

ACS 5.x: Autenticação TACACS+ e autorização de comando com base no exemplo de configuração de associação de grupo do AD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configuração](#)

[Configurar o ACS 5.x para autenticação e autorização](#)

[Configurar o dispositivo IOS Cisco para autenticação e autorização](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece um exemplo de configuração de Autenticação TACACS+ e Autorização de Comando com base na associação de grupo do AD de um usuário com o Cisco Secure Access Control System (ACS) 5.x e posterior. O ACS usa o Microsoft Active Directory (AD) como um armazenamento de identidade externa para armazenar recursos, como usuários, máquinas, grupos e atributos.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O ACS 5.x é totalmente integrado ao domínio do AD desejado. Se o ACS não estiver integrado ao Domínio do AD desejado, consulte [ACS 5.x e posterior: Exemplo de Configuração de Integração com o Microsoft Active Directory](#) para obter mais informações para executar a tarefa de integração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure ACS 5.3

- Software Cisco IOS® versão 12.2(44)SE6.

Observação: essa configuração pode ser feita em todos os dispositivos Cisco IOS.

- Domínio do Microsoft Windows Server 2003

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Configuração

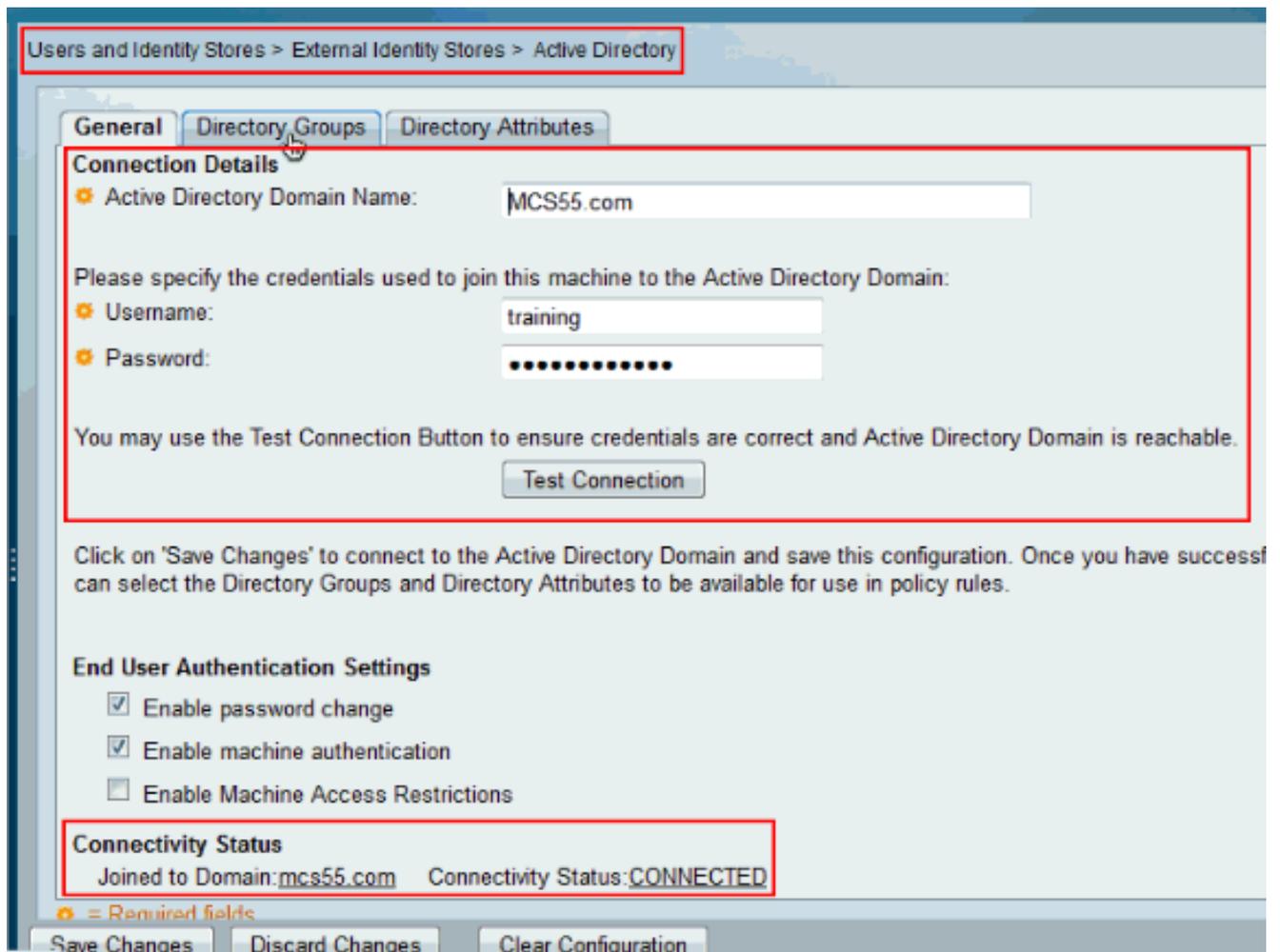
Configurar o ACS 5.x para autenticação e autorização

Antes de iniciar a configuração do ACS 5.x para Autenticação e Autorização, o ACS deve ter sido integrado com êxito ao Microsoft AD. Se o ACS não estiver integrado ao Domínio do AD desejado, consulte [ACS 5.x e posterior: Exemplo de Configuração de Integração com o Microsoft Active Directory](#) para obter mais informações para executar a tarefa de integração.

