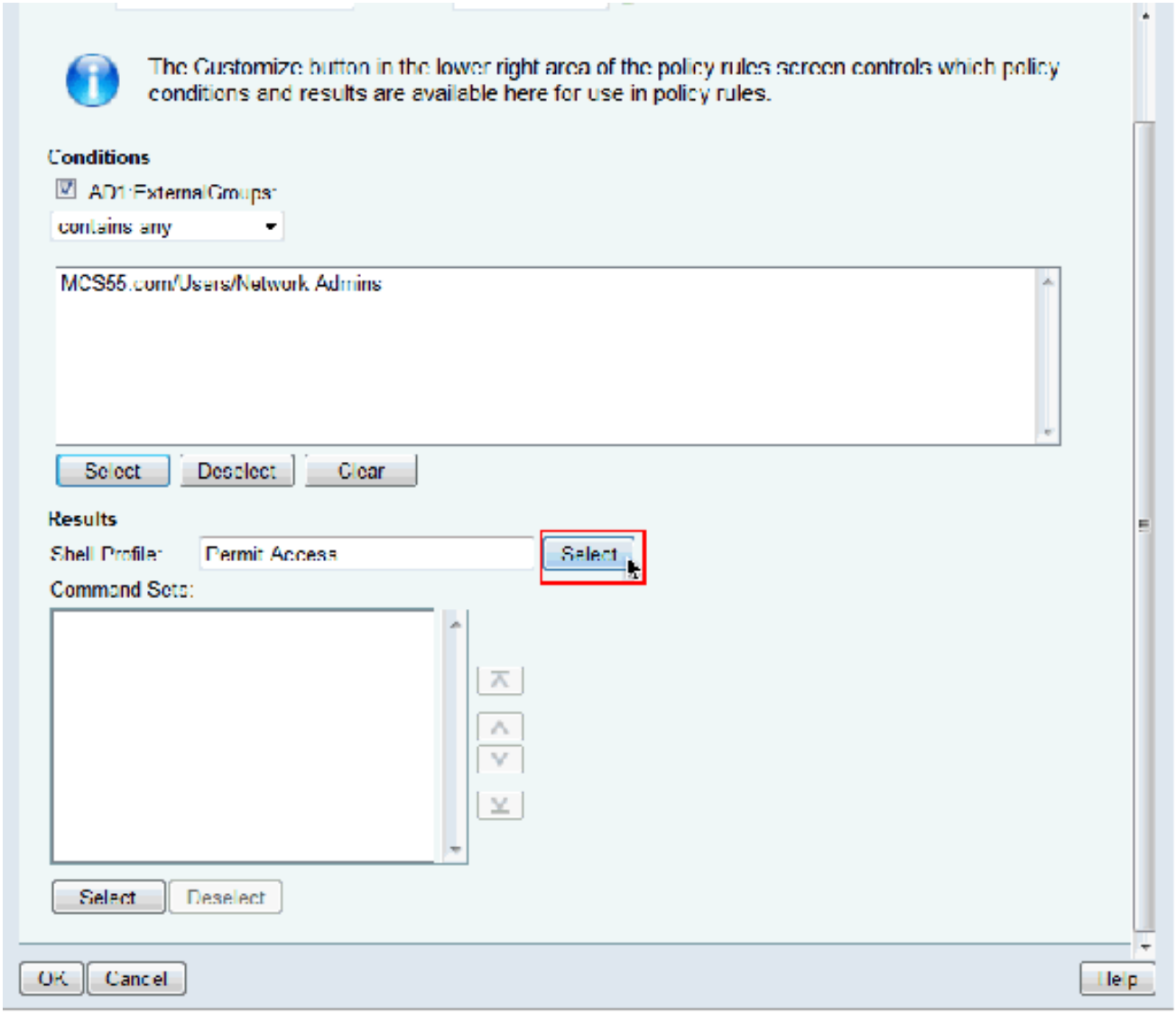

13. انقر على **تحديد** في حالة **AD1:ExternalGroups**.



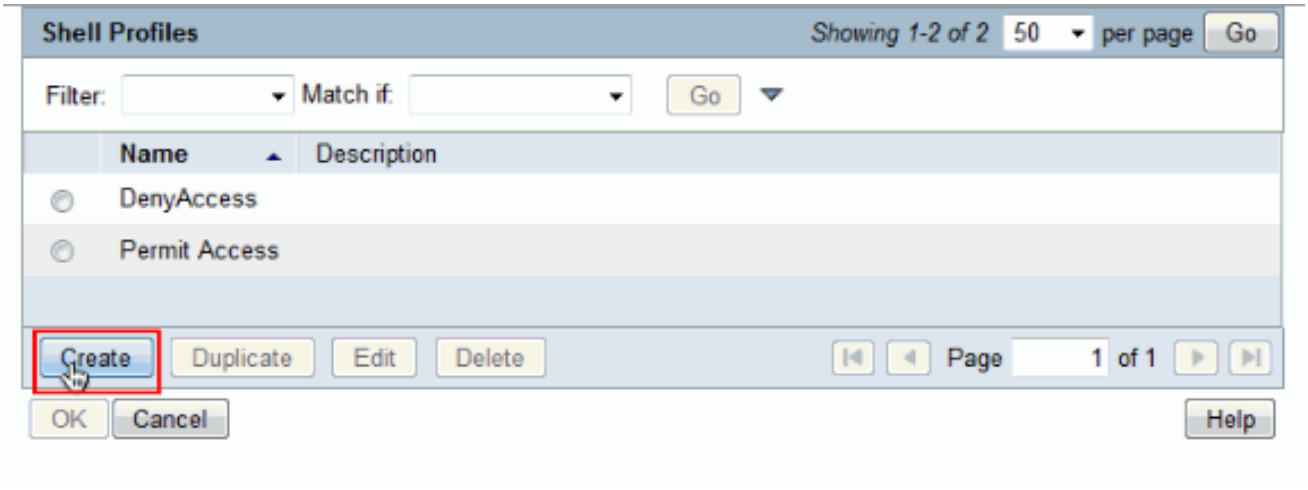

14. أختر المجموعة التي تريد توفير الوصول الكامل عليها على جهاز Cisco IOS. وانقر فوق **OK**.



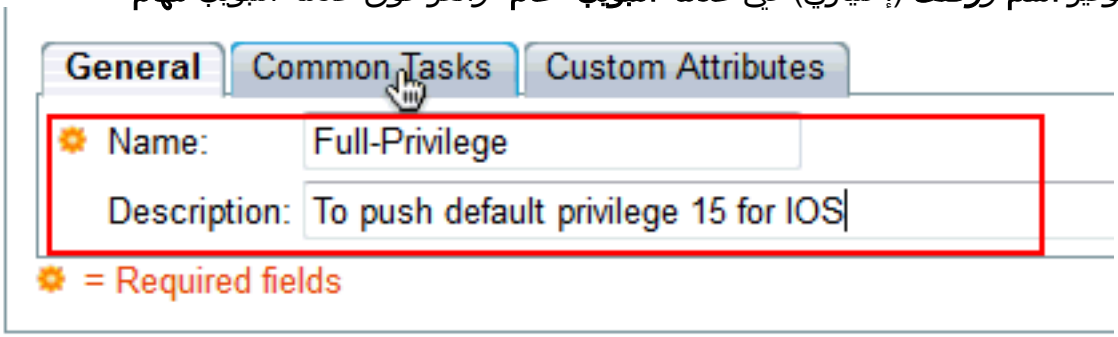

15. انقر على **تحديد** في حقل ملف تعريف Shell.




16. انقر على **إنشاء** لإنشاء **ملف تعريف Shell** جديد لمستخدمي الوصول الكامل.

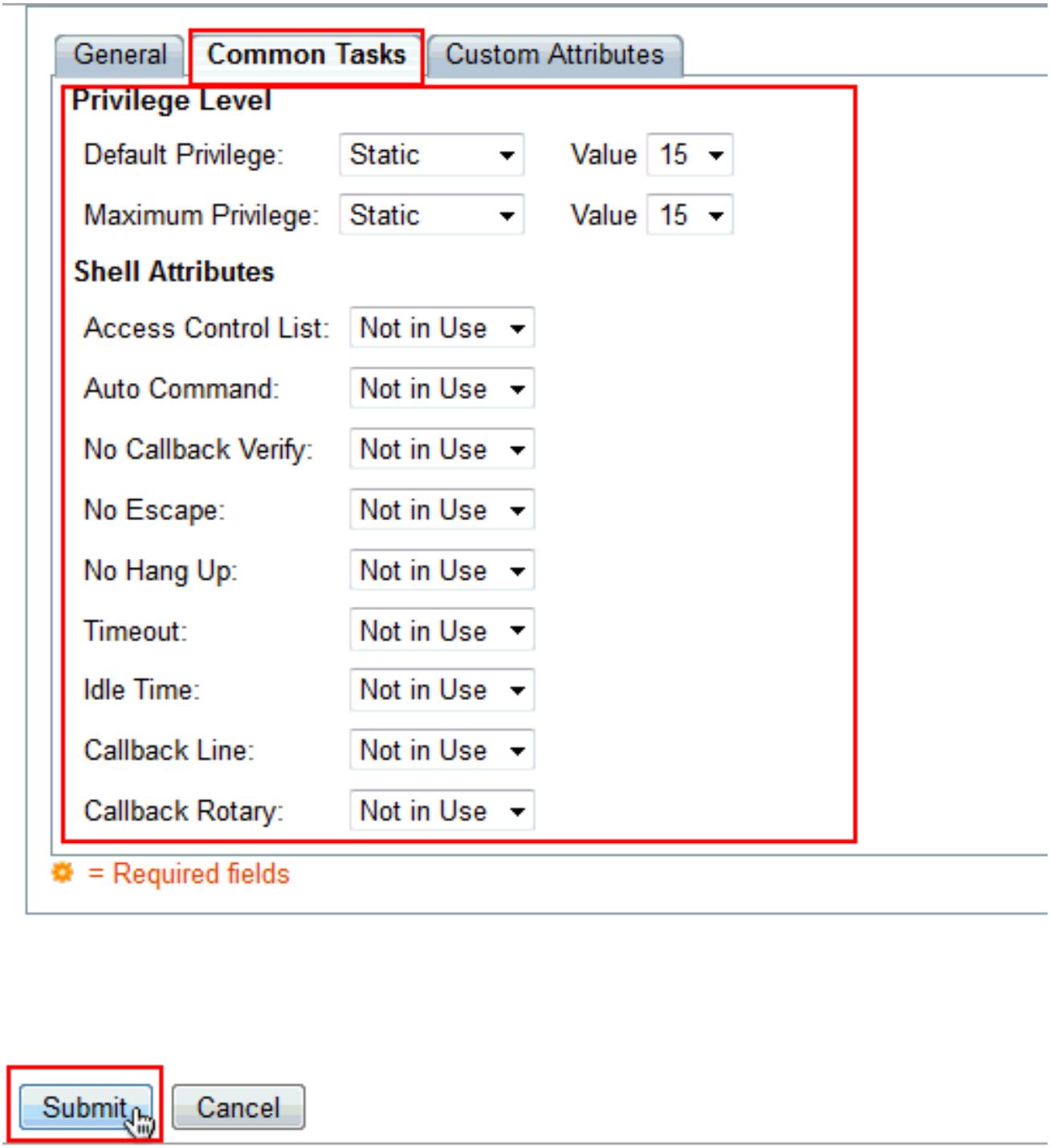



17. قم بتوفير **اسم** و**وصف** (إختياري) في **علامة التبويب "عام"** وانقر فوق علامة التبويب **مهام**

