

ACS 5.x:ADグループメンバーシップに基づくTACACS+認証およびコマンド認可の設定例

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[コンフィギュレーション](#)

[認証および認可のためのACS 5.xの設定](#)

[認証および認可のためのCisco IOSデバイスの設定](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Access Control System(ACS)5.x以降を使用するユーザのADグループメンバーシップに基づくTACACS+認証およびコマンド認可の設定例を紹介します。ACSは外部IDストアとしてユーザ、マシン、グループ、および属性を保存するためにMicrosoft Active Directory (AD)を使用します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ACS 5.xは、目的のADドメインに完全に統合されています。ACSが必要なADドメインと統合されていない場合、統合タスクを実行するための詳細については、『[ACS 5.x以降 : Microsoft Active Directoryとの統合の設定例](#)』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure ACS 5.3
- Cisco IOS®ソフトウェアリリース12.2(44)SE6。

注：この設定は、すべてのCisco IOSデバイスで実行できます。

- Microsoft Windows Server 2003 ドメイン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

コンフィギュレーション

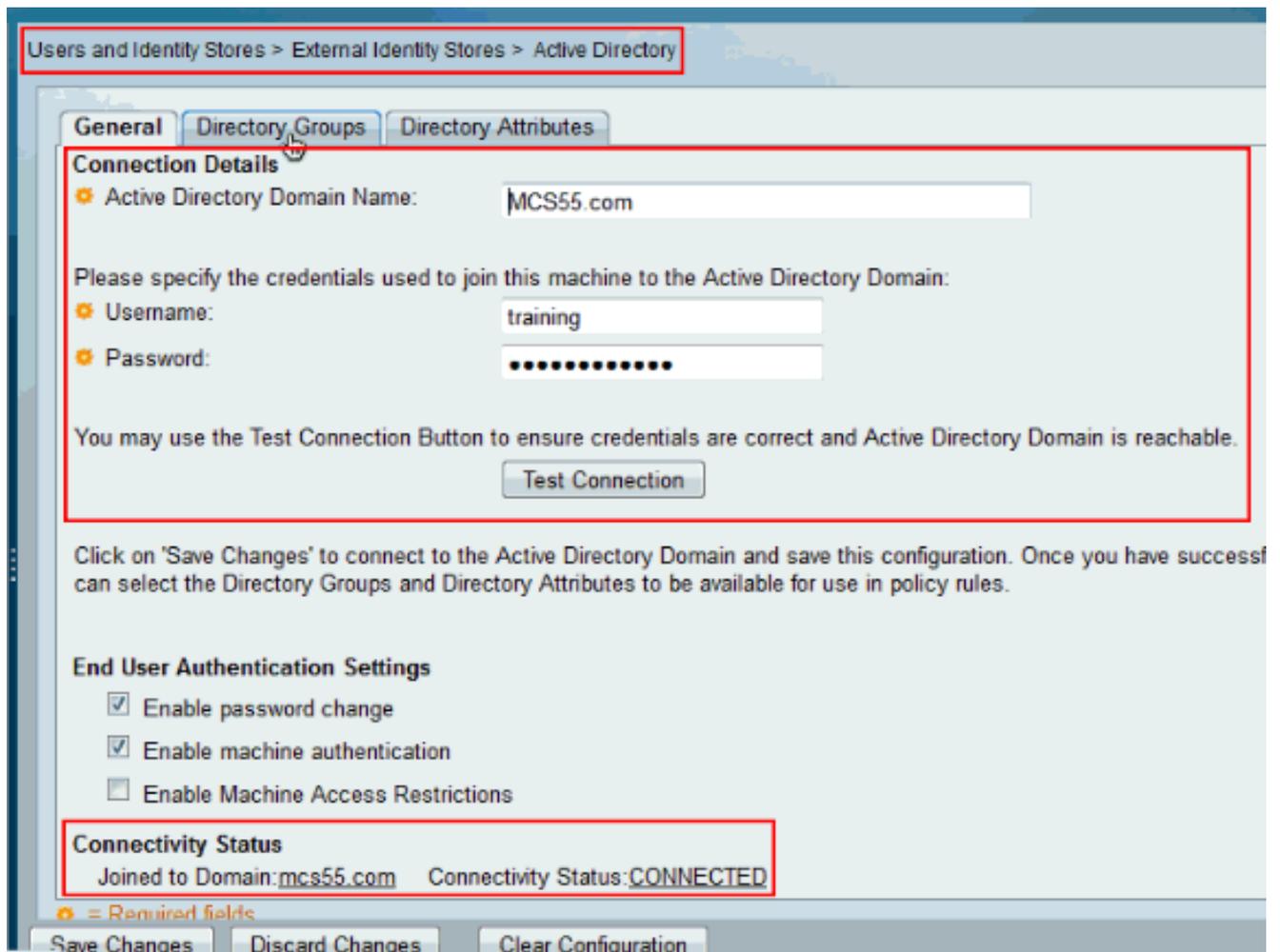
認証および認可のためのACS 5.xの設定

認証と認可のためのACS 5.xの設定を開始する前に、ACSはMicrosoft ADと正常に統合されている必要があります。ACSが必要なADドメインと統合されていない場合、統合タスクを実行するための詳細については、『[ACS 5.x以降：Microsoft Active Directoryとの統合の設定例](#)』を参照してください。

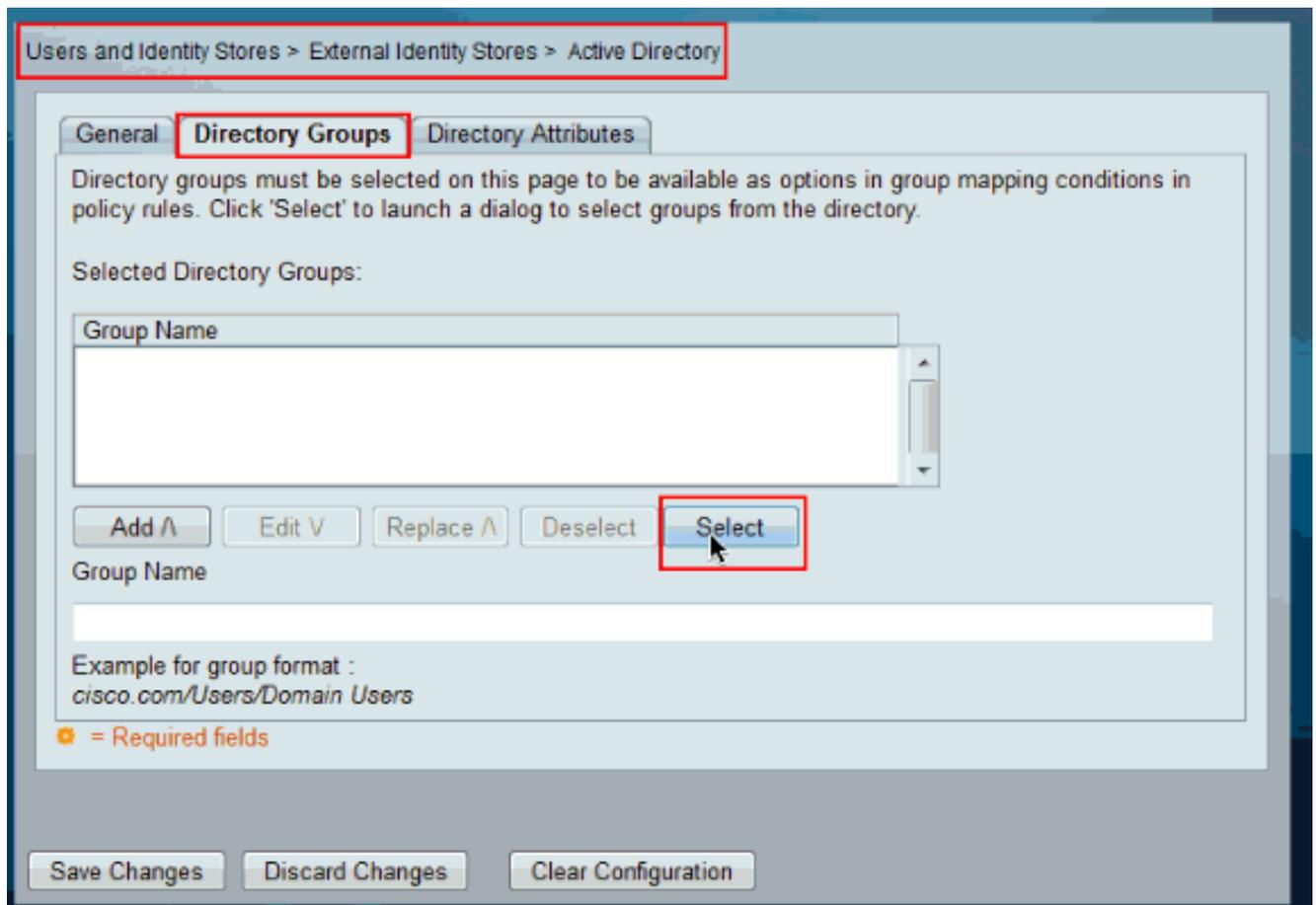
このセクションでは、2つのADグループを、2つの異なるコマンドセットと2つのシェルスクリプトファイルにマッピングします。一方はフルアクセスを使用し、もう一方はCisco IOSデバイス上で制限付きアクセスを使用します。

1. 管理者クレデンシャルを使用してACS GUIにログインします。
2. Users and Identity Stores > External Identity Stores > Active Directoryの順に選択し、ACSが目的のドメインに参加していること、および接続ステータスがconnectedと表示されていることを確認します。

