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

المحتويات

المقدمة

يقدم هذا المستند المثال الالتكوين مصادقة TACACS+ وتفويض الأوامر استنادا إلى عضوية مجموعة AD لمستخدم باستخدام نظام التحكم في الوصول الآمن (ACS) من Cisco الإصدار 5.x 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 المُستخدمة 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

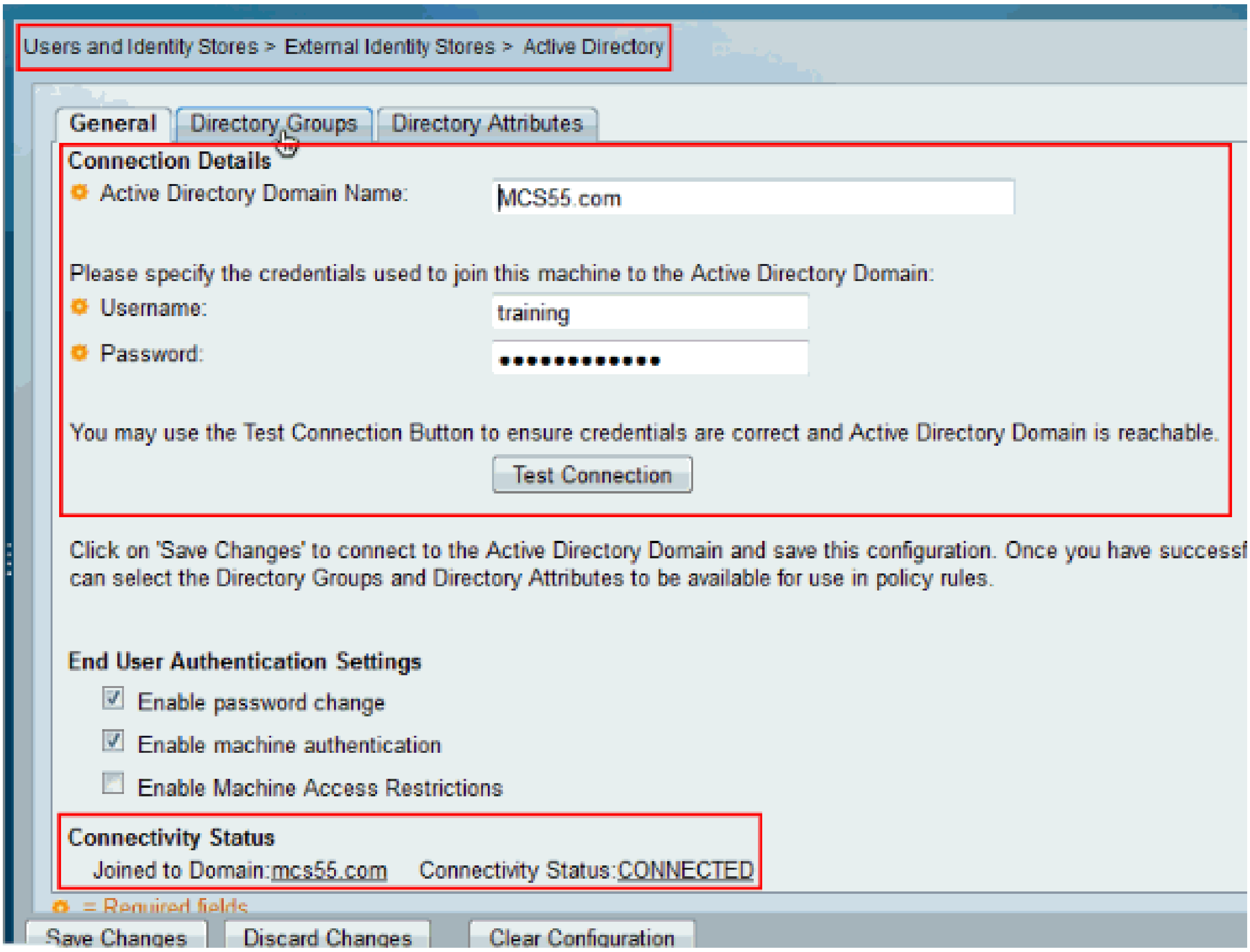
قبل البدء في تكوين ACS 5.x للمصادقة والتفويض، كان يجب دمج ACS بنجاح مع Microsoft AD. إذا لم يتم دمج ACS مع مجال AD المرغوب، ارجع إلى ACS 5.x والإصدارات الأحدث: التكامل مع مثال تكوين Microsoft Active Directory للحصول على مزيد من المعلومات لتنفيذ مهمة التكامل.

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".


Users and Identity Stores > External Identity Stores > Active Directory

Connection Details

Active Directory Domain Name: MCS55.com

Please specify the credentials used to join this machine to the Active Directory Domain:

Username: training

Password: ●●●●●●●●●●●●●

You may use the Test Connection Button to ensure credentials are correct and Active Directory Domain is reachable.

Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have successf
can select the Directory Groups and Directory Attributes to be available for use in policy rules.

End User Authentication Settings

☑ Enable password change

☑ Enable machine authentication

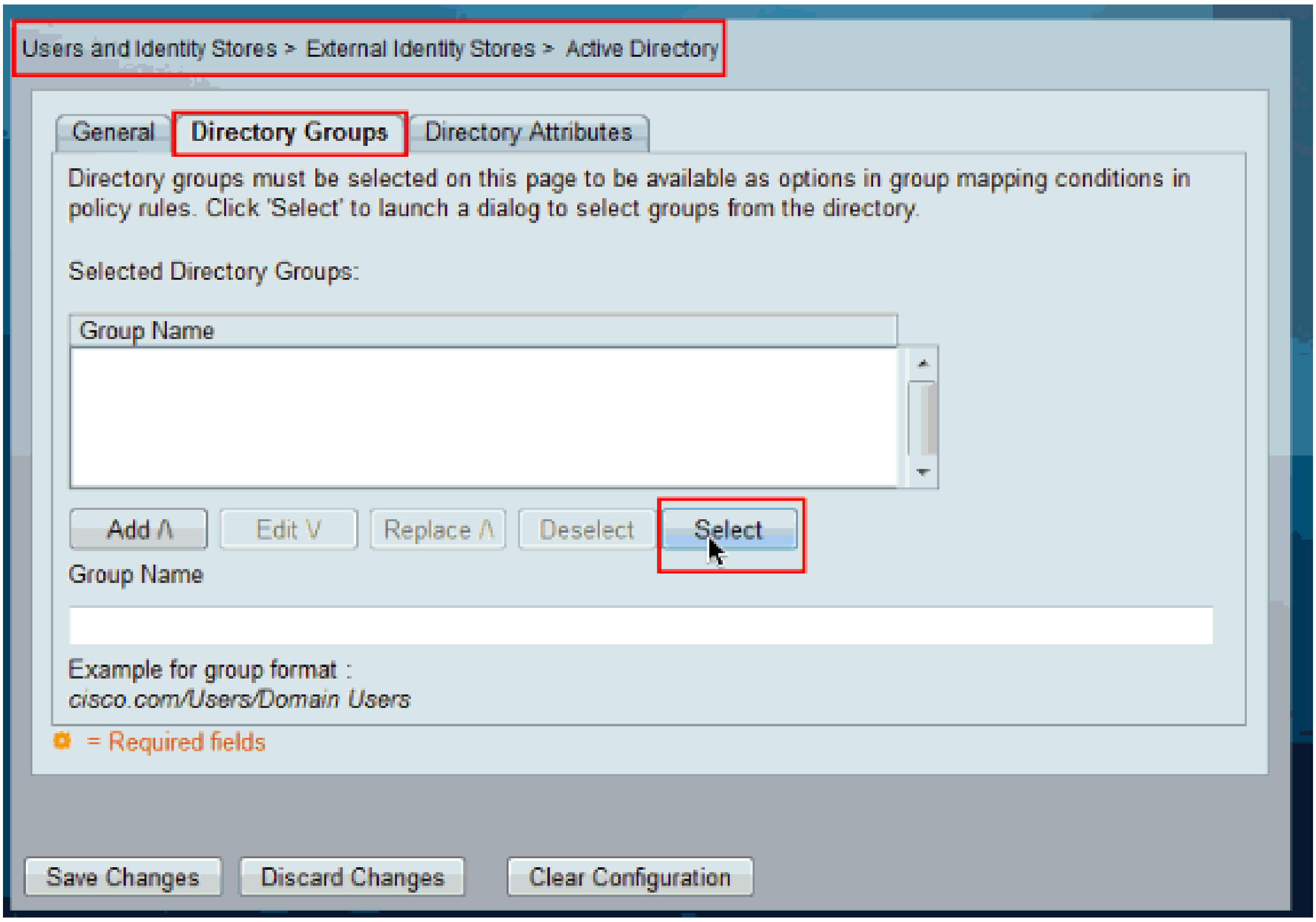
☐ Enable Machine Access Restrictions

Connectivity Status

Joined to Domain: mcs55.com   Connectivity Status: CONNECTED

= Required fields

3. انقر فوق تحديد.



Users and Identity Stores > External Identity Stores > Active Directory

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:

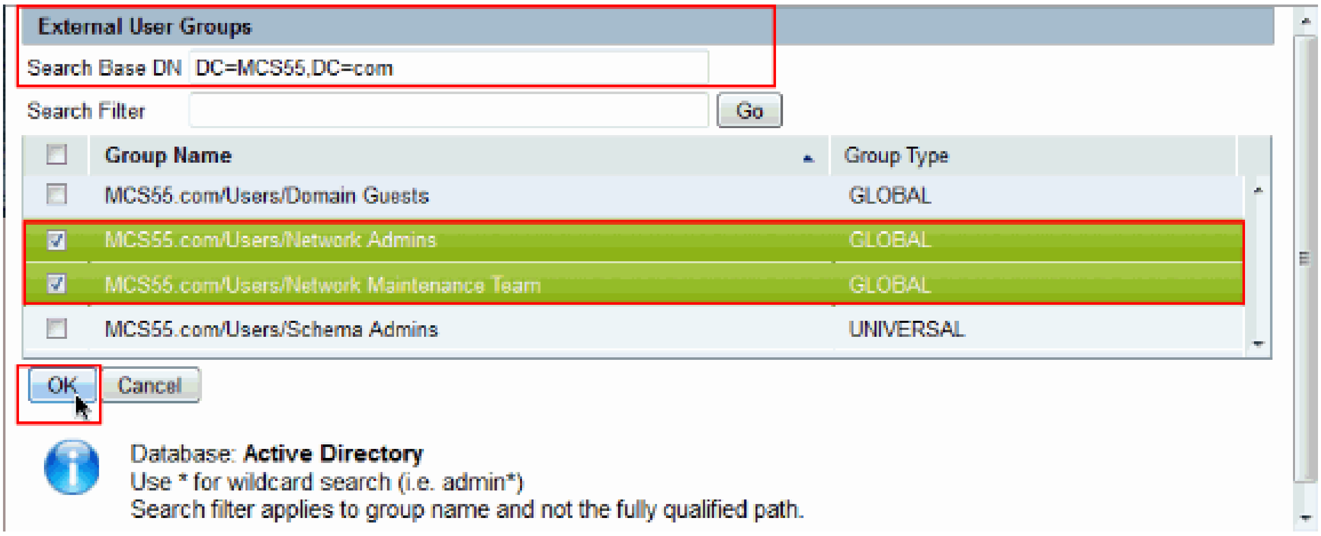
Group Name

Group Name

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

= Required fields

أختر المجموعات التي تحتاج أن تكون معينة إلى ملفات تخصيص Shell ومجموعات الأوامر4.
في الجزء الأحدث من التكوين. وانقر فوق OK.



External User Groups

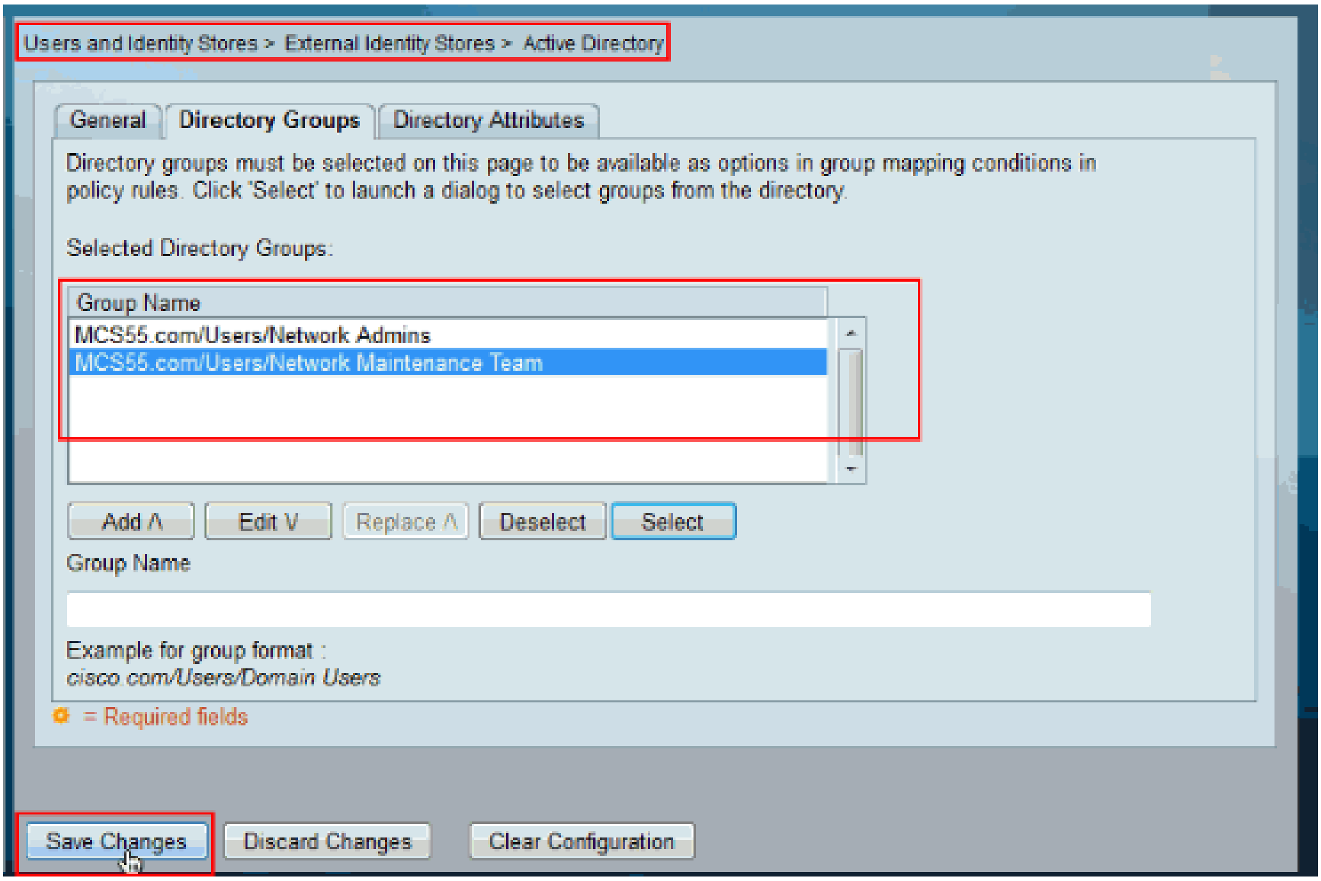
Search Base DN DC=MCS55,DC=com

Search Filter

□	Group Name	Group Type
□	MCS55.com/Users/Domain Guests	GLOBAL
☑	MCS55.com/Users/Network Admins	GLOBAL
☑	MCS55.com/Users/Network Maintenance Team	GLOBAL
□	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.

انقر فوق حفظ التغييرات.5.



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:

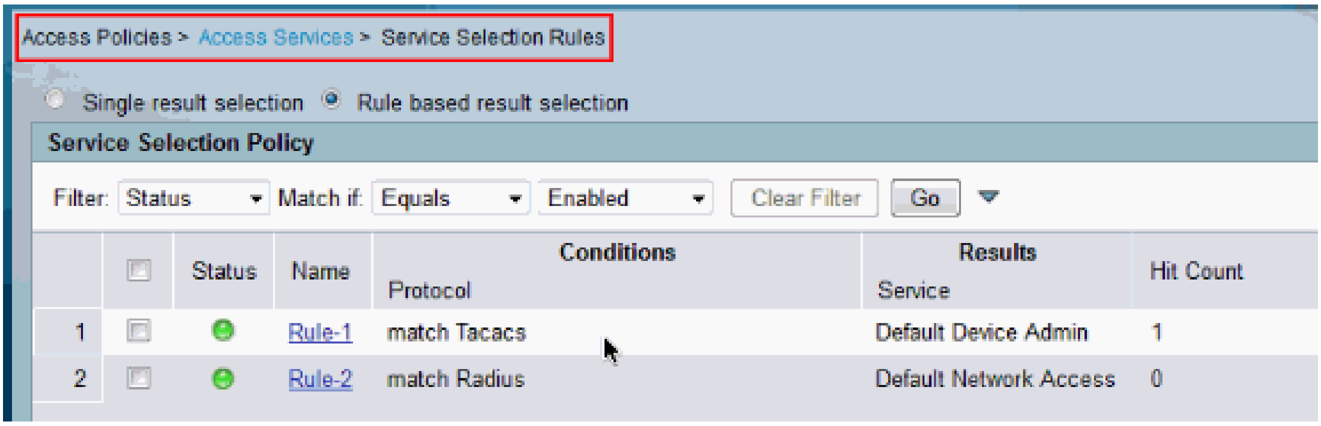
Group Name
MCS55.com/Users/Network Admins
MCS55.com/Users/Network Maintenance Team