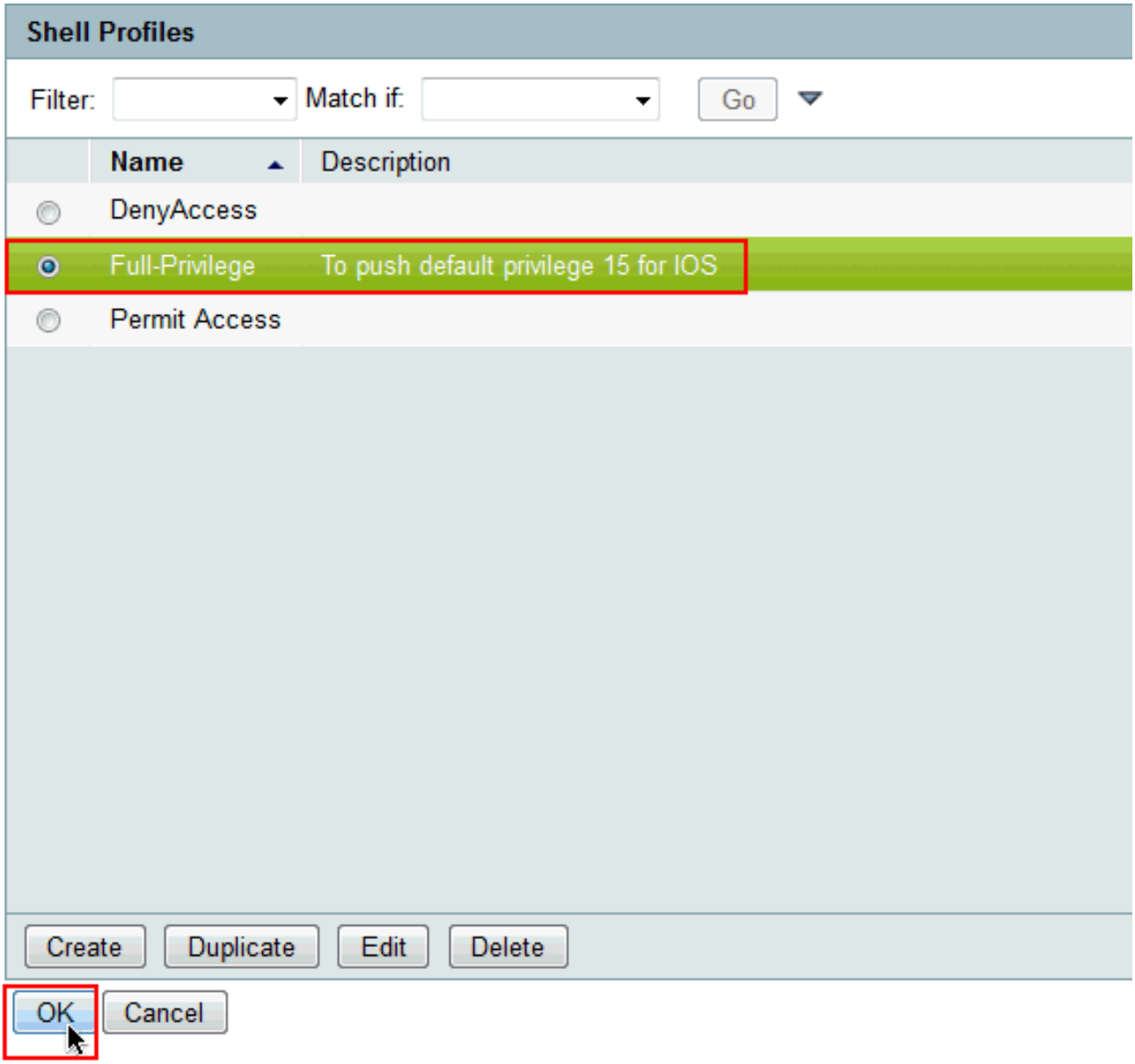



**عامة**.

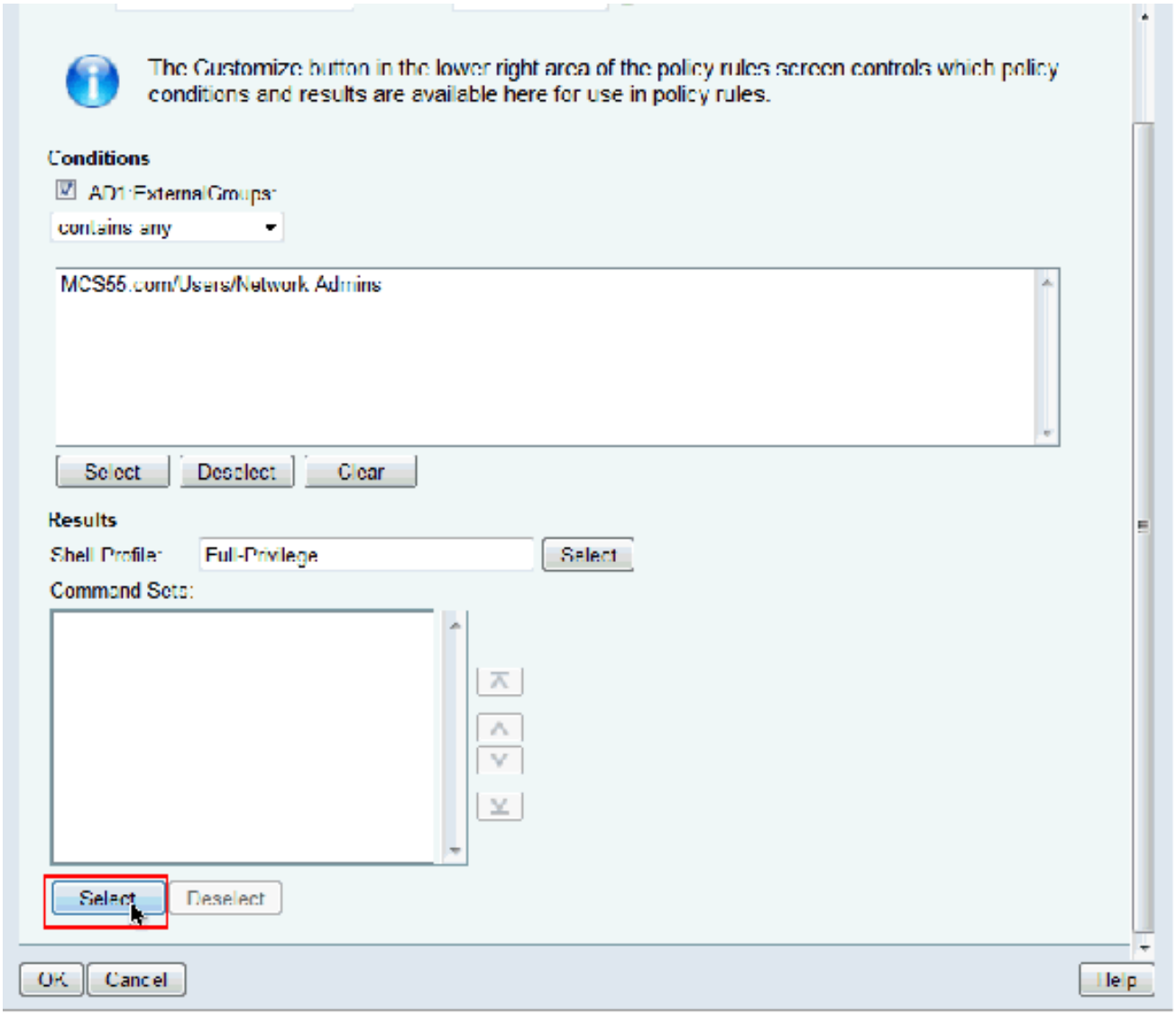
18. غيرت **التقصير امتياز** و**الحد الأقصى امتياز** إلى **ساكن إستاتيكي** مع **القيمة 15**. انقر على **إرسال**.



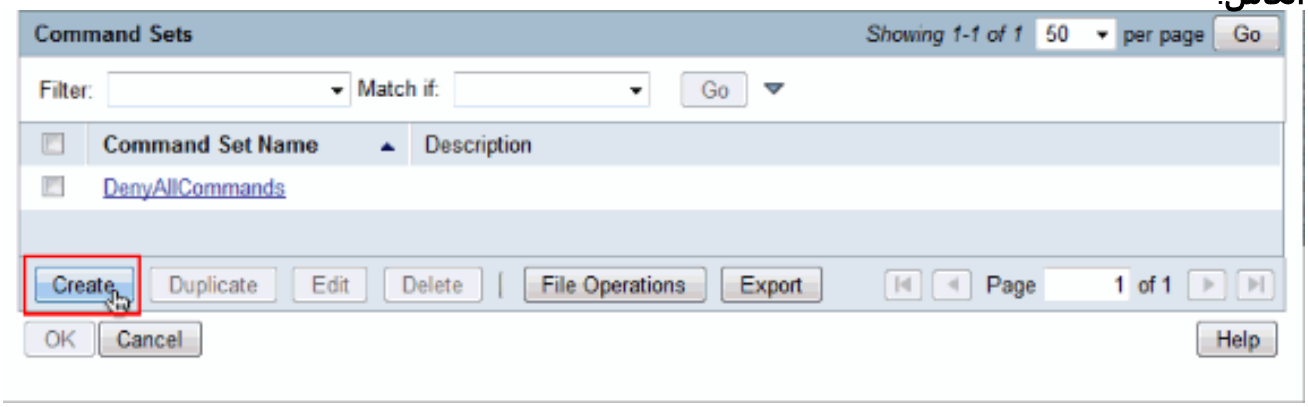

19. أختر الآن ملف تعريف **Shell** للوصول الكامل الذي تم إنشاؤه حديثا (امتياز كامل في هذا المثال) وانقر **موافق**.



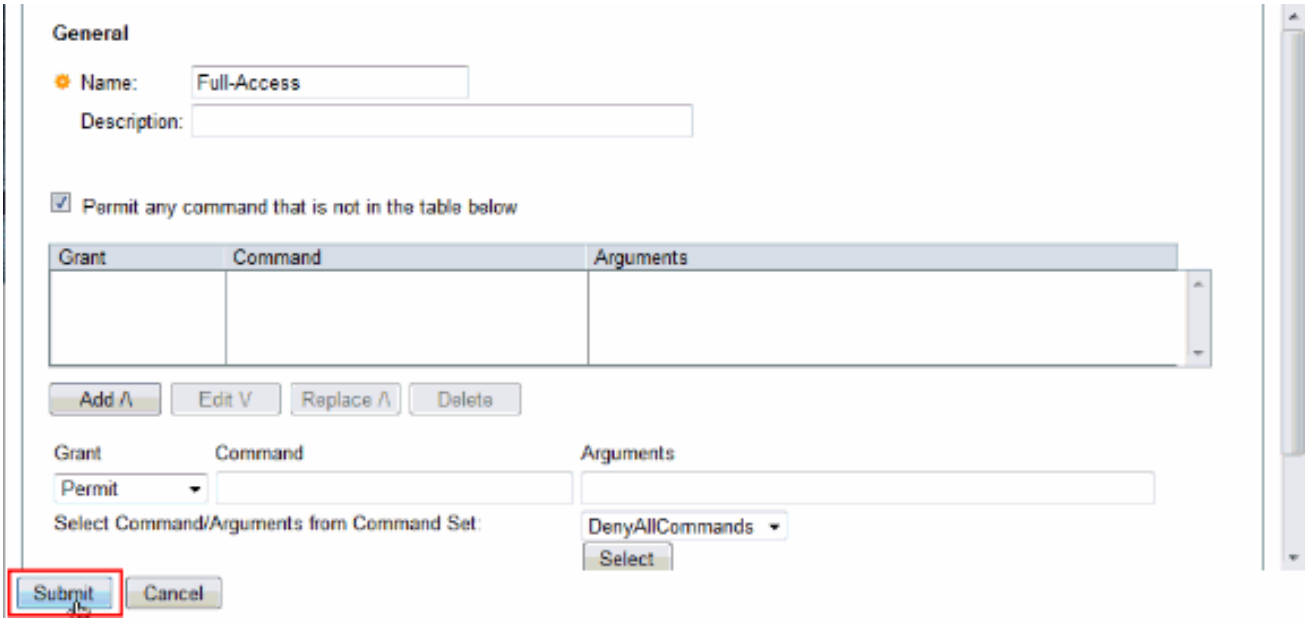

20. انقر **تحديد** في حقل مجموعات الأوامر.