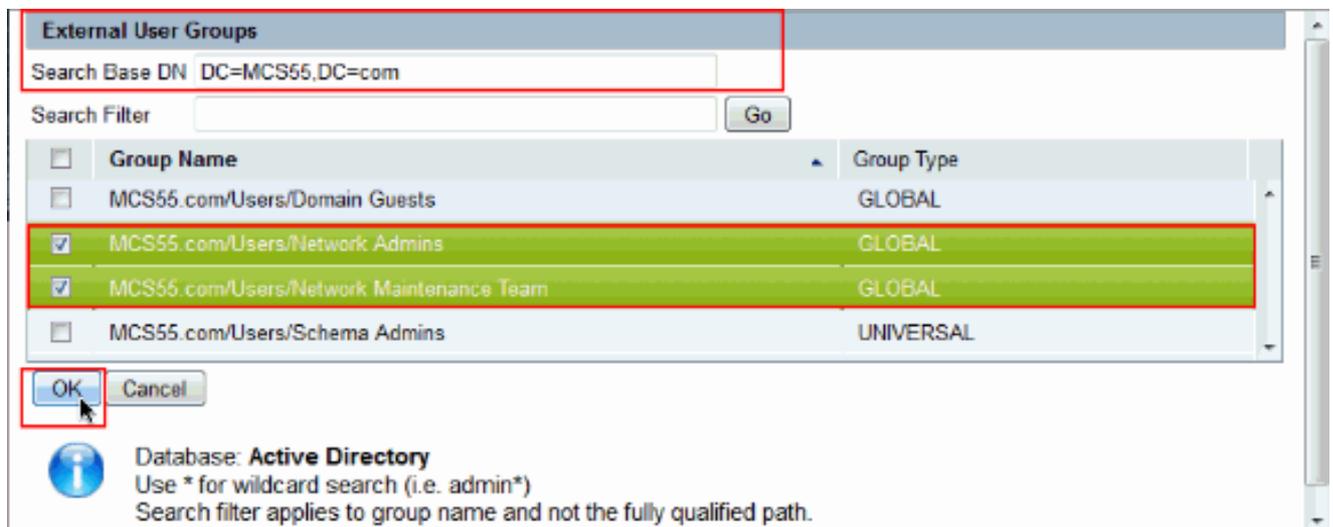
Directory Groupsタブをクリックします。



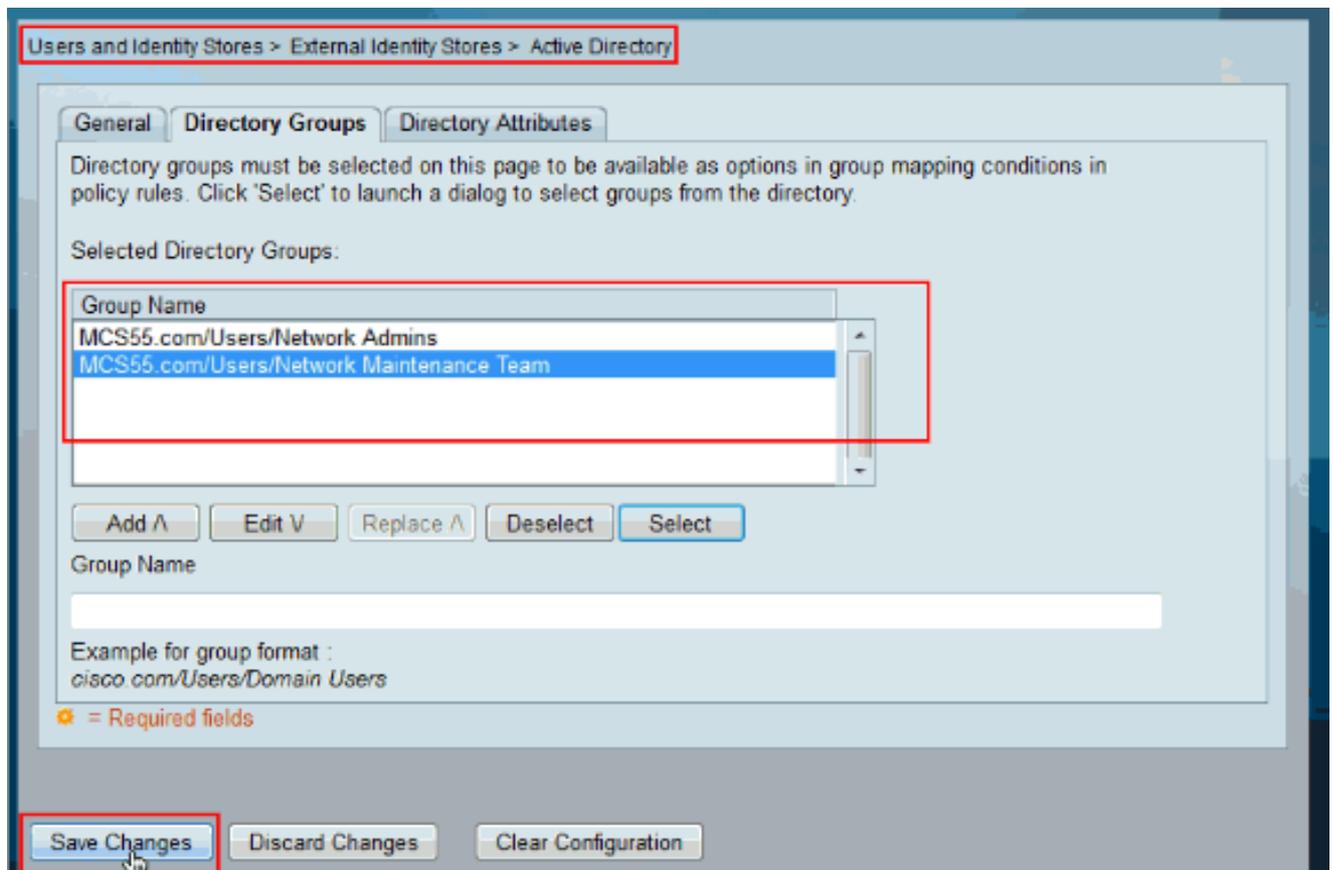
3. [Select] をクリックします。



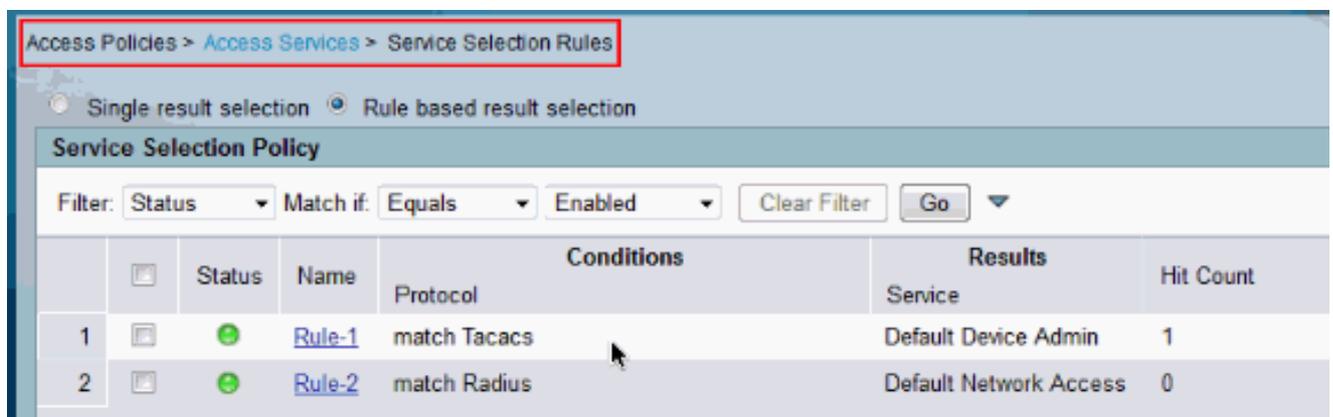
4. 設定の後半で、シェルスプロファイルとコマンドセットにマッピングする必要があるグループを選択します。[OK] をクリックします。