Group Name

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

= Required fields

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



Access Policies > Access Services > Service Selection Rules

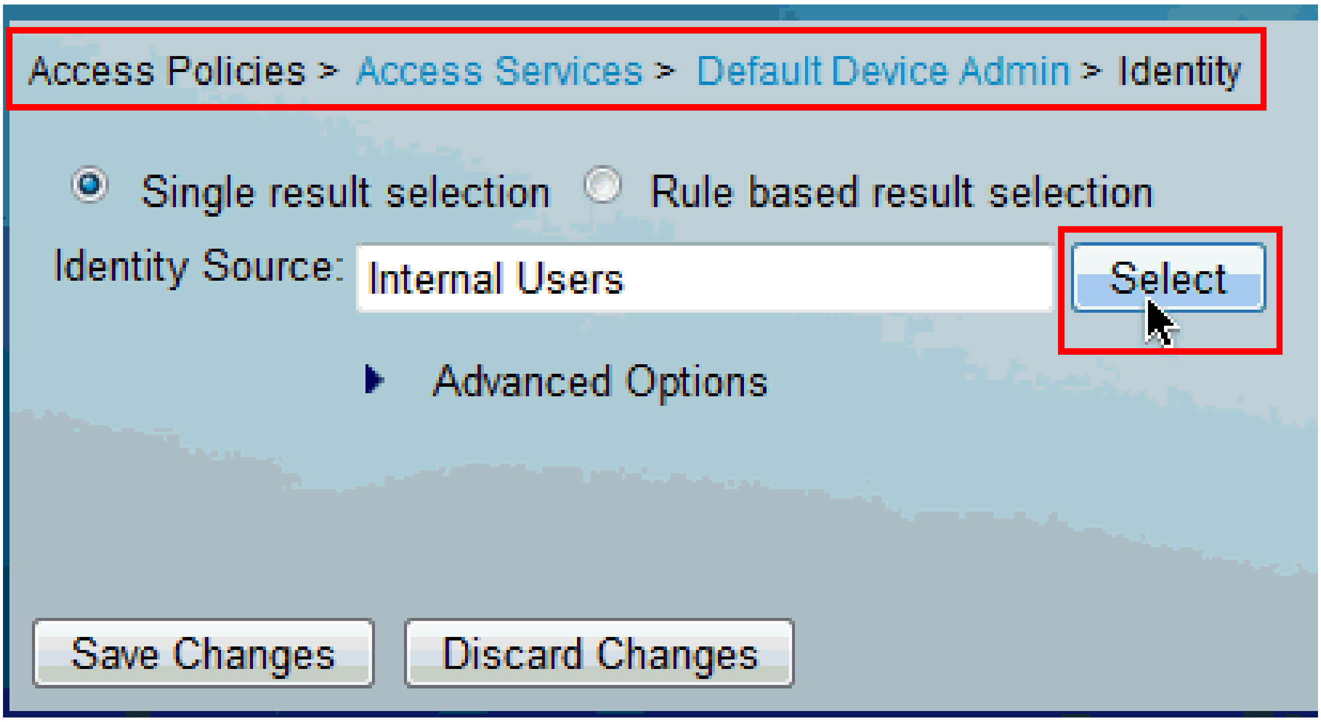
○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status ▾ Match if: Equals ▾ Enabled ▾ Clear Filter Go ▾

				Conditions	Results	
	☐	Status	Name	Protocol	Service	Hit Count
1	☐	●	Rule-1	match Tacacs	Default Device Admin	1
2	☐	●	Rule-2	match Radius	Default Network Access	0

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

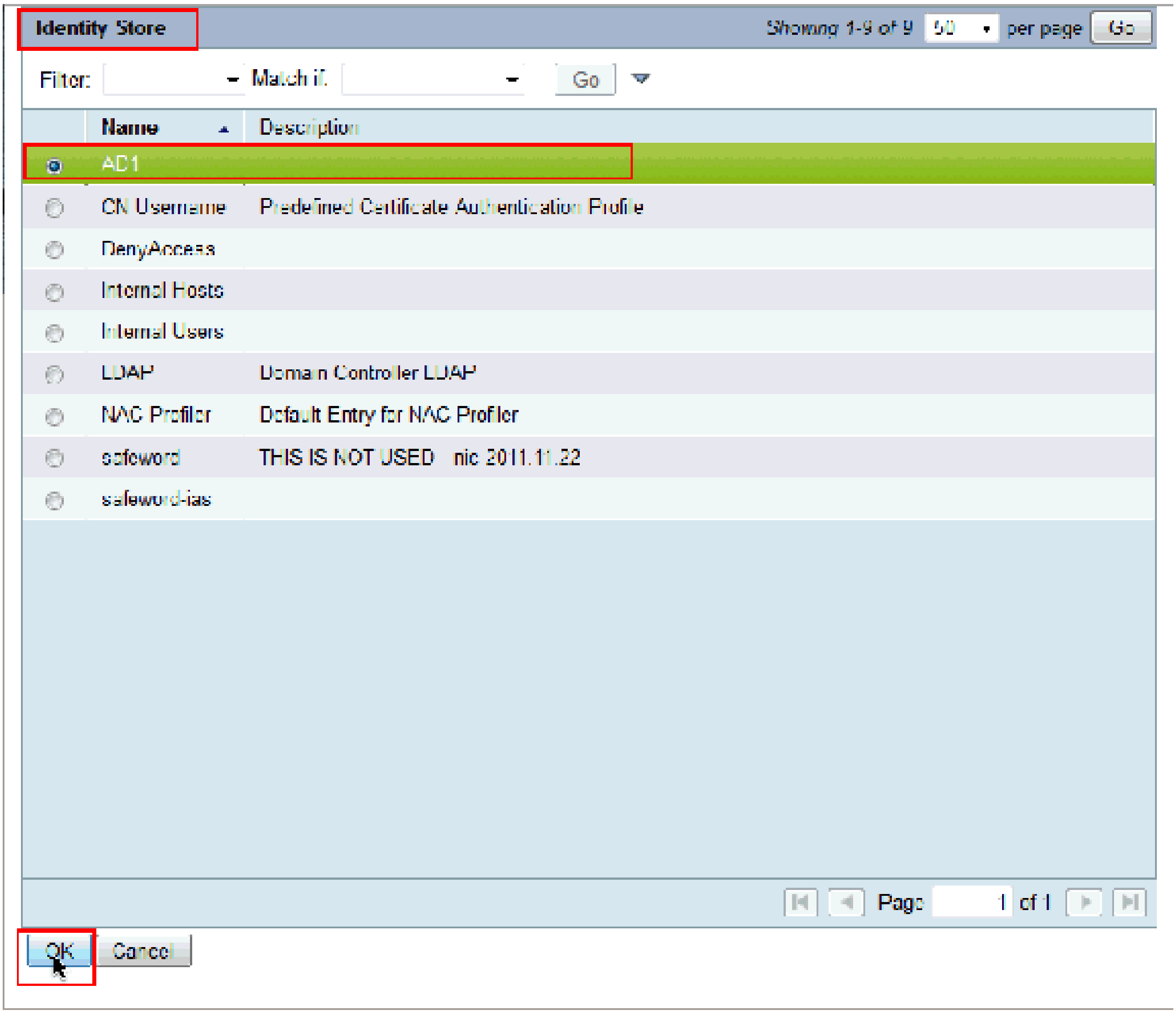


Access Policies > Access Services > Default Device Admin > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Users

8. أخترت AD1 وطقطقة ok.



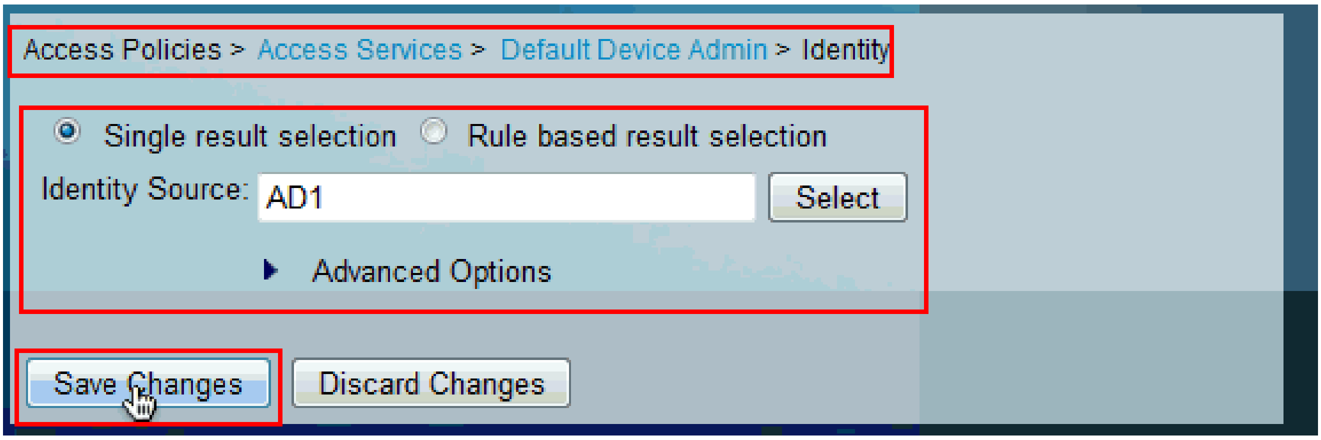
Identity Store

Showing 1-9 of 9 50 per page

	Name ▲	Description
●	AD1	
○	CN Username	Predefined Certificate Authentication Profile
○	DenyAccess	
○	Internal Hosts	
○	Internal Users	
○	LDAP	Domain Controller LDAP
○	NAC Profiler	Default Entry for NAC Profiler
○	safeword	THIS IS NOT USED nic 2011.11.22
○	safeword-ias	

Page 1 of 1

انقر فوق حفظ التغييرات.9.

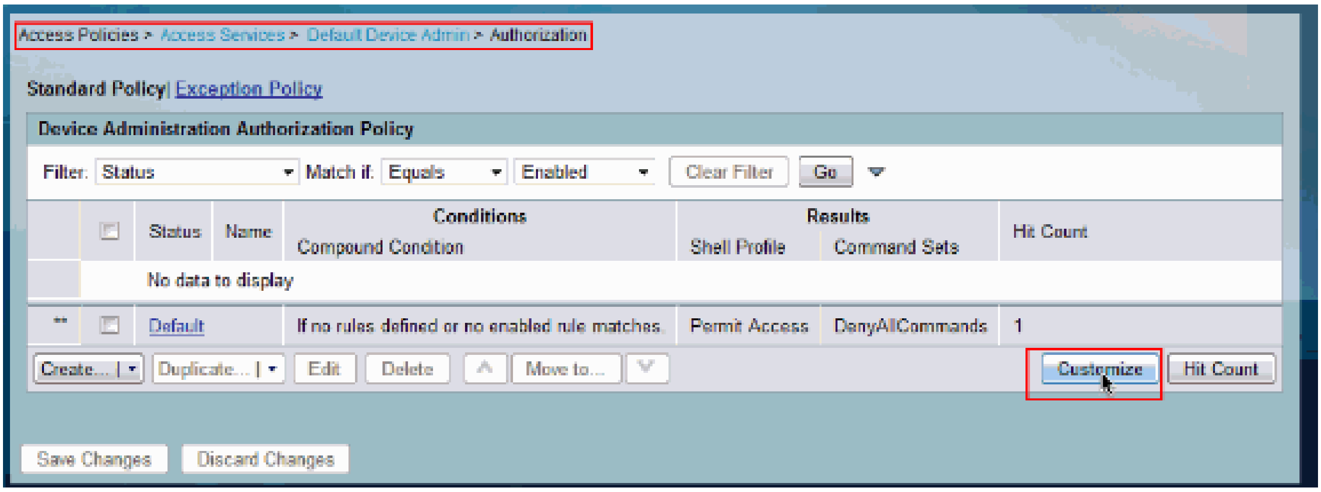


Access Policies > Access Services > Default Device Admin > Identity

● Single result selection ○ Rule based result selection

Identity Source: AD1 Select

أختر سياسات الوصول > خدمات الوصول > إدارة الجهاز الافتراضية > التفويض وانقر10. فوق تخصيص.



Access Policies > Access Services > Default Device Admin > Authorization

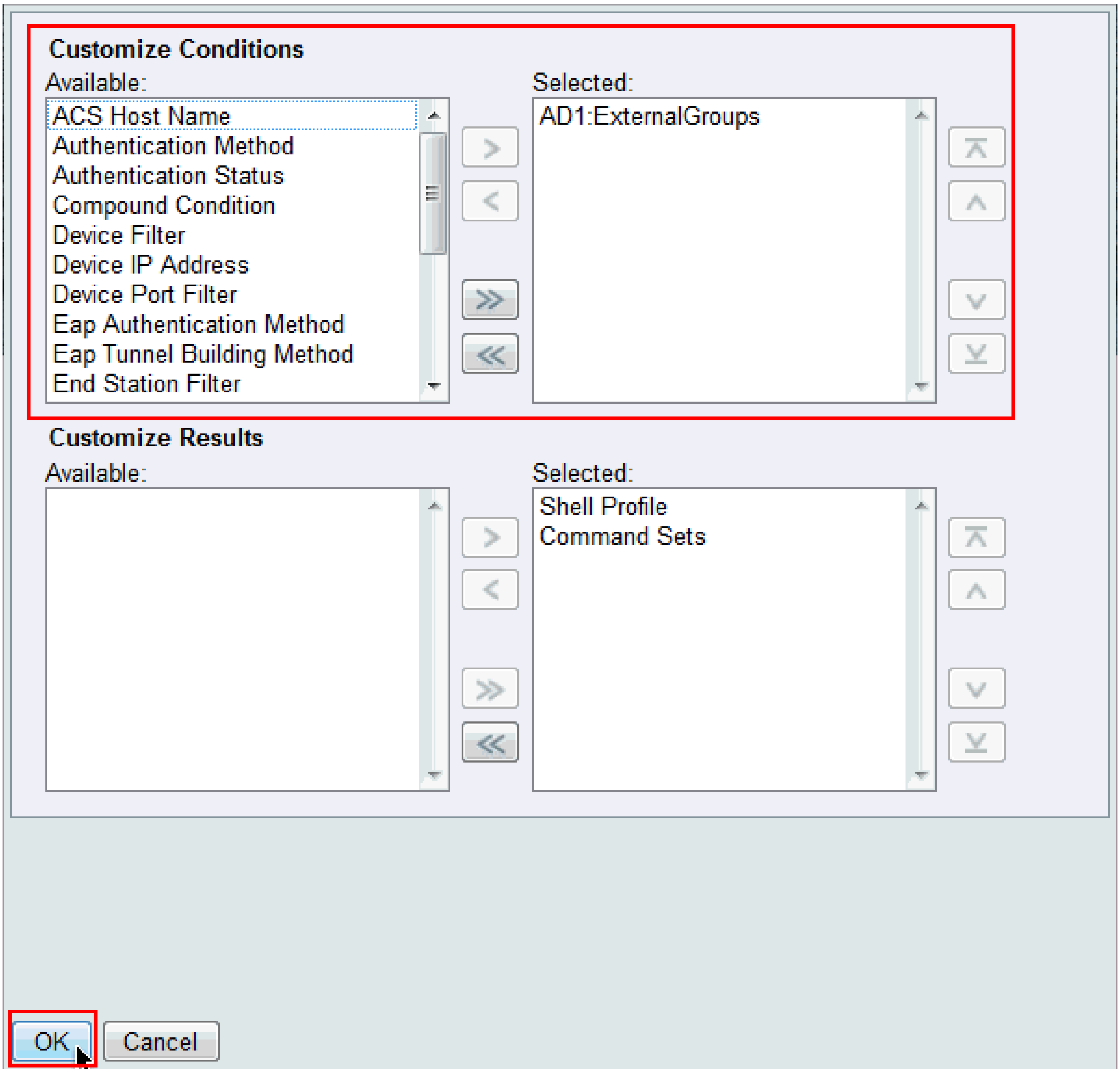
Standard Policy | Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled

	□	Status	Name	Conditions Compound Condition	Results Shell Profile	 Command Sets	Hit Count
		No data to display					
**	□		Default	If no rules defined or no enabled rule matches.	Permit Access	DenyAllCommands	1

انسخ AD1:ExternalGroups من متاح إلى قسم محدد من شروط التخصيص ثم نقل ملف11. تعريف Shell ومجموعات الأوامر من متاح إلى قسم تخصيص النتائج. وانقر الآن فوق OK.


Customize Conditions

Available:

ACS Host Name
Authentication Method
Authentication Status
Compound Condition
Device Filter
Device IP Address
Device Port Filter
Eap Authentication Method
Eap Tunnel Building Method
End Station Filter

Selected:

AD1:ExternalGroups

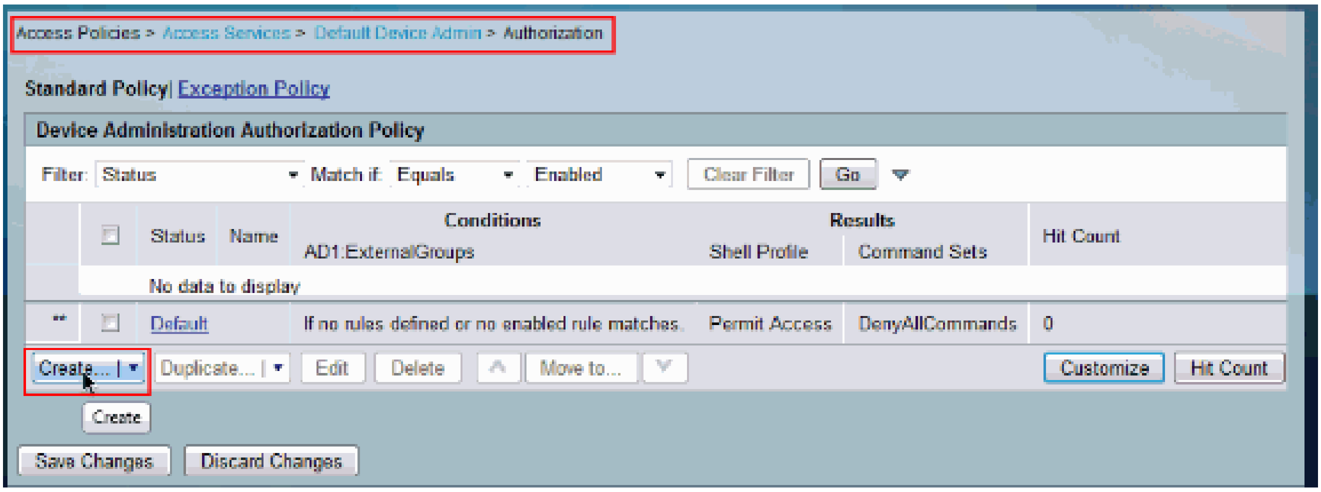
Customize Results

Available:

Selected:

Shell Profile
Command Sets

انقر فوق إنشاء لإنشاء قاعدة جديدة.12.