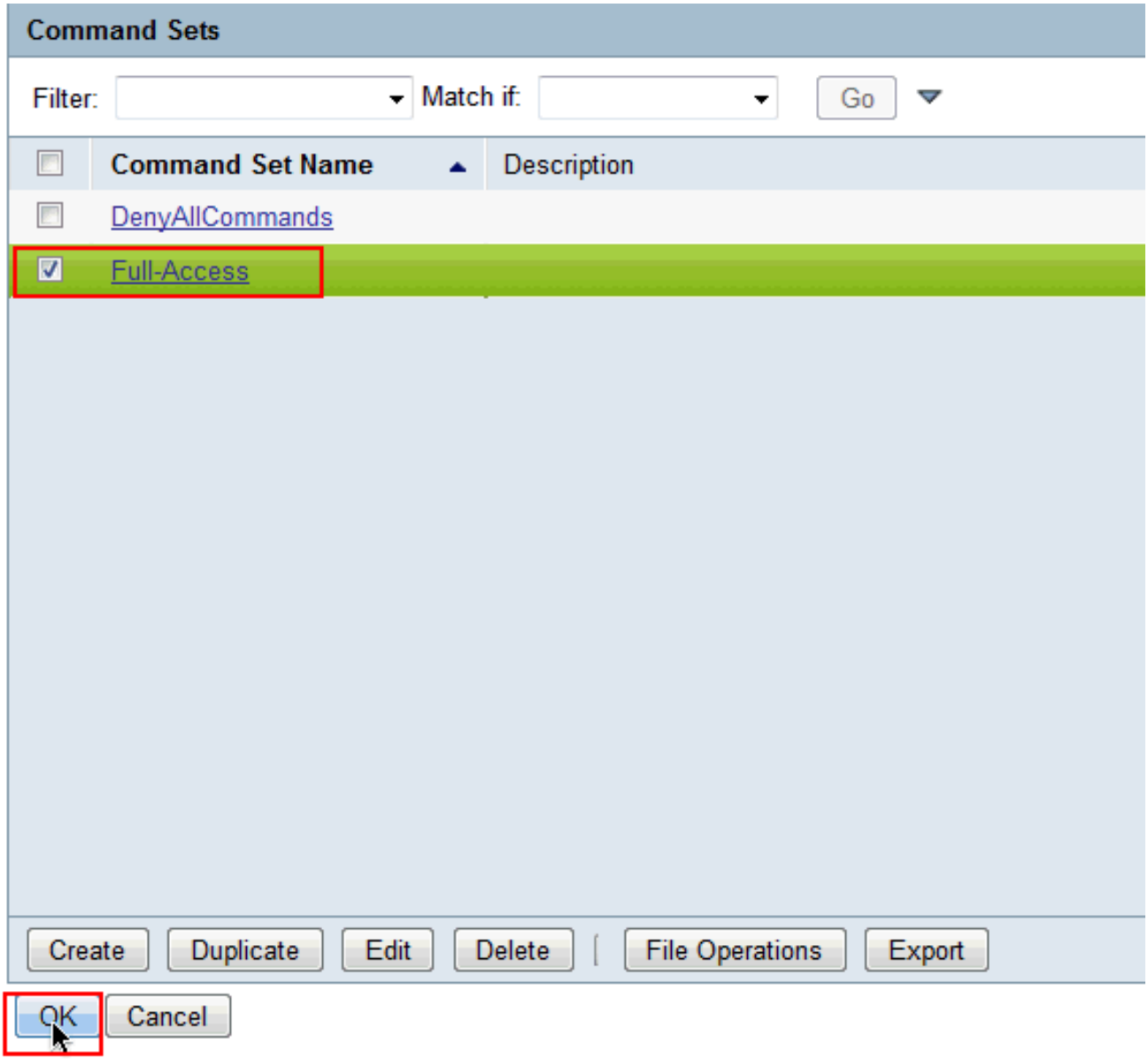

21. انقر فوق **إنشاء** لإنشاء **مجموعة أوامر** جديدة لمستخدمي **الوصول الكامل**.



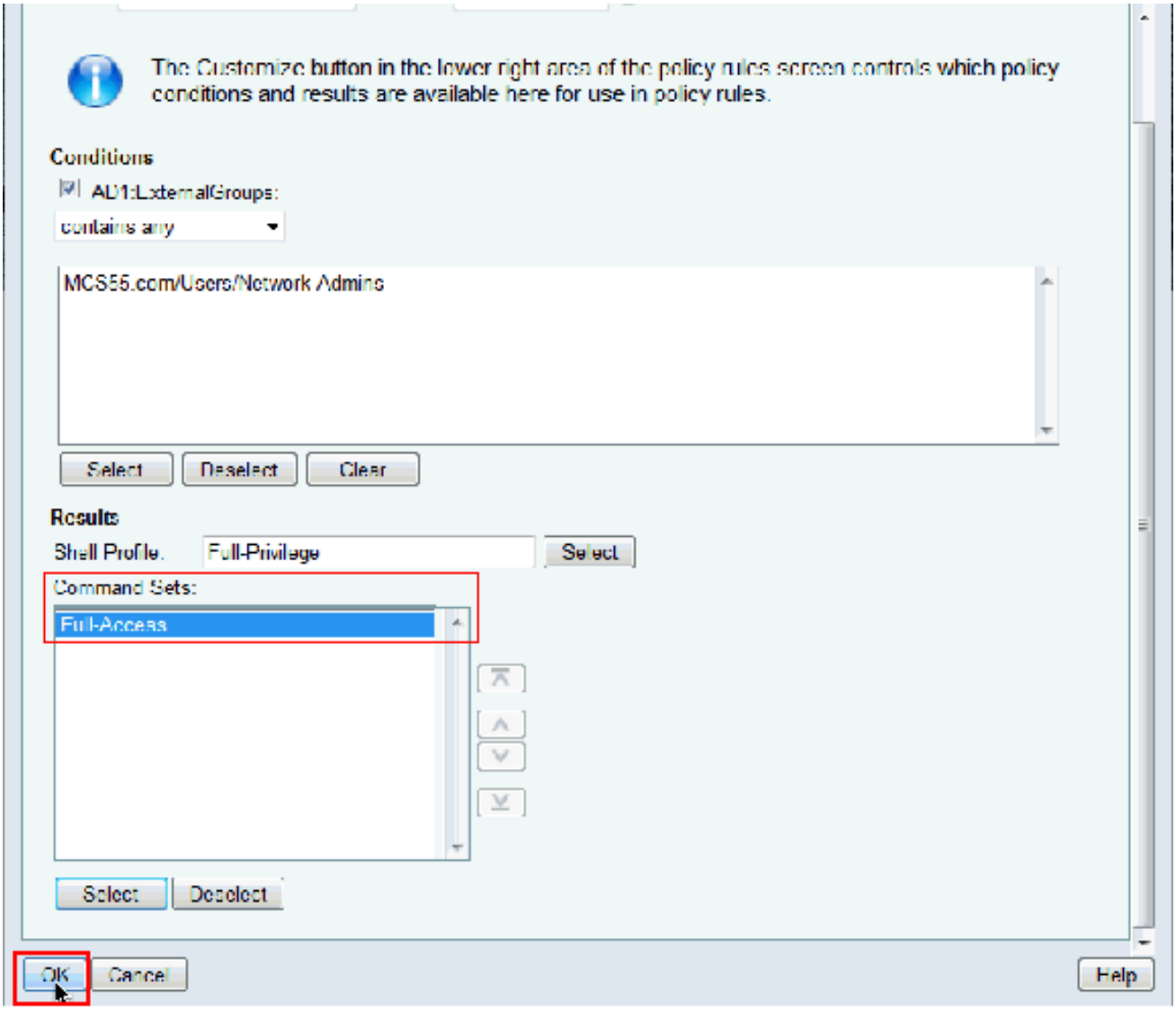

22. قم بتوفير **اسم** وتأكد من تحديد **خانة الاختيار** المجاورة **للسماح بأي أمر غير موجود في الجدول أدناه**. انقر على **إرسال**.**ملاحظة:** راجع إنشاء مجموعات أوامر ومضاعفة وتحريرها لإدارة الأجهزة للحصول على مزيد من المعلومات حول مجموعات الأوامر.



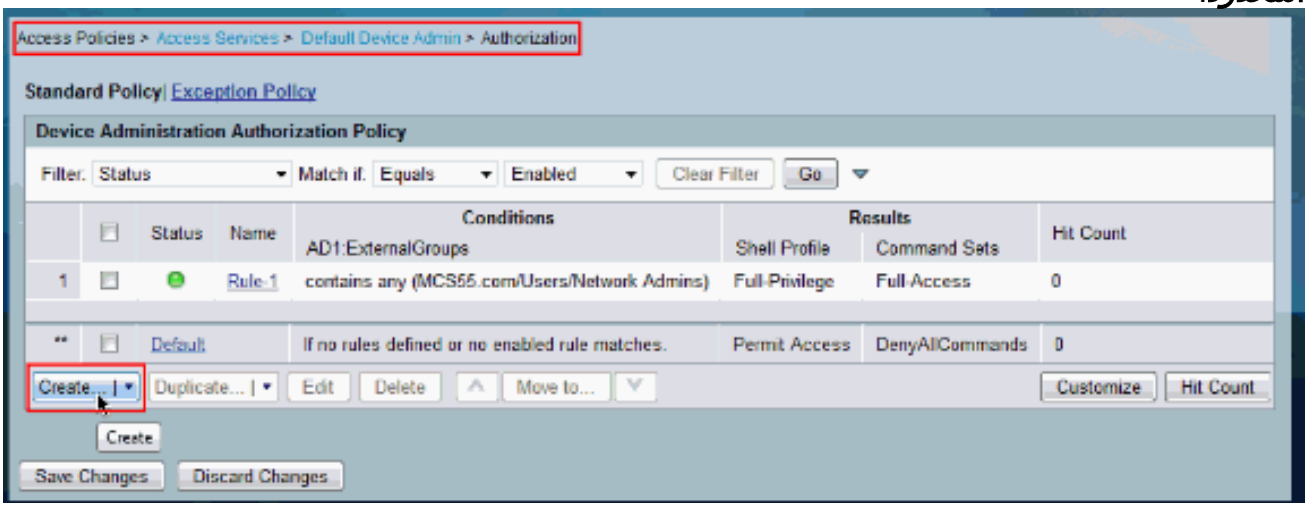

23. وانقر فوق **OK**.



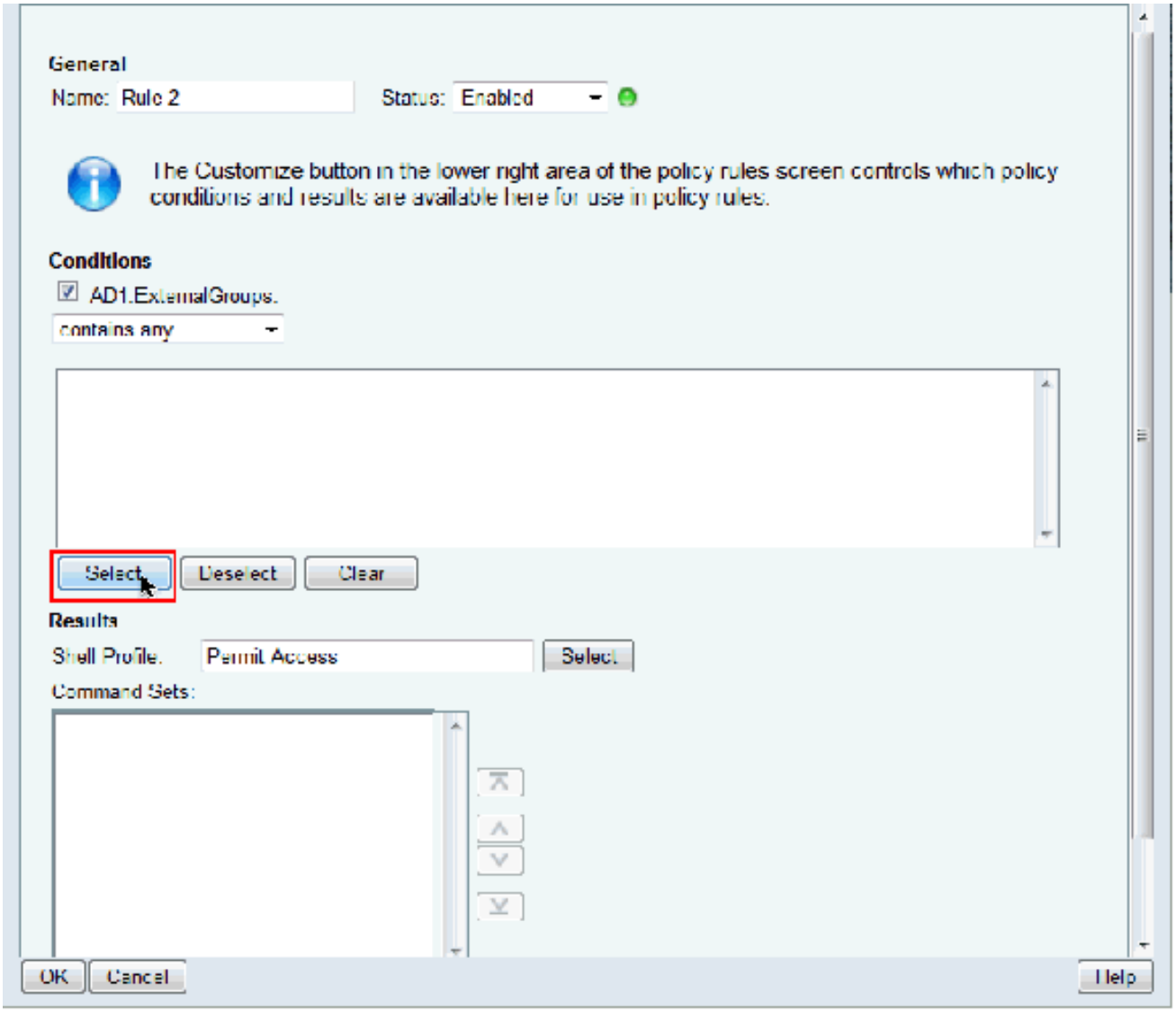

24. وانقر فوق **OK**. يؤدي هذا إلى اكتمال تكوين **القاعدة-1**.