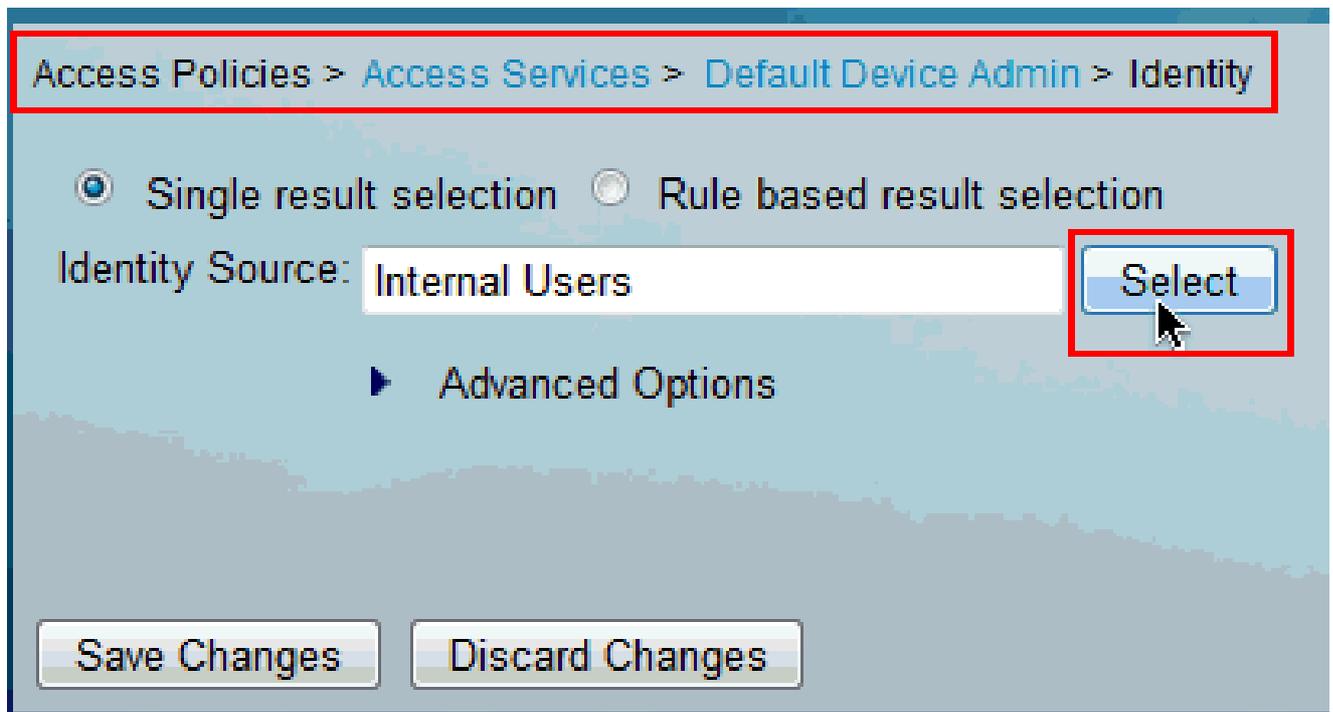
5. [Save Changes] をクリックします。



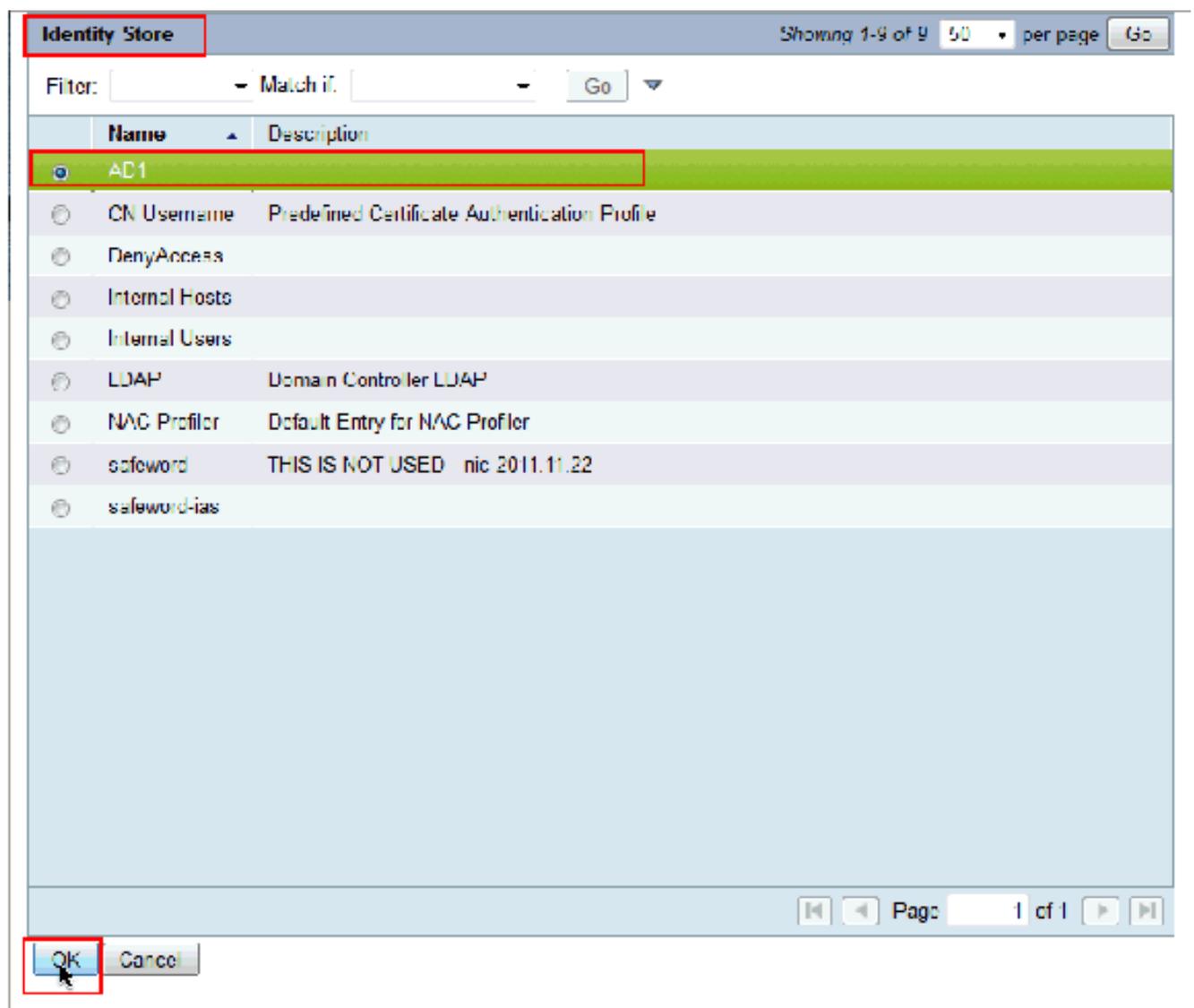
6. Access Policies > Access Services > Service Selection Rulesの順に選択し、TACACS+認証を処理するアクセスサービスを識別します。この例では、Default Device Adminです。



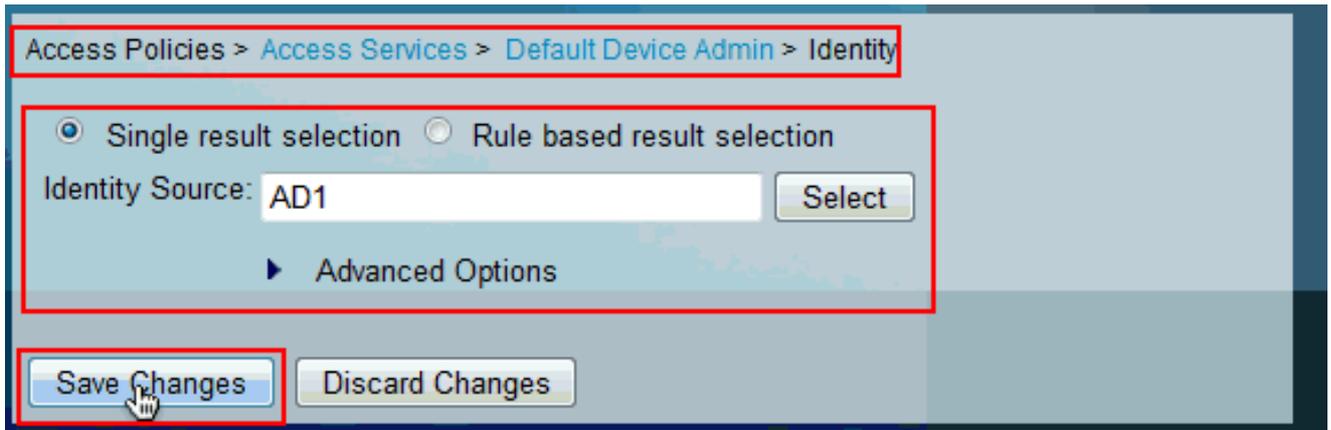
7. Access Policies > Access Services > Default Device Admin > Identityの順に選択し、Identity Sourceの横にあるSelectをクリックします。