Access Policies > Access Services > Default Device Admin > Authorization

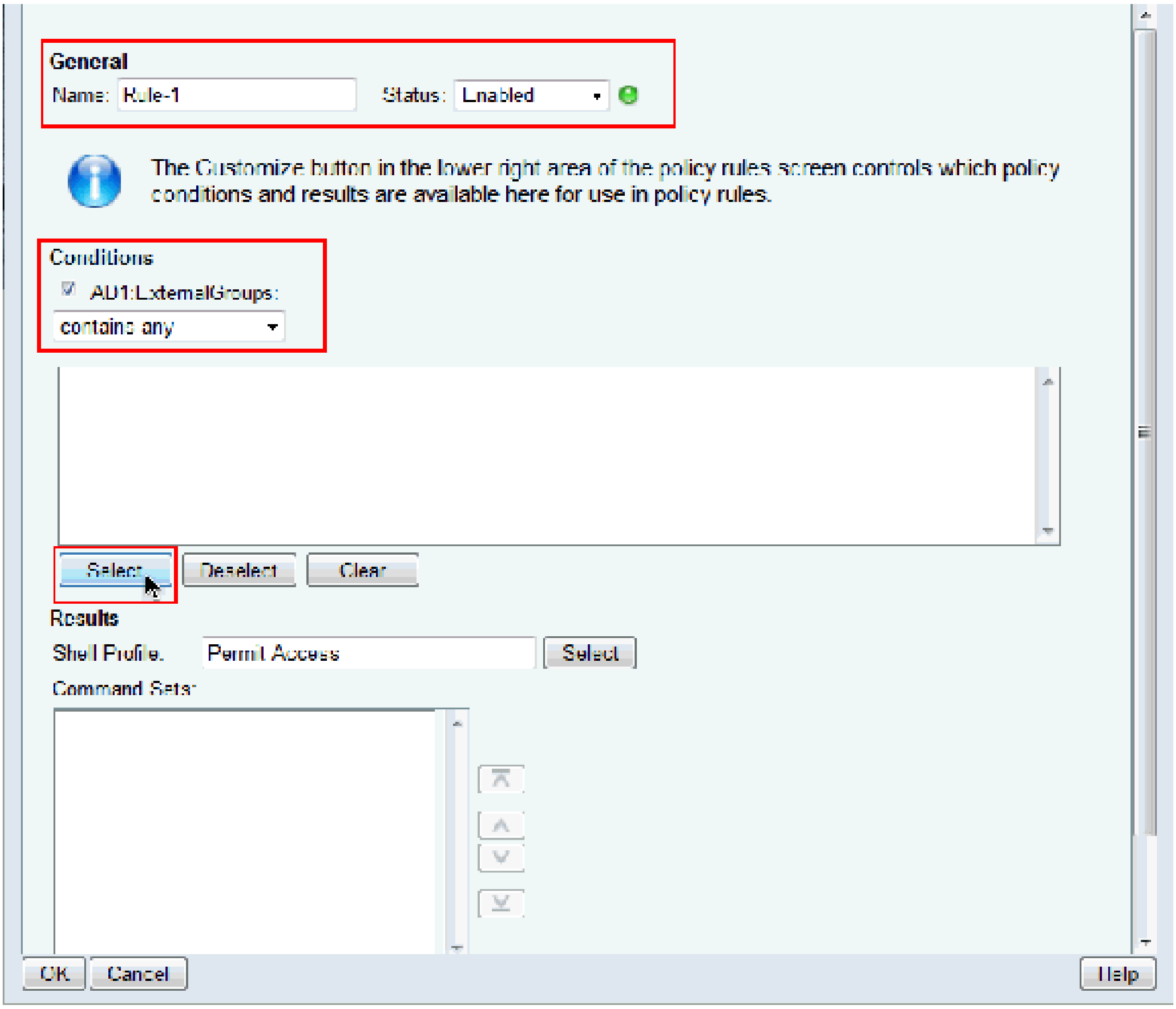
Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status ▾ Match if: Equals ▾ Enabled ▾ Clear Filter Go ▾

				Conditions	Results		
	☐	Status	Name	AD1:ExternalGroups	Shell Profile	Command Sets	Hit Count
		No data to display					
**	☐	Default		If no rules defined or no enabled rule matches.	Permit Access	DenyAllCommands	0

انقر على تحديد في حالة AD1:ExternalGroups.13.



General

Name: Rule-1 Status: Enabled ●

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

Conditions

☑ AD1:ExternalGroups:

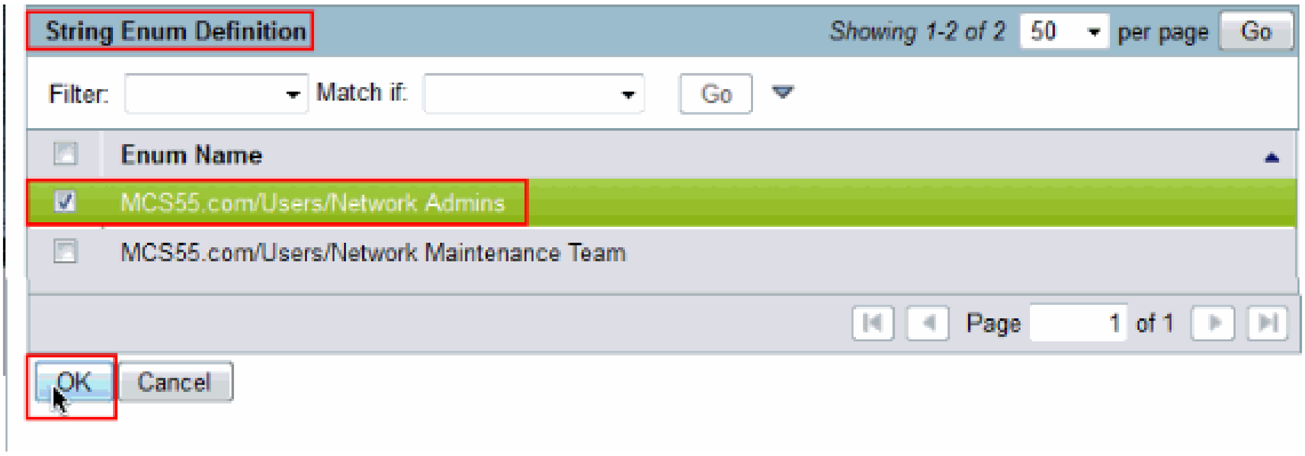
contains any

Results

Shell Profile: Permit Access

Command Sets:

أختر المجموعة التي تريد توفير الوصول الكامل عليها على جهاز Cisco IOS. وانقر فوق14.
OK.



String Enum Definition

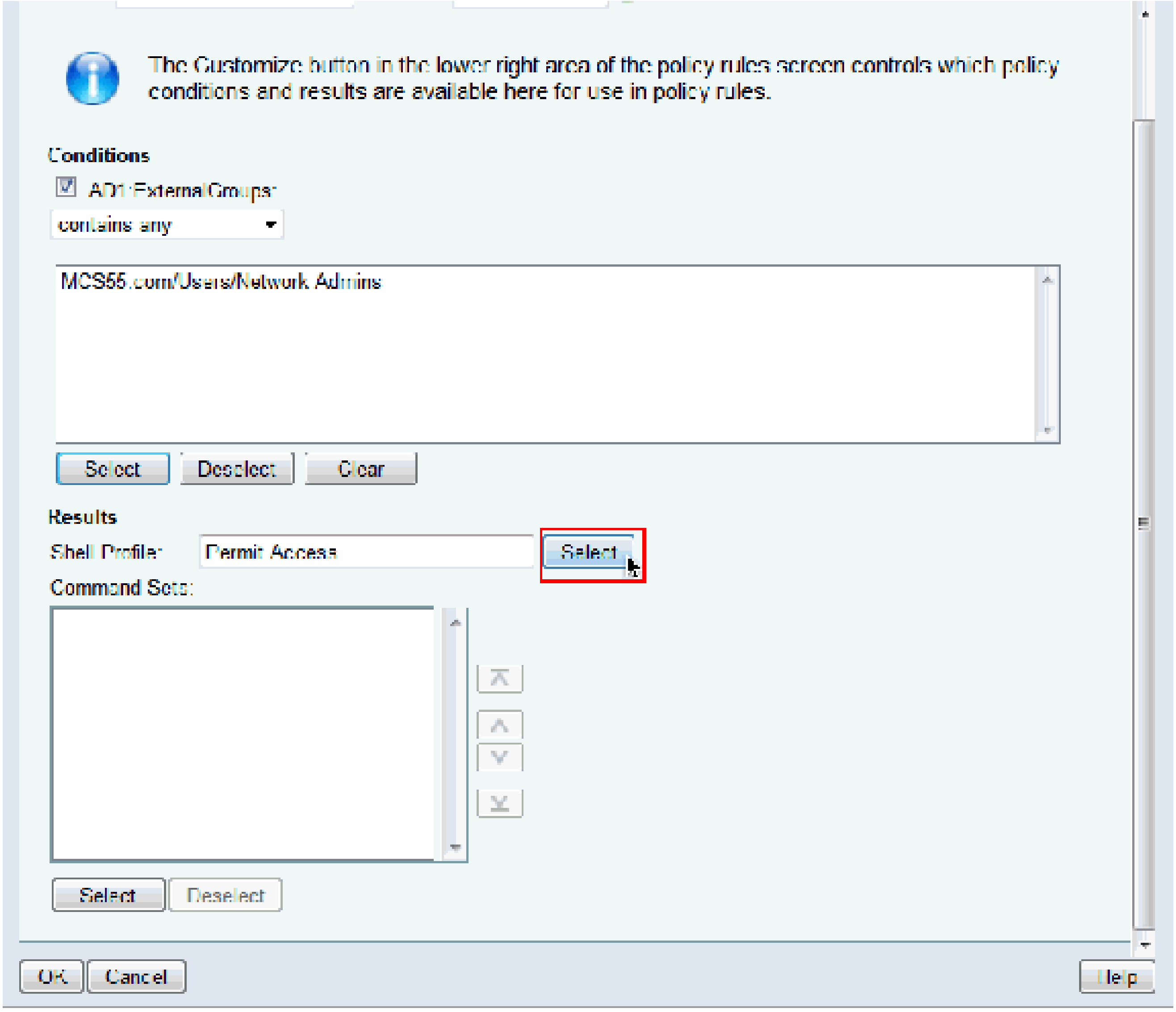
Showing 1-2 of 2 50 per page

Filter: Match if:

□	Enum Name
☑	MCS55.com/Users/Network Admins
□	MCS55.com/Users/Network Maintenance Team

Page 1 of 1

انقر على تحديد في حقل ملف تعريف Shell.15.


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

Conditions

☑ AD1:ExternalGroups:

contains any

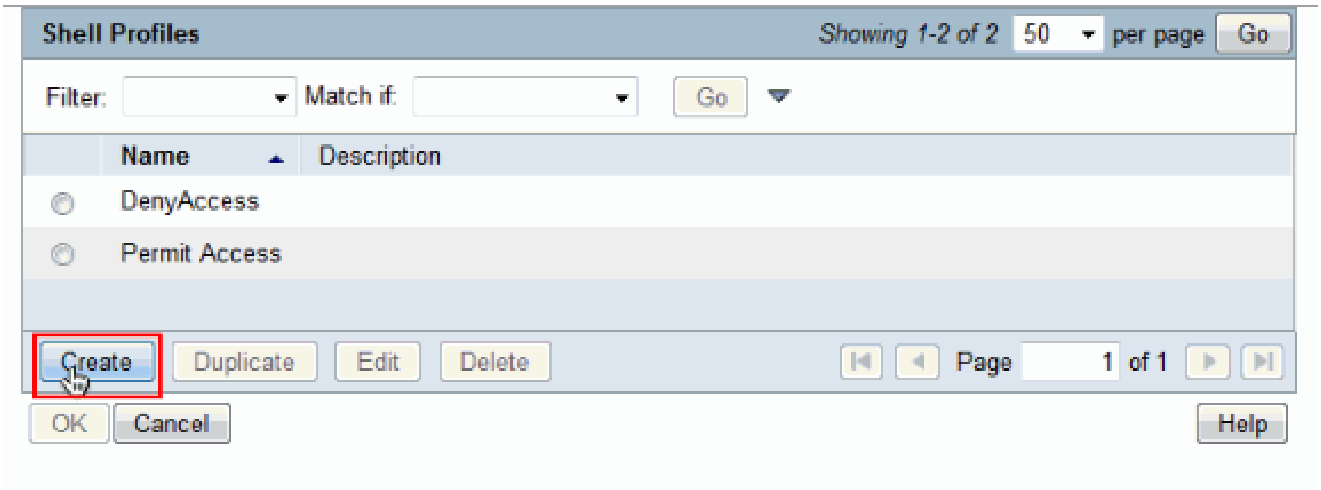
MCS55.com/Users/Network Admins

Results

Shell Profile: Permit Access

Command Sets:

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


Shell Profiles

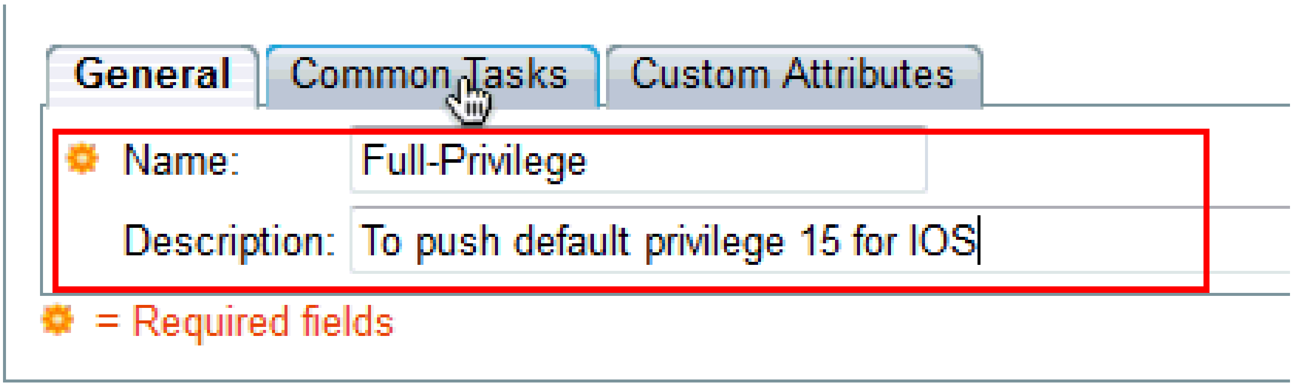
Showing 1-2 of 2 50 per page

Filter: Match if:

	Name ▲	Description
○	DenyAccess	
○	Permit Access	

Page 1 of 1

قم بتوفير اسم ووصف (إختياري) في علامة التبويب "عام" وانقر فوق علامة17.
التبويب مهام عامة.

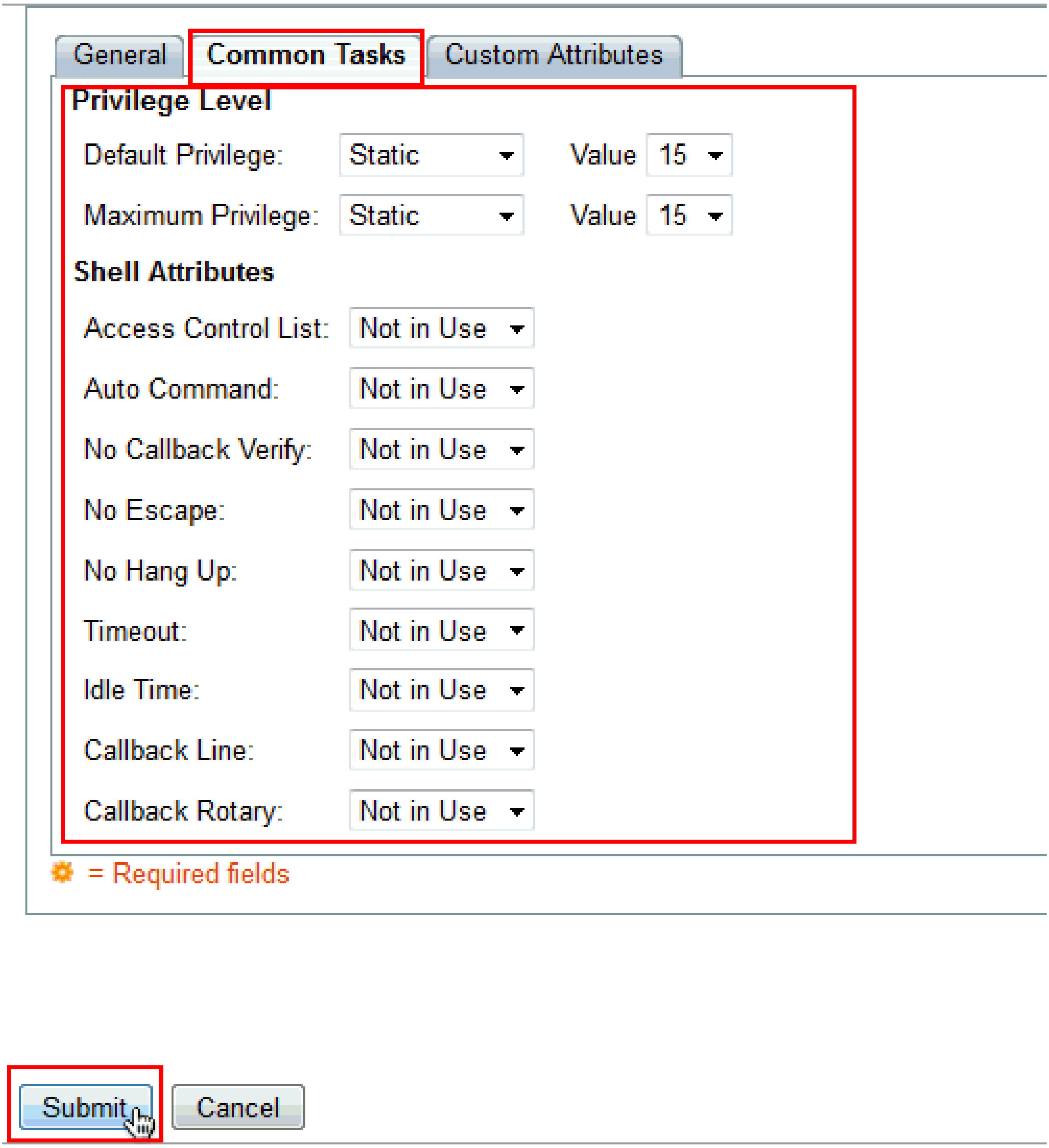


Name: Full-Privilege

Description: To push default privilege 15 for IOS

= Required fields

غيرت التقصير امتياز والحد الأقصى امتياز إلى ساكن إستاتيكي مع القيمة 15.18.
انقر على إرسال.