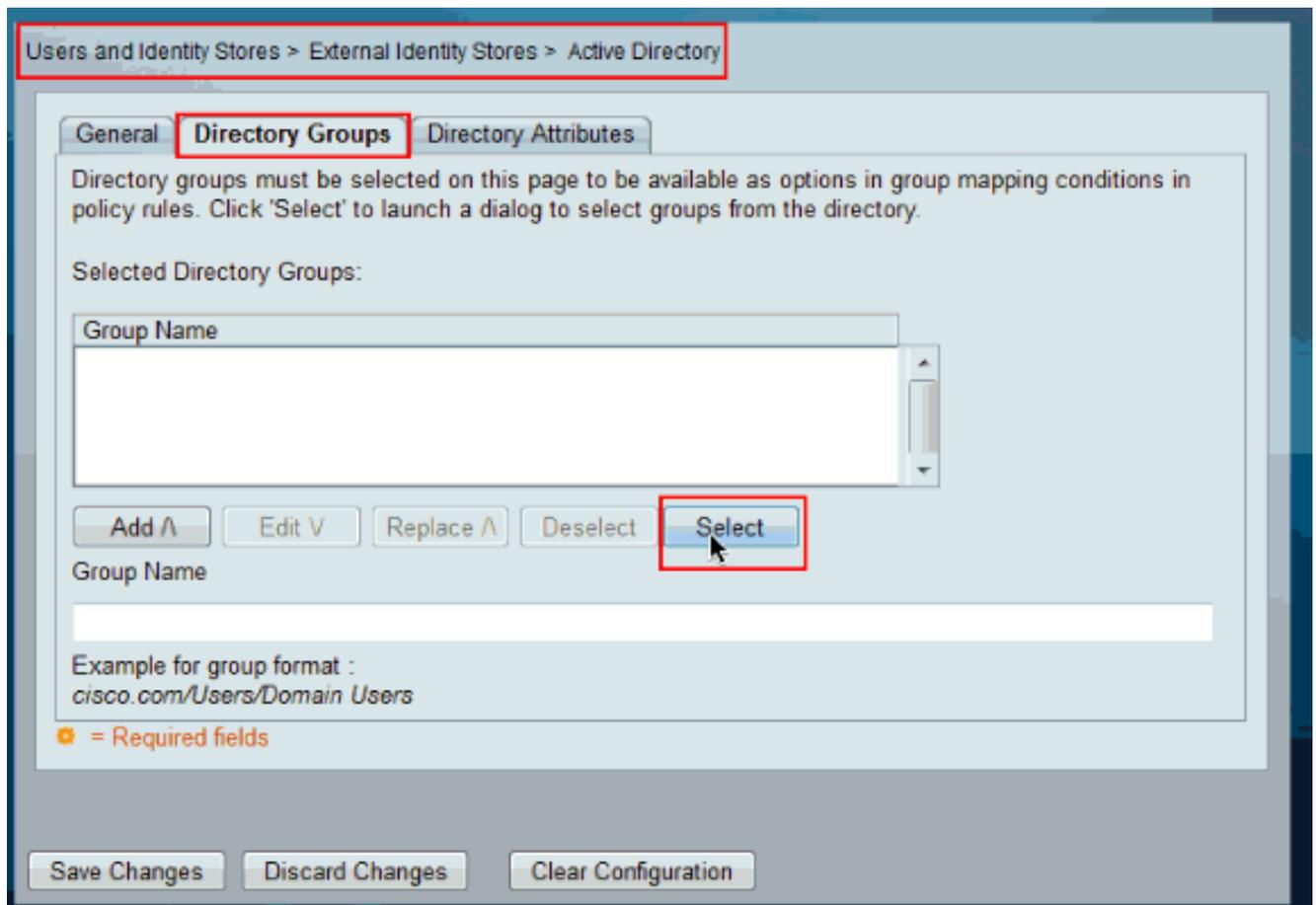
Nesta seção, você mapeia dois grupos do AD para dois conjuntos de comandos diferentes e dois perfis do Shell, um com acesso total e outro com acesso limitado nos dispositivos Cisco IOS.

1. Faça login na GUI do ACS usando as credenciais de Admin.
2. Escolha Users and Identity Stores > External Identity Stores > Active Directory e verifique se o ACS ingressou no domínio desejado e também se o status de conectividade é mostrado como connected.

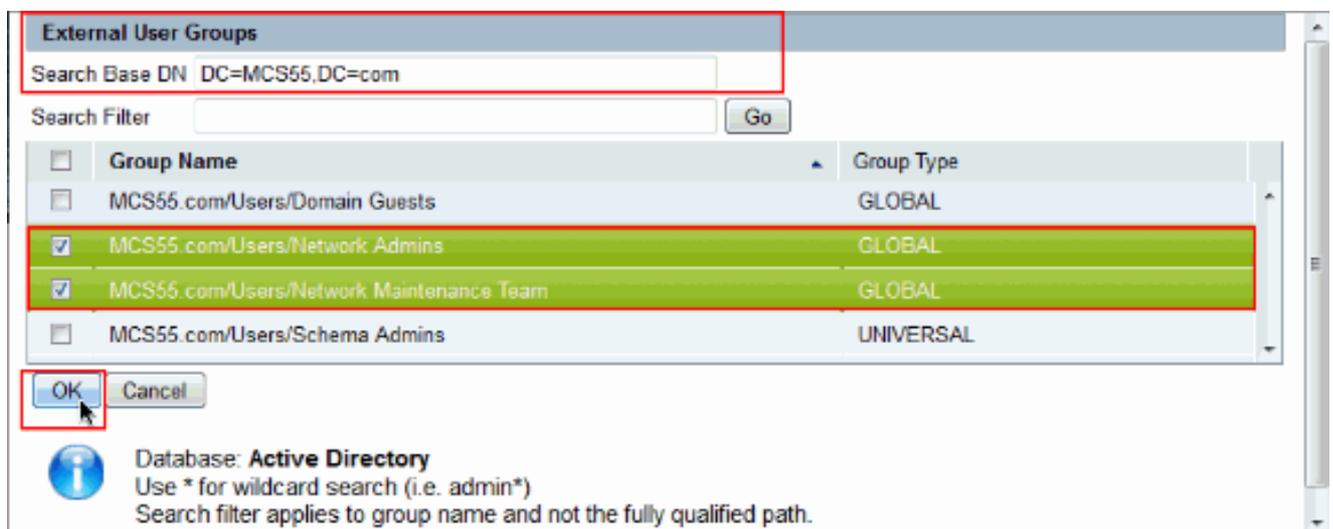
Clique na guia Directory Groups.



