

رم اوأال ضي وفت و TACACS+ ة ق داصم ACS 5.x: ة و م جم ة ي و ض ع ني و ك ت ل ا ث م ي ل ا ا د ا ن ت س ا ت ا ن ا ل ع ا ل ا

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[تكوين ACS 5.x للمصادقة والتفويض](#)

[تكوين جهاز Cisco IOS للمصادقة والتفويض](#)

[التحقق من الصحة](#)

[معلومات ذات صلة](#)

[المقدمة](#)

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

[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 SE6(44)12.2 من Cisco. **ملاحظة:** يمكن تنفيذ هذا التكوين على جميع أجهزة Cisco IOS.

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.](#)

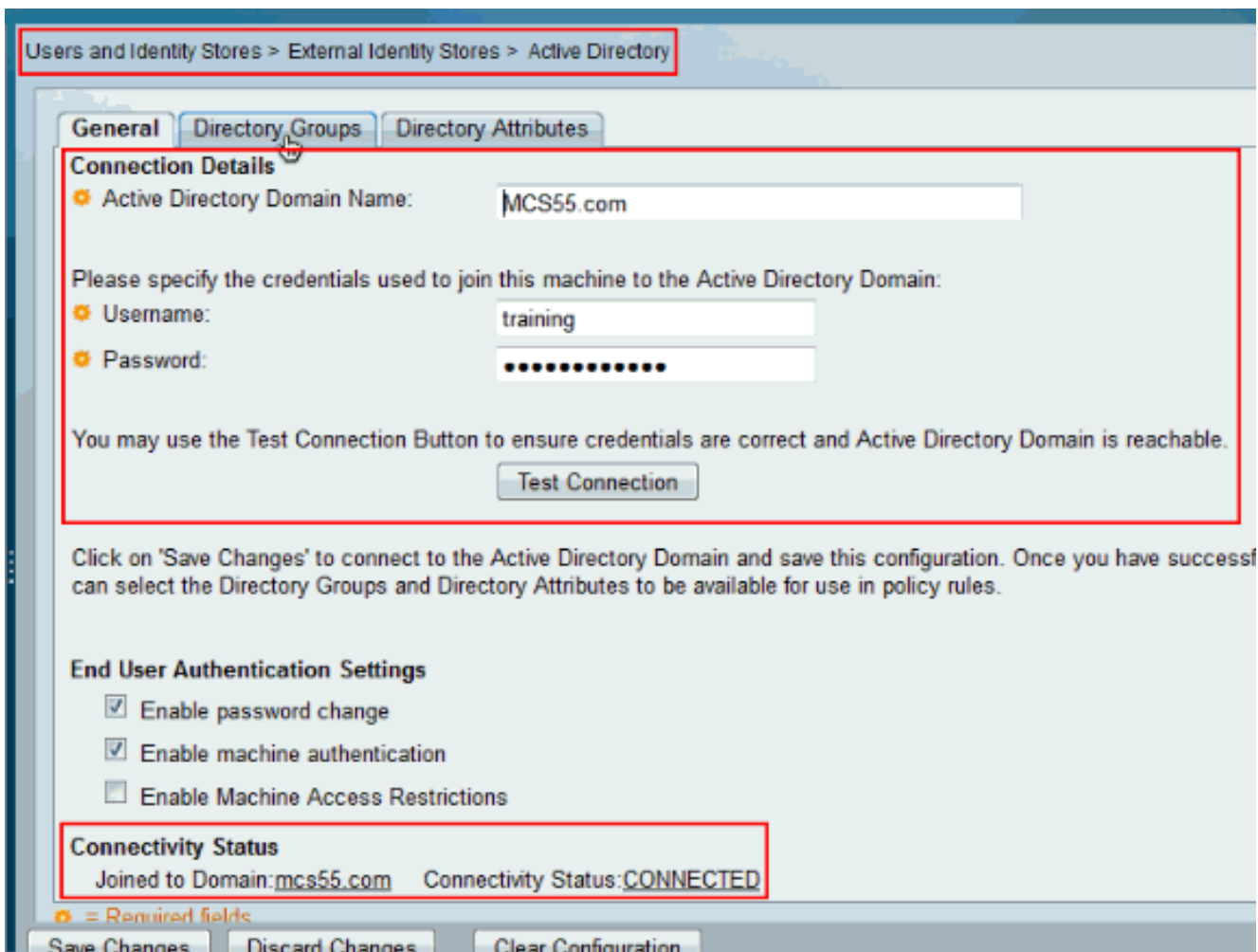
[التكوين](#)

[تكوين ACS 5.x للمصادقة والتفويض](#)

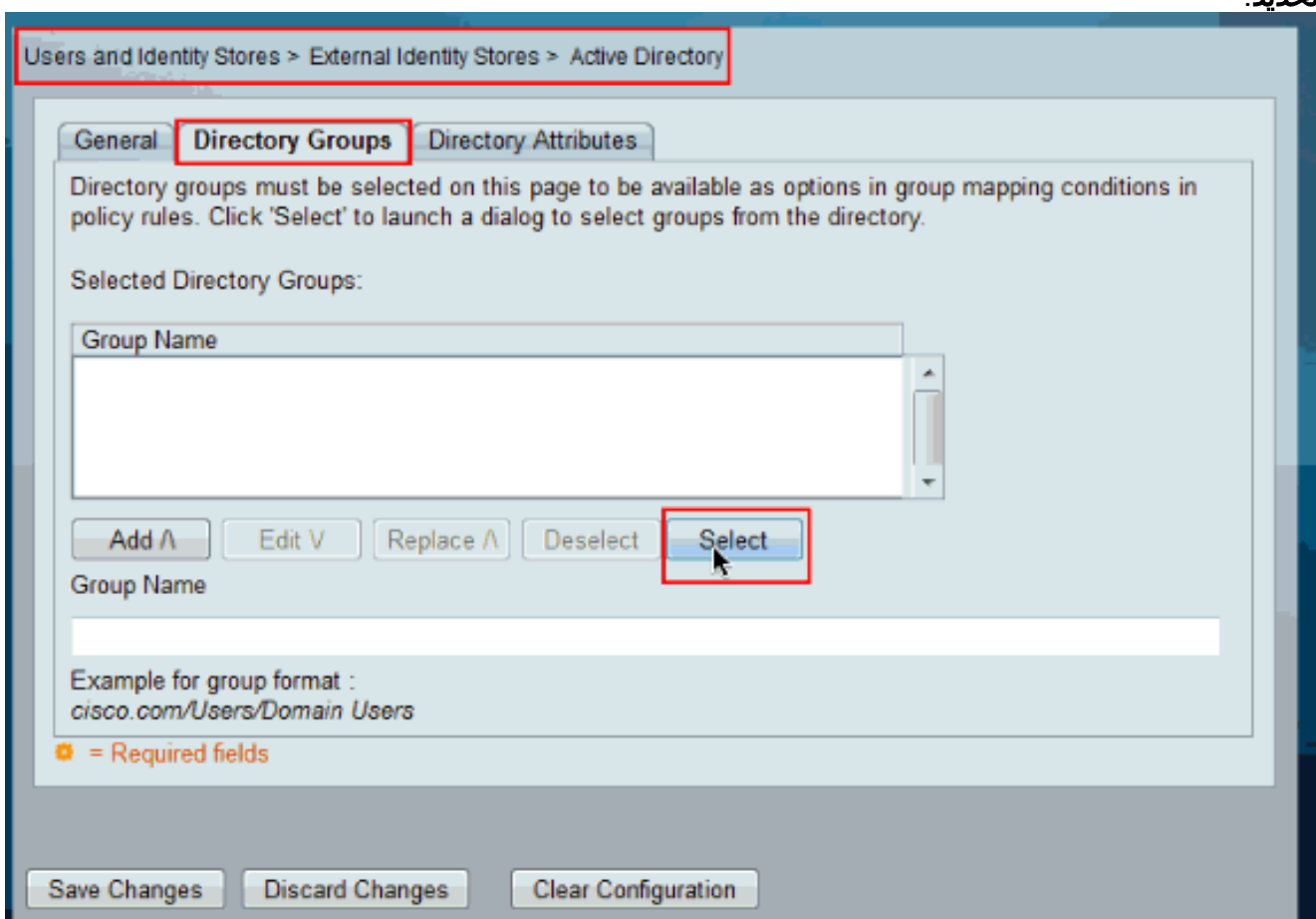
قبل البدء في تكوين ACS 5.x للمصادقة والتفويض، كان يجب دمج ACS بنجاح مع Microsoft AD. إذا لم يتم دمج ACS مع مجال AD المرغوب، ارجع إلى [ACS 5.x والإصدارات الأحدث: التكامل مع مثال تكوين Microsoft Active Directory](#) للحصول على مزيد من المعلومات لتنفيذ مهمة التكامل.