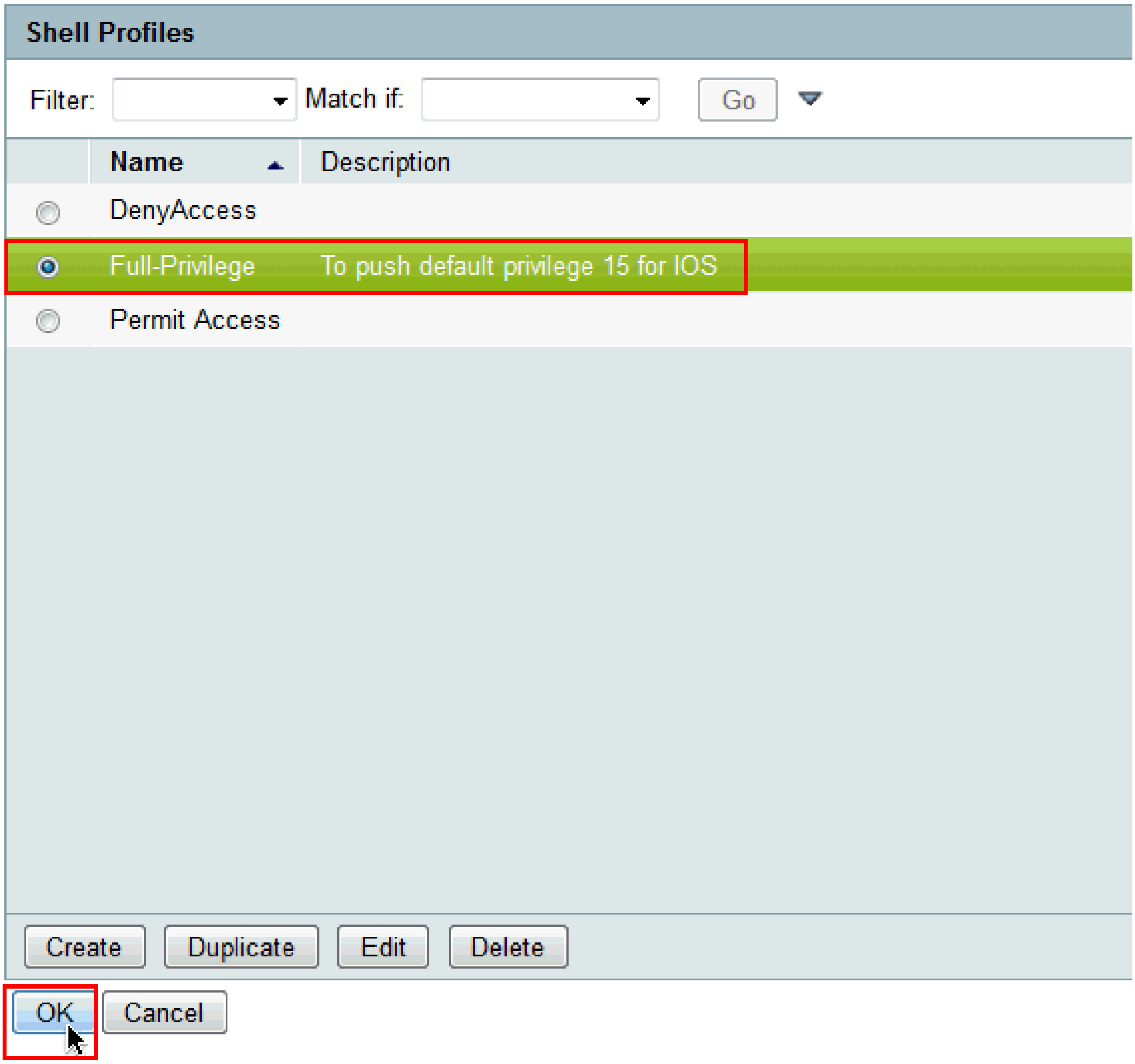
Privilege Level

Default Privilege:	Static	Value	15
Maximum Privilege:	Static	Value	15

Shell Attributes

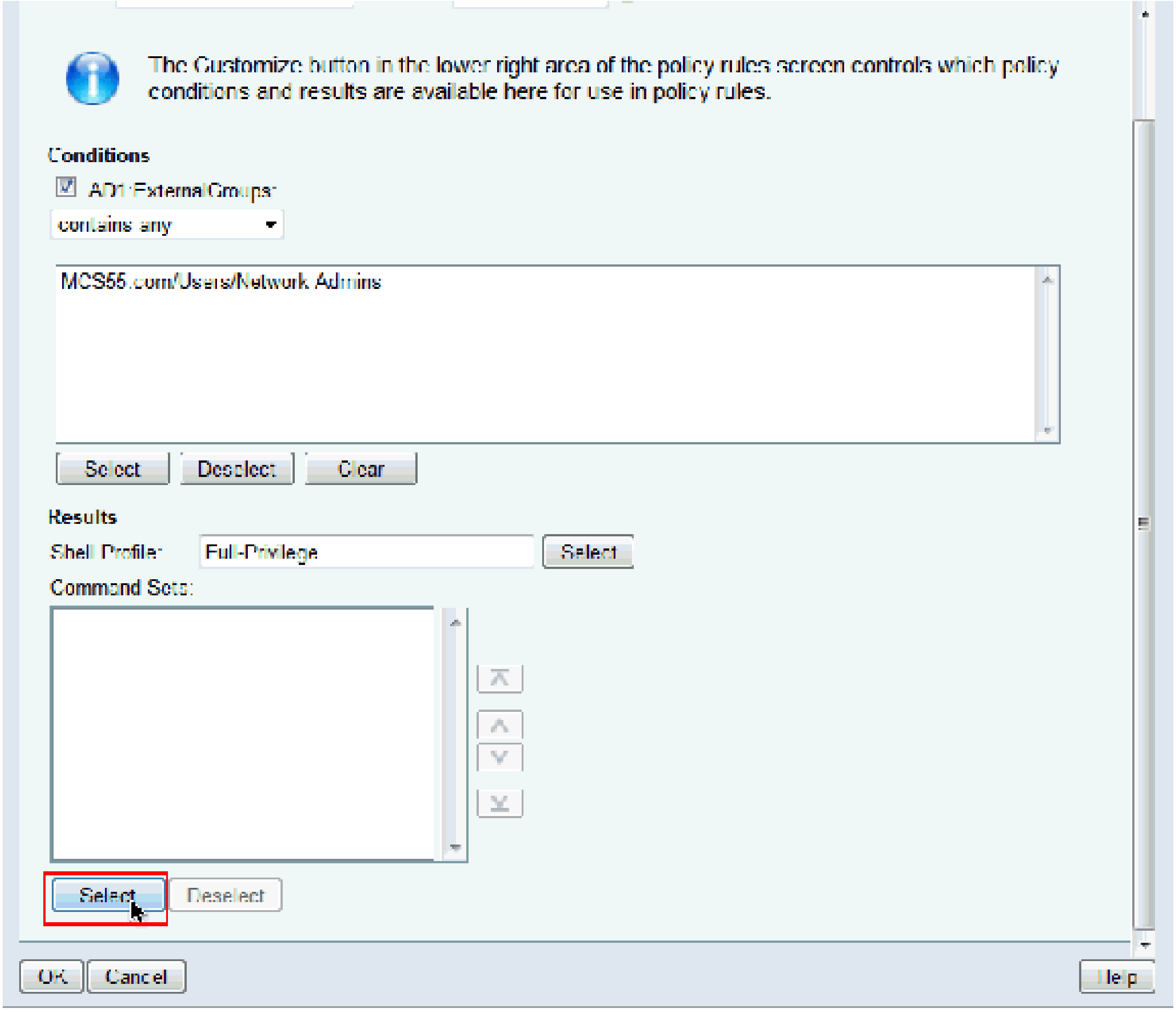
Access Control List:	Not in Use
Auto Command:	Not in Use
No Callback Verify:	Not in Use
No Escape:	Not in Use
No Hang Up:	Not in Use
Timeout:	Not in Use
Idle Time:	Not in Use
Callback Line:	Not in Use
Callback Rotary:	Not in Use

أختر الآن ملف تعريف Shell للوصول الكامل الذي تم إنشاؤه حديثا (امتياز كامل في هذا19.
المثال) وانقر موافق.



	Name	Description
○	DenyAccess	
●	Full-Privilege	To push default privilege 15 for IOS
○	Permit Access	

انقر تحديد في حقل مجموعات الأوامر.20.



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

Conditions

☑ AD1:ExternalGroups: contains any

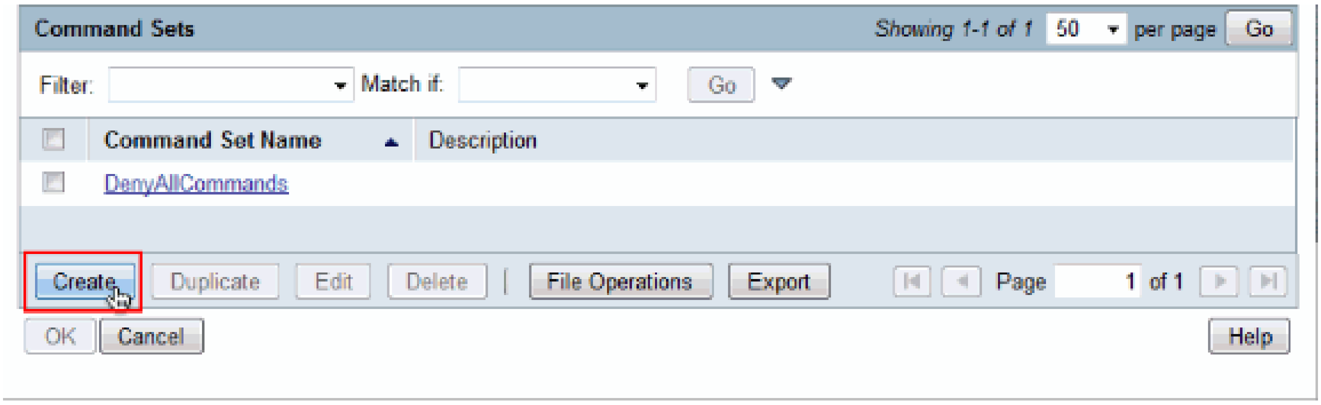
MCS55.com/Users/Network Admins

Results

Shell Profile: Full-Privilege

Command Sets:

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



Command Sets — Showing 1-1 of 1 — 50 per page

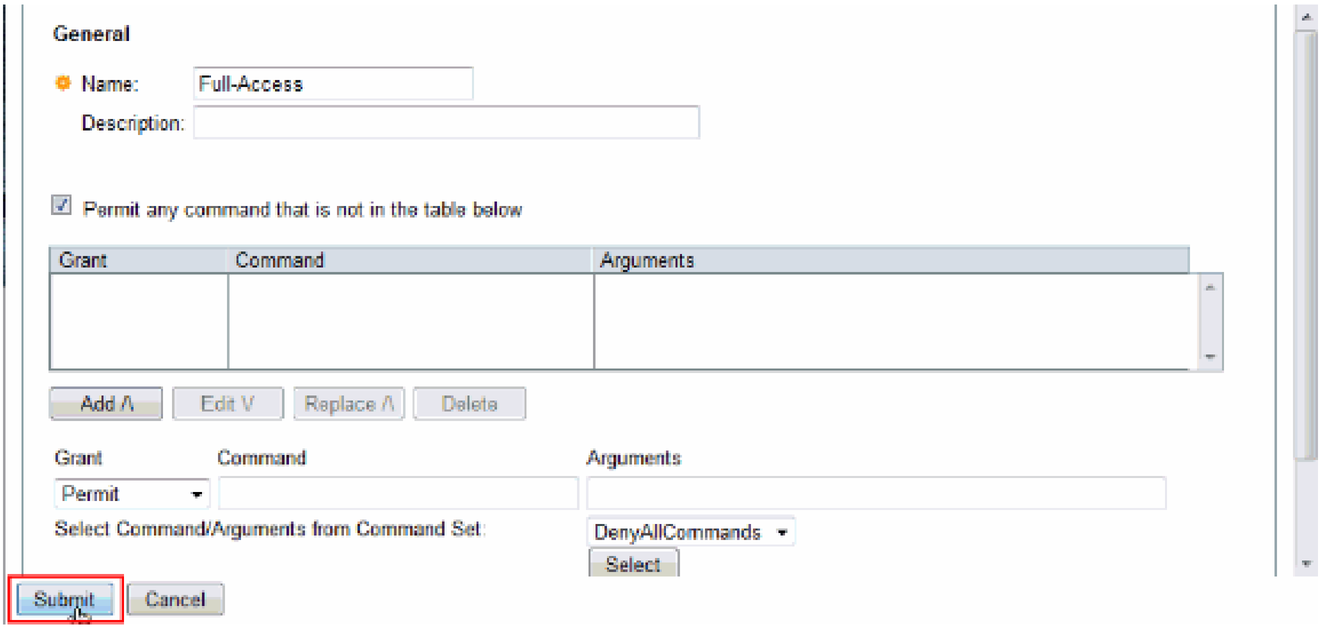
Filter: Match if:

☐	Command Set Name	Description
☐	DenyAllCommands	

Page 1 of 1

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.



General

Name: Full-Access

Description:

☑ Permit any command that is not in the table below

Grant	Command	Arguments

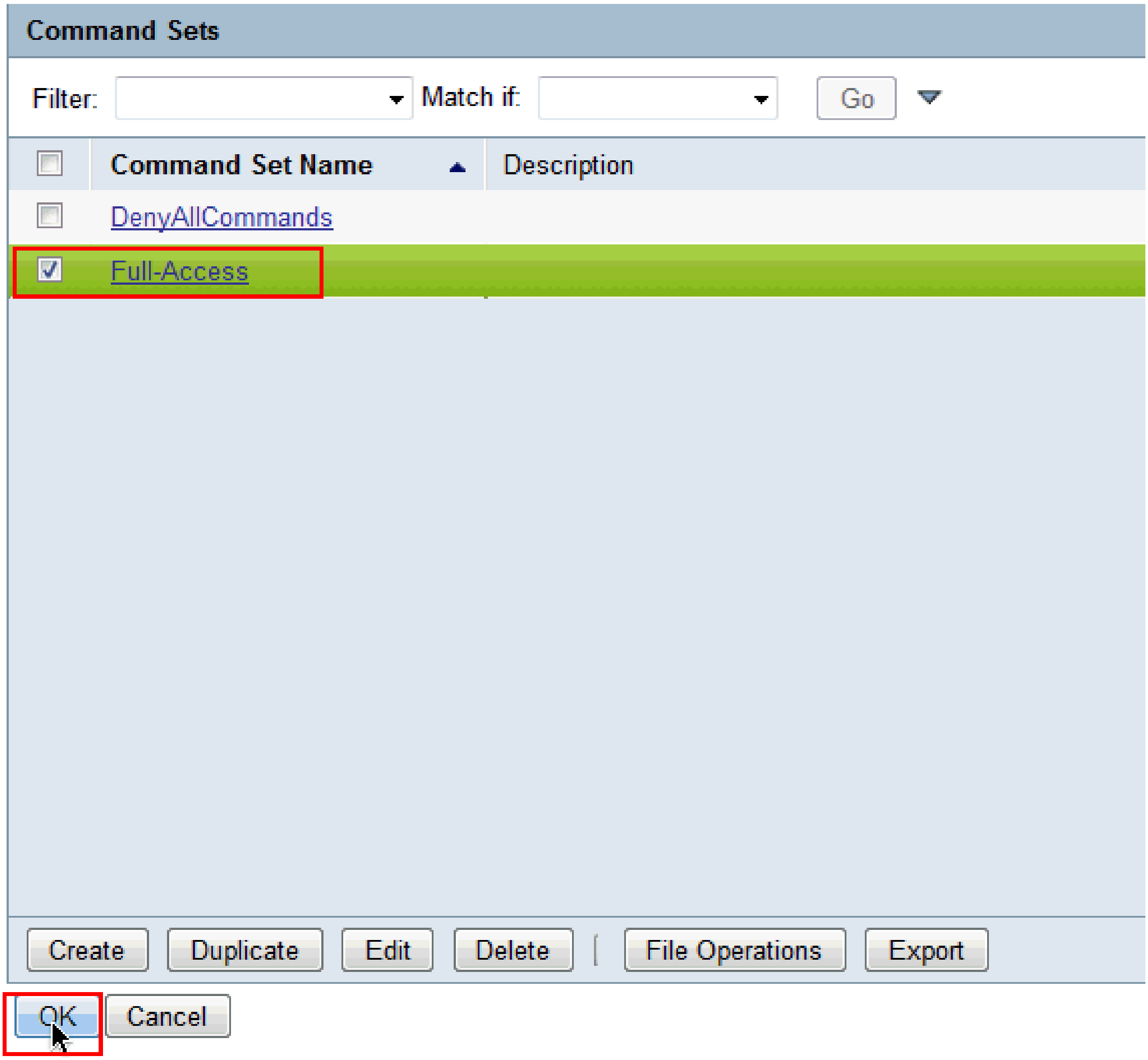
Grant: Permit

Command:

Arguments:

Select Command/Arguments from Command Set: DenyAllCommands

.23 انقر فوق OK.



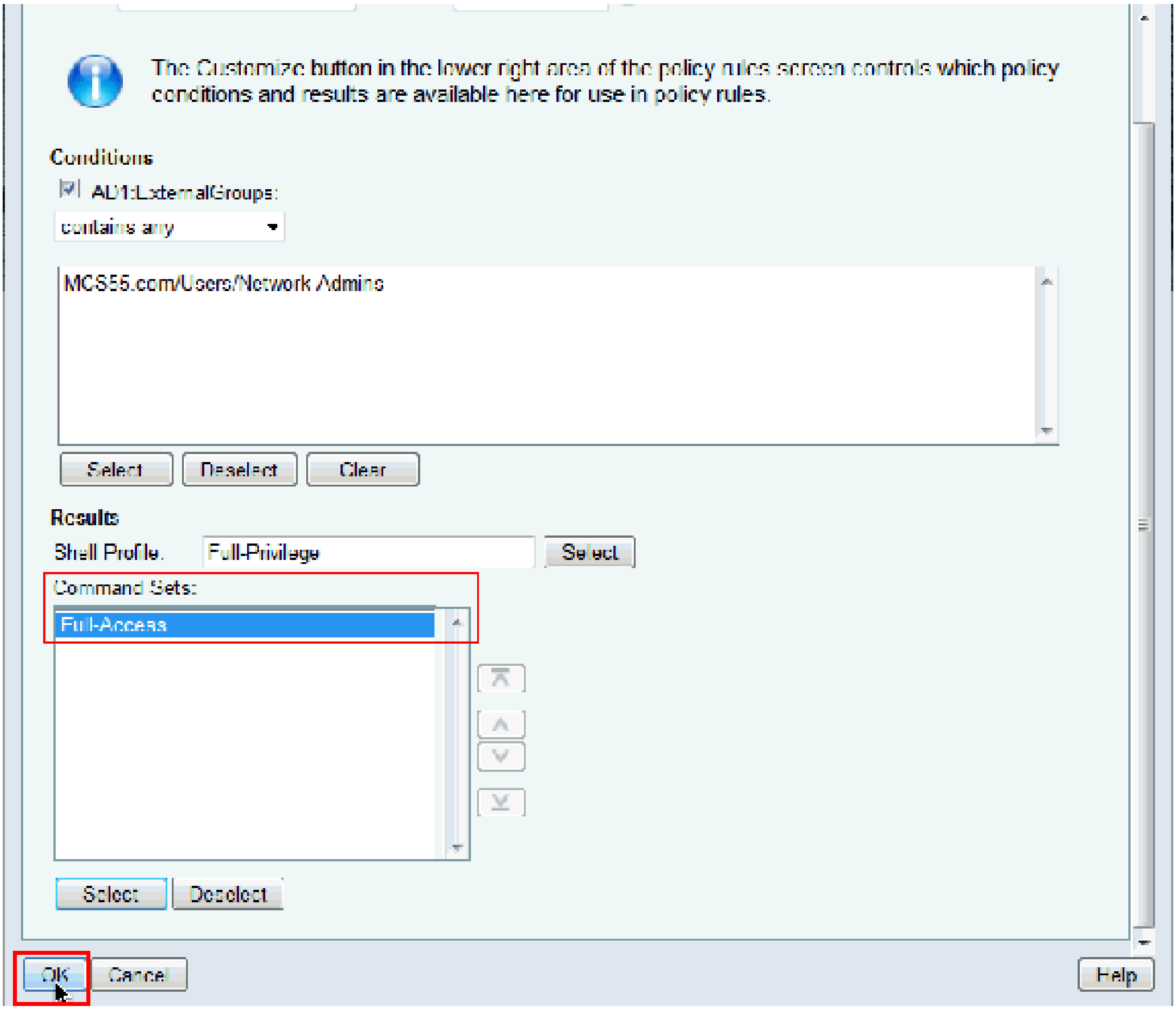
Command Sets

Filter:

Match if:

□	Command Set Name	Description
□	DenyAllCommands	
☑	Full-Access	

وانقر فوق OK. يؤدي هذا إلى اكتمال تكوين القاعدة-1.24.