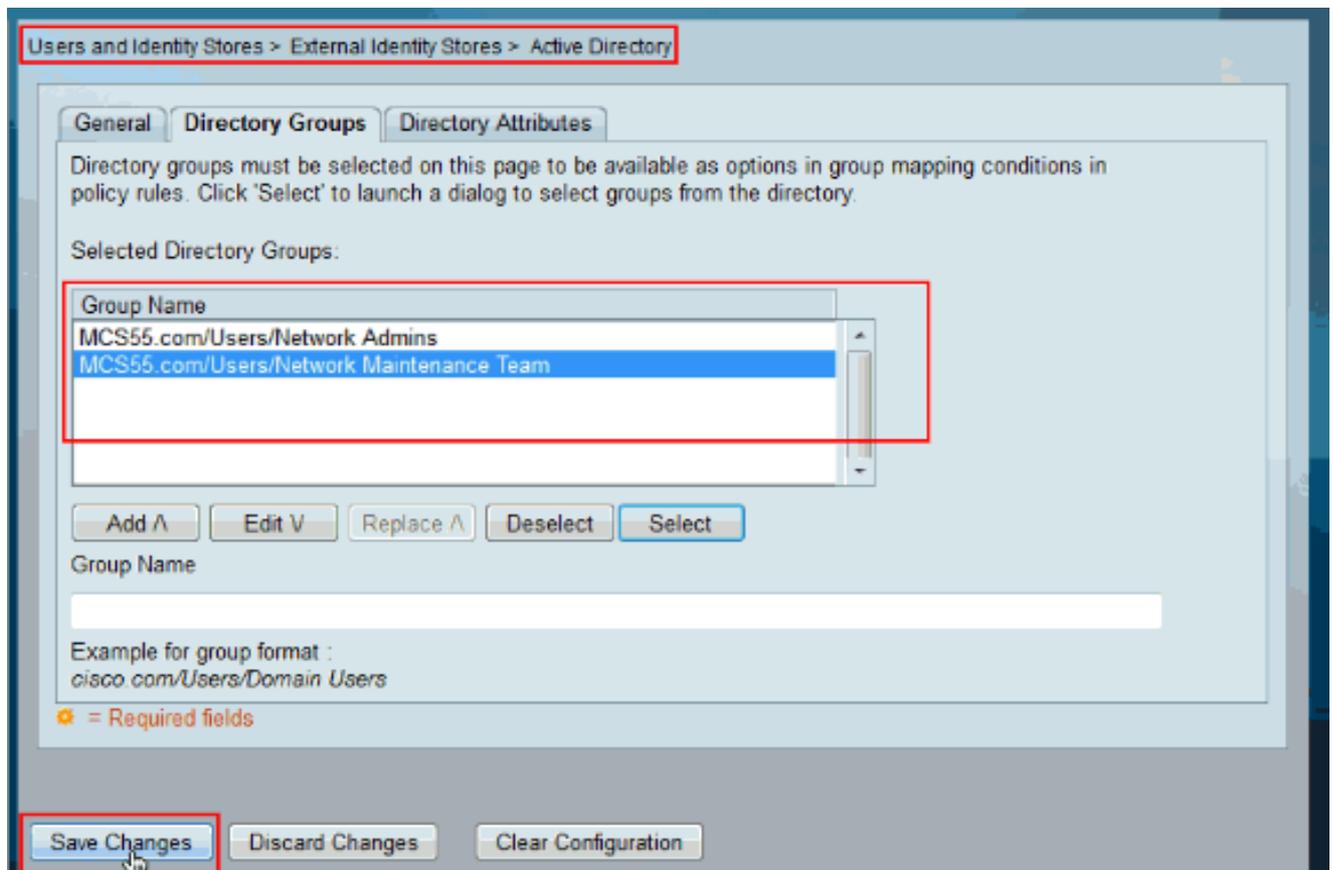
3. Clique em Selecionar.



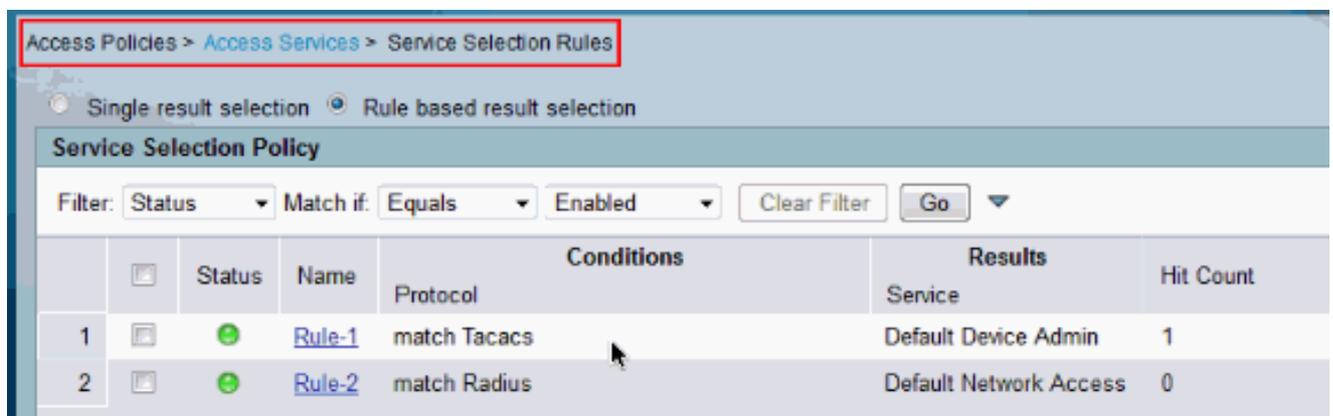
- Escolha os grupos que precisam ser mapeados para os perfis Shell e conjuntos de comandos na parte posterior da configuração. Click OK.



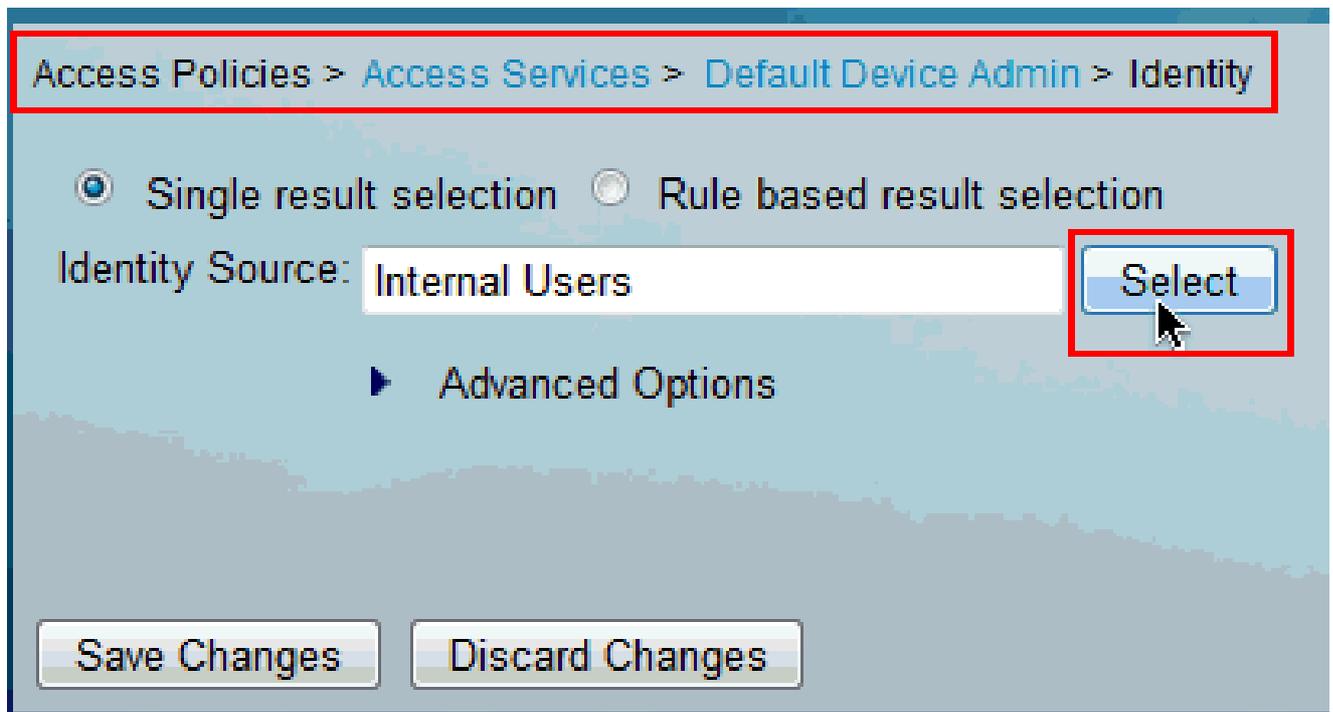
- Clique em Save Changes.