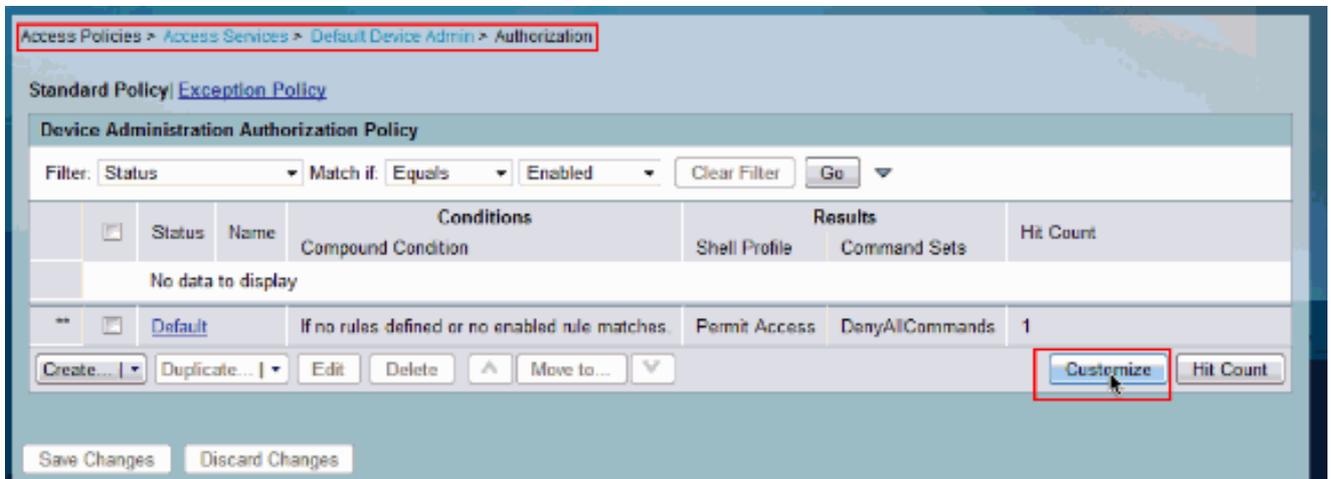
8. [AD1] を選択し、[OK] をクリックします。



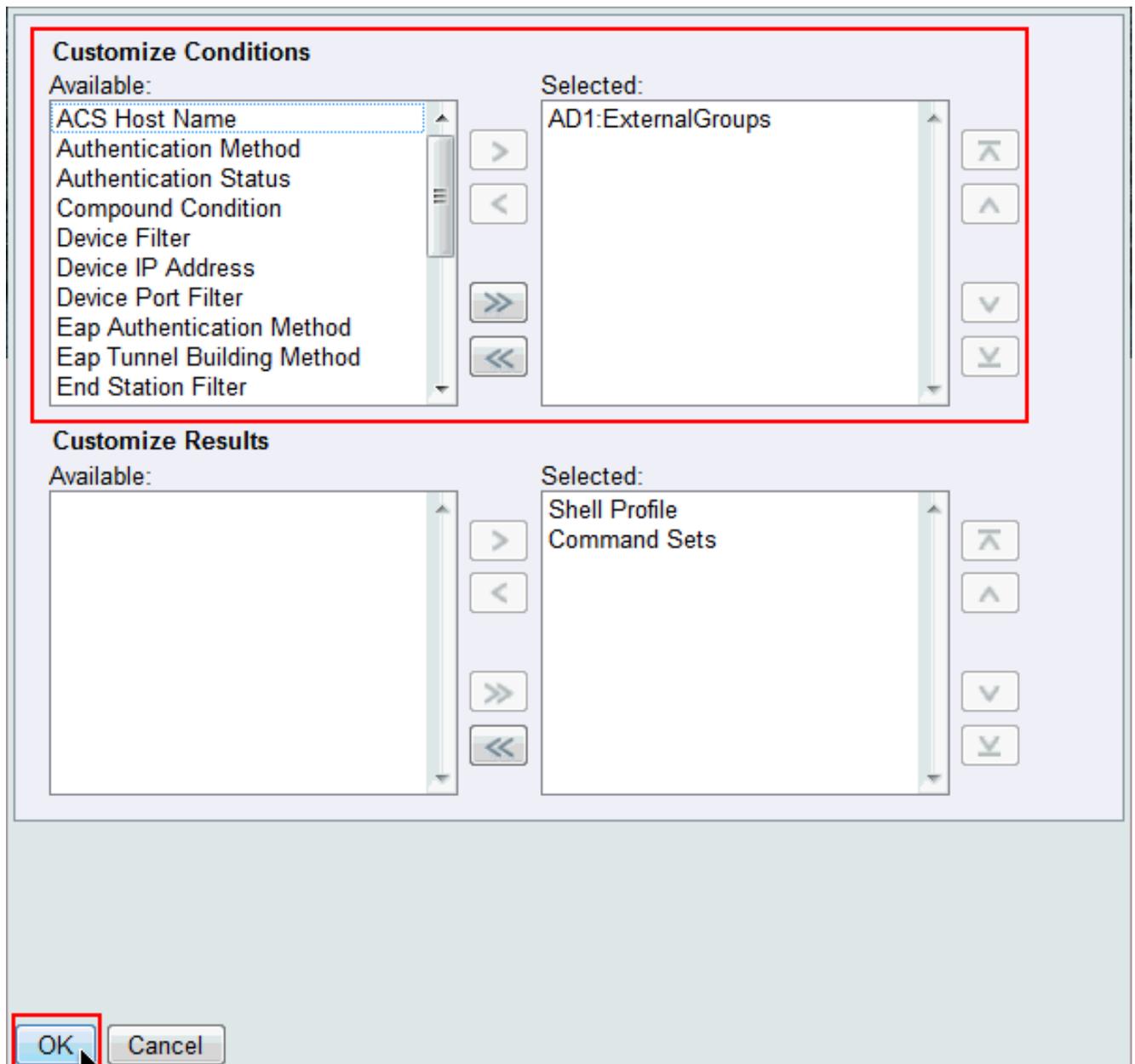
9. [Save Changes] をクリックします。



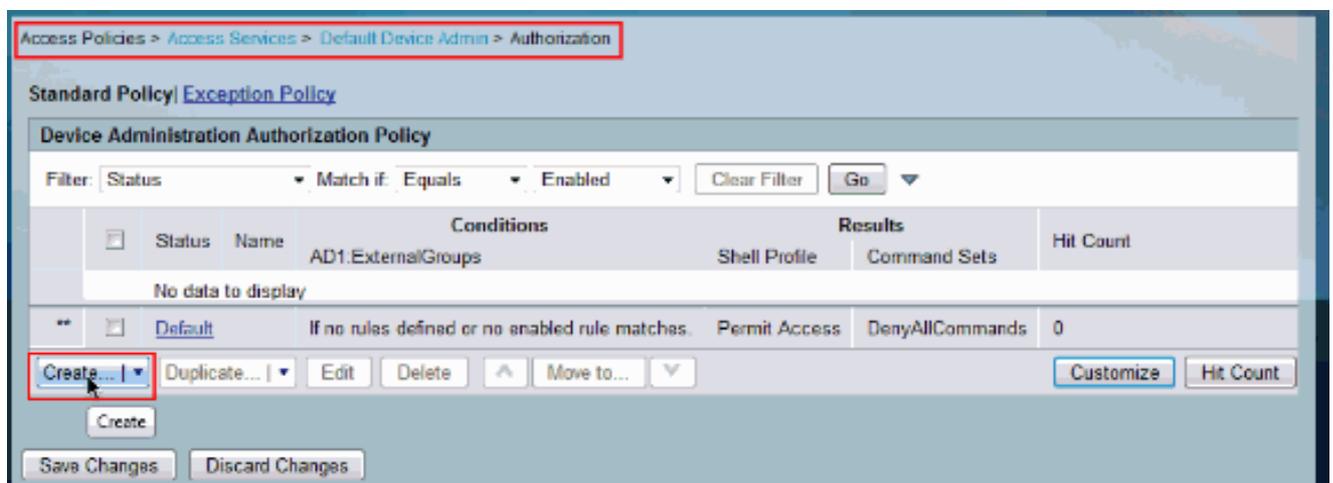
10. Access Policies > Access Services > Default Device Admin > Authorizationの順に選択し、Customizeをクリックします。



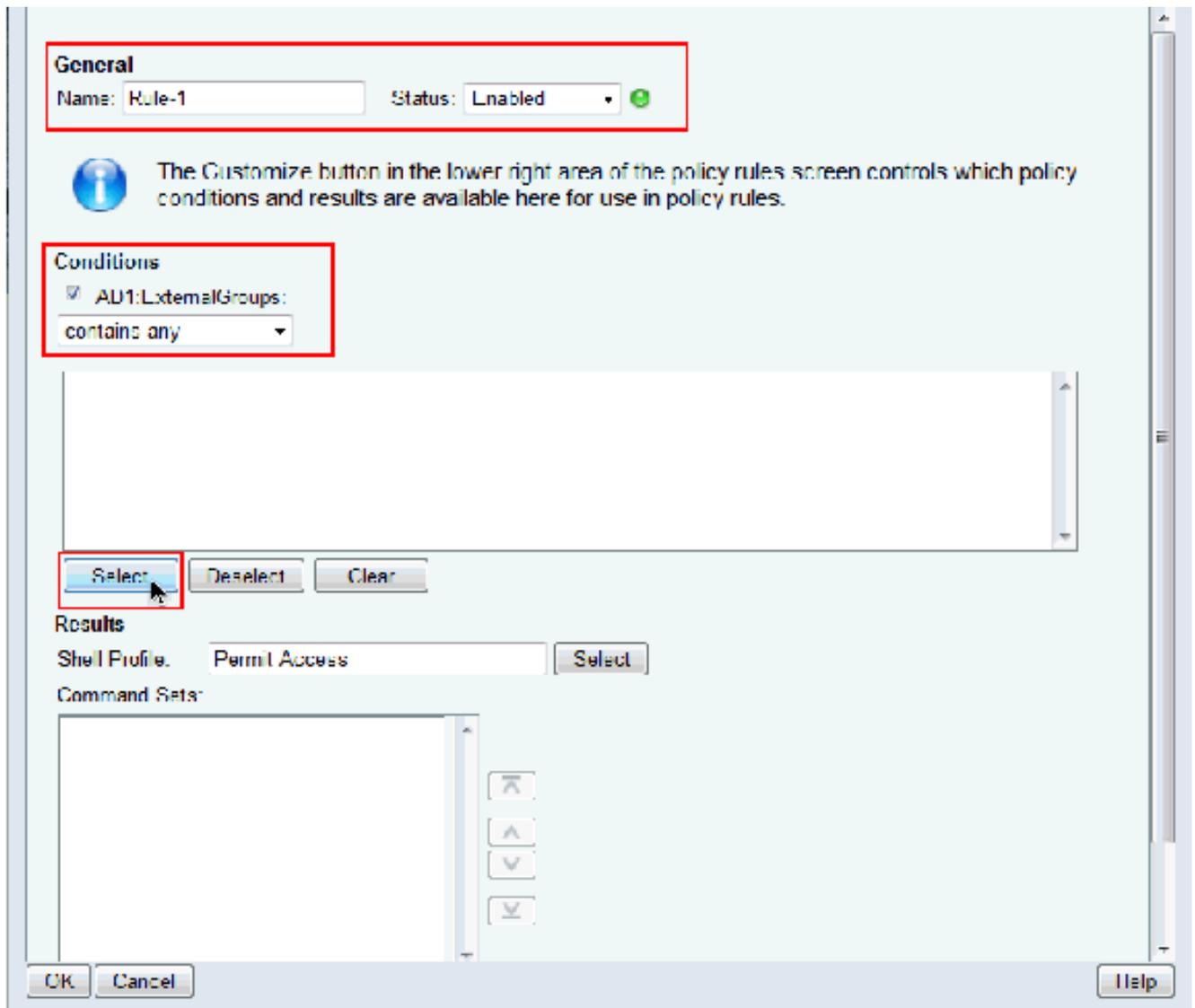
11. AD1:ExternalGroupsをAvailableから Customize ConditionsのSelectedセクションにコピーし、次にシエルプロファイルとコマンドセットをCustomize ResultsのAvailableから Selectedセクションに移動します。ここで、[OK] をクリックします。