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

Conditions

☑ AD1:ExternalGroups:

contains any

MCS55.com/Users/Network Admins

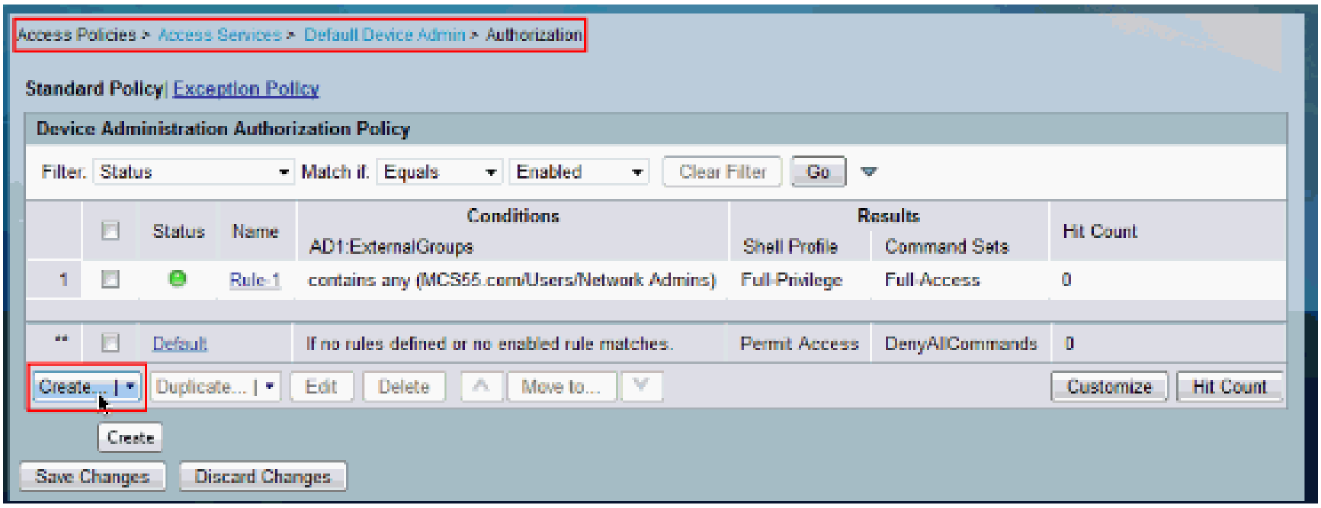
Results

Shell Profile: Full-Privilege

Command Sets:

Full-Access

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



Access Policies > Access Services > Default Device Admin > Authorization

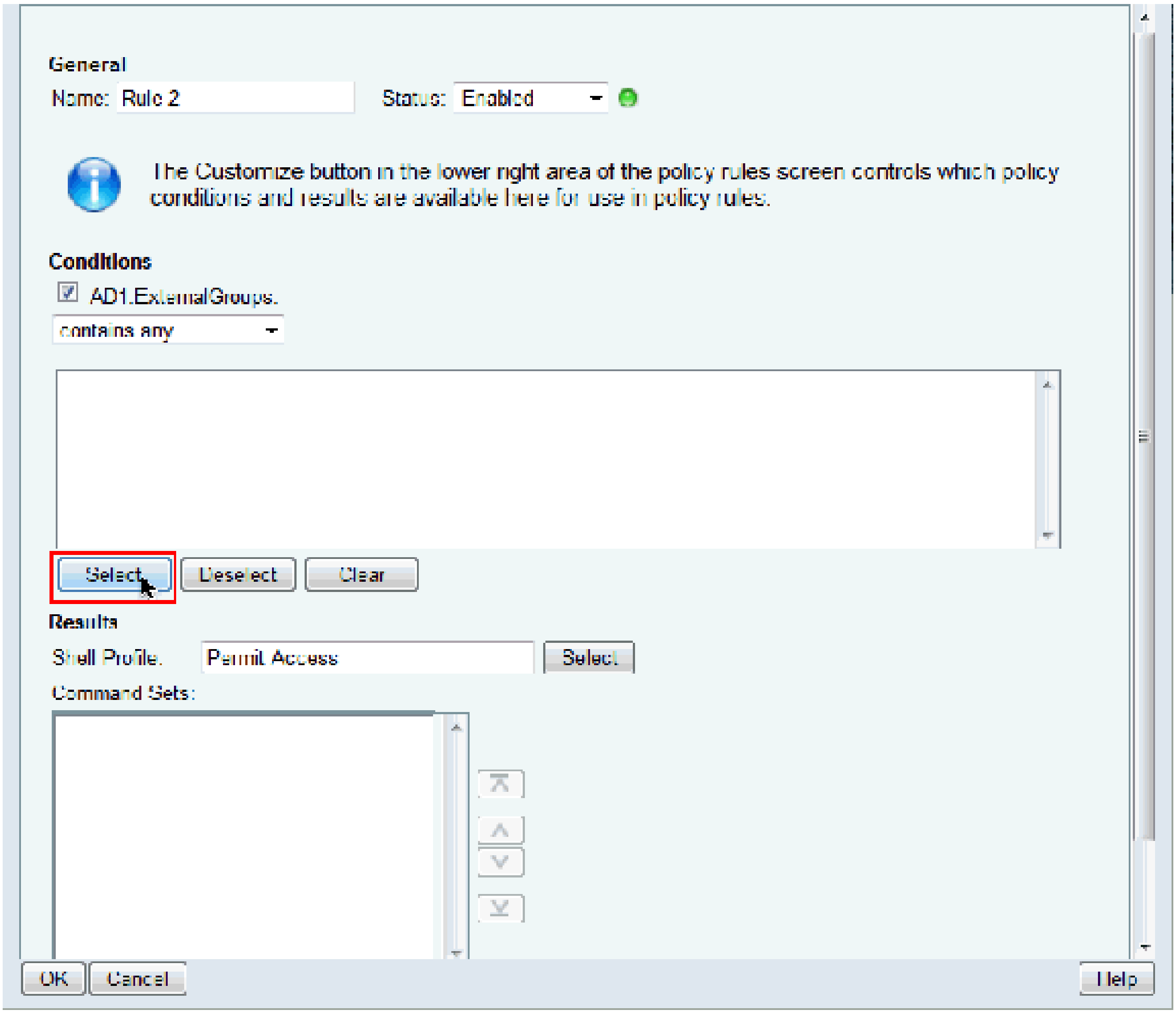
Standard Policy | Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled

				Conditions	Results		
	□	Status	Name	AD1:ExternalGroups	Shell Profile	Command Sets	Hit Count
1	□	●	Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0
**	□		Default	If no rules defined or no enabled rule matches.	Permit Access	DenyAllCommands	0

أختر AD1:ExternalGroups وانقر تحديد.26.



General

Name: Rule 2

Status: Enabled

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

Conditions

☑ AD1.ExternalGroups:

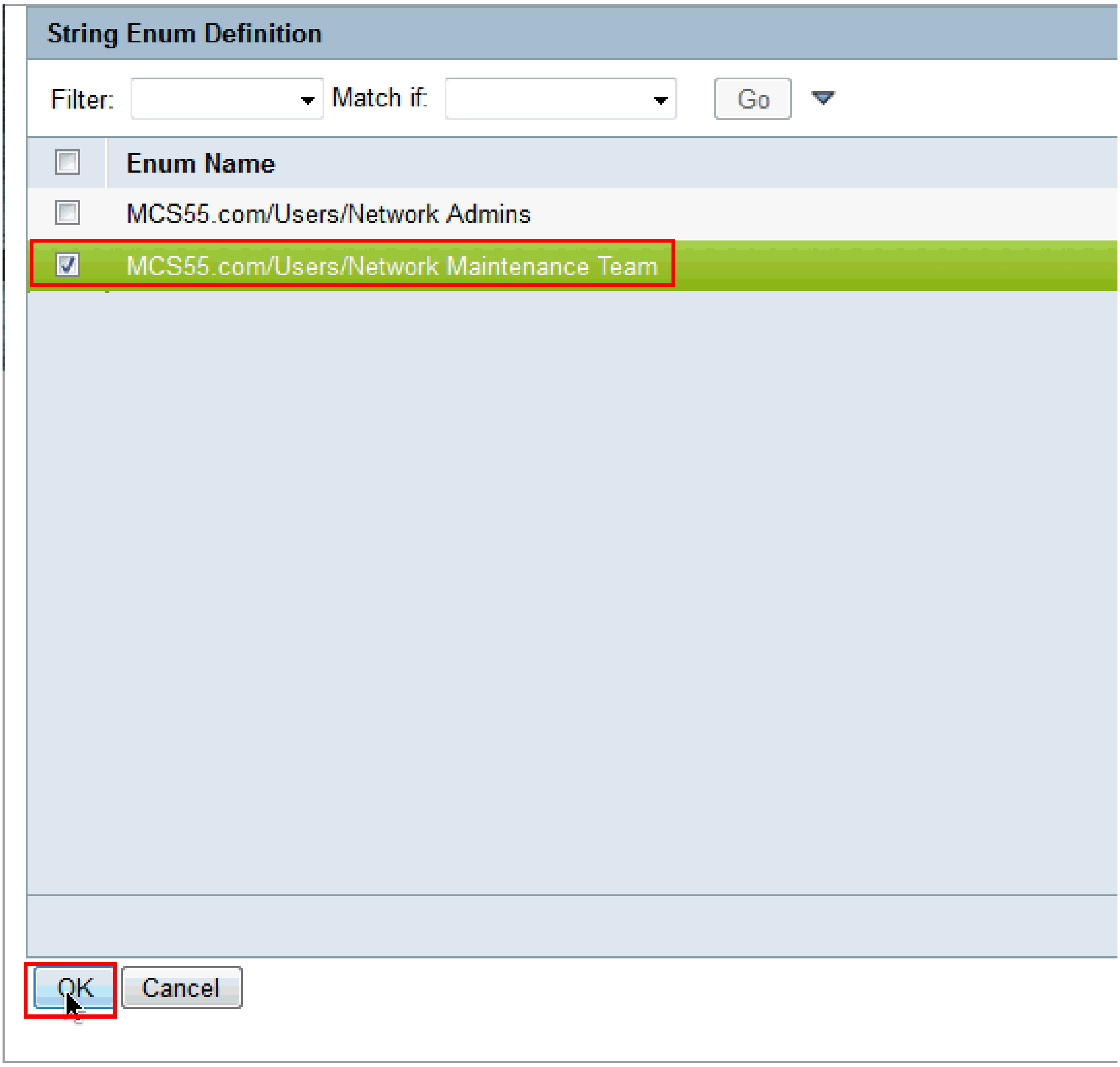
contains any

Results

Shell Profile: Permit Access

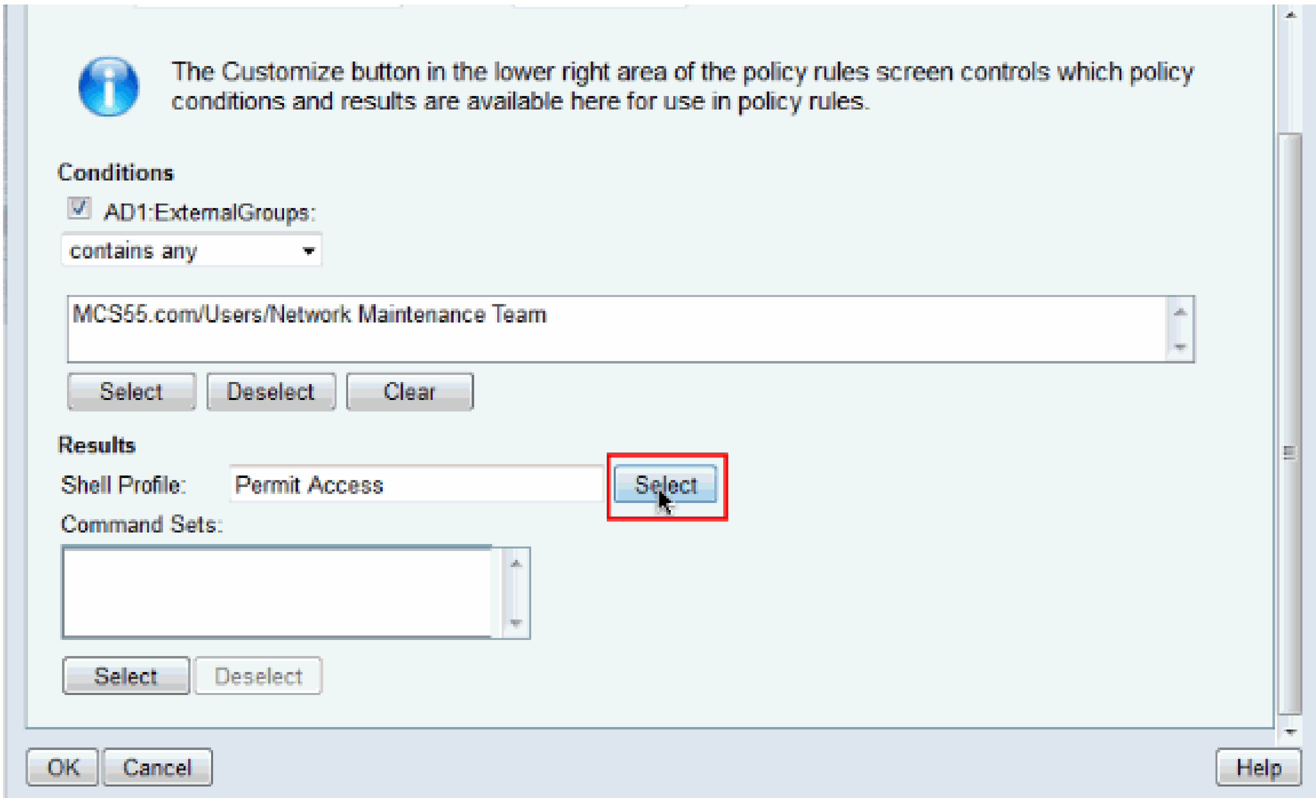
Command Sets:

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



□	Enum Name
□	MCS55.com/Users/Network Admins
☑	MCS55.com/Users/Network Maintenance Team

انقر على تحديد في حقل ملف تعريف Shell.28.



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

Conditions

☑ AD1:ExternalGroups:

contains any

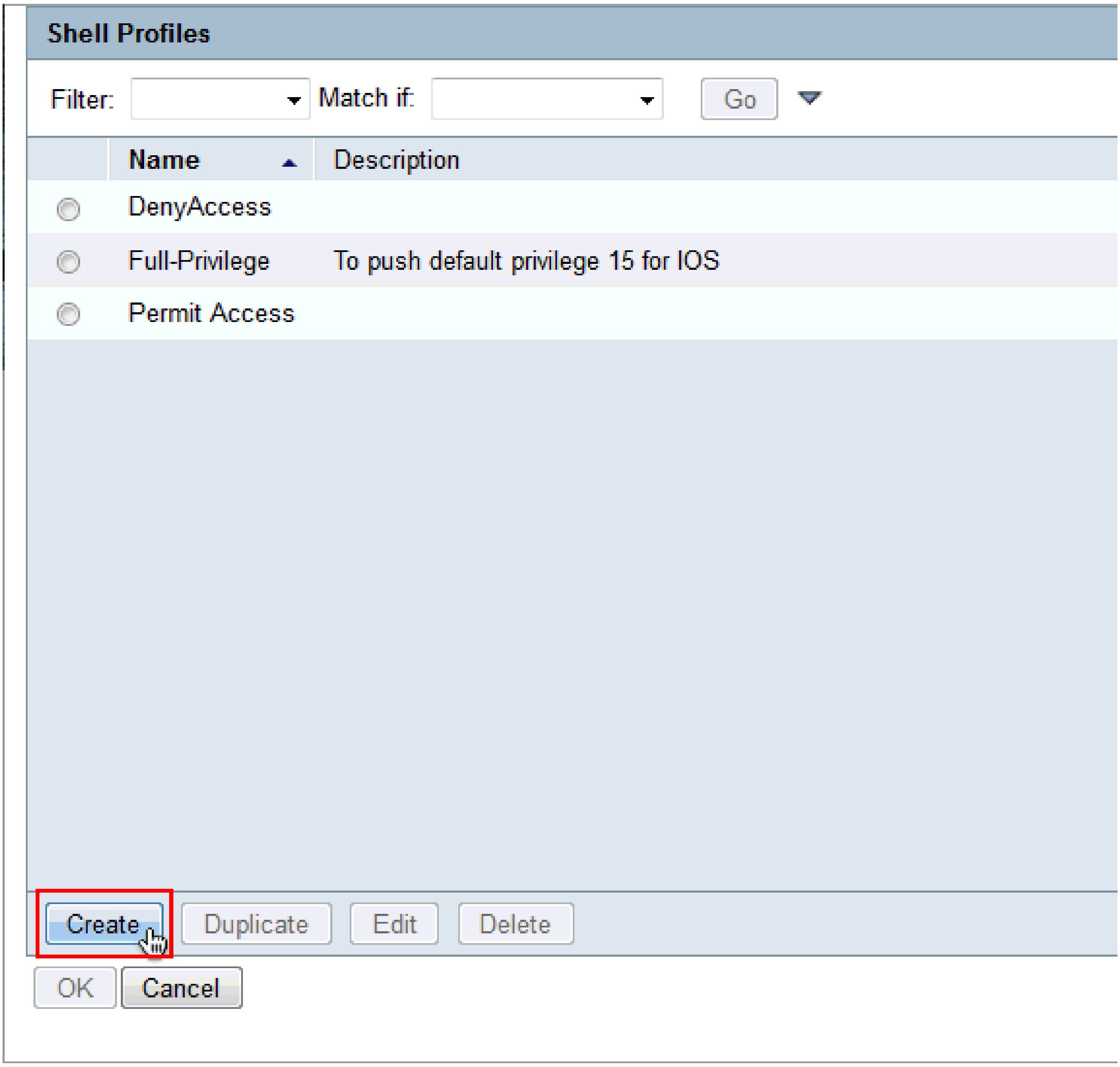
MCS55.com/Users/Network Maintenance Team