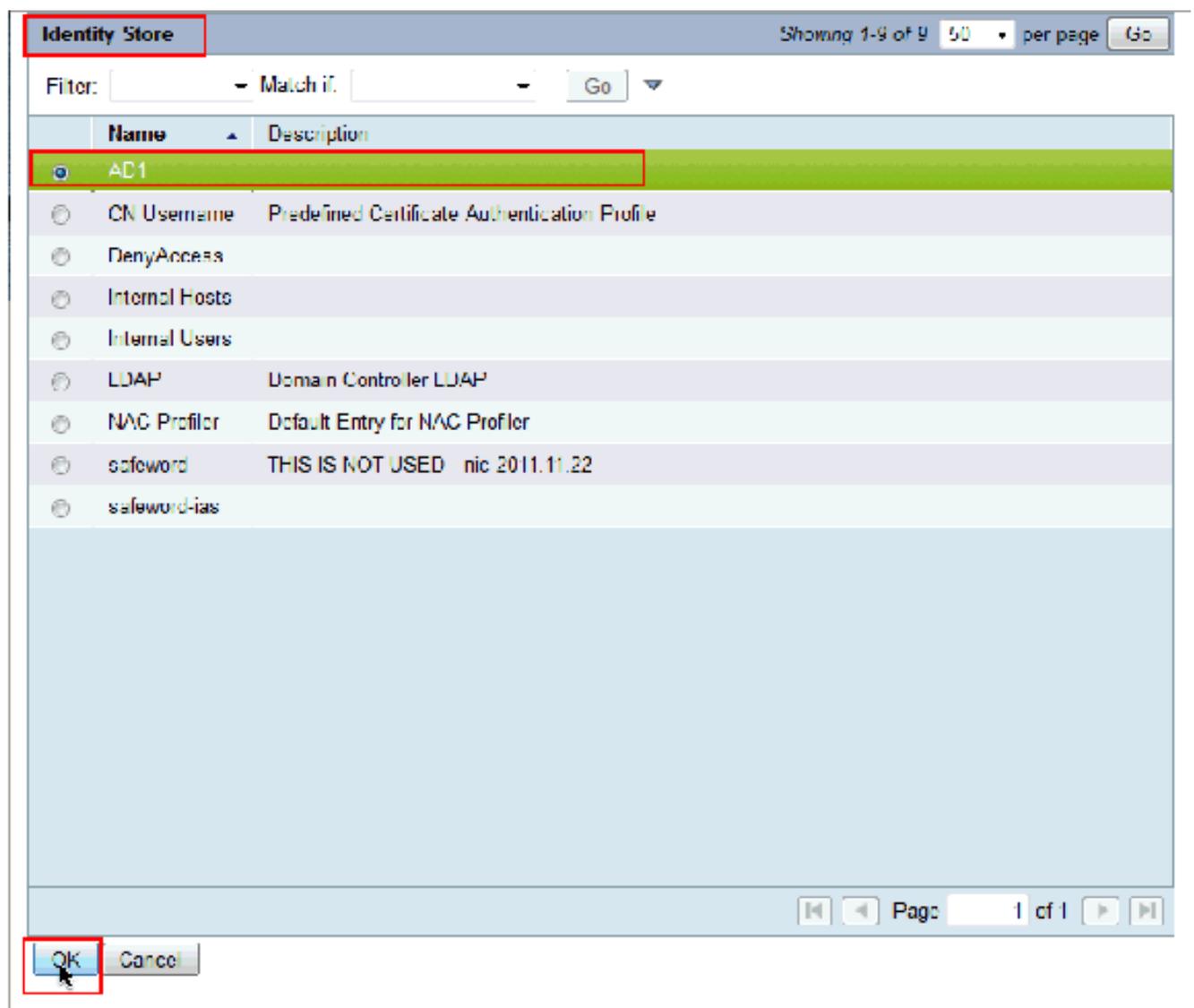
6. Escolha Access Policies > Access Services > Service Selection Rules e identifique o serviço de acesso, que processa a autenticação TACACS+. Neste exemplo, é Default Device Admin.



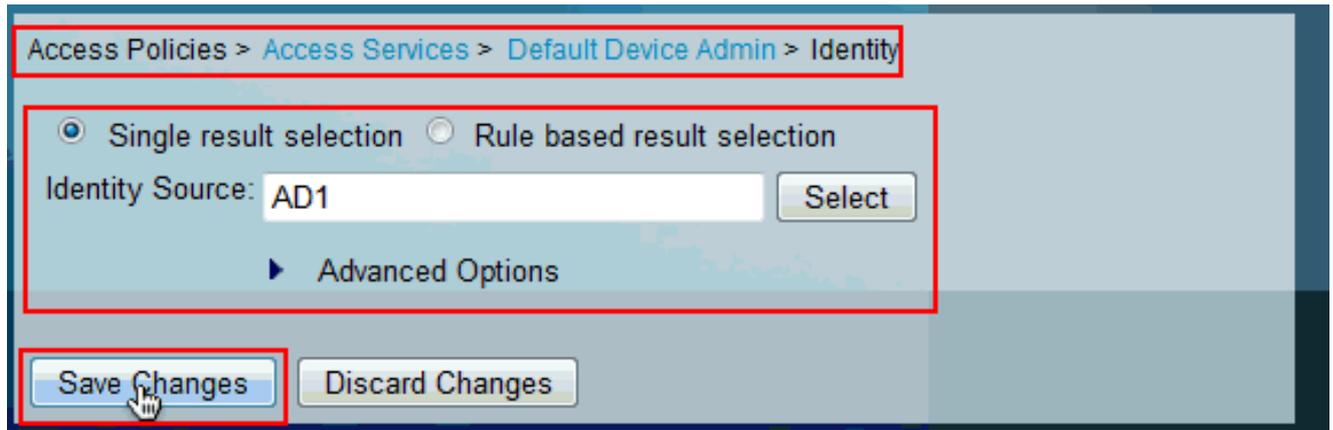
7. Escolha Access Policies > Access Services > Default Device Admin > Identity e clique em Select ao lado de Identity Source.