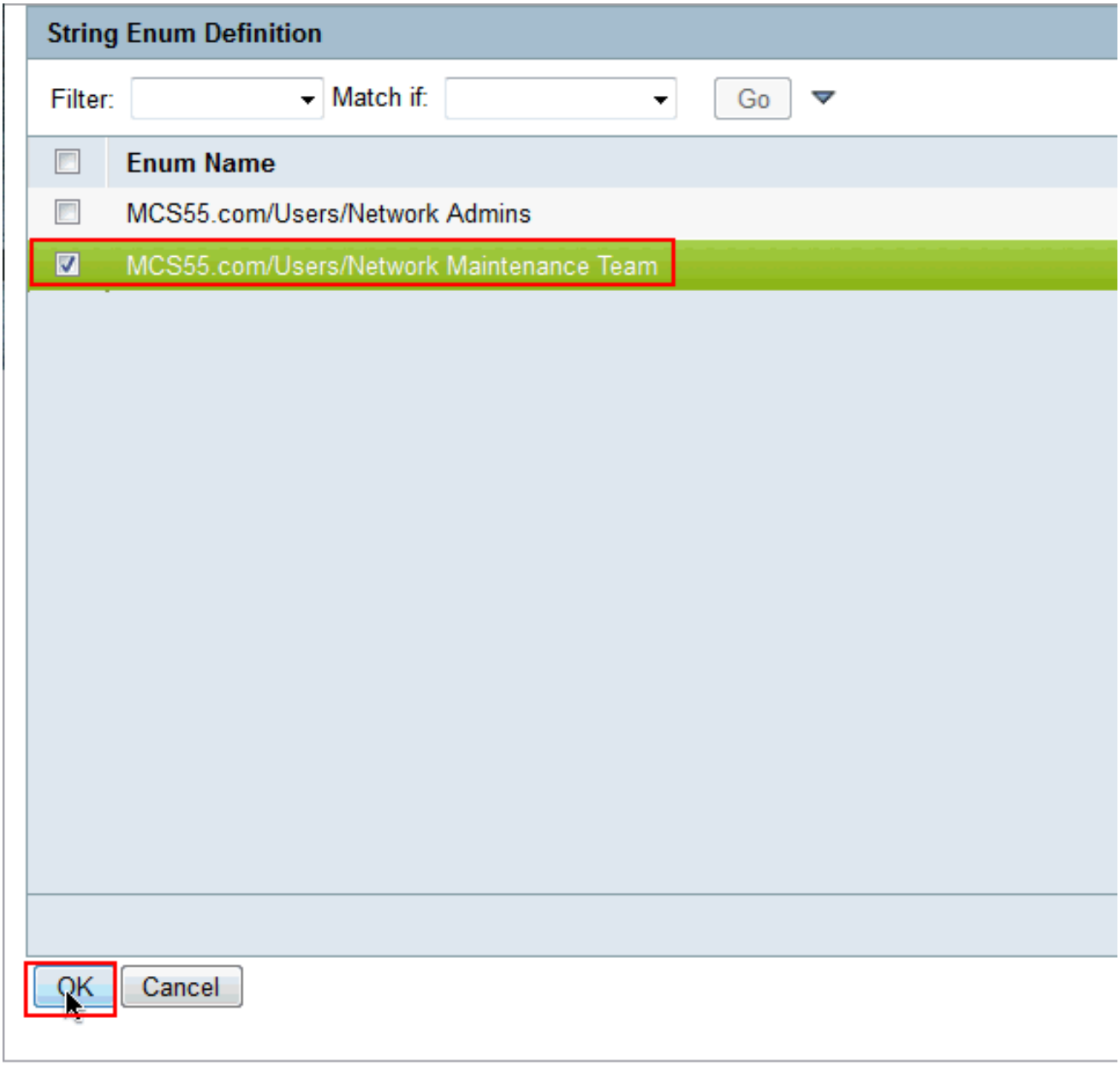

25. انقر فوق **إنشاء** لإنشاء قاعدة جديدة لمستخدمي **الوصول المحدود**.



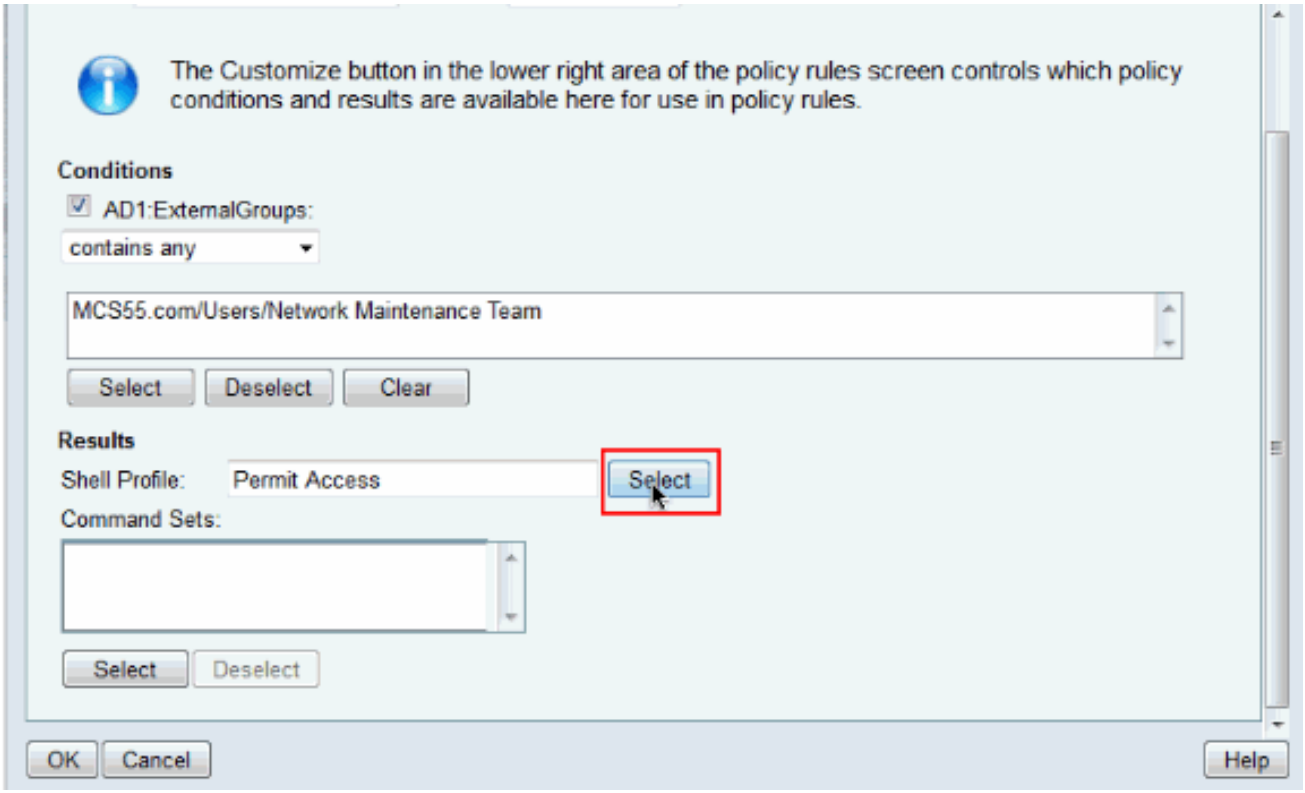

26. أختر **AD1:ExternalGroups** وانقر **تحديد**.



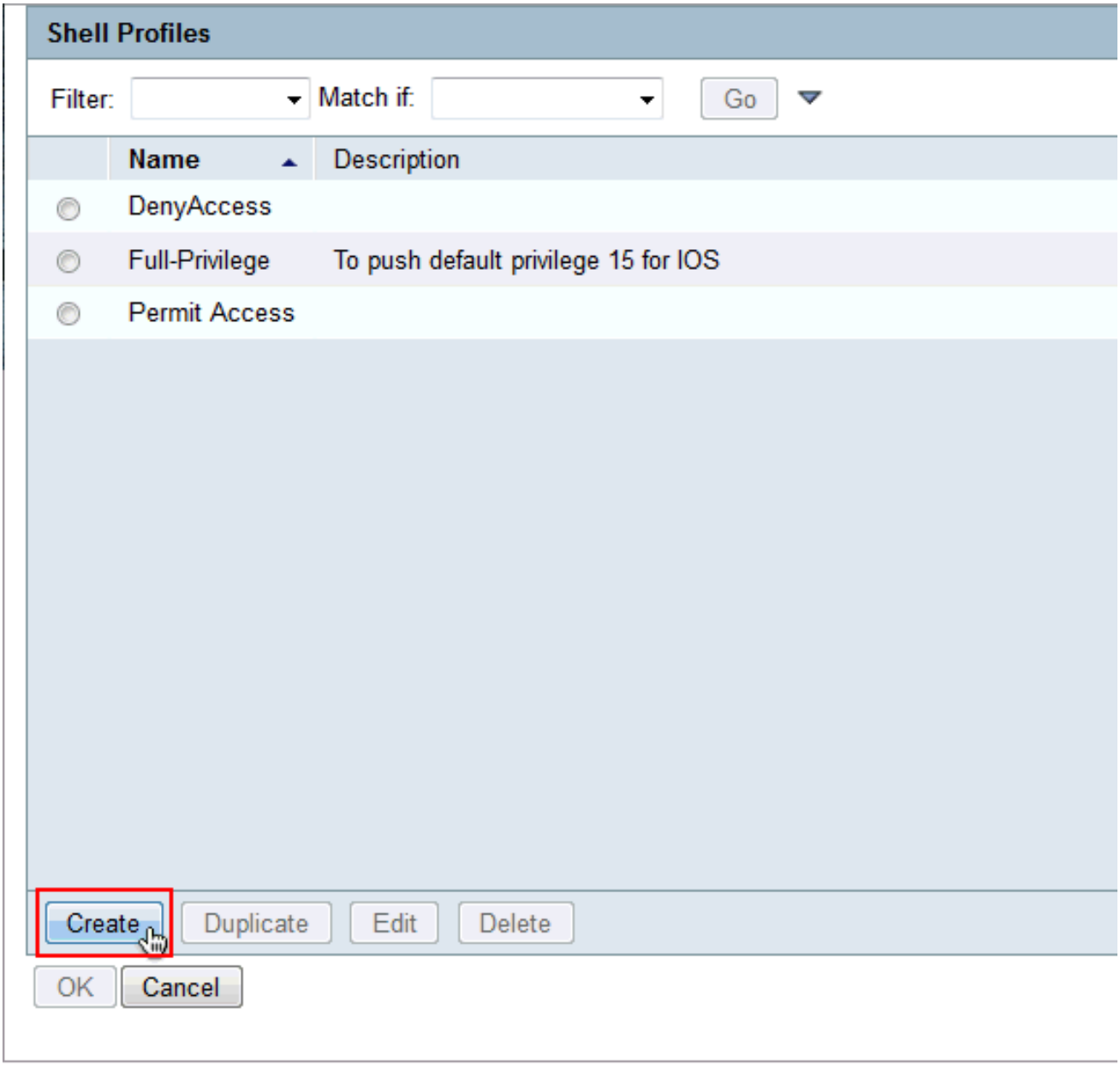

27. أختر مجموعات (أو) المجموعات التي تريد توفير وصول محدود إليها وانقر فوق **موافق**.




28. انقر على **تحديد** في حقل ملف تعريف Shell.