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

Group Name	Group Type
MCS55.com/Users/Domain Guests	GLOBAL
<input checked="" type="checkbox"/> MCS55.com/Users/Network Admins	GLOBAL
<input checked="" type="checkbox"/> MCS55.com/Users/Network Maintenance Team	GLOBAL
<input type="checkbox"/> 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.

5. انقر فوق **حفظ التغييرات**.

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

Buttons: Add ^, Edit V, Replace ^, Deselect, Select

Group Name: _____

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

* = Required fields

Buttons: Save Changes, Discard Changes, Clear Configuration

6. أختار 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

	<input type="checkbox"/>	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>	+	Rule-1	match Tacacs		Default Device Admin	1
2	<input type="checkbox"/>	+	Rule-2	match Radius		Default Network Access	0

7. أختار سياسات الوصول < خدمات الوصول < إدارة الجهاز الافتراضية < الهوية وانقر فوق تحديد بجوار مصدر

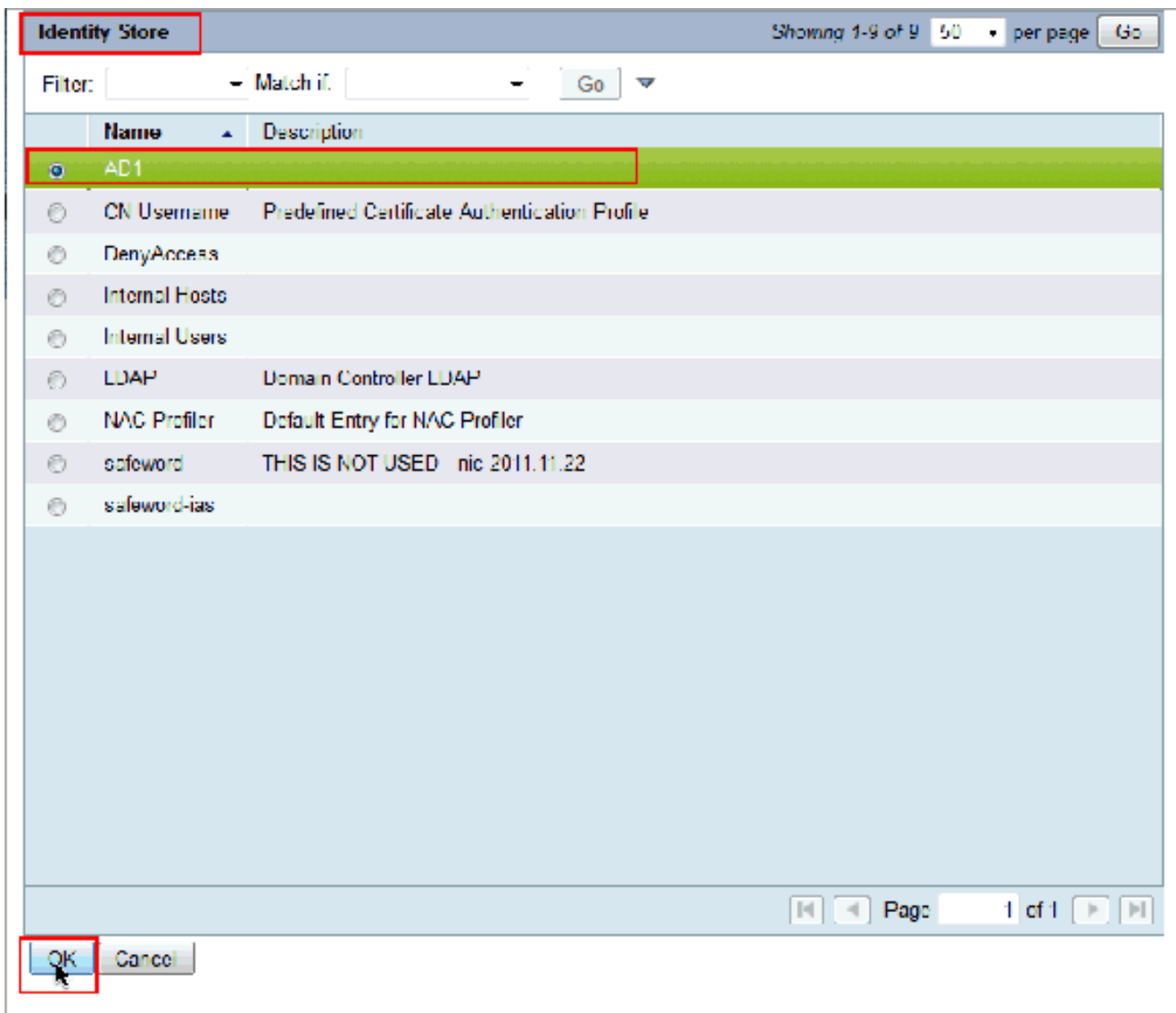
Access Policies > Access Services > Default Device Admin > Identity