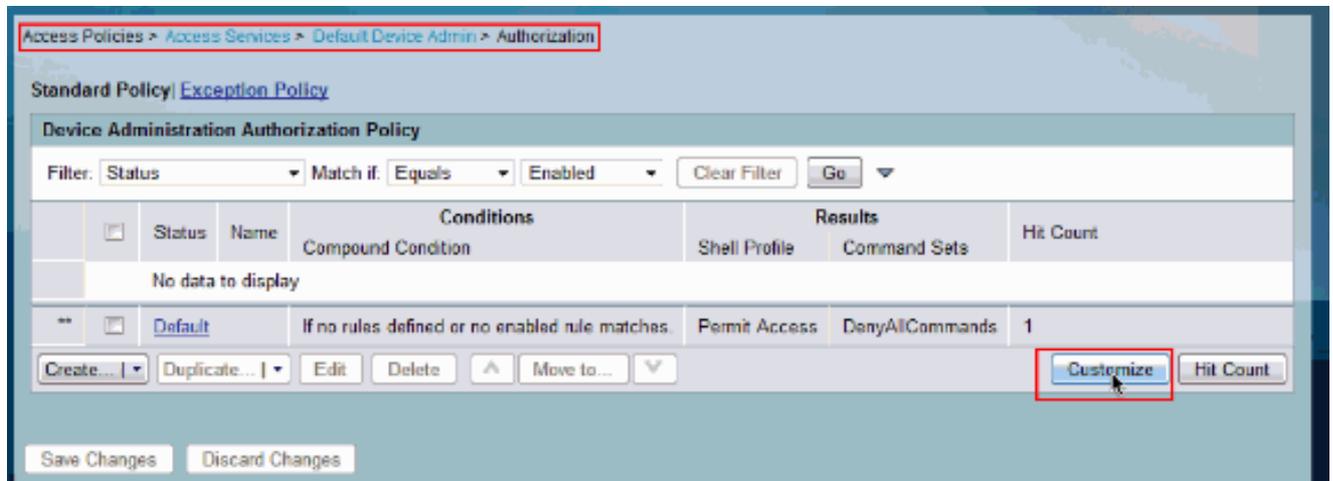
8. Escolha AD1 e clique em OK.



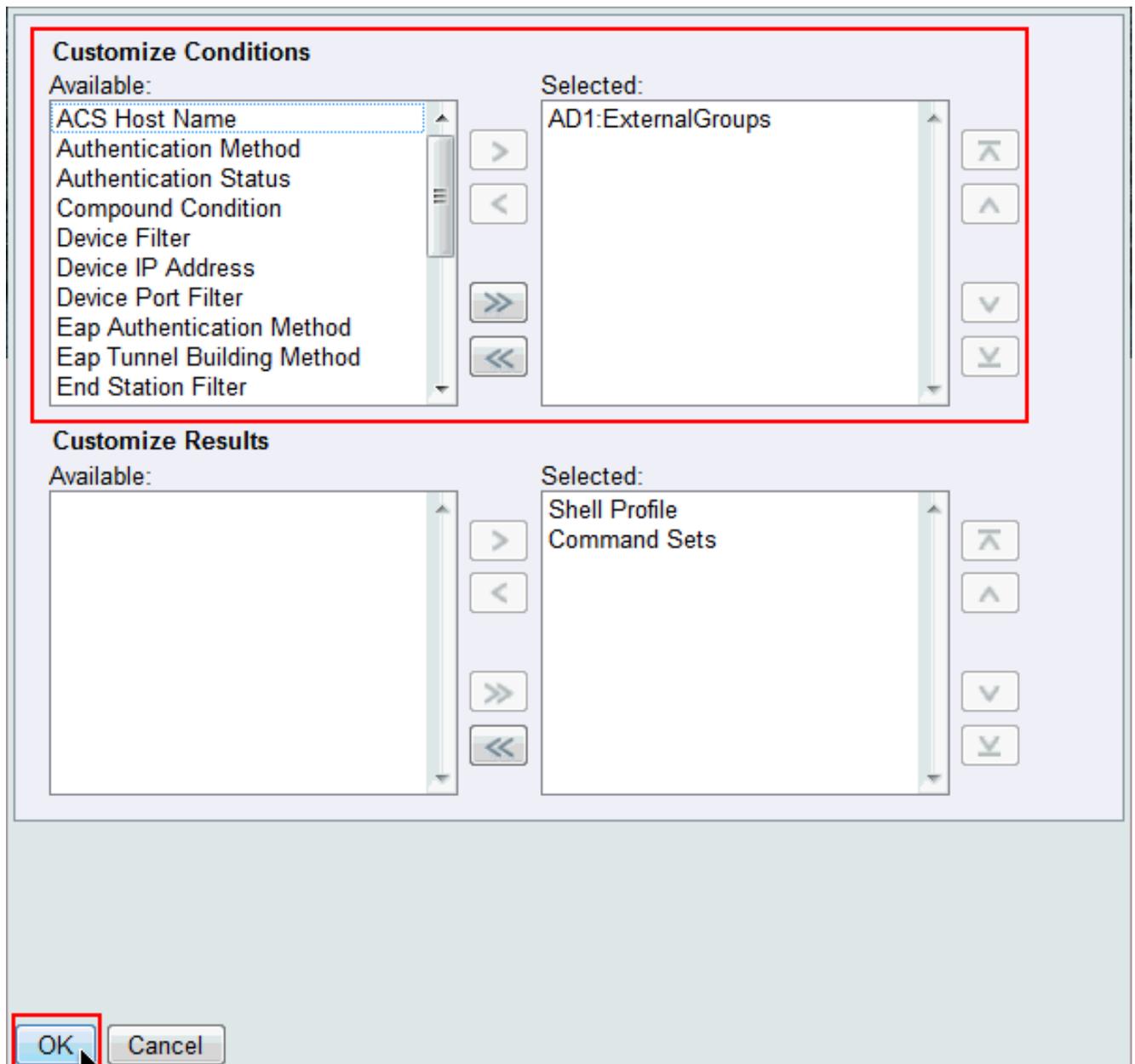
9. Clique em Save Changes.