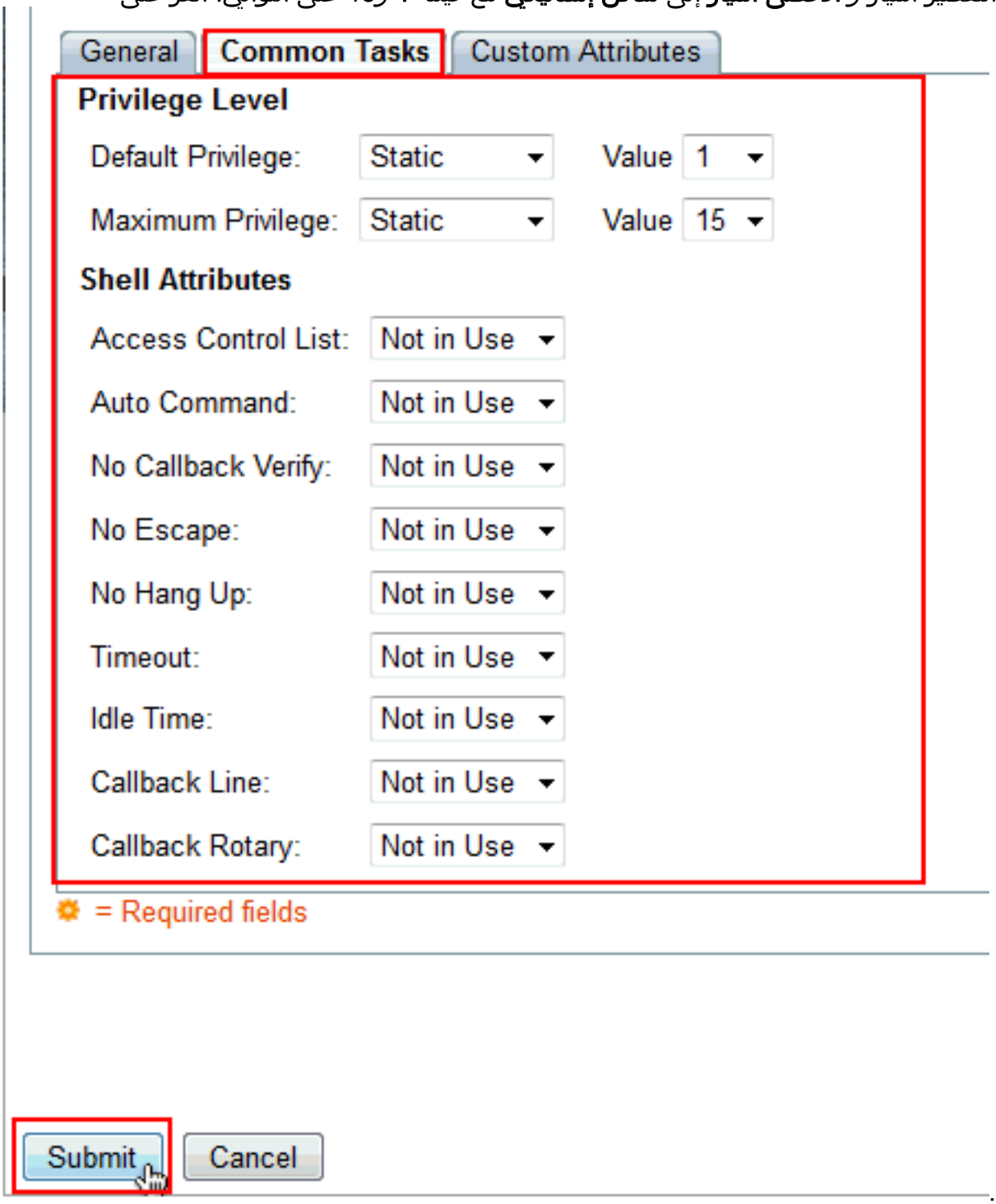



29. انقر على **إنشاء** لإنشاء **ملف تعريف Shell** جديد للوصول المحدود.



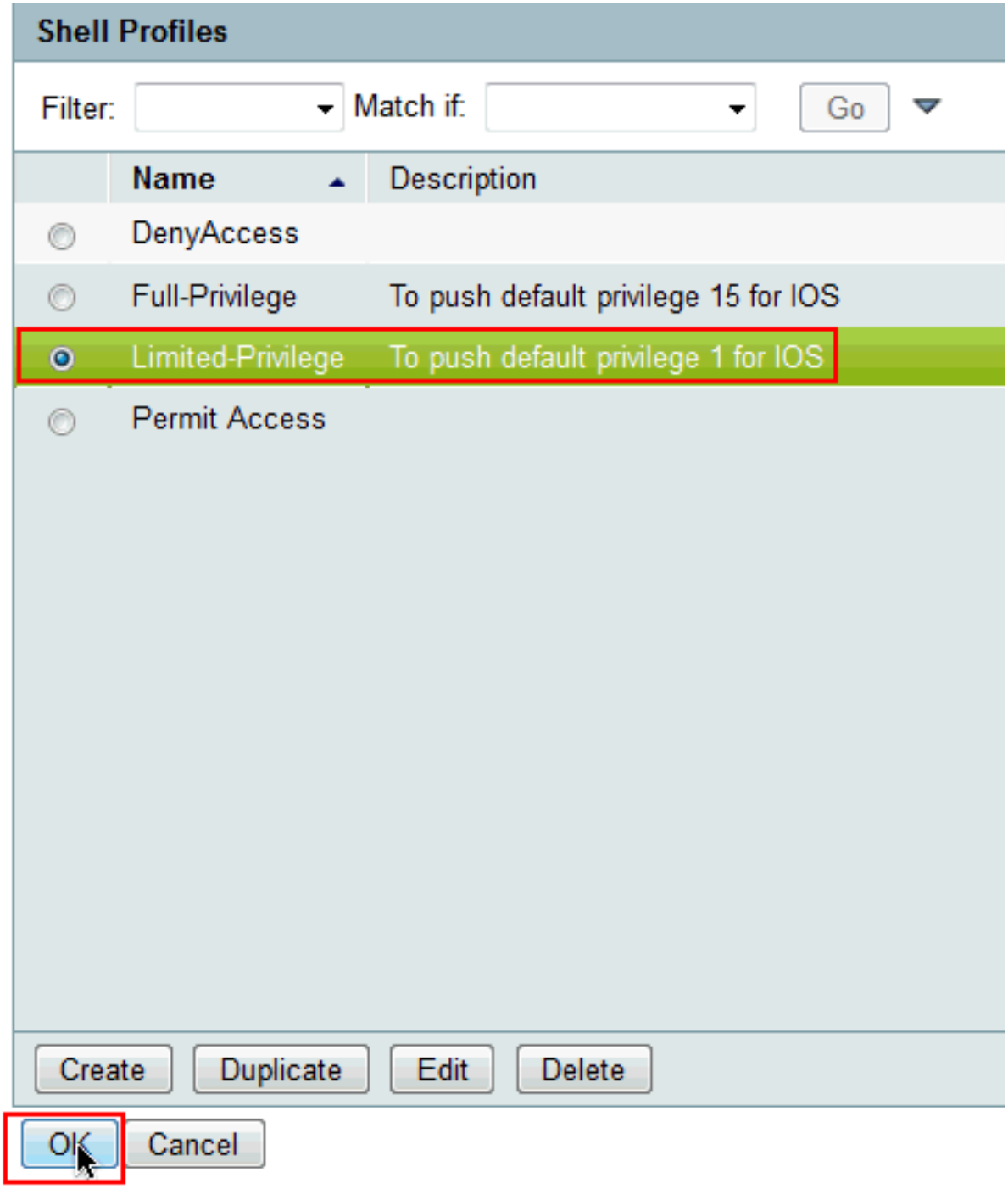

30. قم بتوفير **اسم** و**وصف** (إختياري) في علامة التبويب **عام** وانقر فوق علامة التبويب **مهام مشتركة**.

31. غيرت التقصير امتياز و **الأقصى امتياز** إلى **ساكن إستاتيكي** مع قيمة **1** و15 على التوالي. انقر على



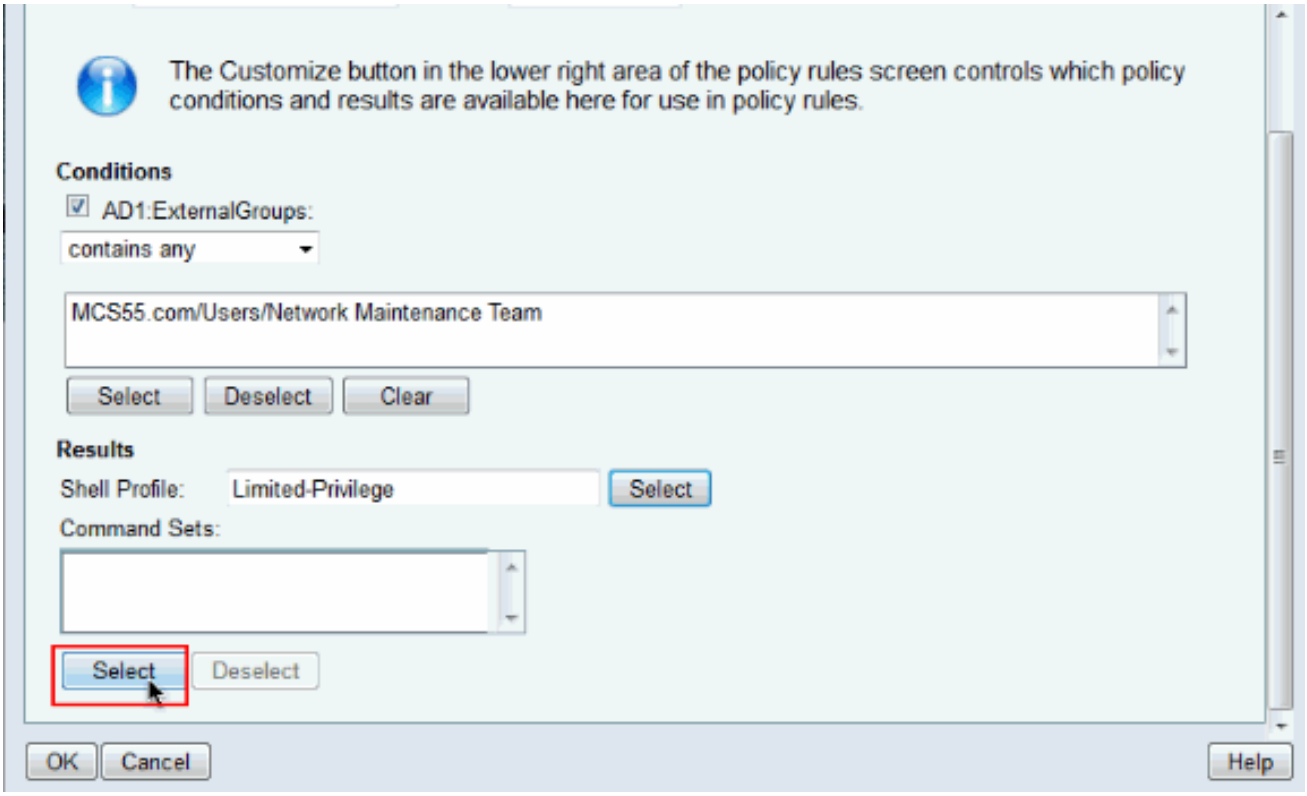

**إرسال**.

32. وانقر فوق

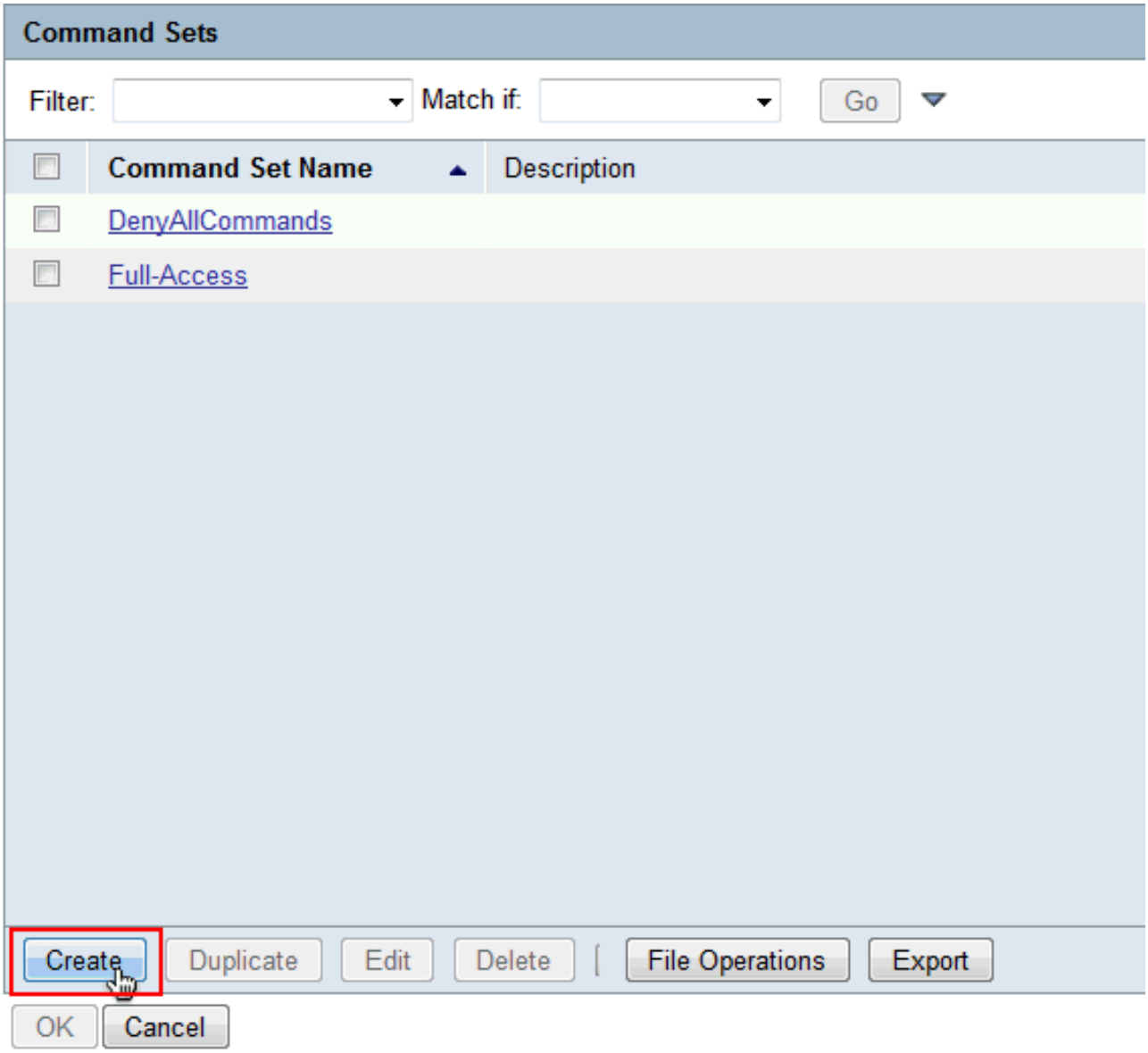



OK.