Single result selection
 Rule based result selection

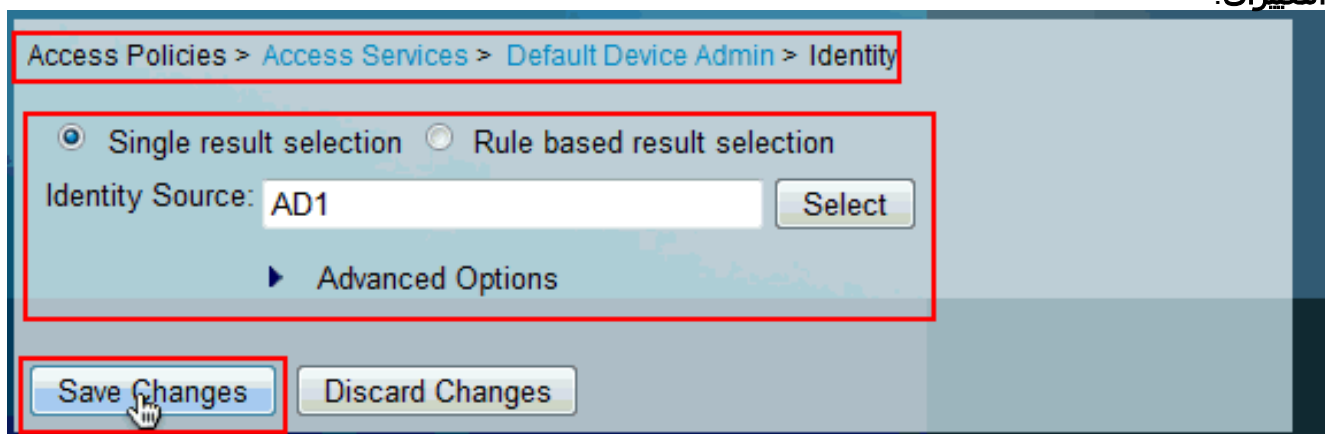
Identity Source: Internal Users

▶ Advanced Options

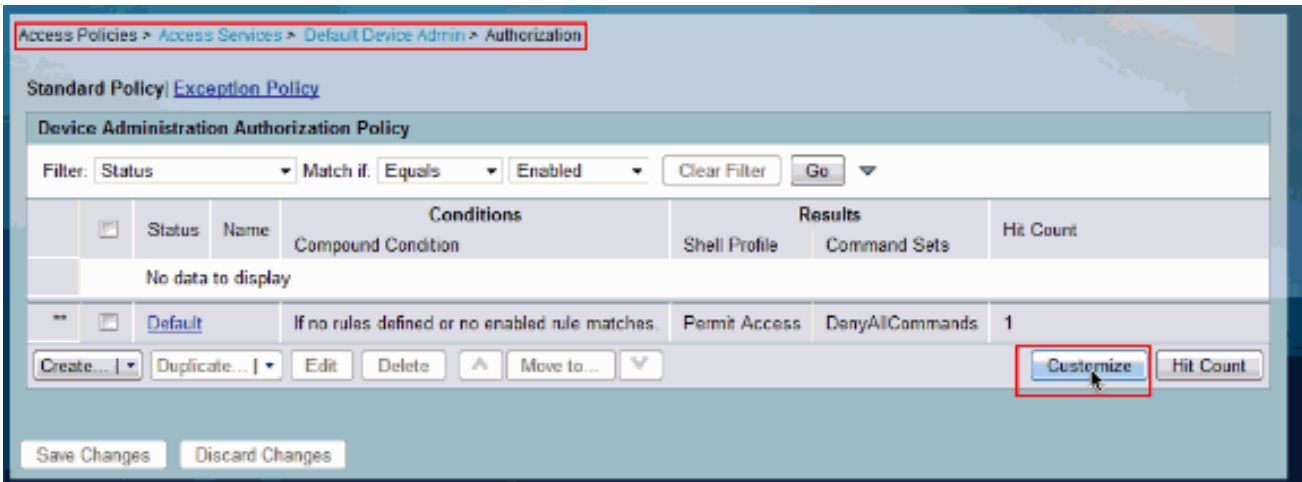
الهوية.
8. أختار AD1 وطققة
.ok



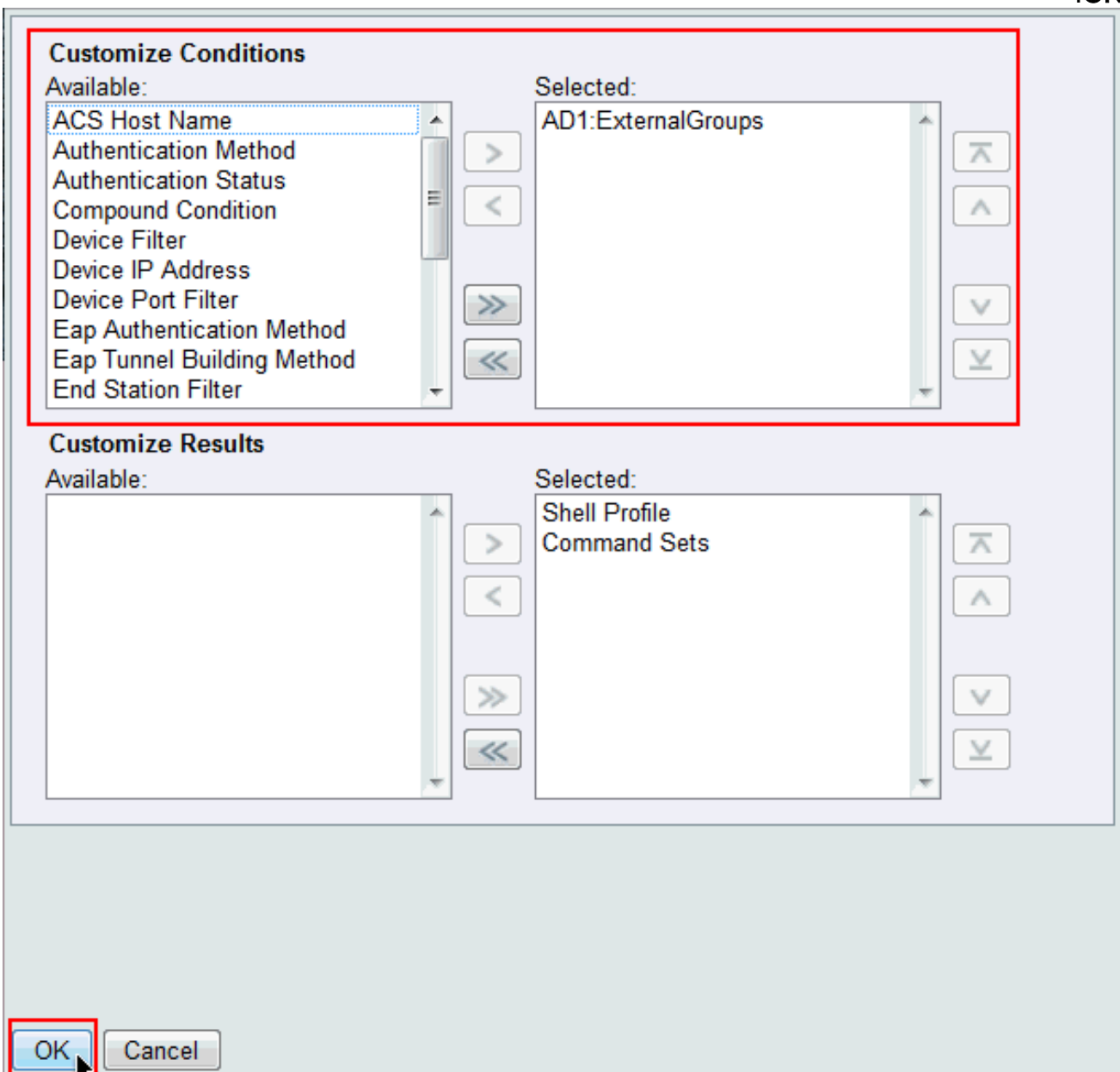
9. انقر فوق حفظ التغييرات.