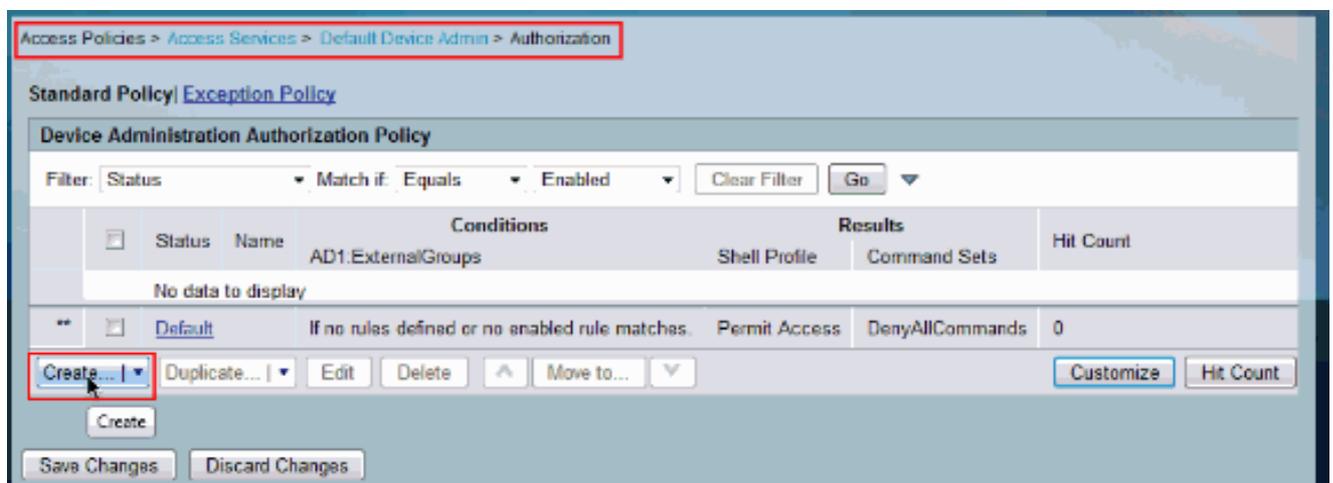
10. Escolha Access Policies > Access Services > Default Device Admin > Authorization e clique em Customize.



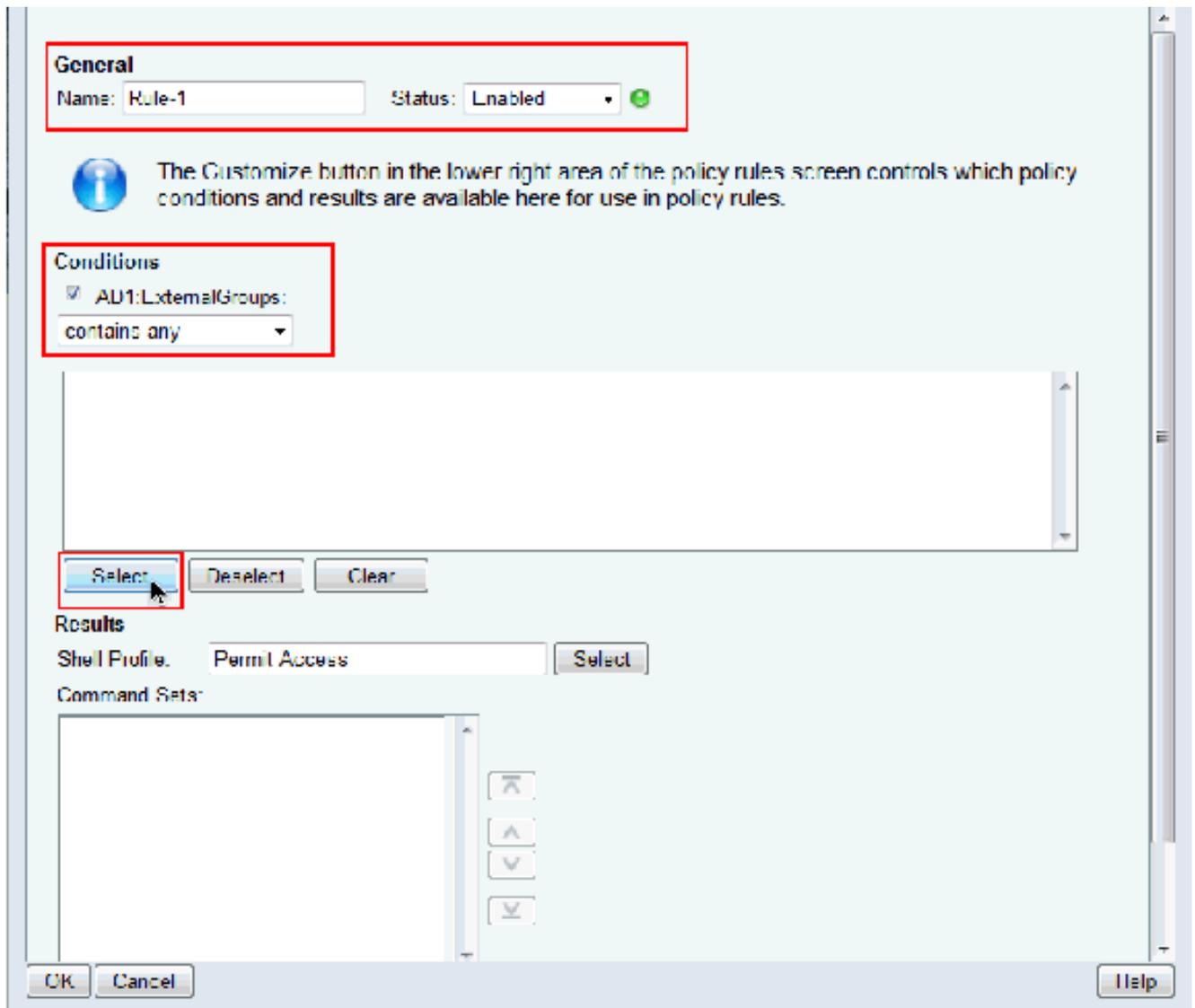
11. Copie AD1:ExternalGroups da seção Available to Selected de Customize Conditions e depois mova o Perfil do Shell e os Conjuntos de Comandos da seção Available to Selected de Customize Results. Agora clique em OK.



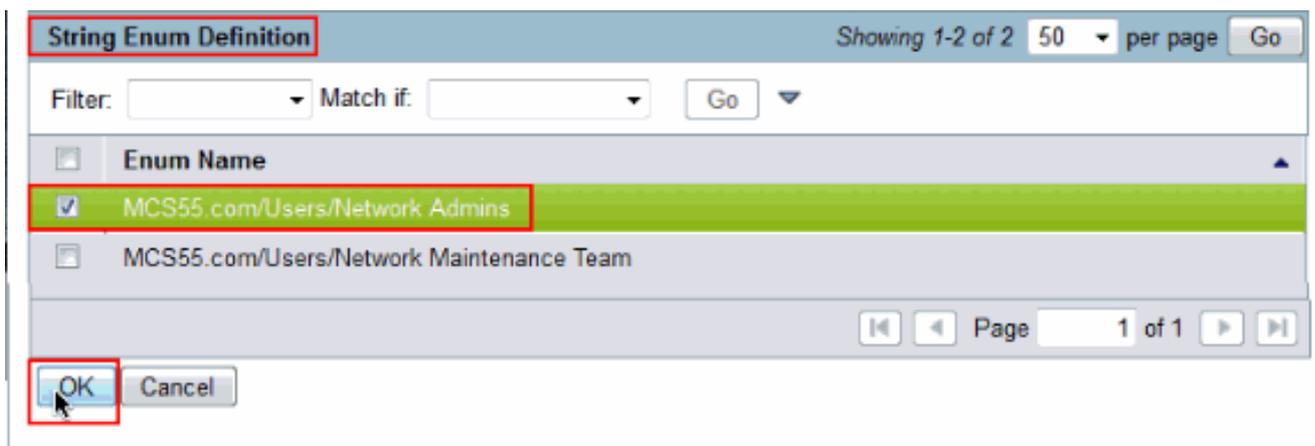
12. Clique em Create para criar uma nova regra.