Results

Shell Profile: Permit Access

Command Sets:

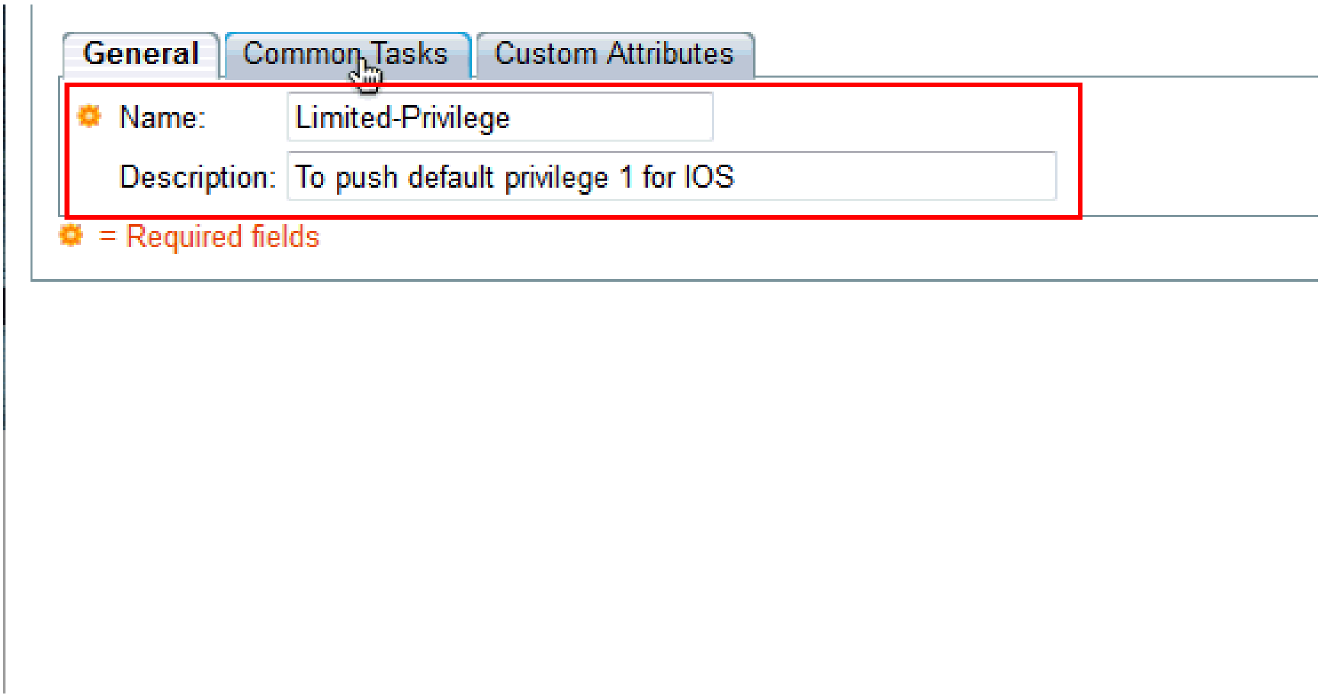
انقر على إنشاء لإنشاء ملف تعريف Shell جديد للوصول المحدود.29.



Shell Profiles

	Name	Description
○	DenyAccess	
○	Full-Privilege	To push default privilege 15 for IOS
○	Permit Access	

قم بتوفير اسم ووصف (إختياري) في علامة التبويب عام وانقر فوق علامة التبويب30.
مهام مشتركة.

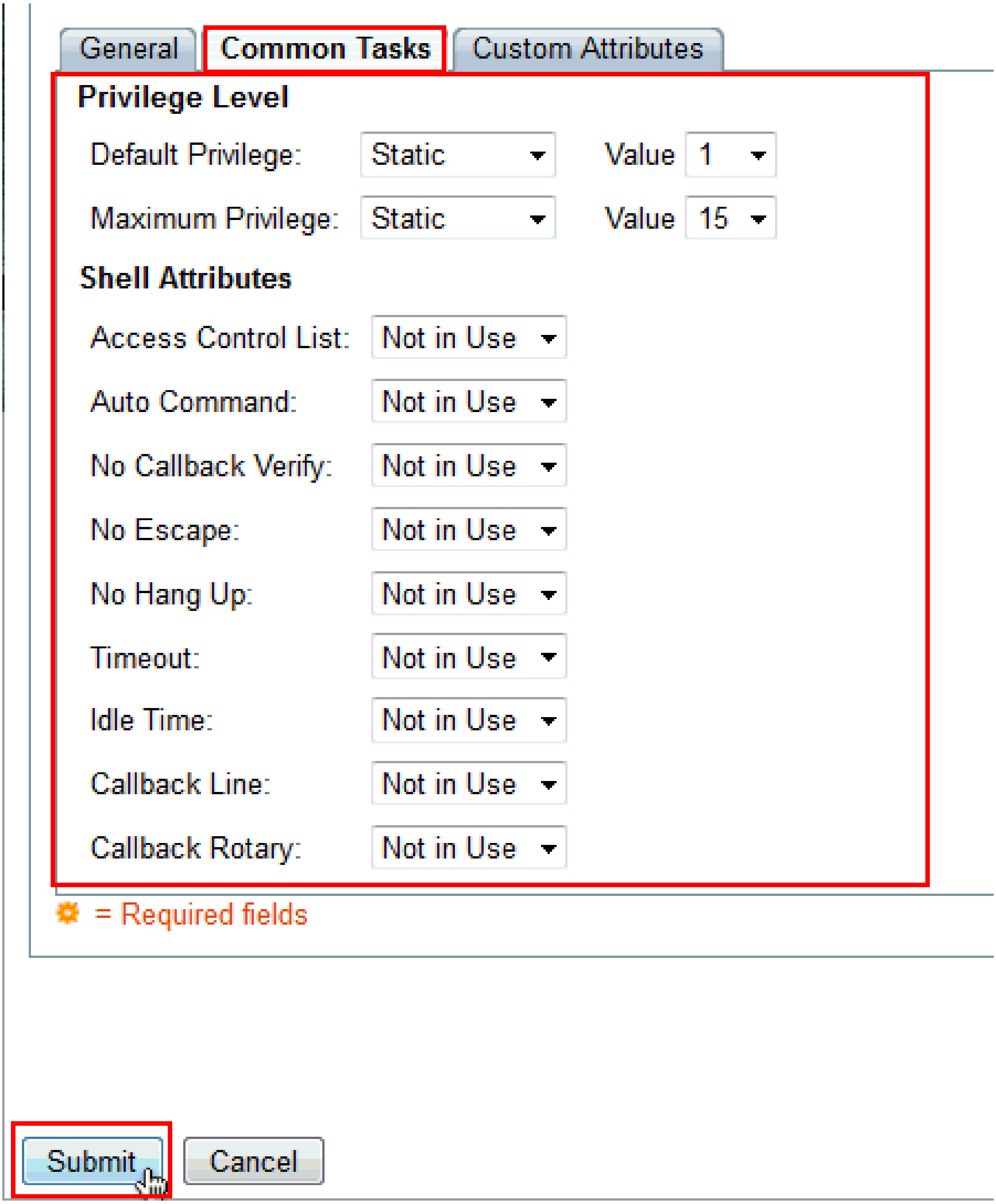


Name: Limited-Privilege

Description: To push default privilege 1 for IOS

= Required fields

غيرت التقصير امتياز و الأقصى امتياز إلى ساكن إستاتيكي مع قيمة 1 و15 على31.
التوالي. انقر على إرسال.



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

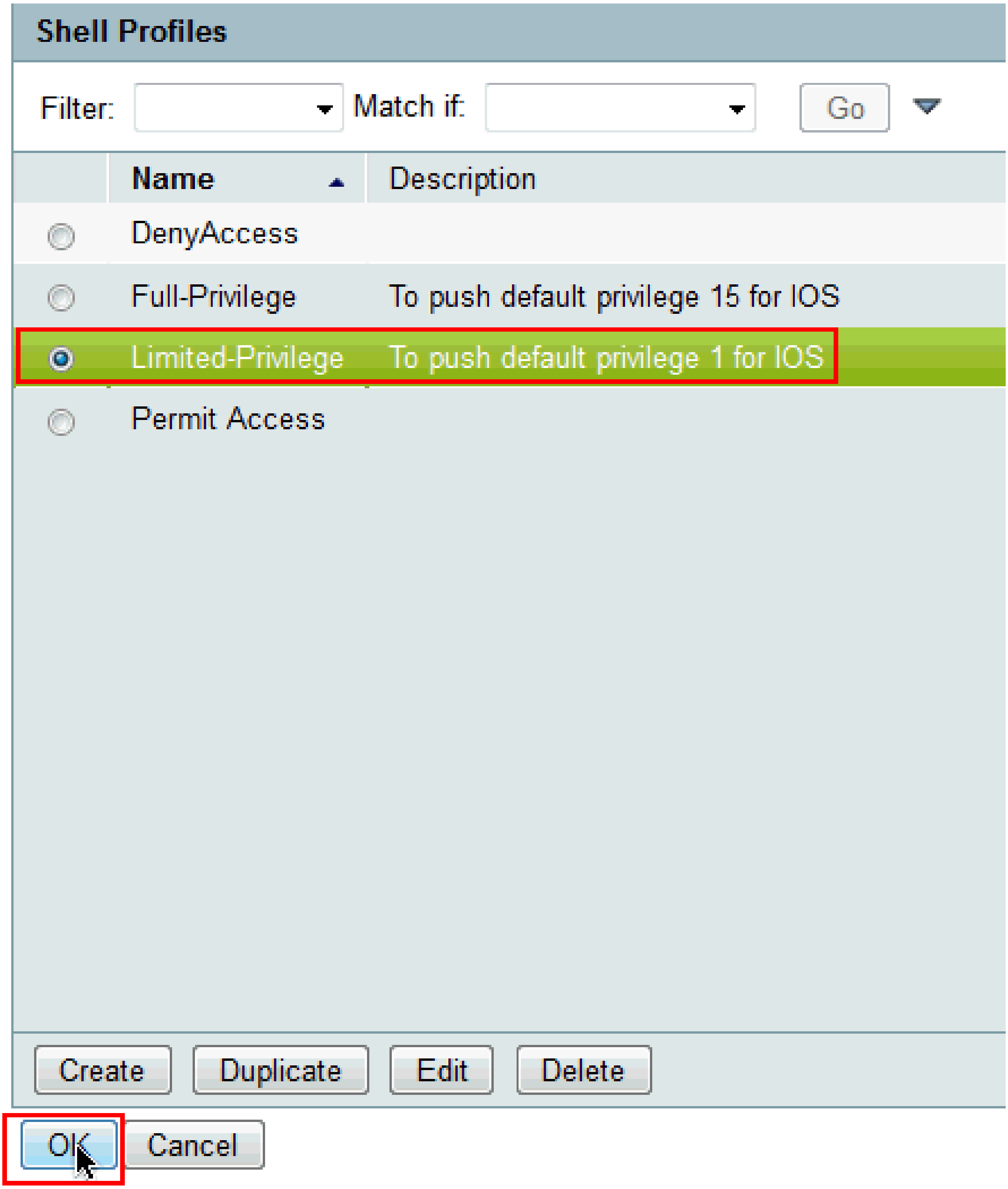
Idle Time: Not in Use

Callback Line: Not in Use

Callback Rotary: Not in Use

✱ = Required fields

وانقر فوق OK.32.

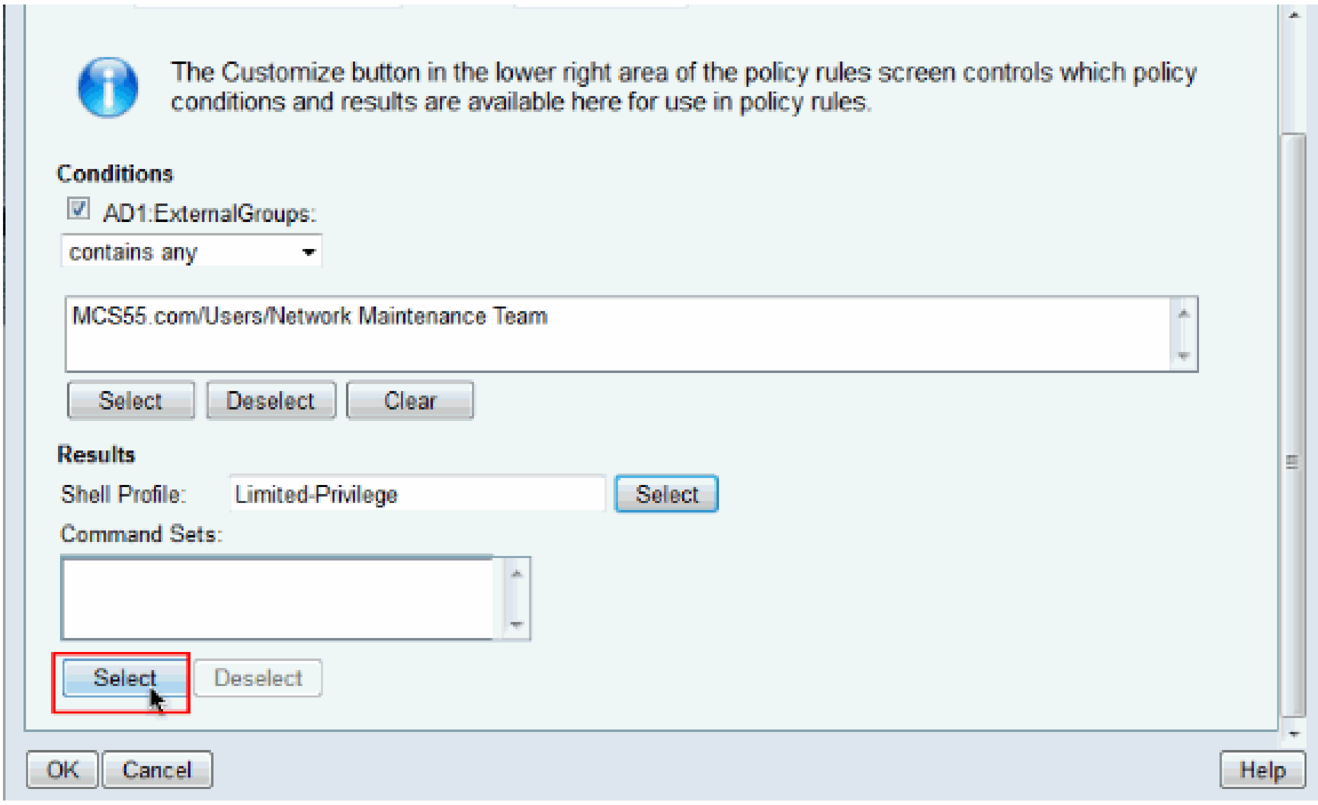


Shell Profiles

Filter: Match if: Go

	Name	Description
○	DenyAccess	
○	Full-Privilege	To push default privilege 15 for IOS
●	Limited-Privilege	To push default privilege 1 for IOS
○	Permit Access	

33. انقر تحديد في حقل مجموعات الأوامر.



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

Conditions

☑ AD1:ExternalGroups:

contains any

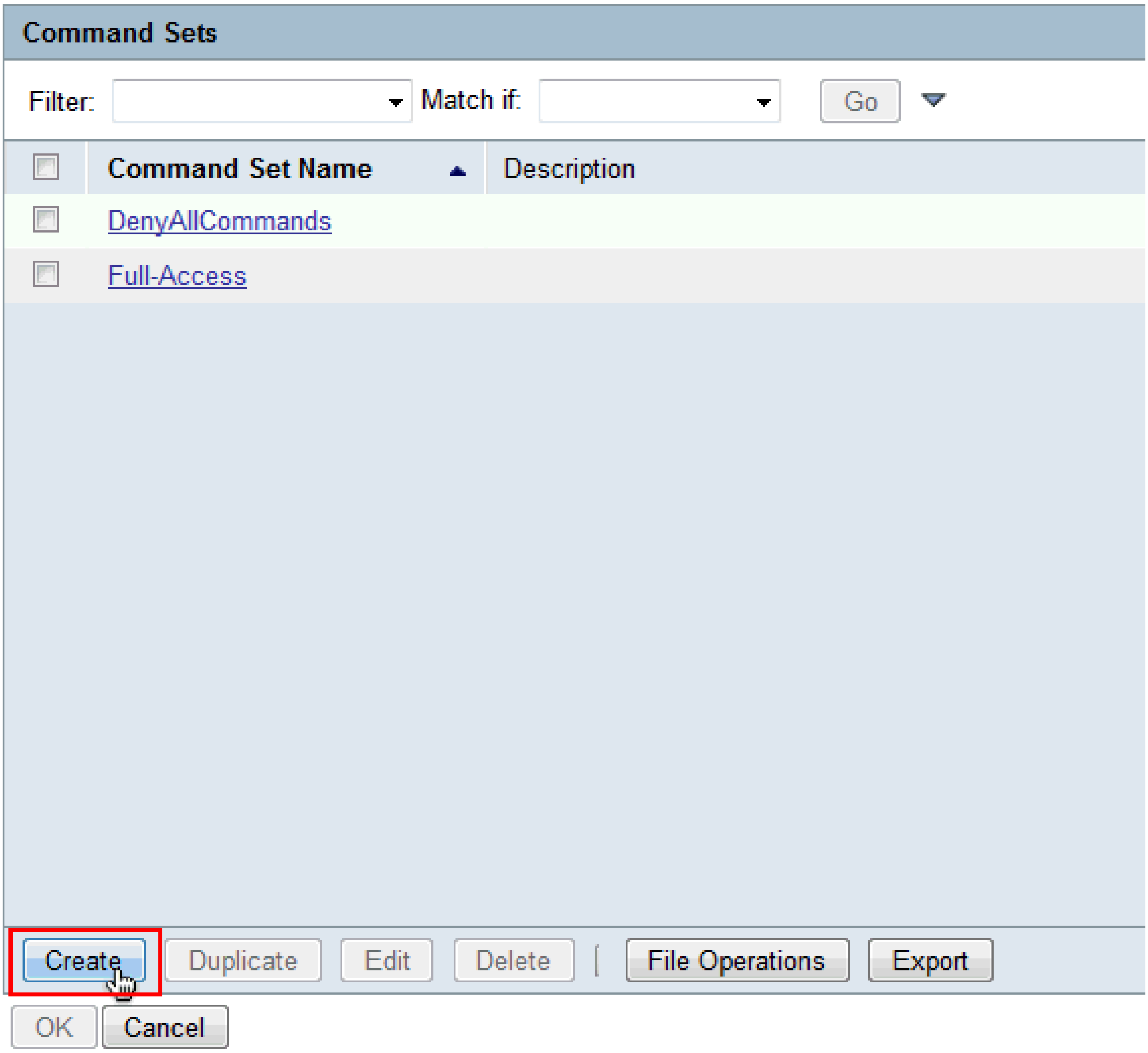
MCS55.com/Users/Network Maintenance Team