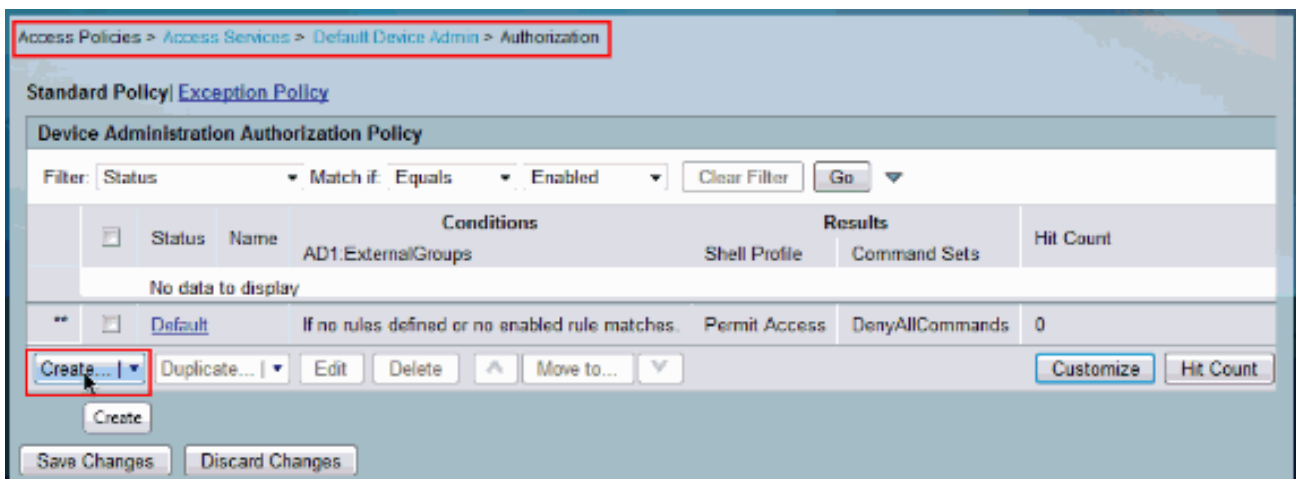
10. أختار سياسات الوصول < خدمات الوصول < إدارة الجهاز الافتراضية < التفويض وانقر فوق تخصيص.



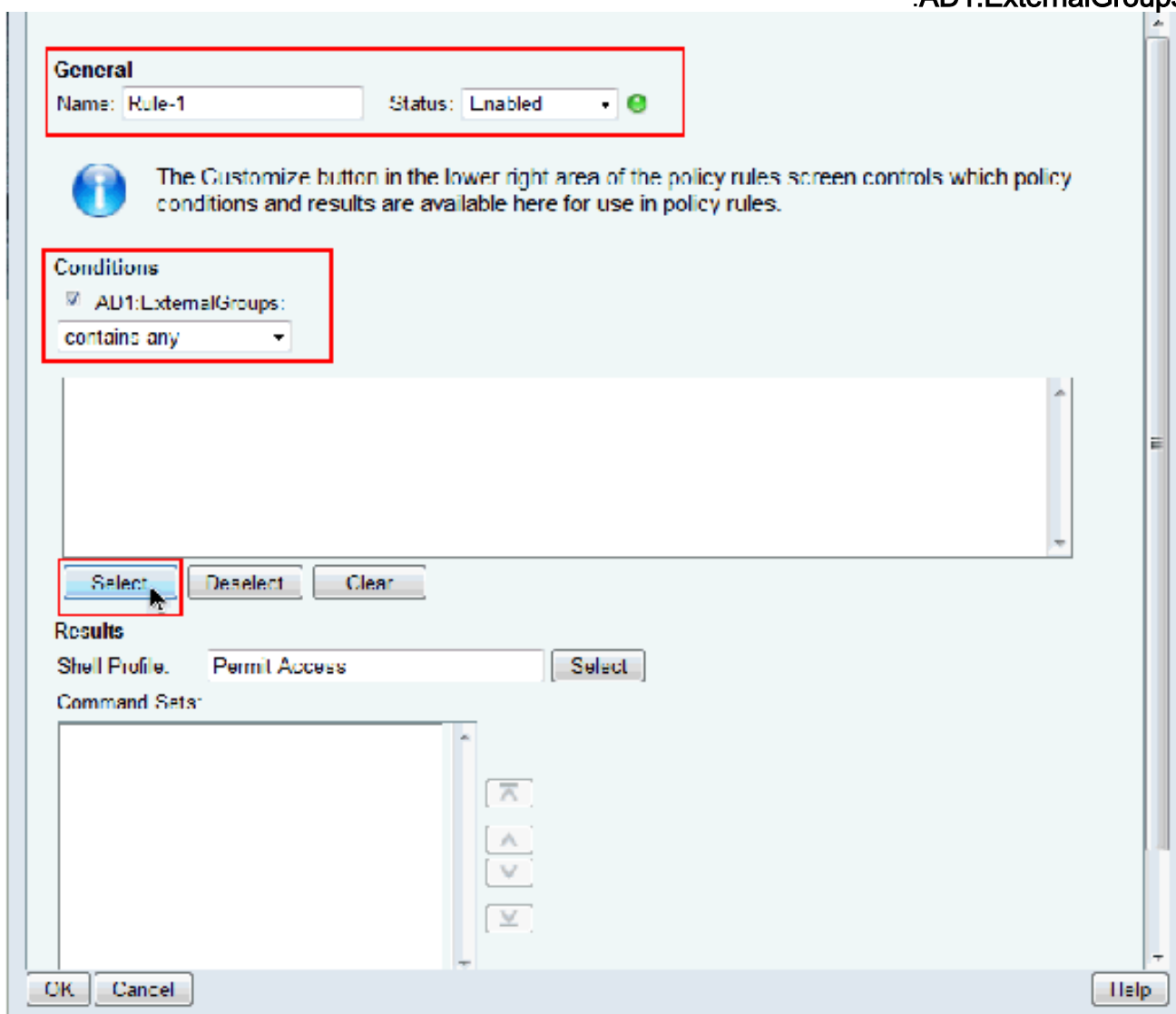
11. انسخ AD1:ExternalGroups من متاح إلى قسم محدد من شروط التخصيص ثم نقل ملف تعريف Shell ومجموعات الأوامر من متاح إلى قسم تخصيص النتائج. وانقر الآن فوق **OK**.