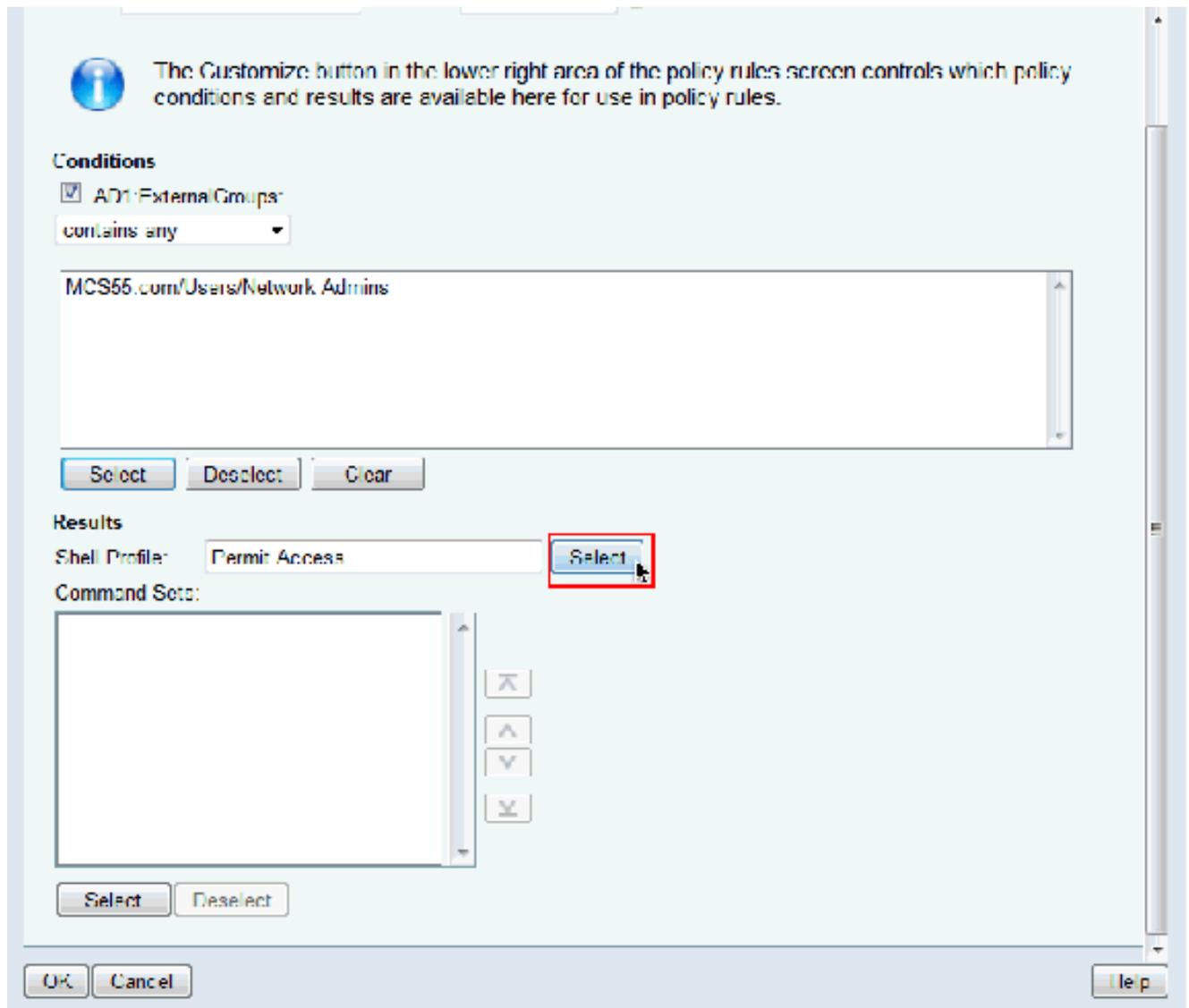
13. Clique em Selecionar na condição AD1:ExternalGroups.



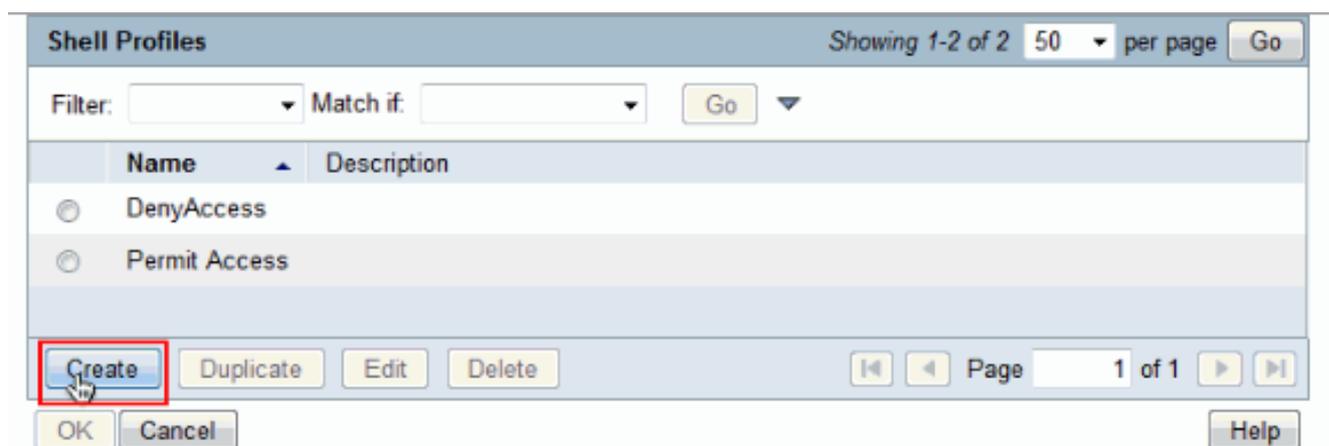
14. Escolha o grupo ao qual você deseja conceder acesso total no dispositivo IOS Cisco. Click OK.