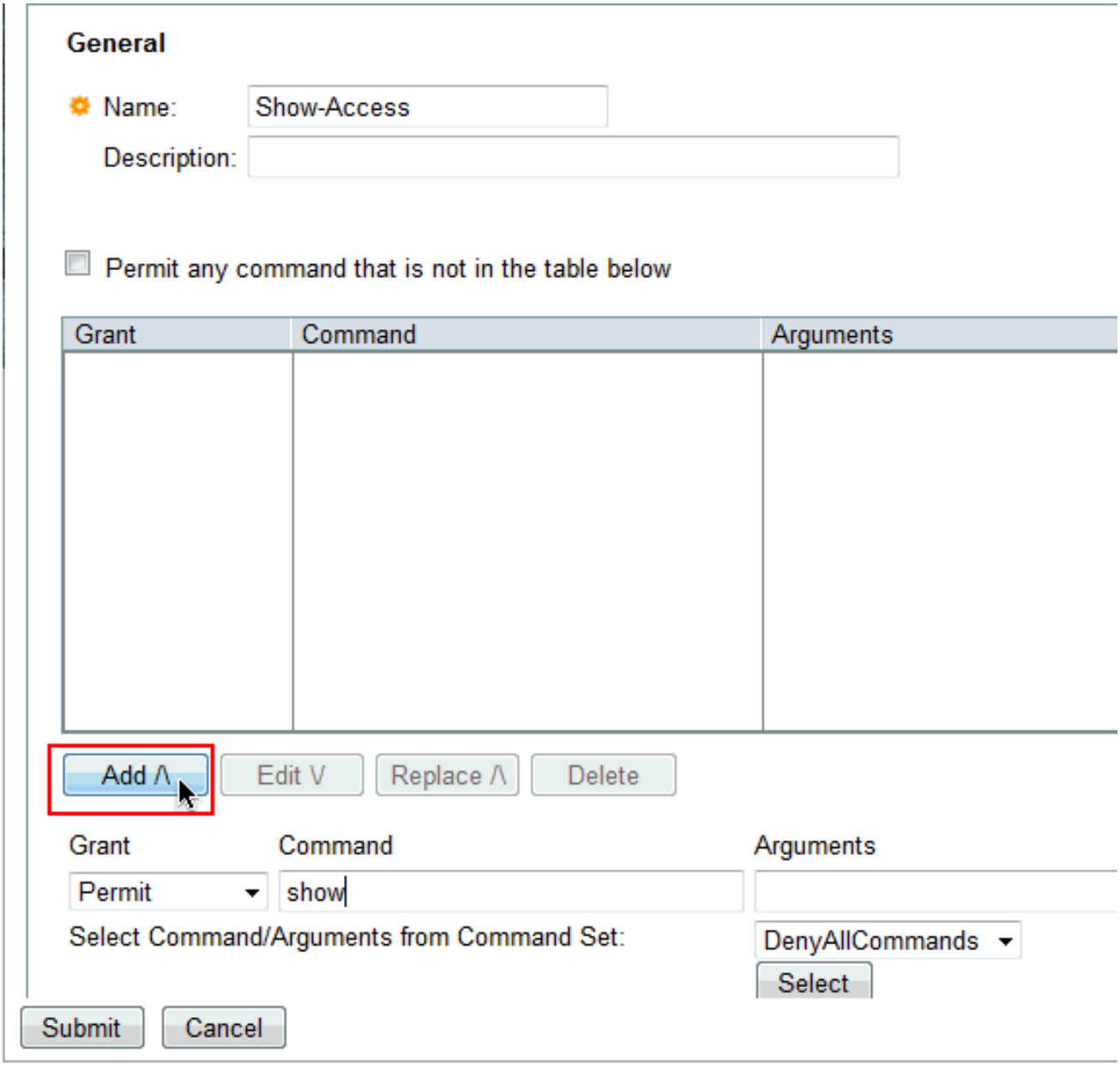
33. انقر **تحديد** في حقل مجموعات الأوامر.



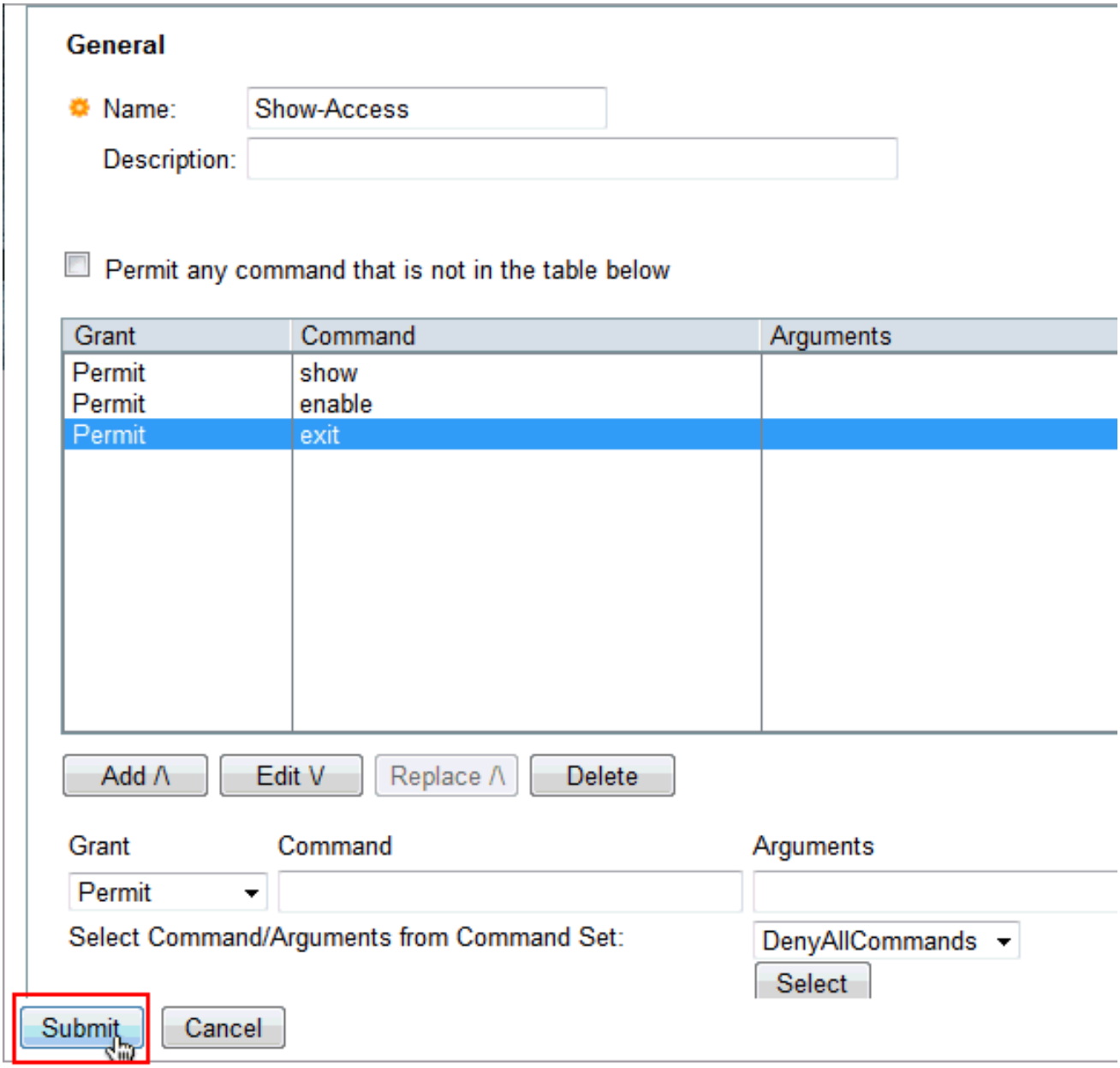

34. انقر فوق **إنشاء** لإنشاء **مجموعة أوامر** جديدة لمجموعة الوصول المحدودة.



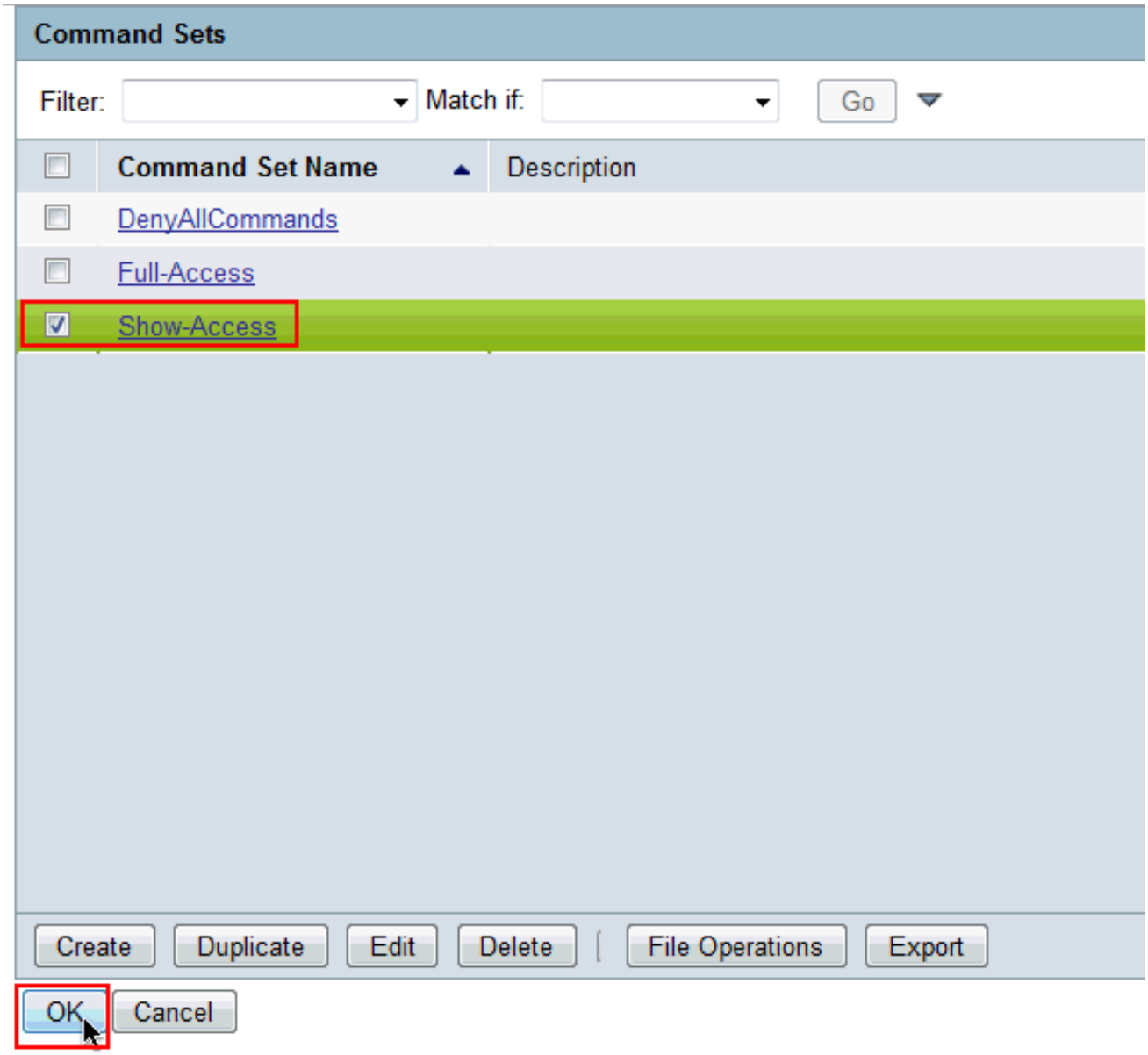

35. قم بتوفير **اسم** وتأكد من عدم تحديد خانة الاختيار المجاورة **للسماح بأي أمر غير موجود في الجدول أدناه**. انقر فوق إضافة بعد كتابة **عرض** في المساحة المتوفرة في قسم **الأوامر** واختر **السماح** في قسم **منح** بحيث يتم السماح فقط لأوامر العرض للمستخدمين في مجموعة الوصول المحدود.