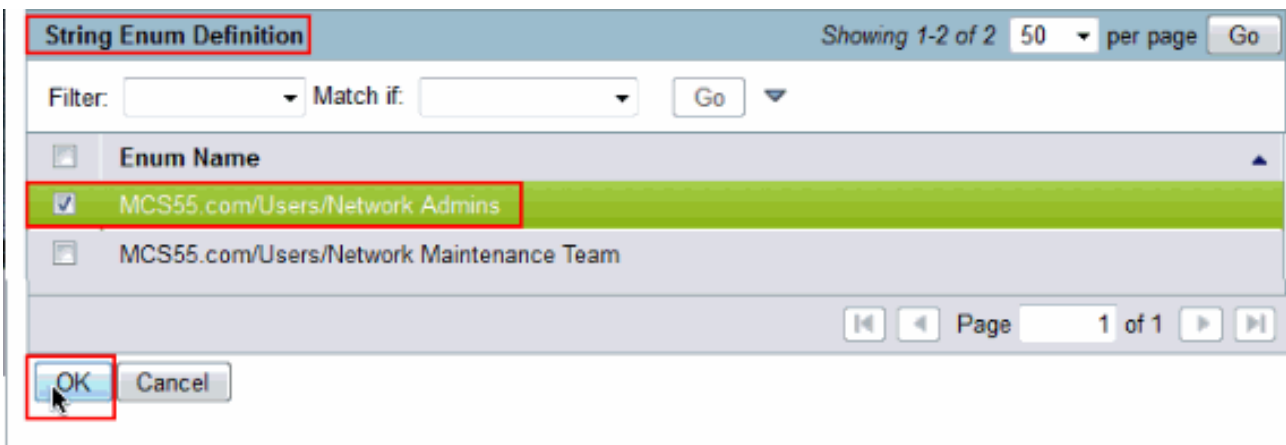
12. انقر فوق **إنشاء** لإنشاء قاعدة جديدة.



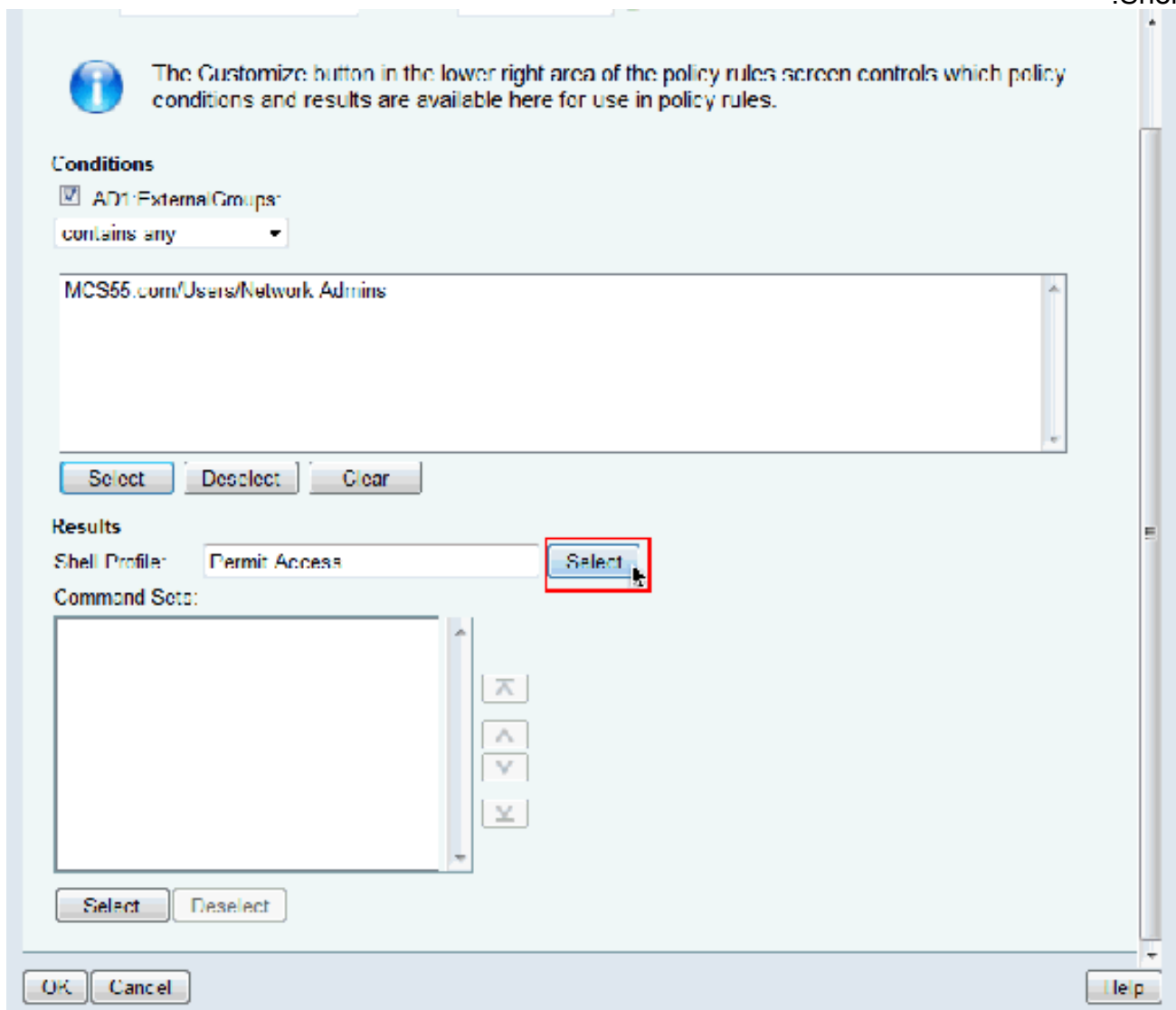
13. انقر على تحديد في حالة
.AD1:ExternalGroups



14. أختار 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.

Shell Profiles Showing 1-2 of 2 50 per page Go

Filter: Match if: Go

Name	Description
<input type="radio"/> DenyAccess	
<input type="radio"/> Permit Access	

Create Duplicate Edit Delete Page 1 of 1

OK Cancel Help

17. قم بتوفير اسم ووصف (إختياري) في علامة التبويب "عام" وانقر فوق علامة التبويب مهم

General Common Tasks Custom Attributes

Name: Full-Privilege

Description: To push default privilege 15 for IOS

⚙ = Required fields

18. غيرت التقصير امتياز والحد الأقصى امتياز إلى ساكن إستاتيكي مع القيمة 15. انقر على إرسال.