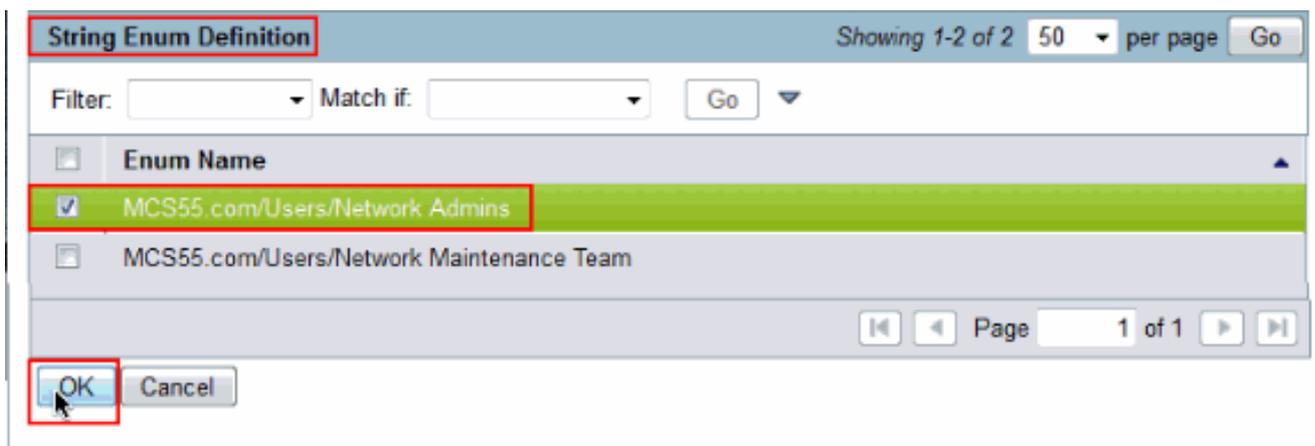
12. 新しいルールを作成するには、[Create] をクリックします。



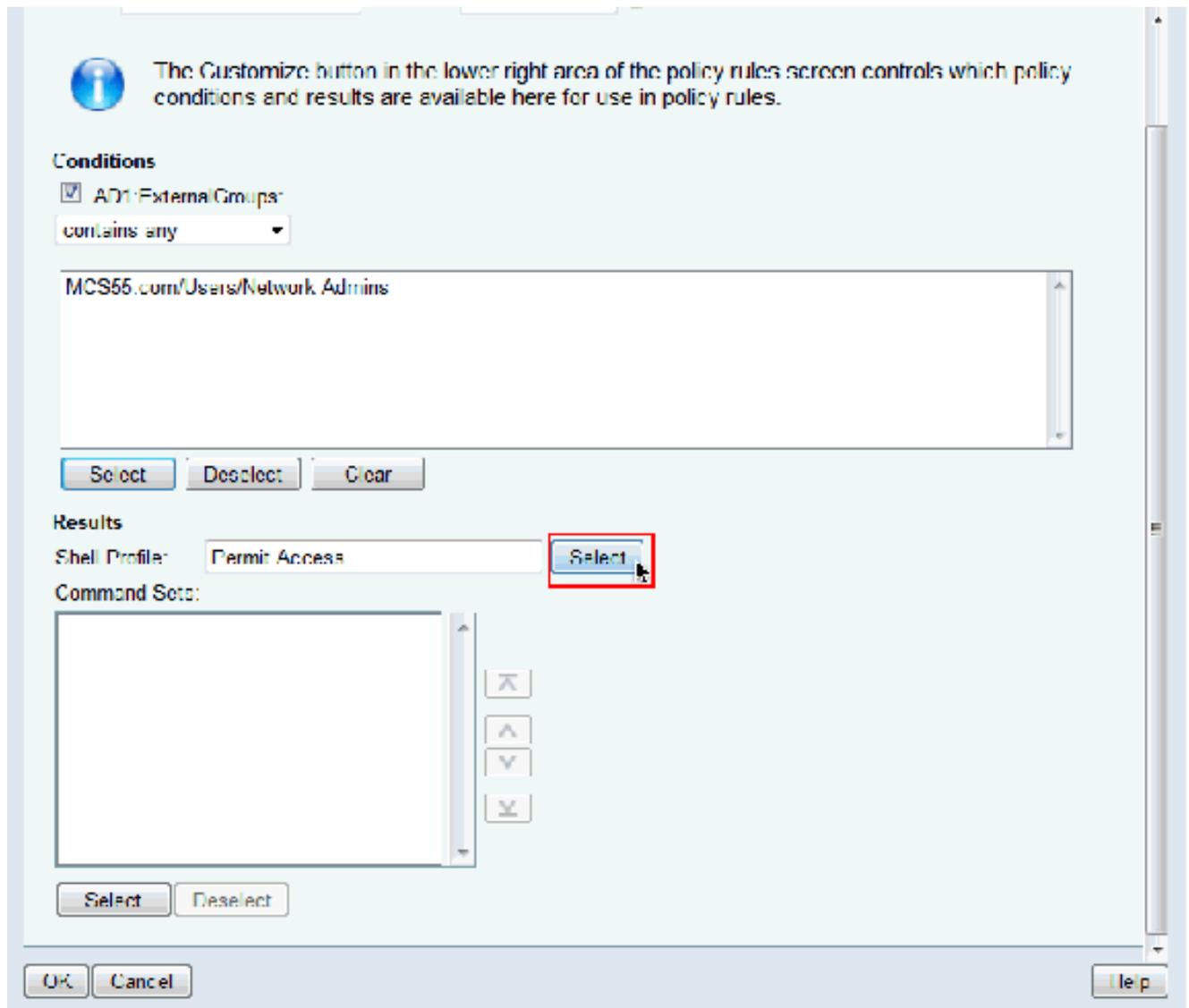
13. AD1:ExternalGroups条件でSelectをクリックします。



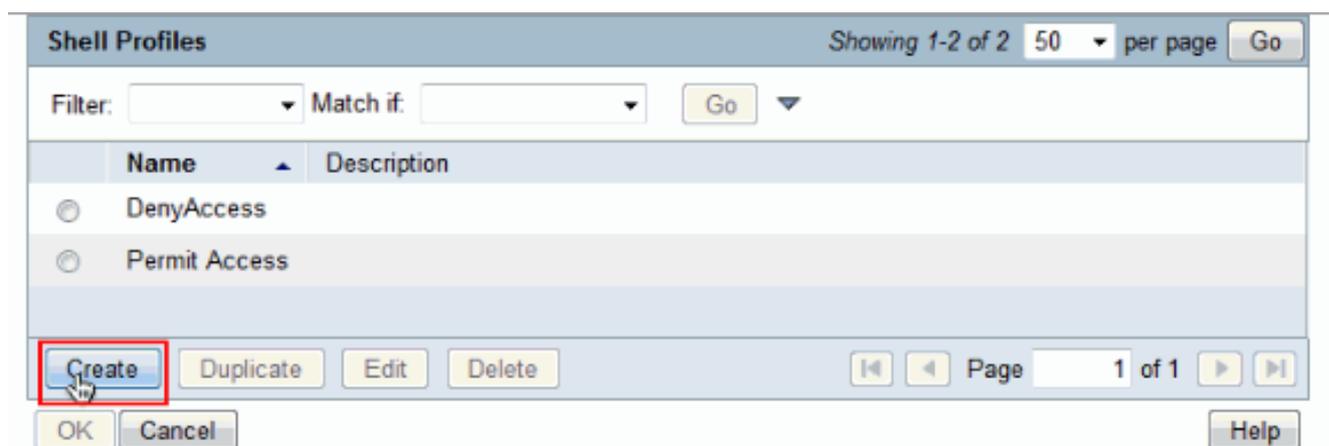
14. Cisco IOSデバイスでフルアクセスを提供するグループを選択します。[OK] をクリックします。



15. Shell ProfileフィールドでSelectをクリックします。



16. Createをクリックして、フルアクセスユーザ用の新しいシェルプロファイルを作成します。



17. GeneralタブでNameとDescription (オプション) を指定し、Common Tasksタブをクリックします。

General Common Tasks Custom Attributes

⚙ Name: Full-Privilege

Description: To push default privilege 15 for IOS

⚙ = Required fields

18. デフォルト権限と最大権限を値15の静的に変更します。[Submit] をクリックします。

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

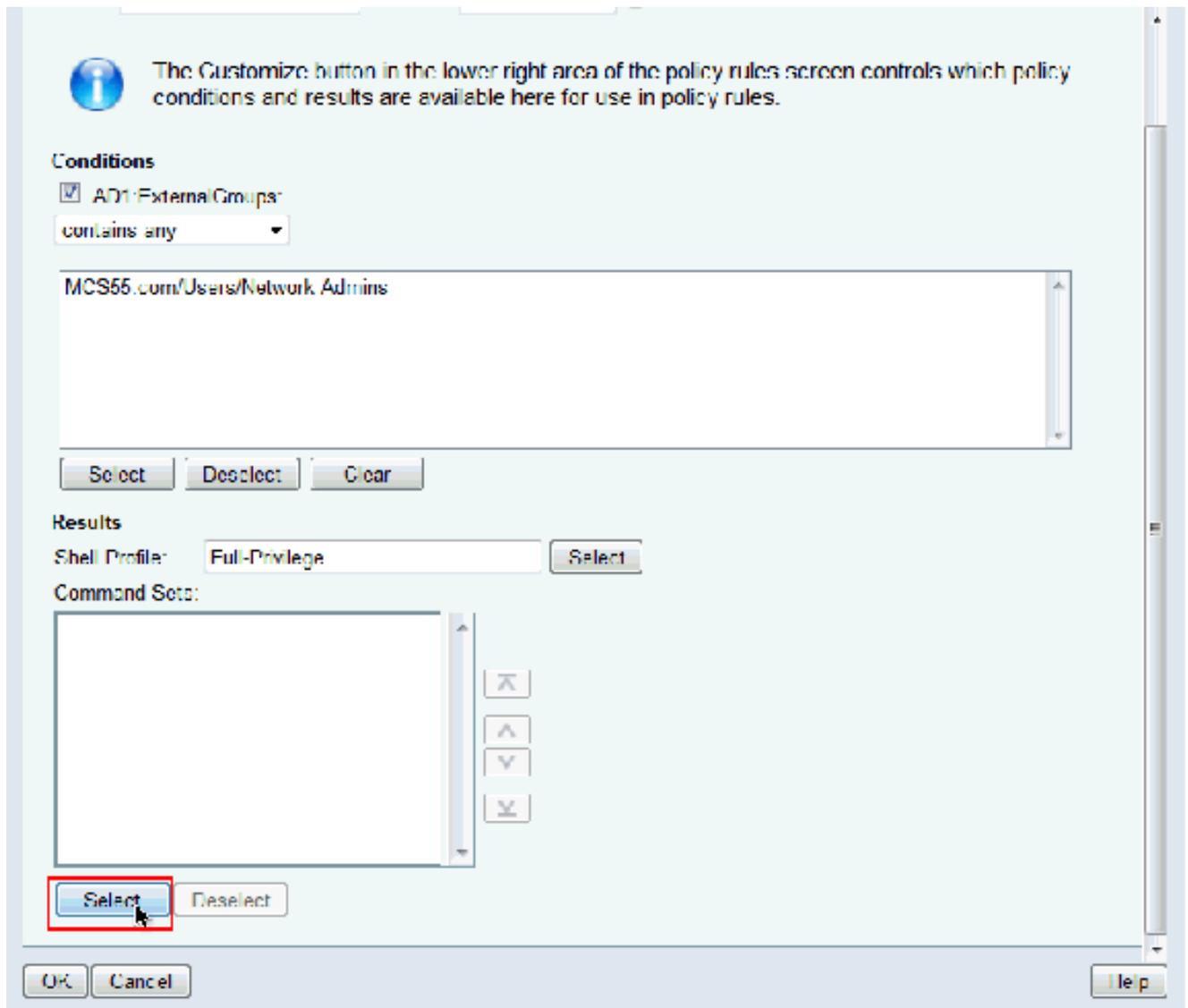
19. 新しく作成したフルアクセスシェルプロファイル（この例ではFull-Privilege）を選択し、OKをクリックします。