Results

Shell Profile: Limited-Privilege

Command Sets:

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

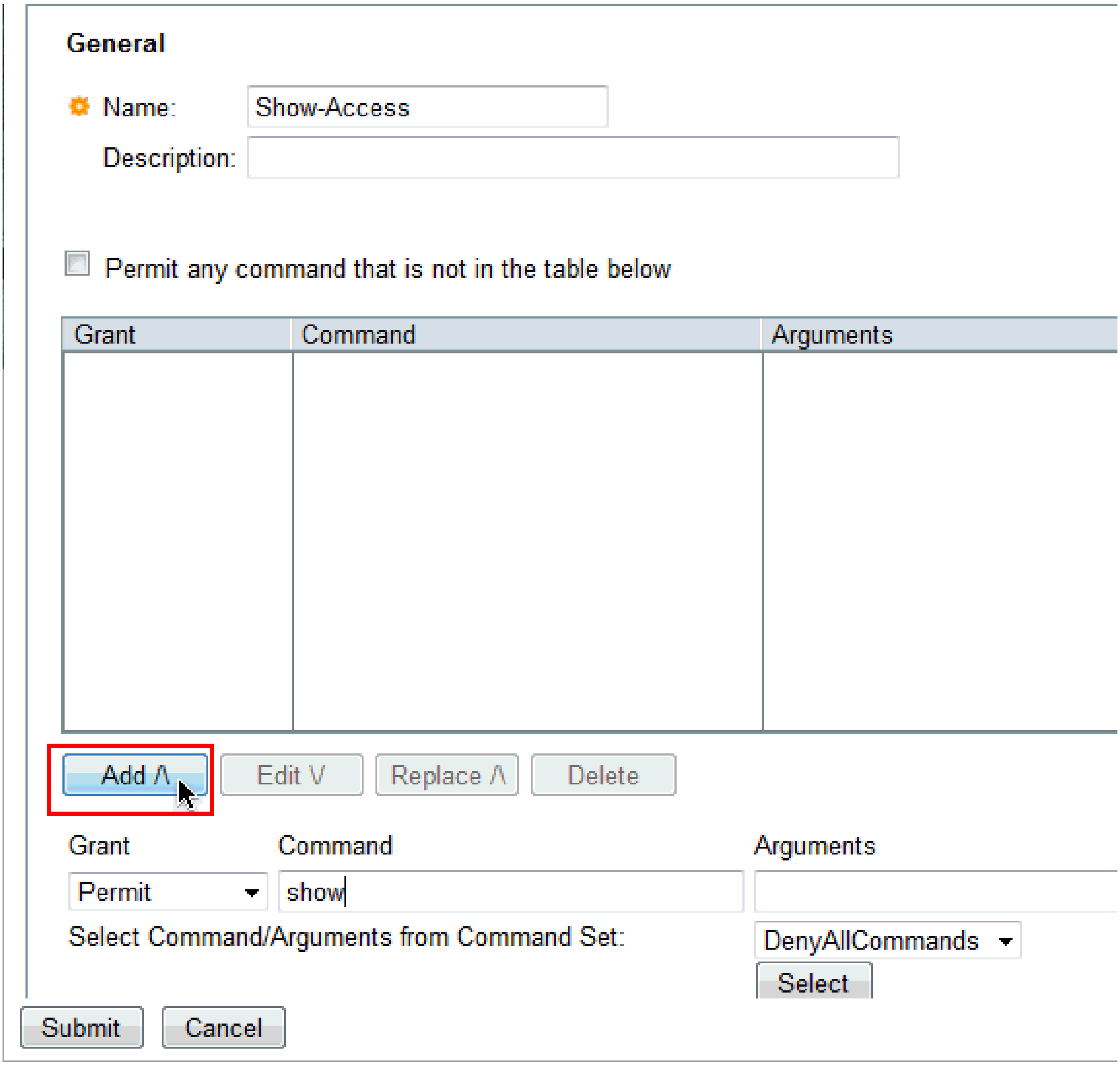


Command Sets

Filter: Match if:

□	Command Set Name ▲	Description
□	DenyAllCommands	
□	Full-Access	

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.



General

Name: Show-Access

Description:

□ Permit any command that is not in the table below

Grant	Command	Arguments

Grant: Permit

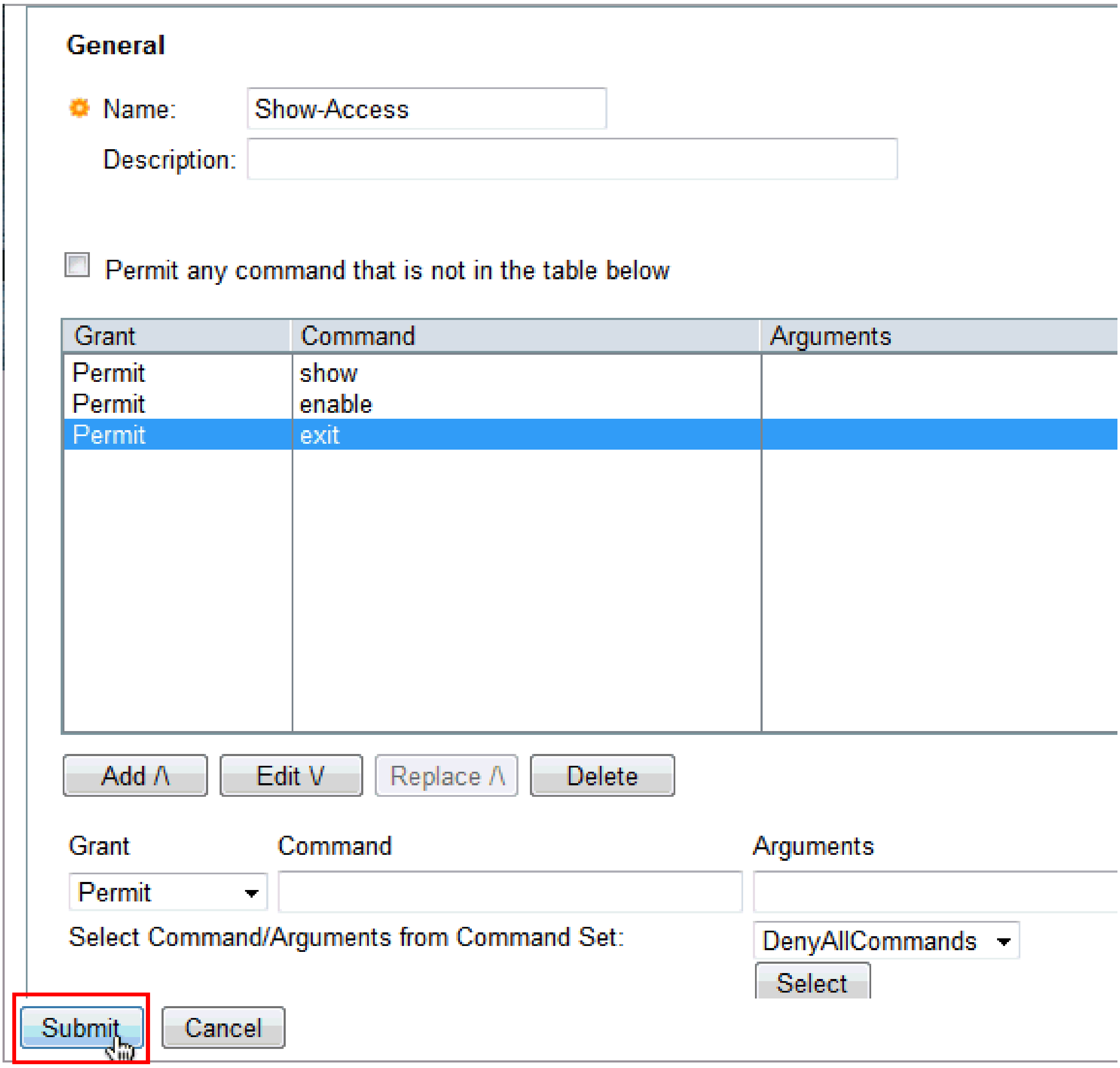
Command: show

Arguments:

Select Command/Arguments from Command Set: DenyAllCommands

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.



General

Name: Show-Access

Description:

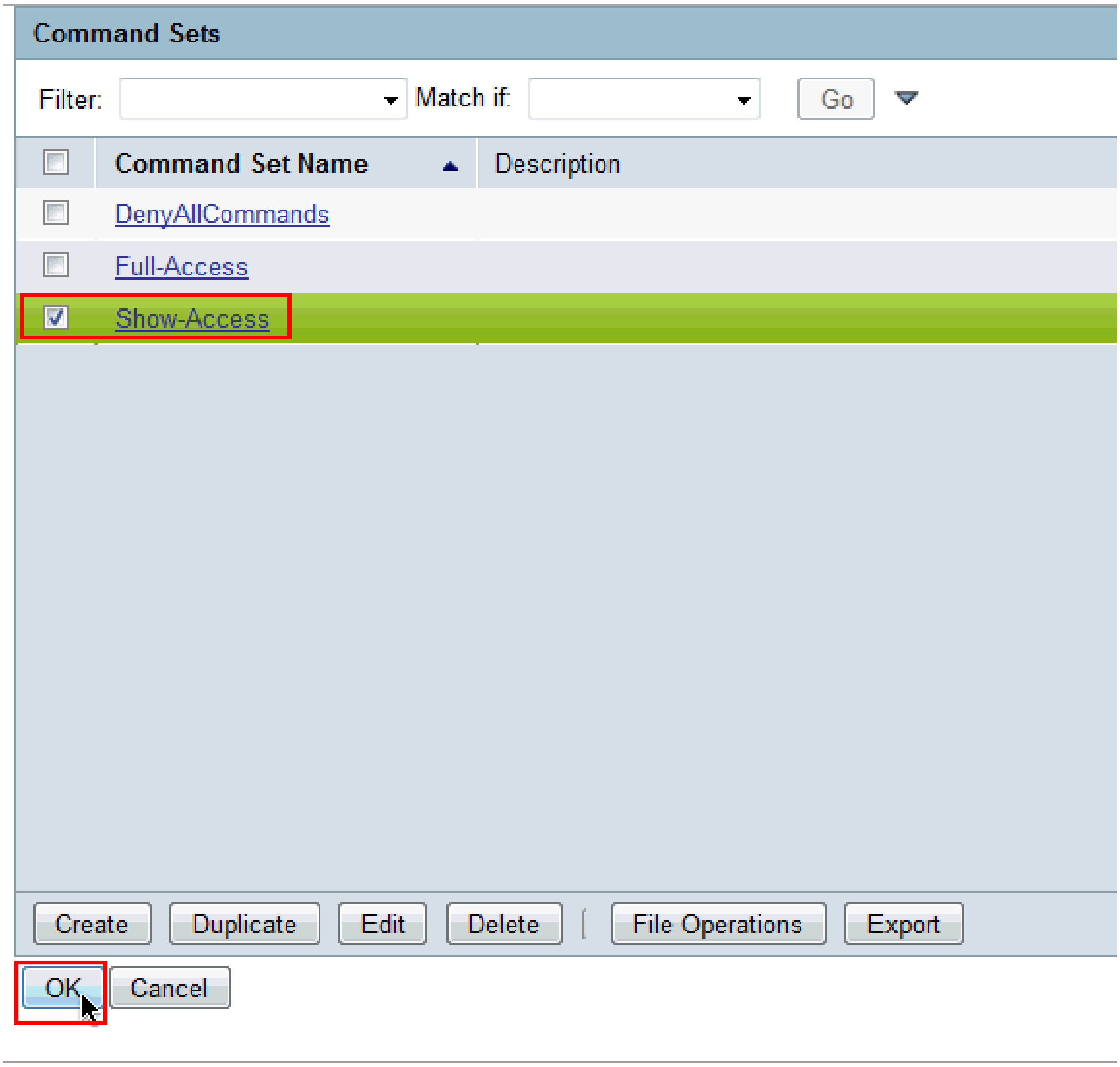
□ Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant	Command	Arguments
Permit		

Select Command/Arguments from Command Set: DenyAllCommands

37. وانقر فوق OK.

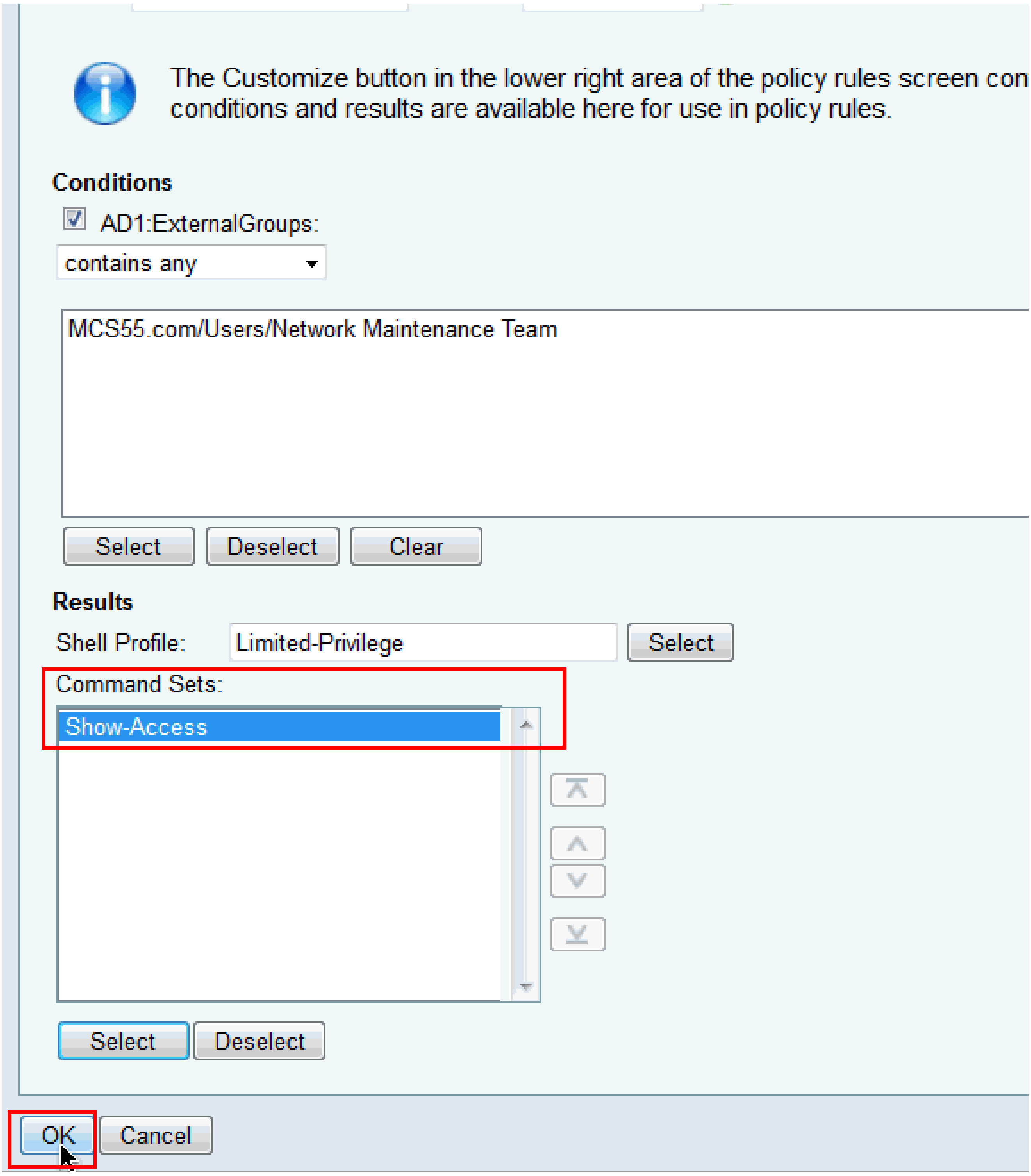


Command Sets

Filter: Match if:

□	Command Set Name ▲	Description
□	DenyAllCommands	
□	Full-Access	
☑	Show-Access	

رقناو قوف OK.38.



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

Conditions

☑ AD1:ExternalGroups:

contains any

MCS55.com/Users/Network Maintenance Team

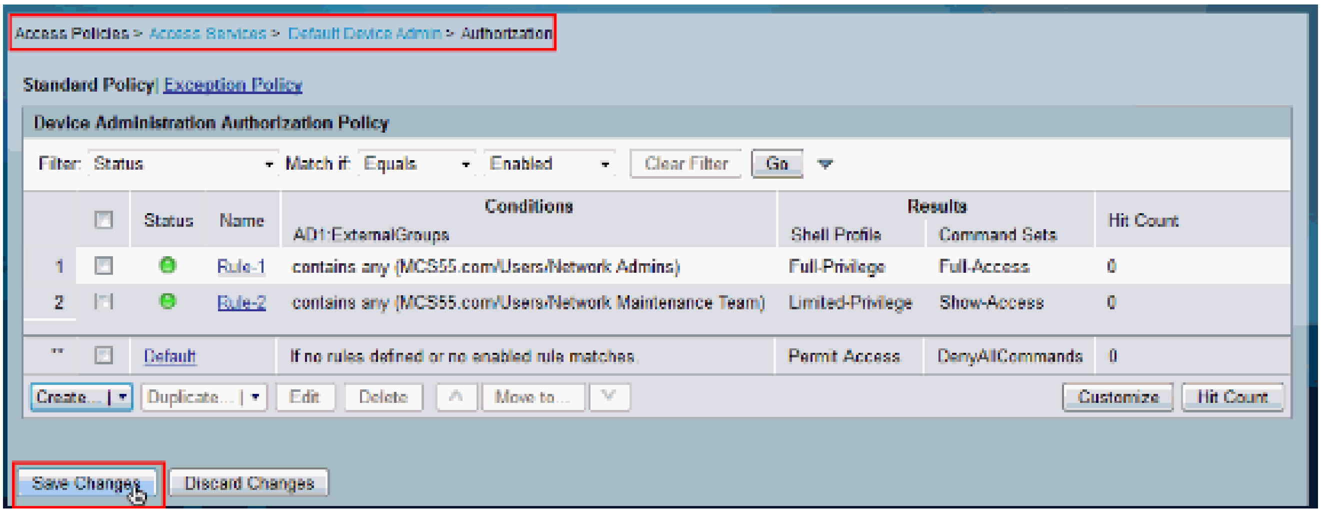
Results

Shell Profile: Limited-Privilege

Command Sets:

Show-Access

انقر فوق حفظ التغييرات.39.