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

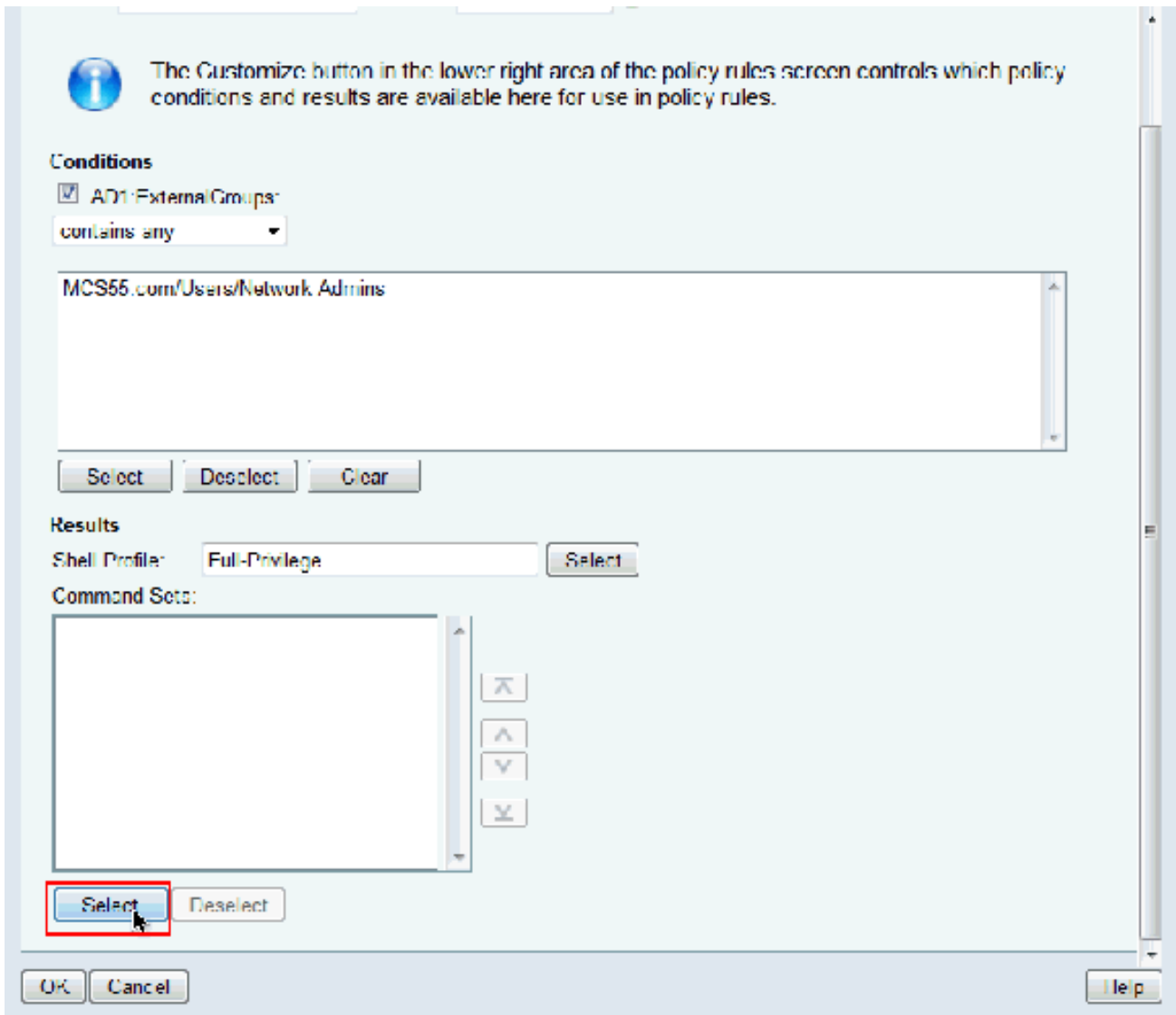
19. أختار الآن ملف تعريف Shell للوصول الكامل الذي تم إنشاؤه حديثاً (امتياز كامل في هذا المثال) وانقر موافق.

Shell Profiles

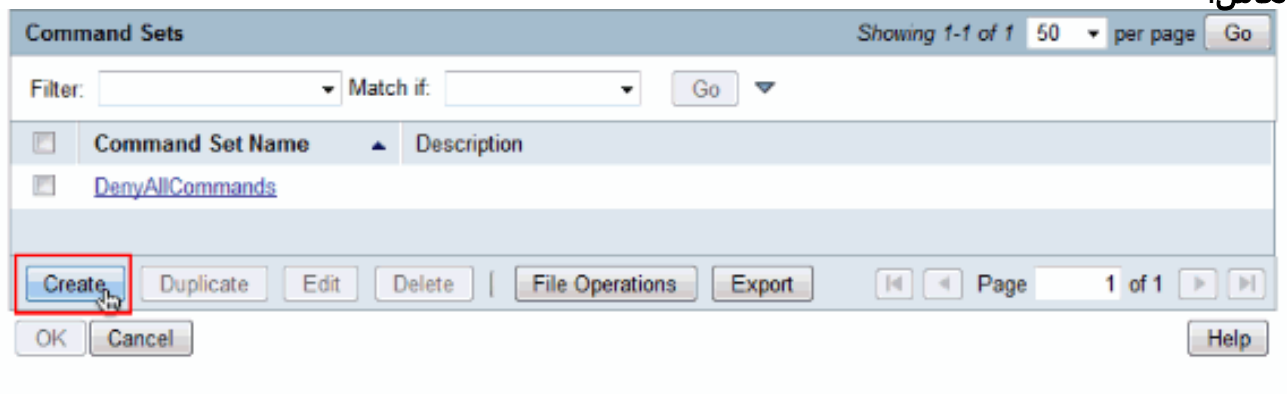
Filter: Match if:

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. 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.