Shell Profiles

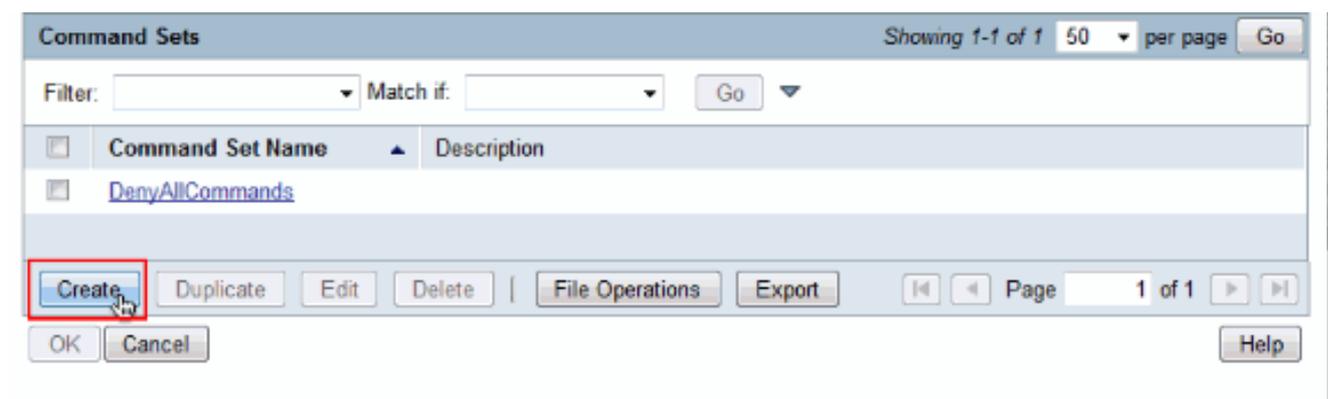
Filter: Match if:

	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. Command SetsフィールドでSelectをクリックします。



21. Createをクリックして、フルアクセスユーザ用の新しいコマンドセットを作成します。



22. 名前を入力し、Permit any command that is not in the table belowの横にあるチェックボックスにチェックマークが付いていることを確認します。[Submit] をクリックします。

注：コマンドセットの詳細については、『[デバイス管理用コマンドセットの作成、複製、および編集](#)』を参照してください。

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. [OK] をクリックします。

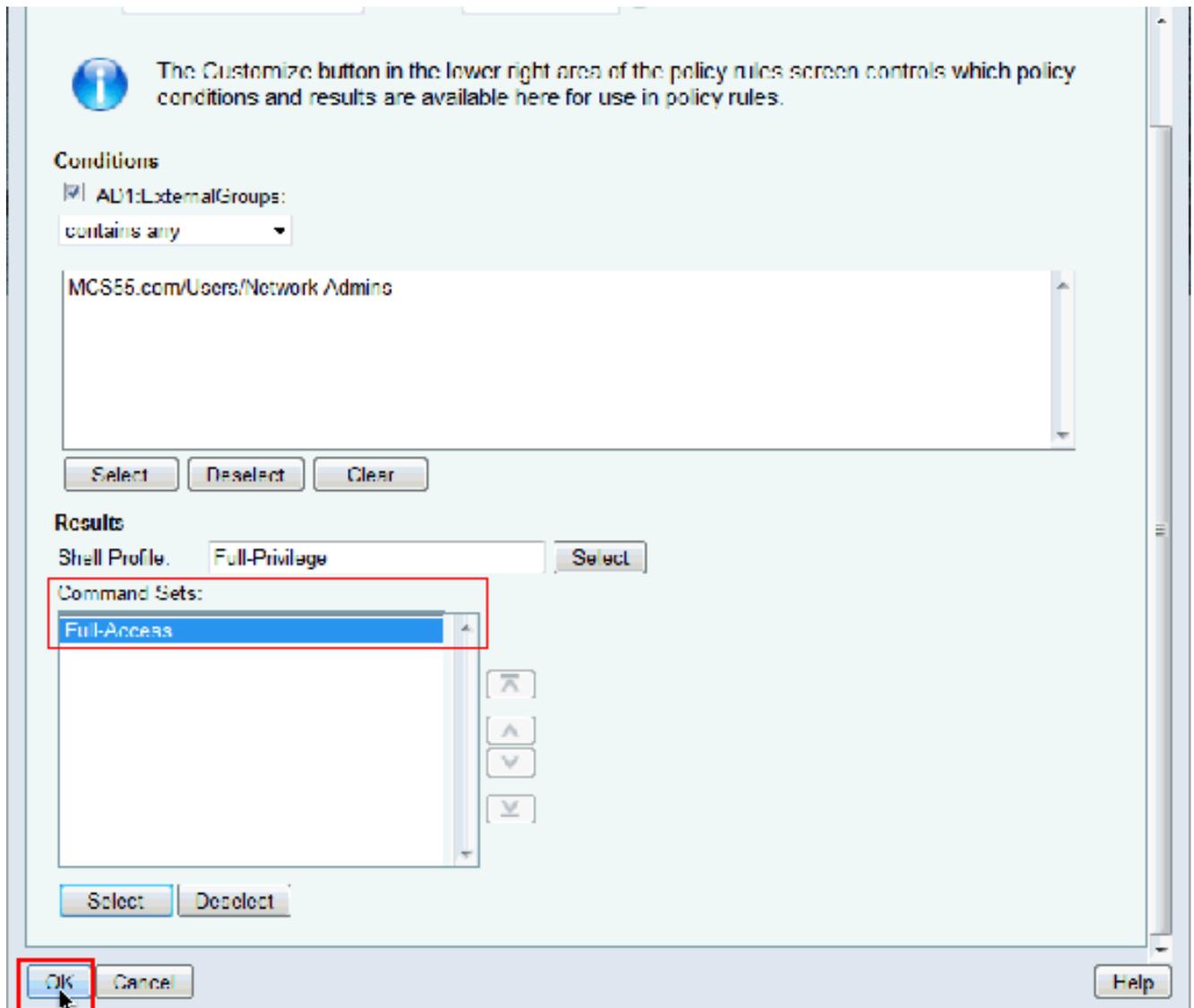
Command Sets

Filter: Match if:

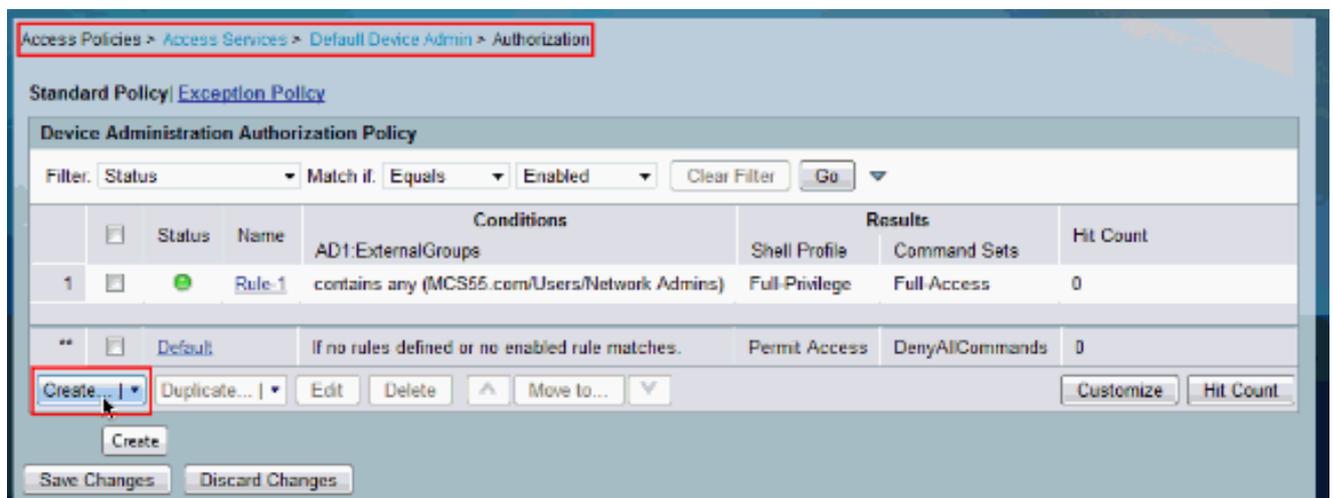
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