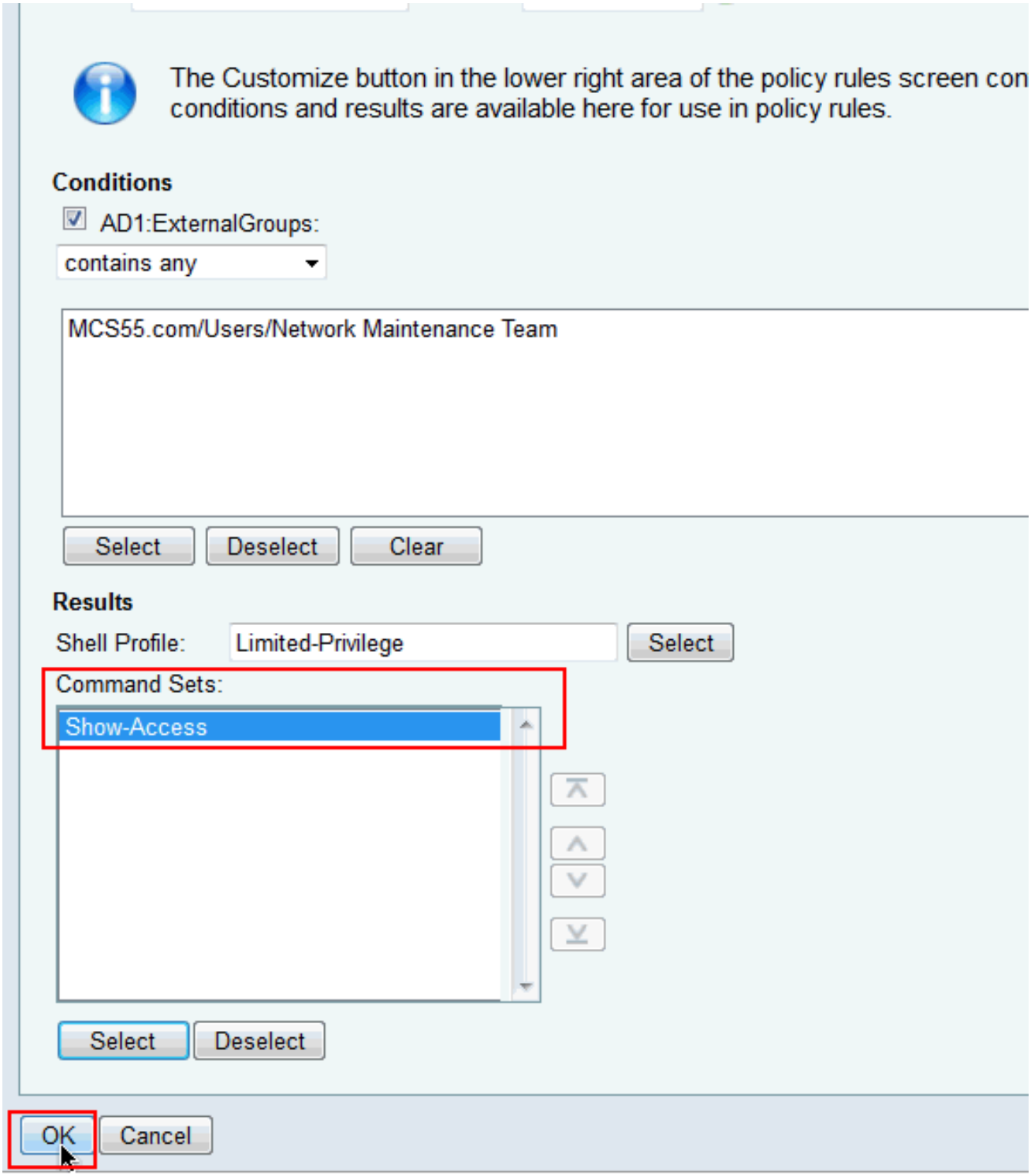

36. وبالمثل قم بإضافة أي أوامر أخرى مسموح بها للمستخدمين في مجموعة الوصول المحدودة باستخدام **Add**.
انقر على **إرسال**.**ملاحظة:** راجع إنشاء مجموعات أوامر ومضاعفة وتحريرها لإدارة الأجهزة للحصول على مزيد من المعلومات حول مجموعات الأوامر.



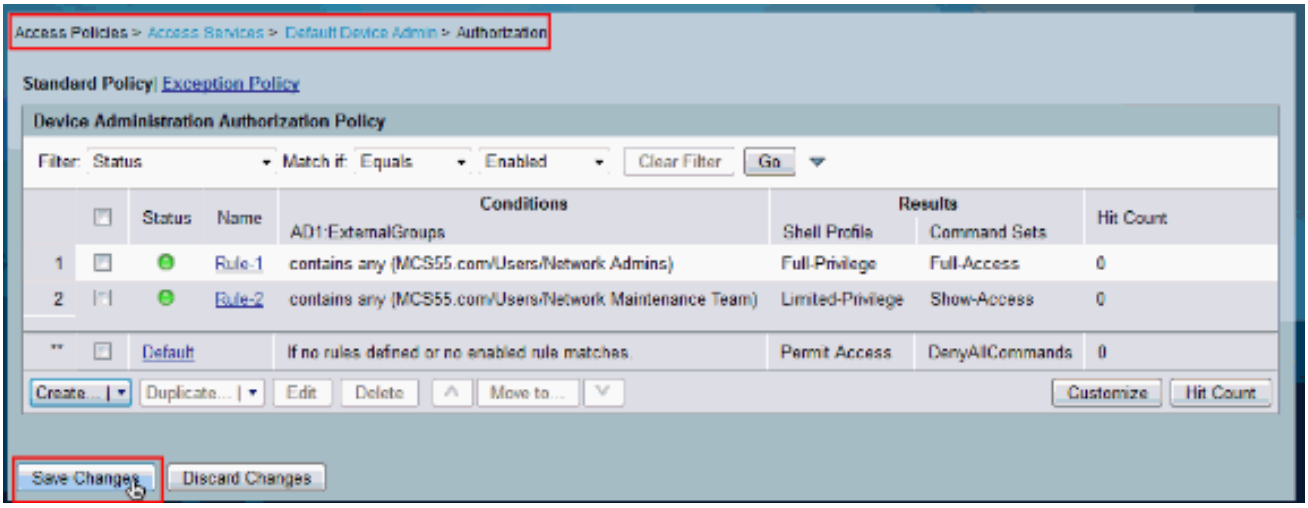

37. وانقر فوق **OK**.



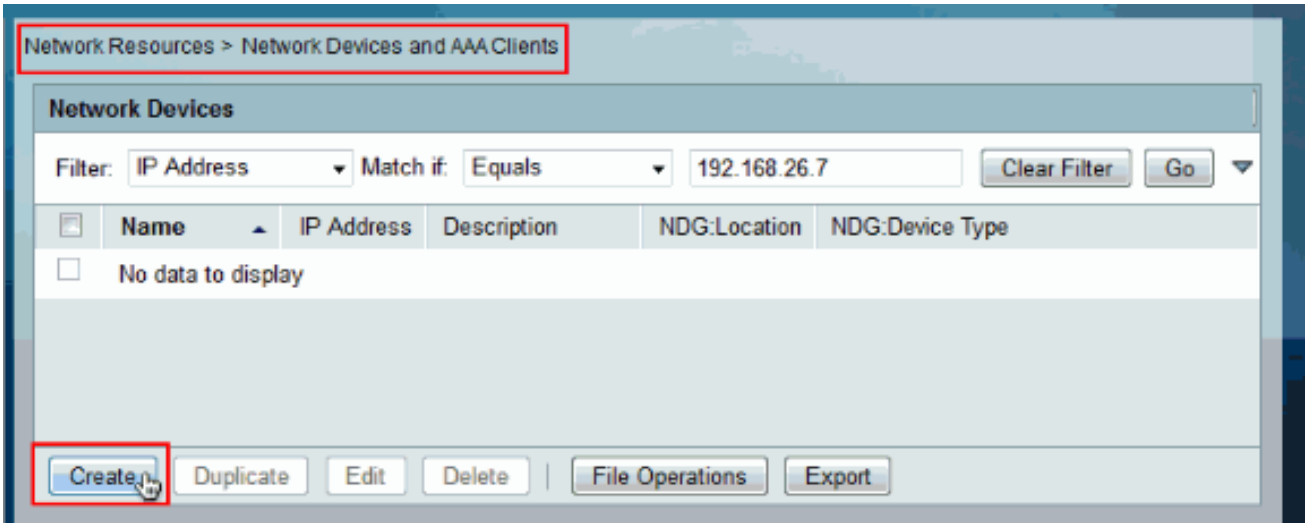

38. وانقر فوق **OK**.



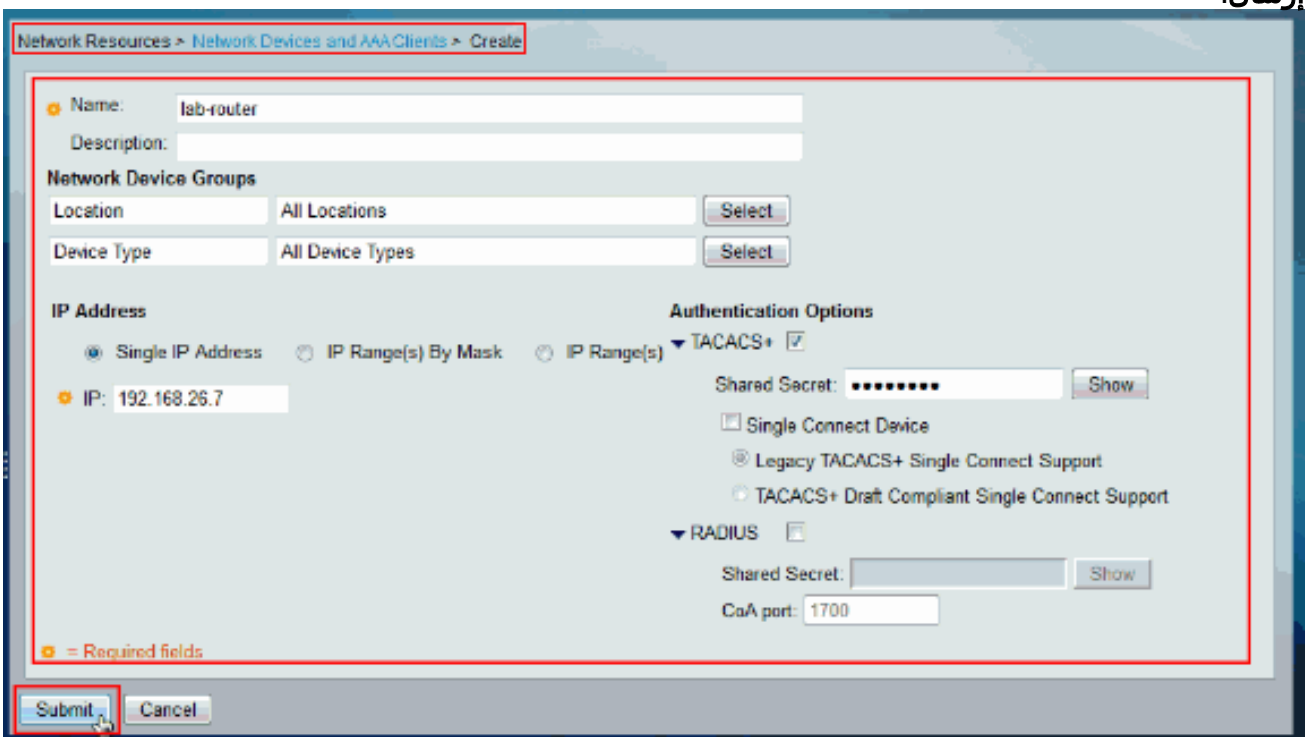

39. انقر فوق **حفظ التغييرات**.