Access Policies > Access Services > Default Device Admin > Authorization

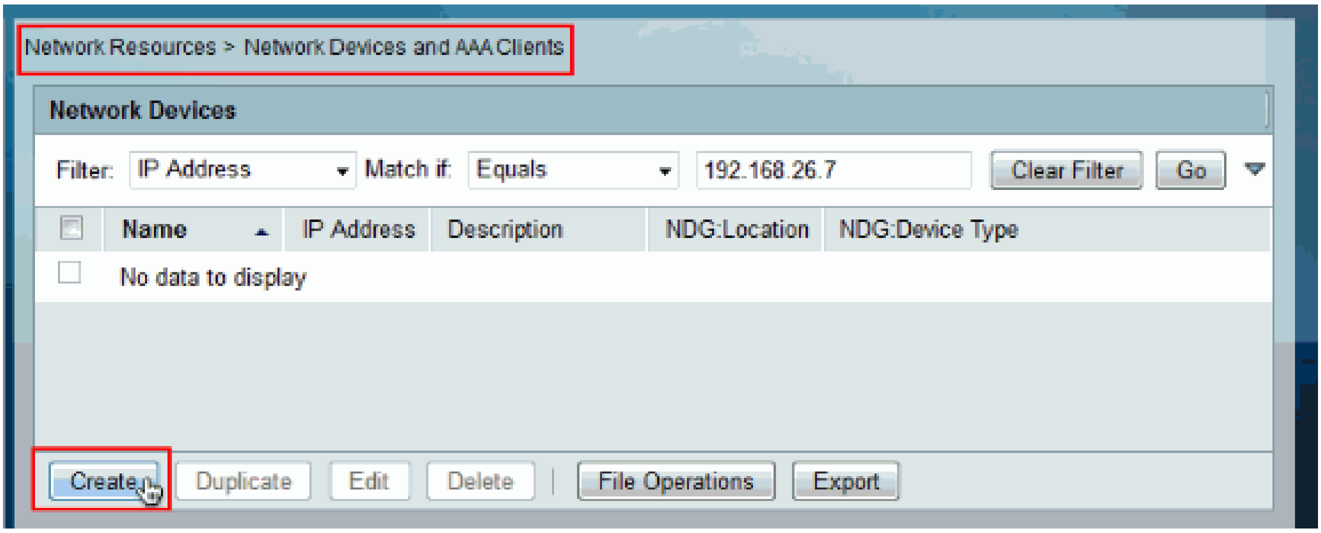
Standard Policy | Exception Policy

Device Administration Authorization Policy

Filter: Status ▾ Match if: Equals ▾ Enabled ▾

				Conditions	Results		
	☐	Status	Name	AD1:ExternalGroups	Shell Profile	Command Sets	Hit Count
1	☐	●	Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0
2	☐	●	Rule-2	contains any (MCS55.com/Users/Network Maintenance Team)	Limited-Privilege	Show-Access	0
**	☐		Default	If no rules defined or no enabled rule matches.	Permit Access	DenyAllCommands	0

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



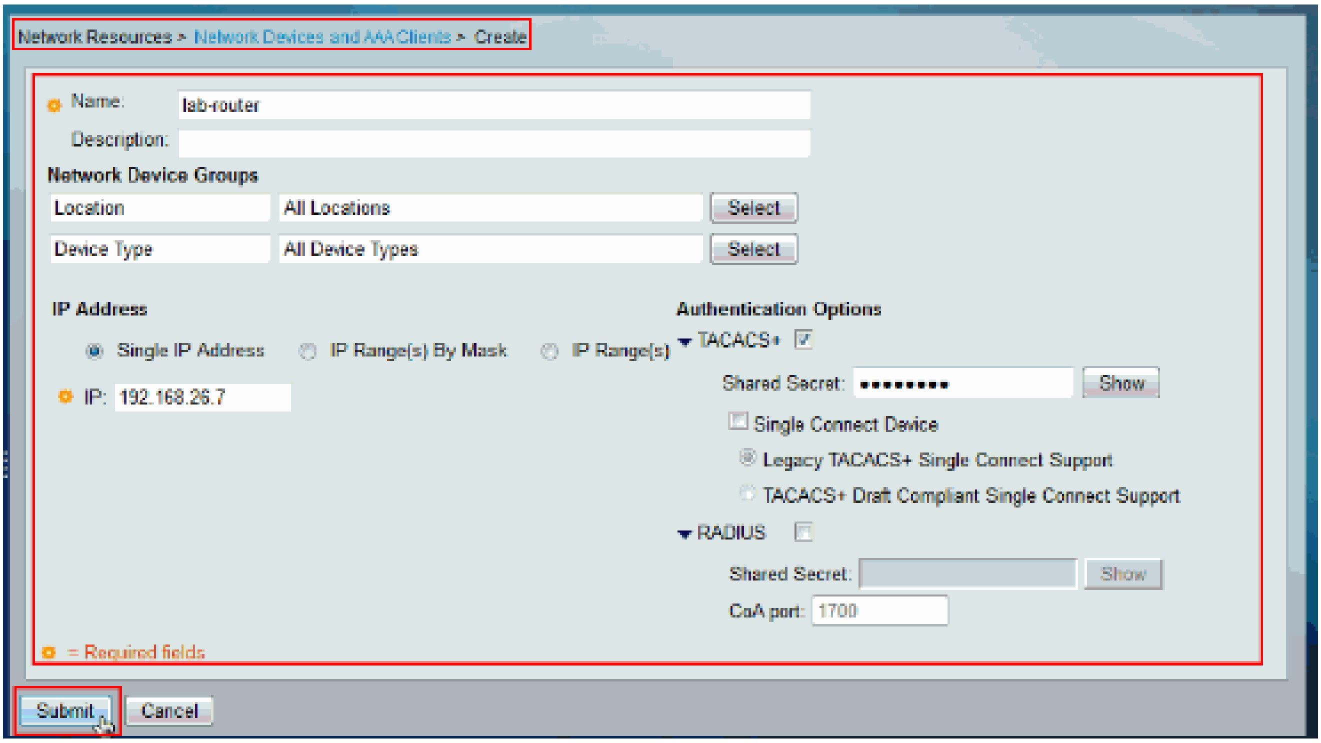
Network Resources > Network Devices and AAA Clients

Network Devices

Filter: IP Address ▾ Match if: Equals ▾ 192.168.26.7

☐	Name ▲	IP Address	Description	NDG:Location	NDG:Device Type
☐	No data to display				

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



Network Resources > Network Devices and AAA Clients > Create

Name: lab-router

Description:

Network Device Groups

Location	All Locations	Select
Device Type	All Device Types	Select

IP Address

● Single IP Address ○ IP Range(s) By Mask ○ IP Range(s)

IP: 192.168.26.7

Authentication Options

TACACS+ ☑

Shared Secret: ••••••••• Show

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

RADIUS □

Shared Secret: Show

CoA port: 1700

= Required fields

Submit Cancel

تكوين جهاز Cisco IOS للمصادقة والتفويض

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

قم بإنشاء مستخدم محلي بامتياز كامل للتعيين الاحتياطي باستخدام الأمر1.
username كما هو موضح هنا:

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

قم بتوفير عنوان IP الخاص ب ACS لتمكين AAA وإضافة ACS 5.x كخادم TACACS.2.

```
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.

اختبر إمكانية الوصول إلى خادم TACACS باستخدام أمر اختبار AAA كما هو موضح.3.

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

يوضح إخراج الأمر السابق أن خادم TACACS يمكن الوصول إليه وقد تمت مصادقة المستخدم بنجاح.

ملاحظة: 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:

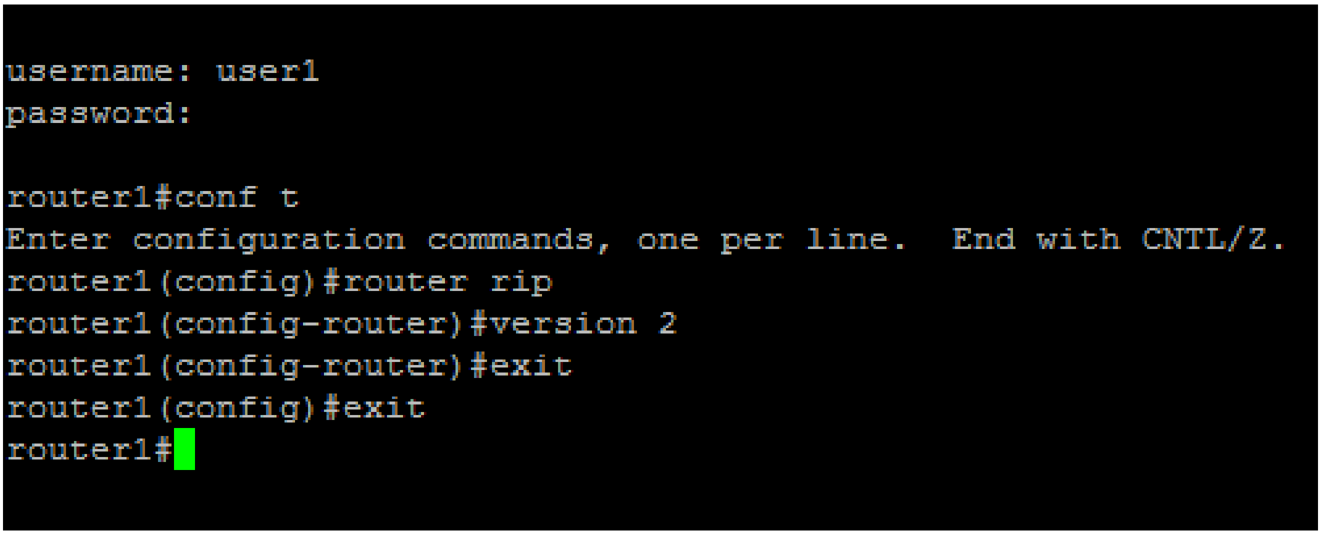
```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 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.

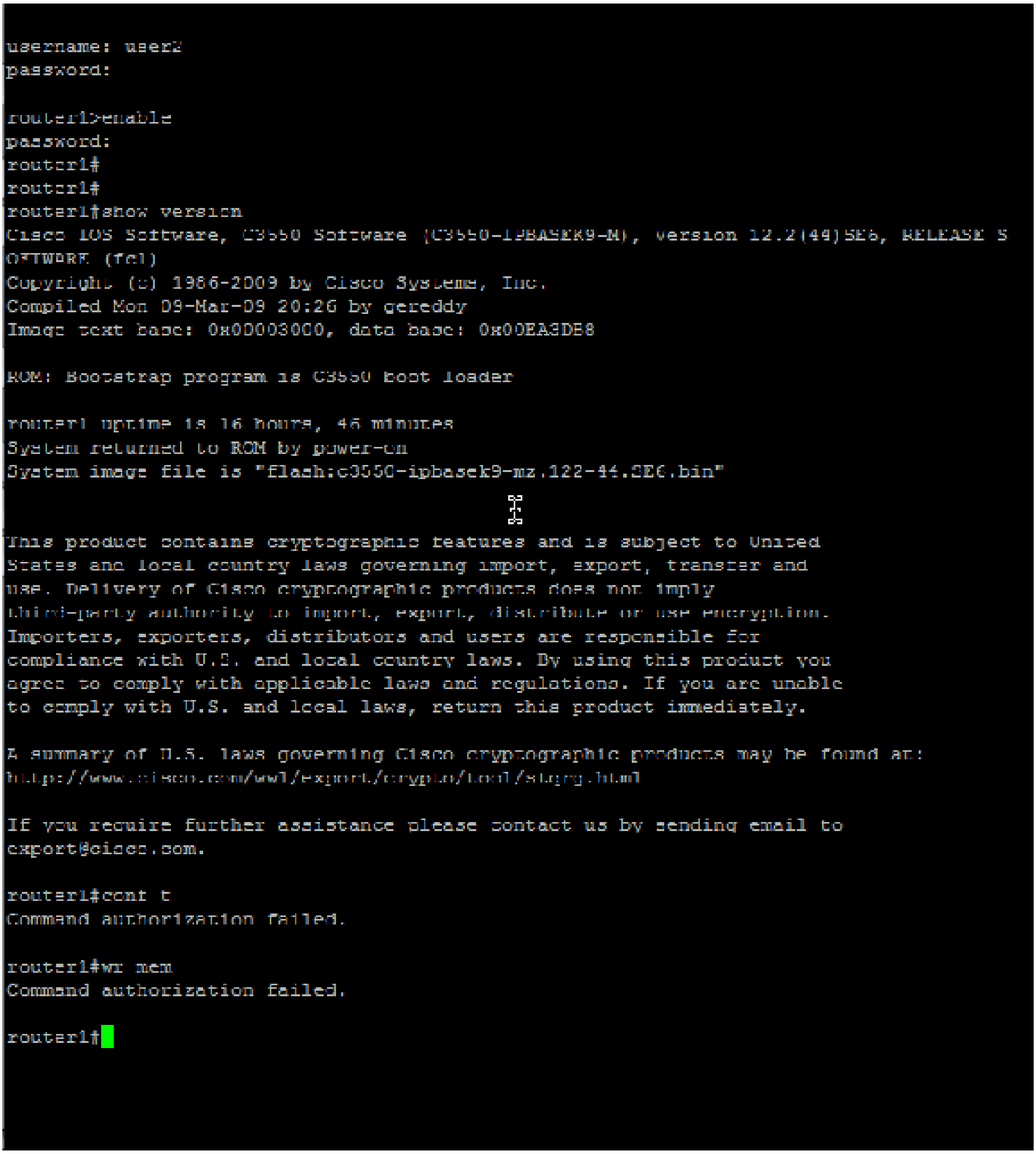
1. Telnet إلى جهاز Cisco IOS كمستخدم1 الذي ينتمي إلى مجموعة الوصول الكامل في AD. مجموعة مسؤولي الشبكة هي المجموعة الموجودة في AD والتي تم تعيينها إلى ملف تعريف Full-Privilege Shell ومجموعة الأمر full-access التي تم تعيينها على ACS. حاول تشغيل أي أمر لضمان حصولك على الوصول الكامل.



```
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#
```

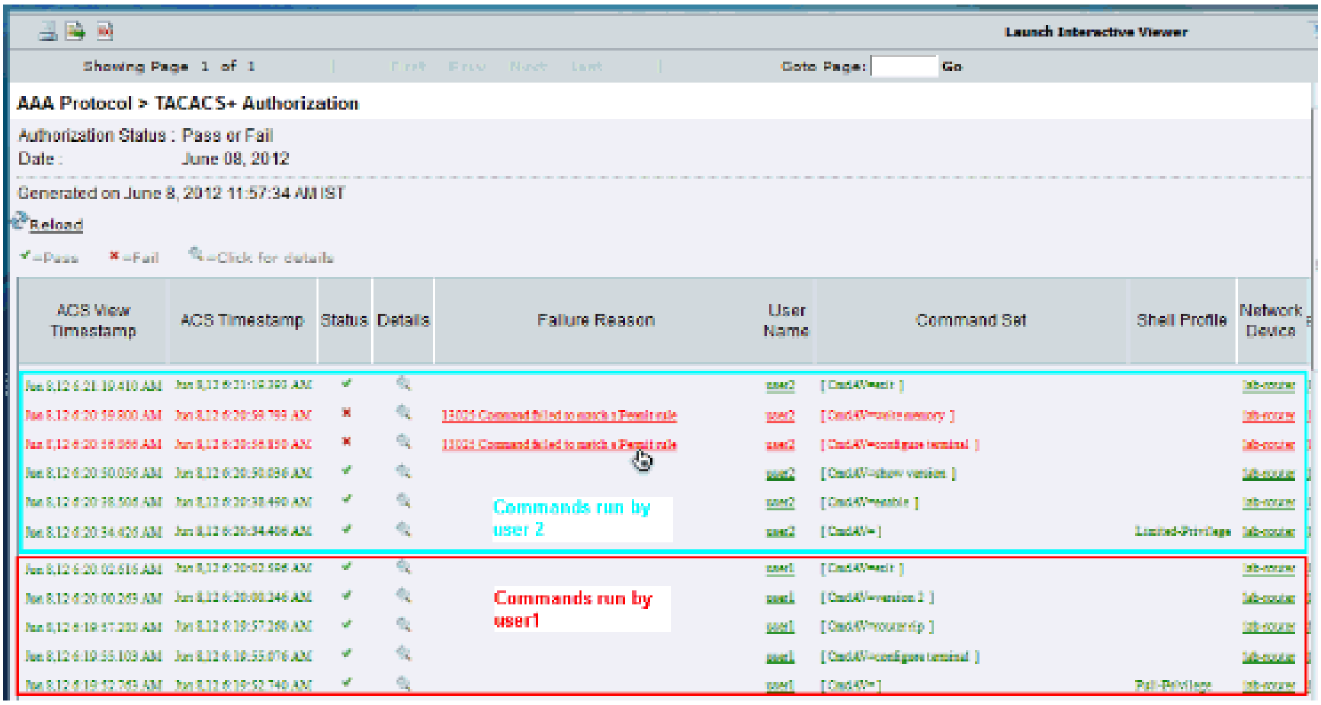
2. Telnet إلى جهاز Cisco IOS ك user2 الذي ينتمي إلى مجموعة الوصول المحدود في AD. (مجموعة فريق صيانة الشبكة هي المجموعة في AD التي يتم تعيينها على ملف تعريف Shell المحدود ومجموعة الأمر show-access على ACS). إذا حاولت تشغيل أي أمر

بخلاف الأوامر المذكورة في مجموعة الأوامر show-access، فيجب أن تحصل على أطخ فشل
تفويض الأوامر، والذي يظهر أن المستخدم2 لديه وصول محدود.



```
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
OFTWARE (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"


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/wwl/export/crypto/tool/stqrg.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#
```

قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل ACS وابدأ برنامج3.
Monitoring and Reporting Viewer. أختر بروتوكول AAA > TACACS+Authorization للتحقق
من الأنشطة التي تم تنفيذها بواسطة المستخدم1 و user2.



AAA Protocol > TACACS+ Authorization

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

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

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 6:21:19.390 AM	✓	🔍		user2	[CmdAV=exit]		lab-router
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.793 AM	✗	🔍	13025 Command failed to match a Permit rule	user2	[CmdAV=write memory]		lab-router
Jun 8,12 6:20:56.066 AM	Jun 8,12 6:20:56.050 AM	✗	🔍	13025 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=exit]		lab-router
Jun 8,12 6:20:00.263 AM	Jun 8,12 6:20:00.246 AM	✓	🔍		user1	[CmdAV=version 2]		lab-router
Jun 8,12 6:19:57.283 AM	Jun 8,12 6:19:57.260 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 6:19:52.763 AM	Jun 8,12 6:19:52.740 AM	✓	🔍		user1	[CmdAV=]	Full-Privilege	lab-router

Commands run by user 2

Commands run by user1

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).