|

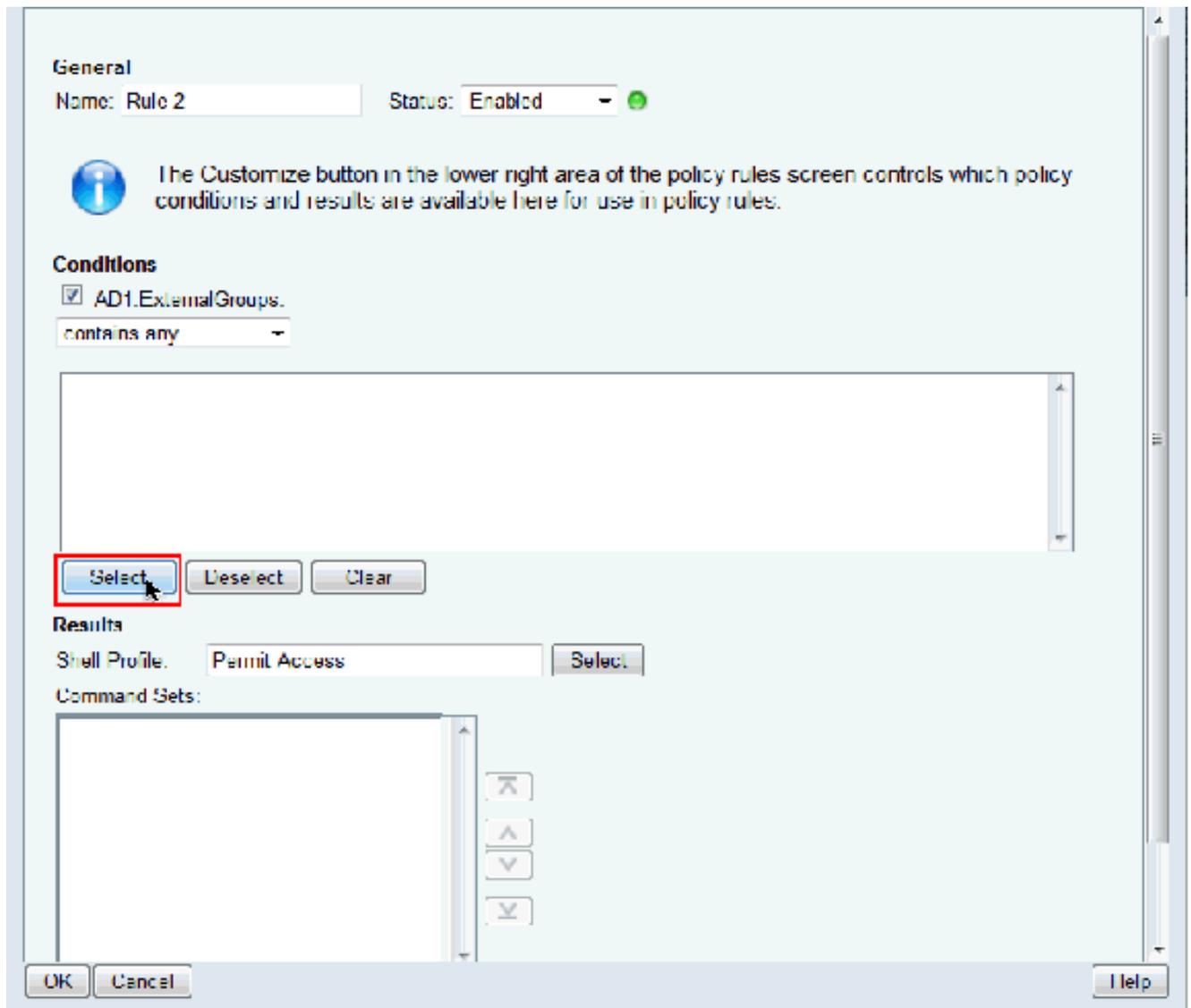
24. [OK] をクリックします。これで、Rule-1の設定は完了です。



25. Createをクリックして、制限付きアクセスユーザ用の新しいルールを作成します。



26. AD1:ExternalGroupsを選択して、Selectをクリックします。



27. 制限付きアクセスを提供するグループを選択し、OKをクリックします。

String Enum Definition

Filter: Match if: Go

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

28. Shell ProfileフィールドでSelectをクリックします。



29. Createをクリックして、制限付きアクセス用の新しいシェルプロファイルを作成します。

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. GeneralタブでNameとDescription (オプション) を指定し、Common Tasksタブをクリックします。

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

⚙ = Required fields

31. デフォルト権限と最大権限をそれぞれ値1と15で静的に変更します。[Submit] をクリックします。

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

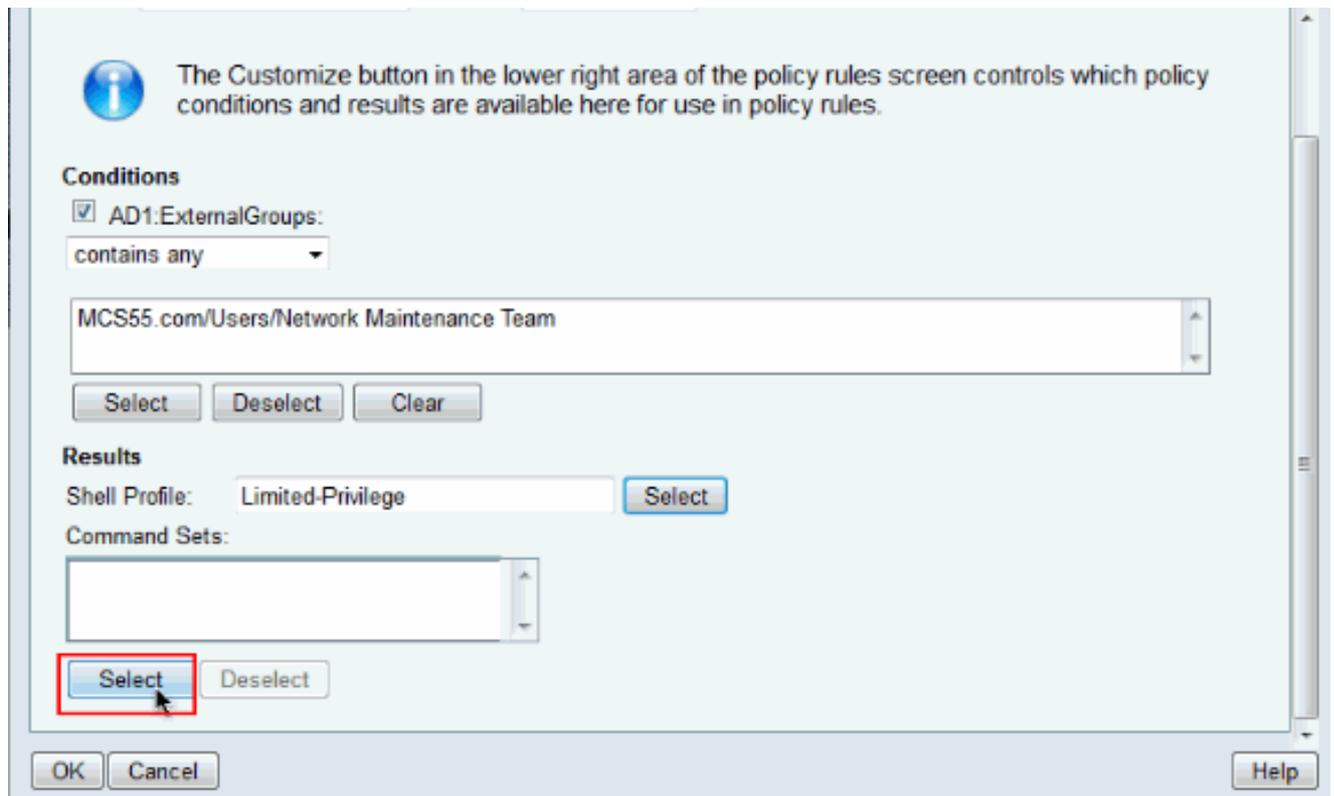
32. [OK] をクリックします。

Shell Profiles

Filter: Match if: Go

	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	

33. Command SetsフィールドでSelectをクリックします。



34. Createをクリックして、制限付きアクセスグループ用の新しいコマンドセットを作成します

。

Command Sets

Filter: Match if:

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

|

35. 名前を入力し、次の表に記載されていないコマンドを許可の横にあるチェックボックスが選択されていないことを確認します。Addをクリックし、commandセクションにあるスペースでshowと入力して、GrantセクションでPermitを選択し、制限付きアクセスグループのユーザーにshowコマンドだけが許可されるようにします。

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. 同様に、Addを使用して、制限付きアクセスグループのユーザに許可するその他のコマンドを追加します。[Submit] をクリックします。

注：コマンドセットの詳細については、『[デバイス管理用コマンドセットの作成、複製、および編集](#)』を参照してください。

General

Name:

Description:

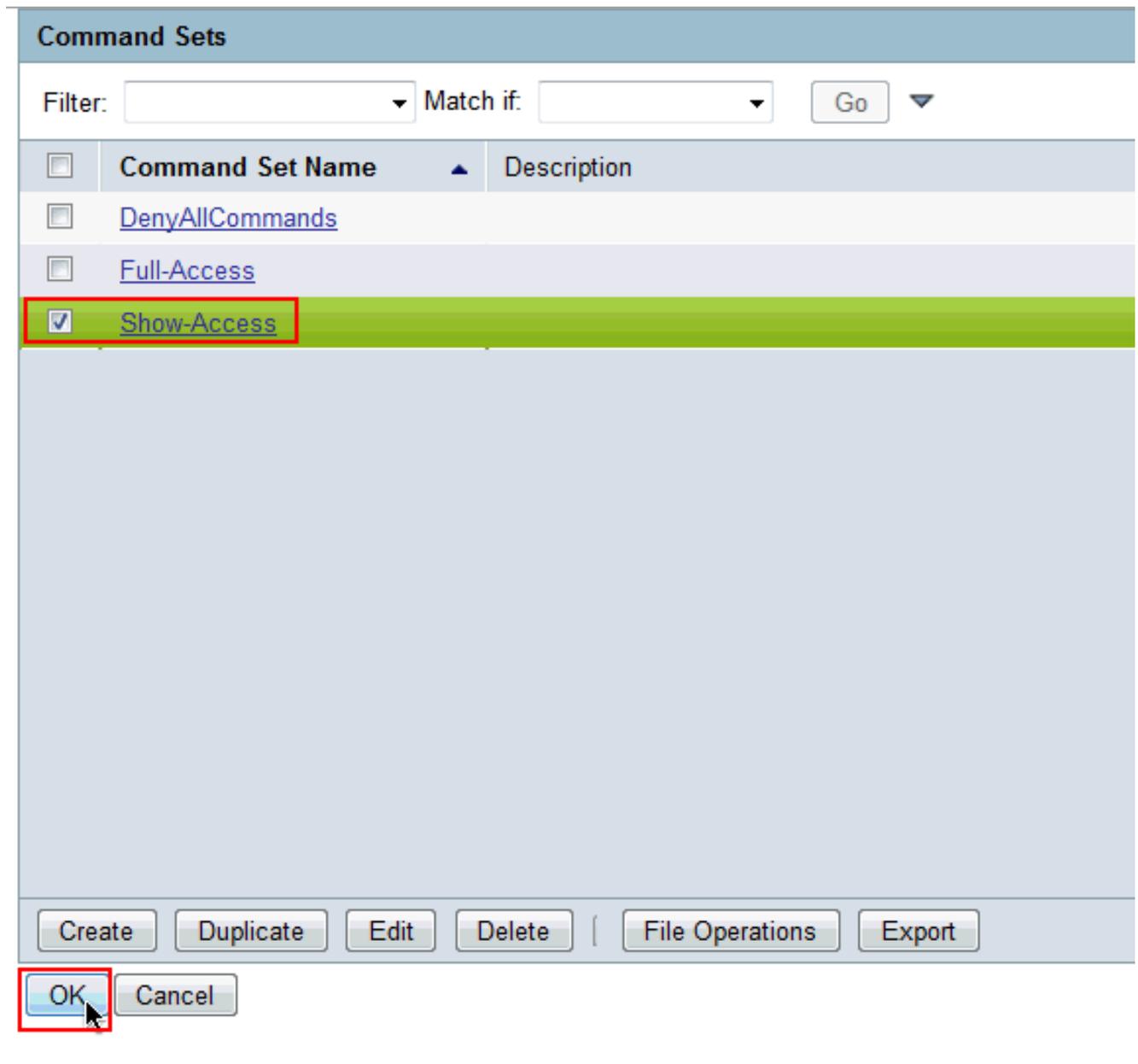
Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

37. [OK] をクリックします。



38. [OK] をクリックします。



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

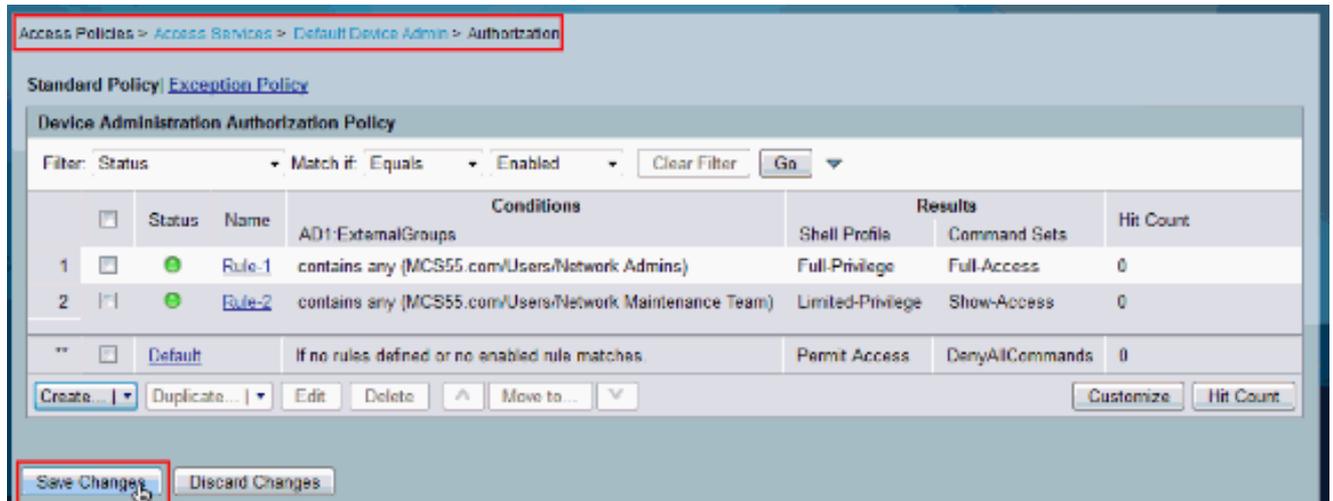
Select

Deselect

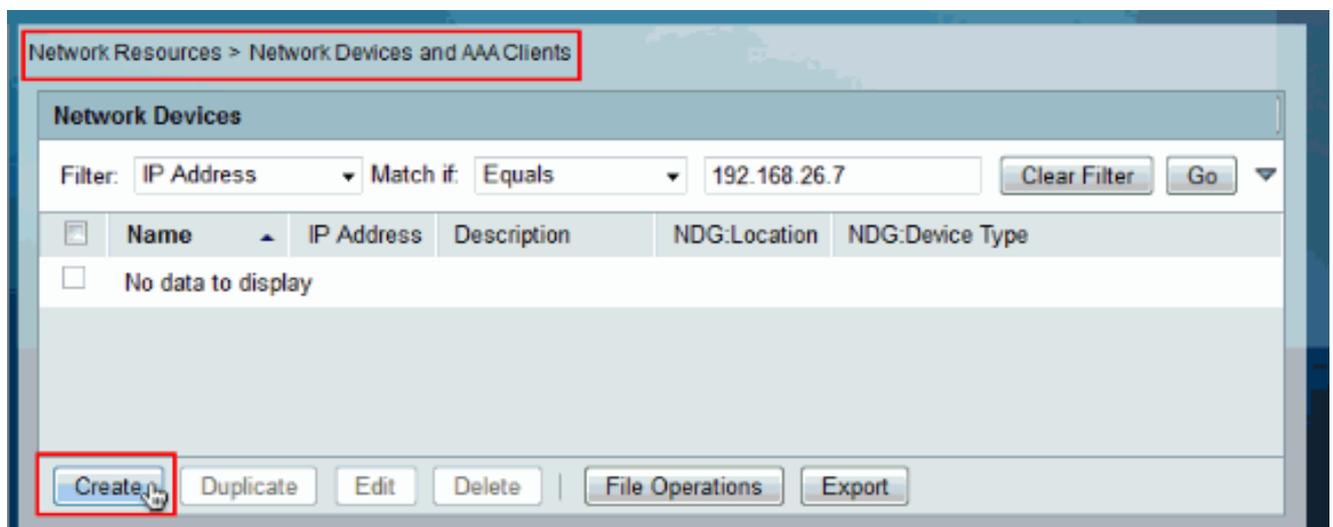
OK

Cancel

39. [Save Changes] をクリックします。



40. Createをクリックして、Cisco IOSデバイスをAAAクライアントとしてACSに追加します。



41. TACACS+に対してName, IP Address, Shared Secretを指定し、Submitをクリックします。

認証および認可のためのCisco IOSデバイスの設定

認証と認可のためにCisco IOSデバイスとACSを設定するには、次の手順を実行します。

1. 次に示すように、フォールバックの完全な権限を持つローカルユーザをusernameコマンドで作成します。

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

2. AAAを有効にして、TACACSサーバとしてACS 5.xを追加するために、ACSのIPアドレスを指定します。

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

注：キーは、このCisco IOSデバイス用にACSで提供される共有秘密と一致する必要があります。

3. 次に示すように、aaa コマンドにより、TACACS サーバの到達可能性をテストします。

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

前のコマンドの出力では、TACACS サーバが到達可能であり、ユーザが正常に認証されたことを示しています。

注：User1とパスワードxxxはADに属しています。テストに失敗した場合は、前の手順で指定した共有秘密が正しいことを確認してください。

4. ログインを設定して認証を有効にし、次に示すようにExecおよびコマンド認可を使用します。

```
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：TACACSサーバに到達できない場合、LocalおよびEnableキーワードは、Cisco IOSローカルユーザおよびenable secretへのフォールバックにそれぞれ使用されます。

確認

認証と認可を確認するには、Telnetを使用してCisco IOSデバイスにログインします。

1. ADのフルアクセスグループに属するuser1としてCisco IOSデバイスにTelnet接続します。Network Adminsグループは、ACSで設定されるFull-Privilege Shell ProfileとFull-Access CommandにマッピングされるADのグループです。フルアクセス権があることを確認するために、任意のコマンドを実行してみてください。

```
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. ADの制限付きアクセスグループに属するuser2としてCisco IOSデバイスにTelnet接続します(Network Maintenance Teamグループは、ACSでLimited-Privilegeシェルスプロファイルと

Show-AccessコマンドセットにマッピングされるADのグループです)。Show-Accessコマンドセットに記載されているコマンド以外のコマンドを実行しようとすると、「Command Authorization Failed」エラーが発生し、user2によるアクセスが制限されていることが示されます。

```
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
SOFTWARE (rcl)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text base: 0x00003000, data base: 0x00EA3DB8

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"

          3
          2
          1

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/cond/stip.html

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

router1#cont t
Command authorization failed.

router1#wr mem
Command authorization failed.

router1#
```

3. ACS GUIにログインし、モニタリングとレポートビューアを起動します。AAA Protocol > TACACS+Authorizationの順に選択して、user1とuser2が実行したアクティビティを確認します。

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=conf t] [CmdAV=write 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=conf t] [CmdAV=write 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

関連情報

- [Cisco Secure Access Control System](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。