40. انقر فوق **إنشاء** لإضافة جهاز **Cisco IOS** كعميل **AAA** على ACS.




41. قم بتوفير **اسم وعنوان IP وسر مشترك** ل **TACACS+** وانقر فوق **إرسال**.




## تكوين جهاز Cisco IOS للمصادقة والتفويض

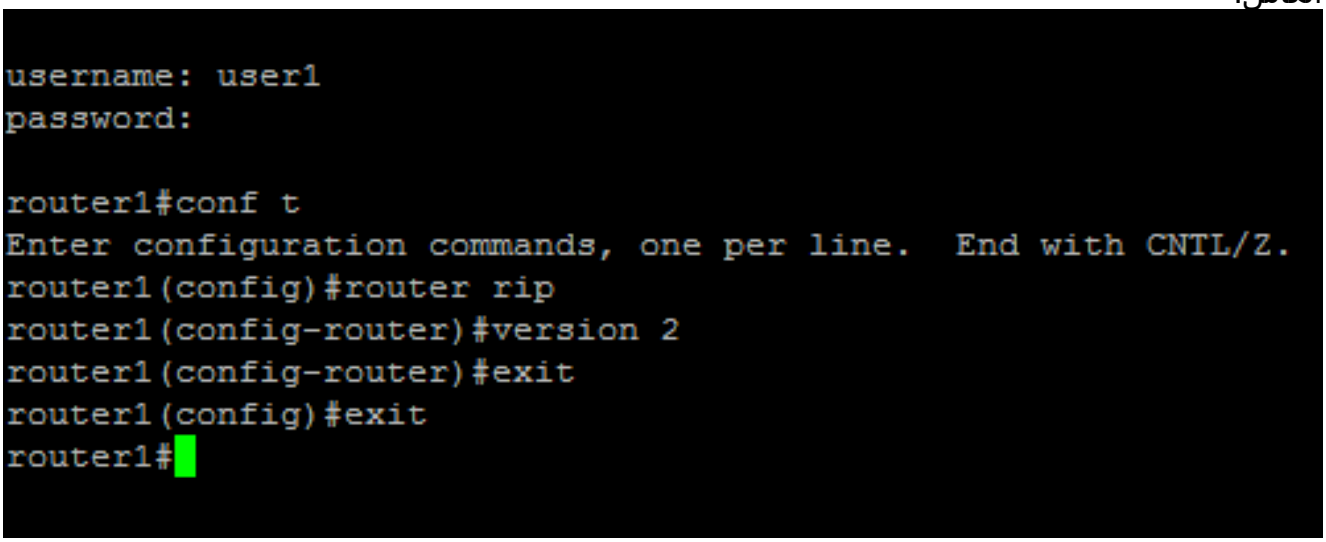
أكمل هذه الخطوات لتكوين جهاز Cisco IOS و ACS للمصادقة والتفويض.

1. قم بإنشاء مستخدم محلي بامتياز كامل للتعيين الاحتياطي باستخدام الأمر **username** كما هو موضح هنا:
```
!username admin privilege 15 password 0 cisco123
```
2. قم بتوفير عنوان IP الخاص ب ACS لتمكين AAA وإضافة ACS 5.x كخادم TACACS.
```
aaa new-model
tacacs-server host 192.168.26.51 key cisco123
```
**ملاحظة:** يجب أن يتطابق المفتاح مع السر المشترك المتوفر على ACS لجهاز Cisco IOS هذا.
3. اختبر إمكانية الوصول إلى خادم TACACS باستخدام أمر إختبار AAA كما هو موضح.
```
test aaa group tacacs+ user1 xxxxx legacy
+Attempting authentication test to server-group tacacs+ using tacacs
.User was successfully authenticated
```
**ملاحظة:** يوضح إخراج الأمر السابق أن خادم TACACS يمكن الوصول إليه وقد تمت مصادقة المستخدم بنجاح. ينتمي كل من User1 وكلمة المرور xxx إلى AD. في حالة فشل الاختبار، يرجى التأكد من أن السر المشترك المتوفر في الخطوة السابقة صحيح.
4. قم بتكوين تسجيل الدخول وتمكين المصادقة ثم أستخدم EXEC وترخيصات الأوامر كما هو موضح هنا:
```
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
```
**ملاحظة:** يتم إستخدام الكلمات الأساسية المحلية والتمكين لرجوع إلى المستخدم المحلي لبرنامج Cisco IOS والتمكين السري على التوالي إذا كان خادم TACACS يتعذر الوصول إليه.

## التحقق من الصحة

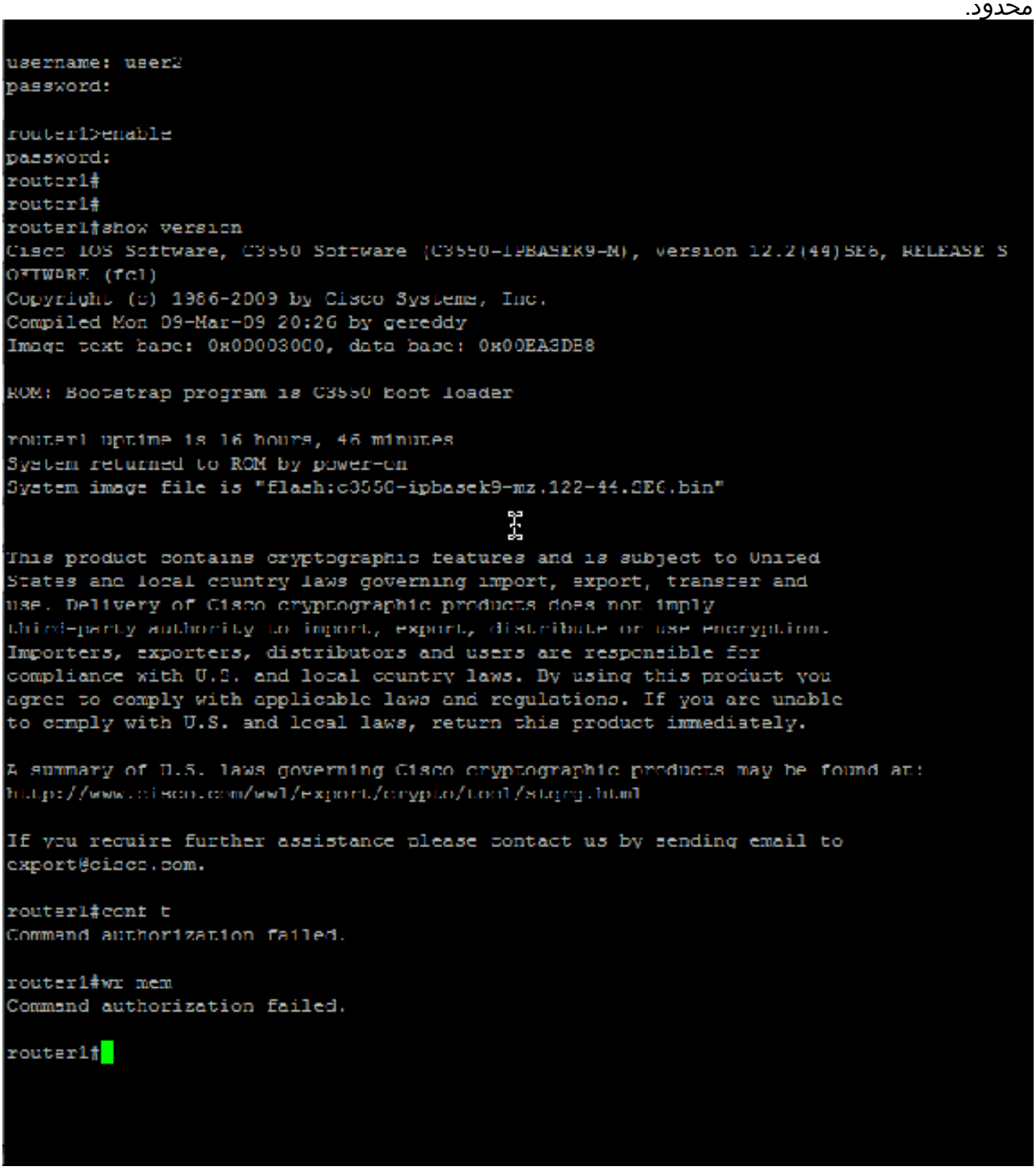
للتحقق من تسجيل دخول المصادقة والتفويض إلى جهاز Cisco IOS من خلال برنامج Telnet.

1. Telnet إلى جهاز Cisco IOS كمستخدم1 الذي ينتمي إلى مجموعة الوصول الكامل في AD. مجموعة مسؤولي الشبكة هي المجموعة الموجودة في AD والتي تم تعيينها إلى ملف تعريف Full-Privilege Shell ومجموعة الأمر full-access التي تم تعيينها على ACS. حاول تشغيل أي أمر لضمان حصولك على الوصول الكامل.

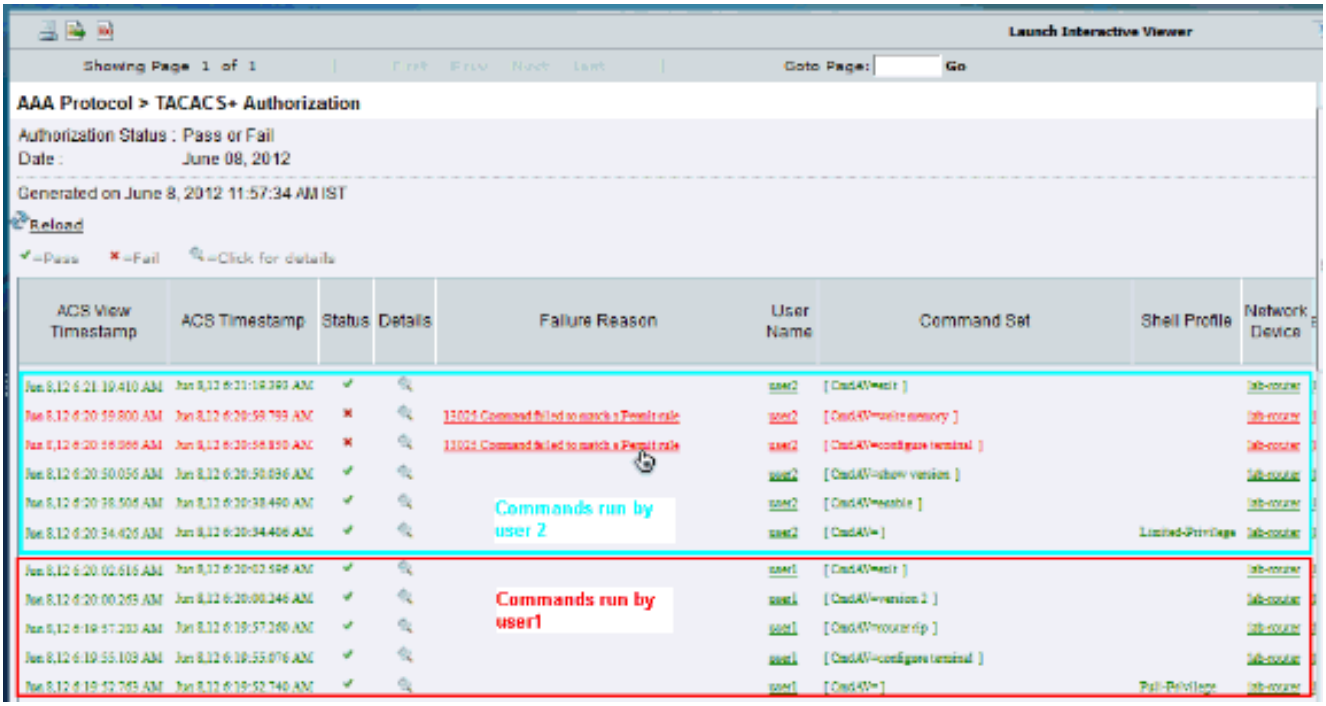



2. Telnet إلى جهاز Cisco IOS ك user2 الذي ينتمي إلى مجموعة الوصول المحدود في AD. (مجموعة **فريق صيانة الشبكة** هي المجموعة في AD التي يتم تعيينها على **ملف تعريف Shell المحدود** و**مجموعة الأمر show-access** على ACS). إذا حاولت تشغيل أي أمر بخلاف الأوامر المذكورة في مجموعة الأوامر show-access، فيجب أن تحصل على خطأ والذي يظهر أن المستخدم2 لديه وصول

محدود.




3. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل ACS وابدأ **برنامج** Monitoring and Reporting Viewer. أختر **بروتوكول** AAA > TACACS+Authorization للتحقق من الأنشطة التي تم تنفيذها بواسطة المستخدم1 و user2.




## معلومات ذات صلة

- نظام التحكم في الوصول الآمن من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).