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:

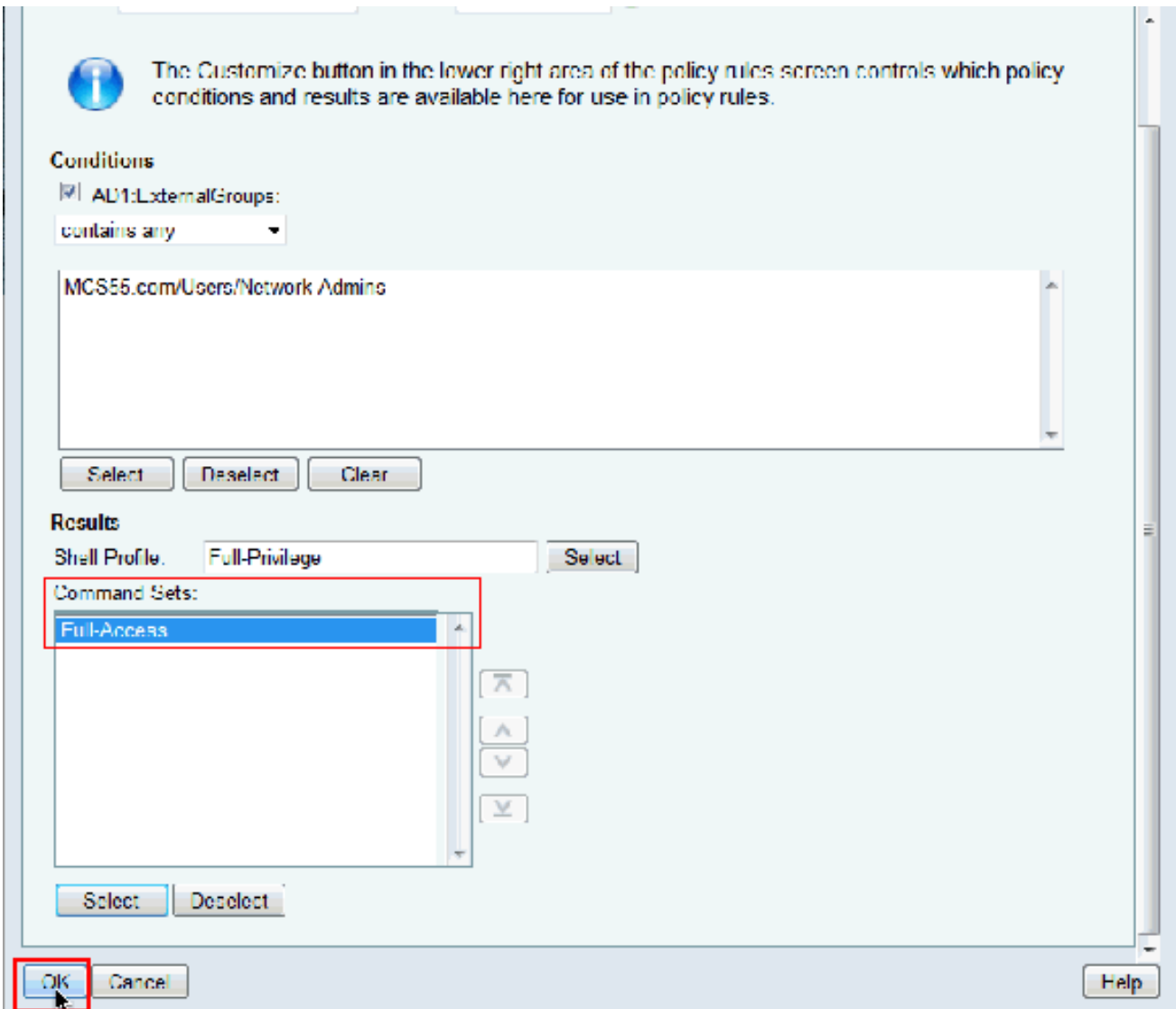
23. وانقر فوق
.OK

Command Sets

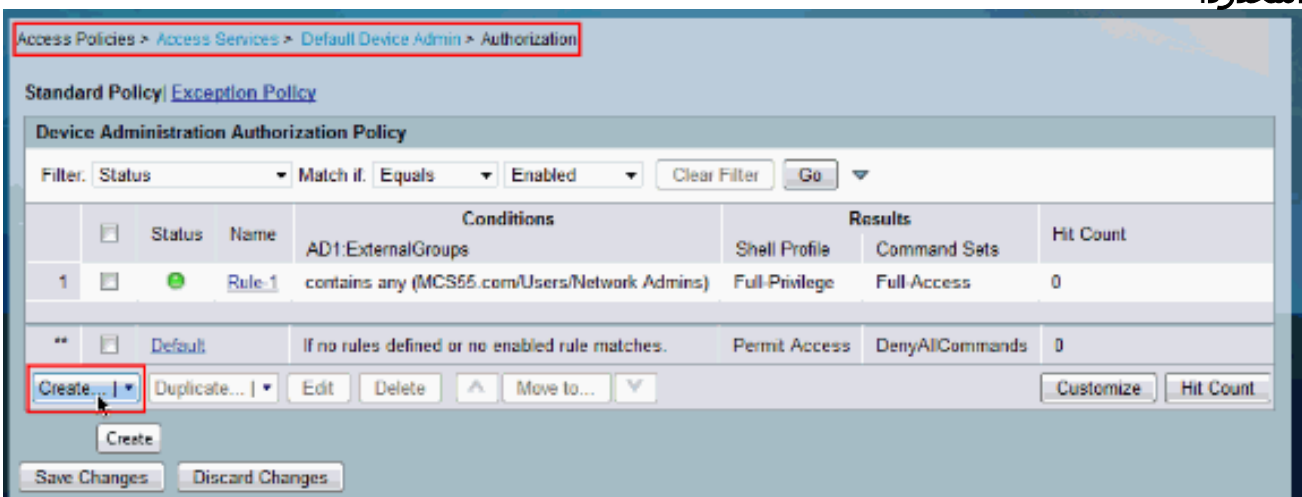
Filter: Match if:

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


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




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



26. أختار AD1:ExternalGroups وانقر تحديد.

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:

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

String Enum Definition

Filter: Match if:

<input type="checkbox"/>	Enum Name
<input type="checkbox"/>	MCS55.com/Users/Network Admins
<input checked="" type="checkbox"/>	MCS55.com/Users/Network Maintenance Team

28. انقر على تحديد في حقل ملف تعريف .Shell



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

Select

Deselect

Clear

Results

Shell Profile: Permit Access

Select

Command Sets:

Select

Deselect

OK

Cancel

Help

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

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

General **Common Tasks** **Custom Attributes**

31. غيرت التقصير امتياز و الأقصى امتياز إلى ساكن إستاتيكي مع قيمة 1 و 15 على التوالي. انقر على

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

إرسال

32. وانقر فوق

Shell Profiles

Filter: Match if:

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. 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

Select

Deselect

Clear

Results

Shell Profile: Limited-Privilege

Select

Command Sets:

Select

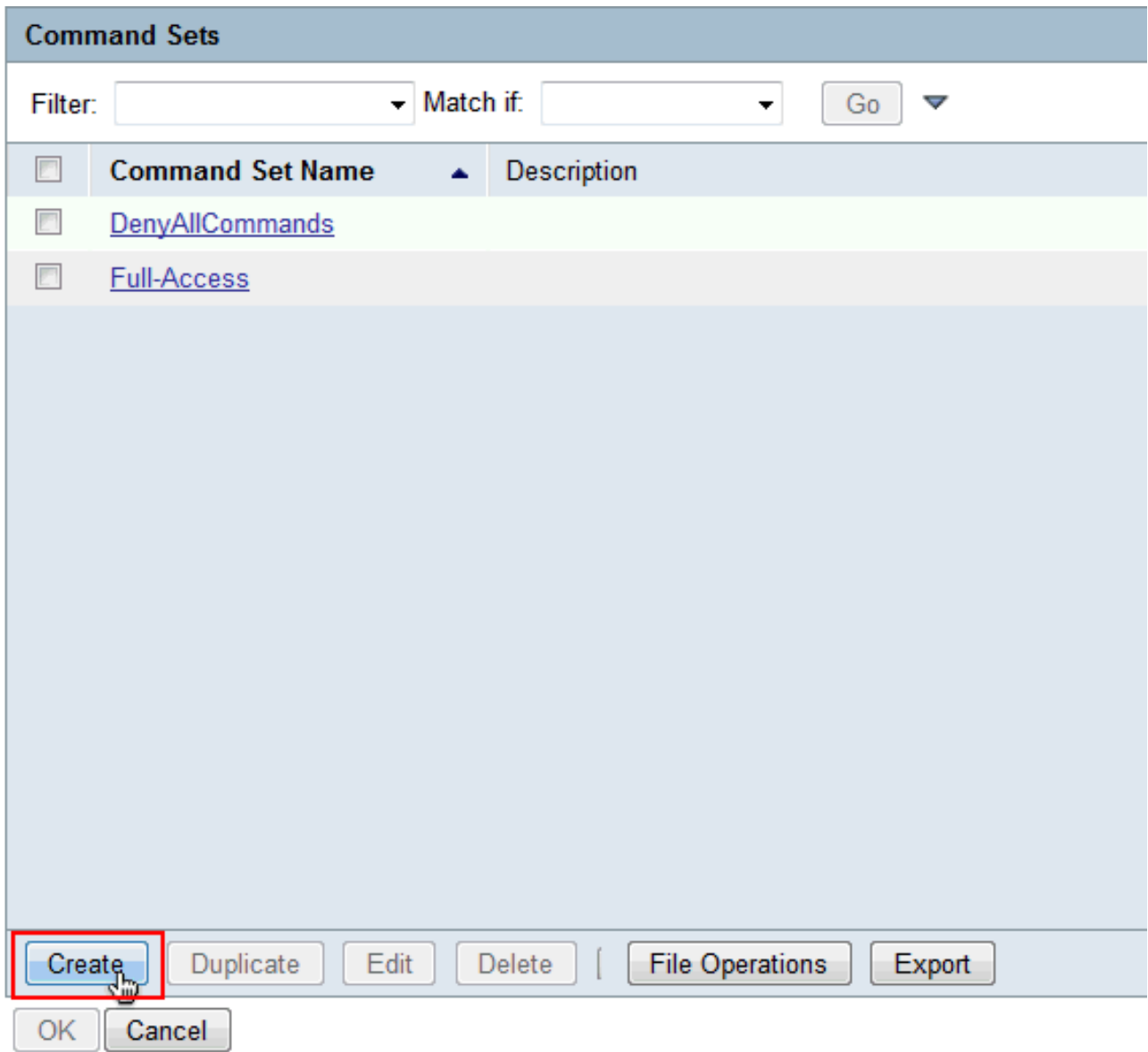
Deselect

OK

Cancel

Help

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.

General

Name: Show-Access

Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Add ^

Edit V

Replace ^

Delete

Grant

Command

Arguments

Permit

show

Select Command/Arguments from Command Set:

DenyAllCommands

Select

Submit

Cancel

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:

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. وانقر فوق
.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. وانقر فوق
.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. انقر فوق حفظ
التغييرات.

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

	Status	Name	Conditions	Shell Profile	Command Sets	Hit Count
1	<input type="checkbox"/>	Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0
2	<input type="checkbox"/>	Rule-2	contains any (MCS55.com/Users/Network Maintenance Team)	Limited-Privilege	Show-Access	0
**	<input type="checkbox"/>	Default	If no rules defined or no enabled rule matches	Permit Access	DenyAllCommands	0

Create... Duplicate... Edit Delete Move to... Customize Hit Count

Save Changes Discard Changes

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

Network Resources > Network Devices and AAA Clients

Network Devices

Filter: IP Address Match if: Equals 192.168.26.7 Clear Filter Go

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

Create Duplicate Edit Delete File Operations Export

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

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)
 TACACS+

IP: 192.168.26.7

Authentication Options

Shared Secret: Show

Single Connect Device
 Legacy TACACS+ Single Connect Support
 TACACS+ Draft Compliant Single Connect Support

RADIUS

Shared Secret: Show

CaA port: 1700

Submit Cancel

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
```

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 استخدم 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 استخدام 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 كمستخدم 1 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 خطأ والذي يظهر أن المستخدم 2 لديه وصول

```

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 (rc1)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text base: 0x0D0030C0, data base: 0x00EA3DE8

ROM: Bootstrap program is C3550 boot loader

router1 uptime is 16 hours, 45 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/ww1/export/cryptolocal/stiprg.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#

```

3. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) لـ ACS وابدأ برنامج Monitoring and Reporting Viewer. اختر بروتوكول AAA > TACACS+Authorization للتحقق من الأنشطة التي تم تنفيذها بواسطة المستخدم 1 و .user2

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Launch Interactive Viewer

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	[Cmd4V=exit]		lab-router
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.793 AM	✗		11021 Command failed to match a Privilege	user2	[Cmd4V=write memory]		lab-router
Jun 8,12 6:20:59.888 AM	Jun 8,12 6:20:59.870 AM	✗		11021 Command failed to match a Privilege	user2	[Cmd4V=configure terminal]		lab-router
Jun 8,12 6:20:50.036 AM	Jun 8,12 6:20:50.036 AM	✓			user2	[Cmd4V=show version]		lab-router
Jun 8,12 6:20:38.506 AM	Jun 8,12 6:20:38.490 AM	✓			user2	[Cmd4V=enable]		lab-router
Jun 8,12 6:20:34.426 AM	Jun 8,12 6:20:34.406 AM	✓			user2	[Cmd4V=]	Limited-Privilege	lab-router
Jun 8,12 6:20:02.616 AM	Jun 8,12 6:20:02.596 AM	✓			user1	[Cmd4V=exit]		lab-router
Jun 8,12 6:20:00.265 AM	Jun 8,12 6:20:00.246 AM	✓			user1	[Cmd4V=version 2]		lab-router
Jun 8,12 6:19:57.203 AM	Jun 8,12 6:19:57.180 AM	✓			user1	[Cmd4V=router rip]		lab-router
Jun 8,12 6:19:55.103 AM	Jun 8,12 6:19:55.076 AM	✓			user1	[Cmd4V=configure terminal]		lab-router
Jun 8,12 6:19:52.793 AM	Jun 8,12 6:19:52.740 AM	✓			user1	[Cmd4V=]	Full-Privilege	lab-router

معلومات ذات صلة

- [نظام التحكم في الوصول الآمن من CISCO](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنل دن تسمل