15. Clique em Select no campo Shell Profile.



16. Clique em Create para criar um novo Shell Profile para usuários com acesso total.



17. Forneça um Nome e Descrição (opcional) na guia Geral e clique na guia Tarefas comuns.

General Common Tasks Custom Attributes

 Name: Full-Privilege

Description: To push default privilege 15 for IOS

 = Required fields

18. Altere Default Privilege e Maximum Privilege para Static com o Valor 15. Clique em Submit.

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

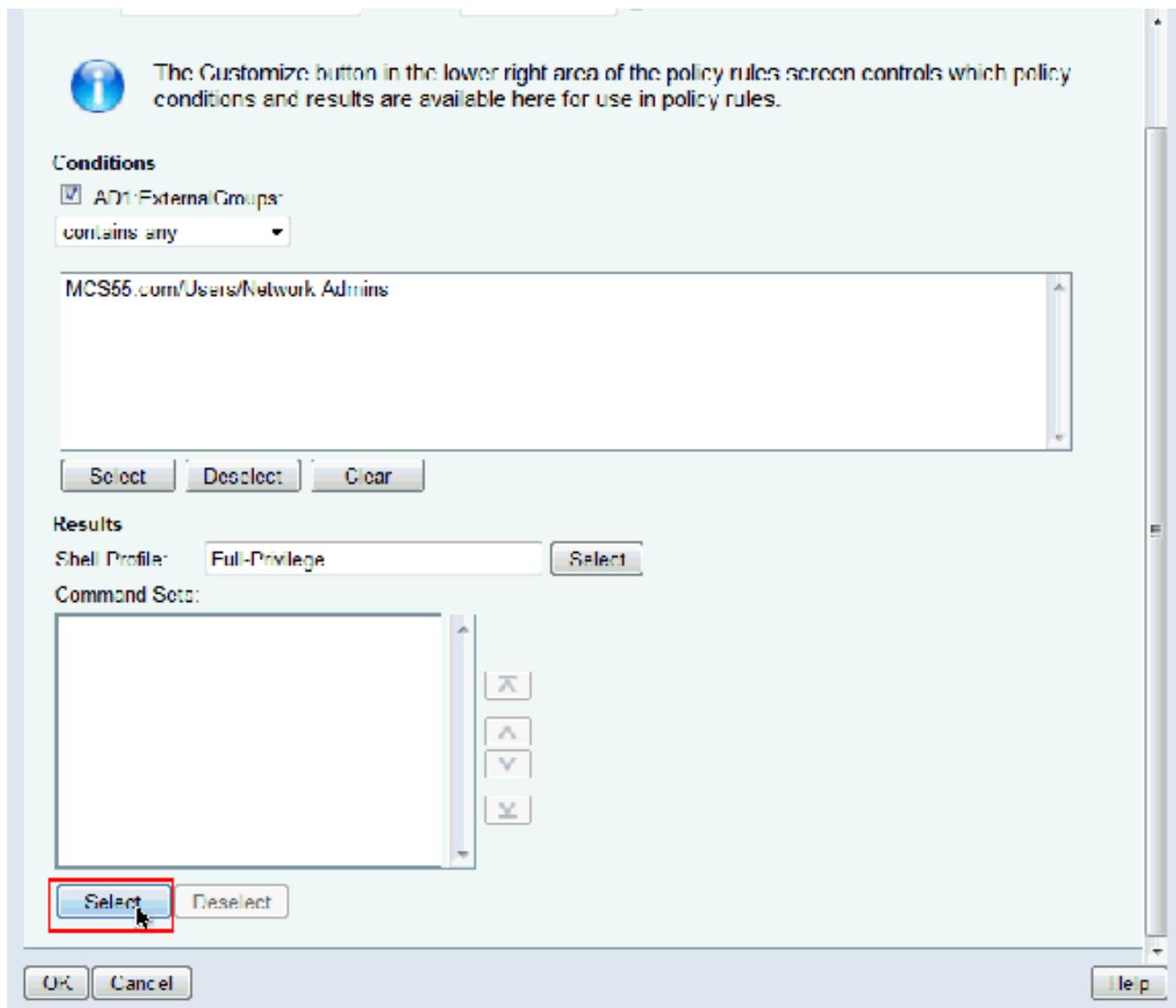
19. Agora, escolha o Perfil do shell de acesso completo recém-criado (Privilégio completo neste exemplo) e clique em OK.

Shell Profiles

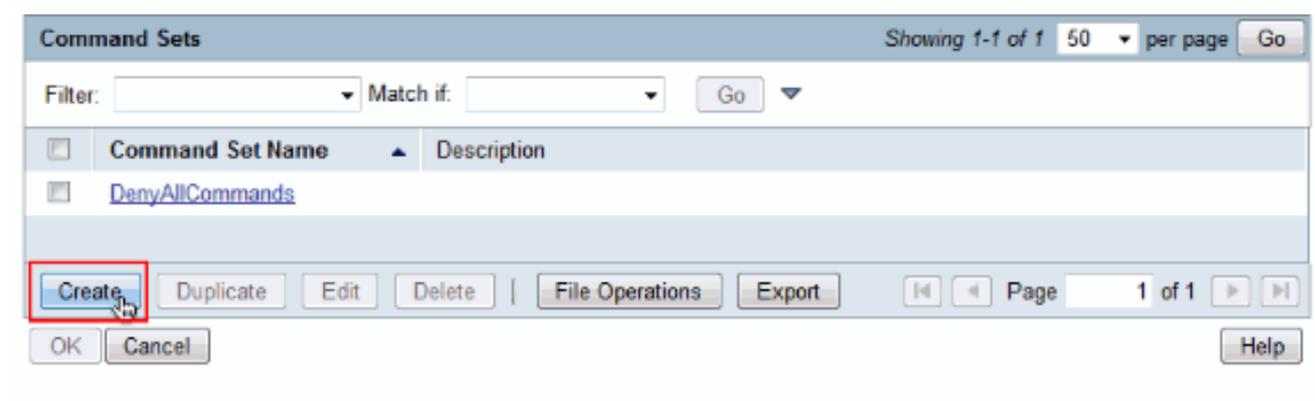
Filter: Match if: ▼

	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. Clique em Selecionar no campo Conjuntos de Comandos.



21. Clique em Create para criar um novo conjunto de comandos para usuários de Full-Access.



22. Forneça um Nome e verifique se a caixa de seleção ao lado de Permitir qualquer comando que não esteja na tabela abaixo está marcada. Clique em Submit.

Observação: consulte [Criação, Duplicação e Edição de Conjuntos de Comandos para Administração de Dispositivos](#) para obter mais informações sobre Conjuntos de Comandos.

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. Click OK.

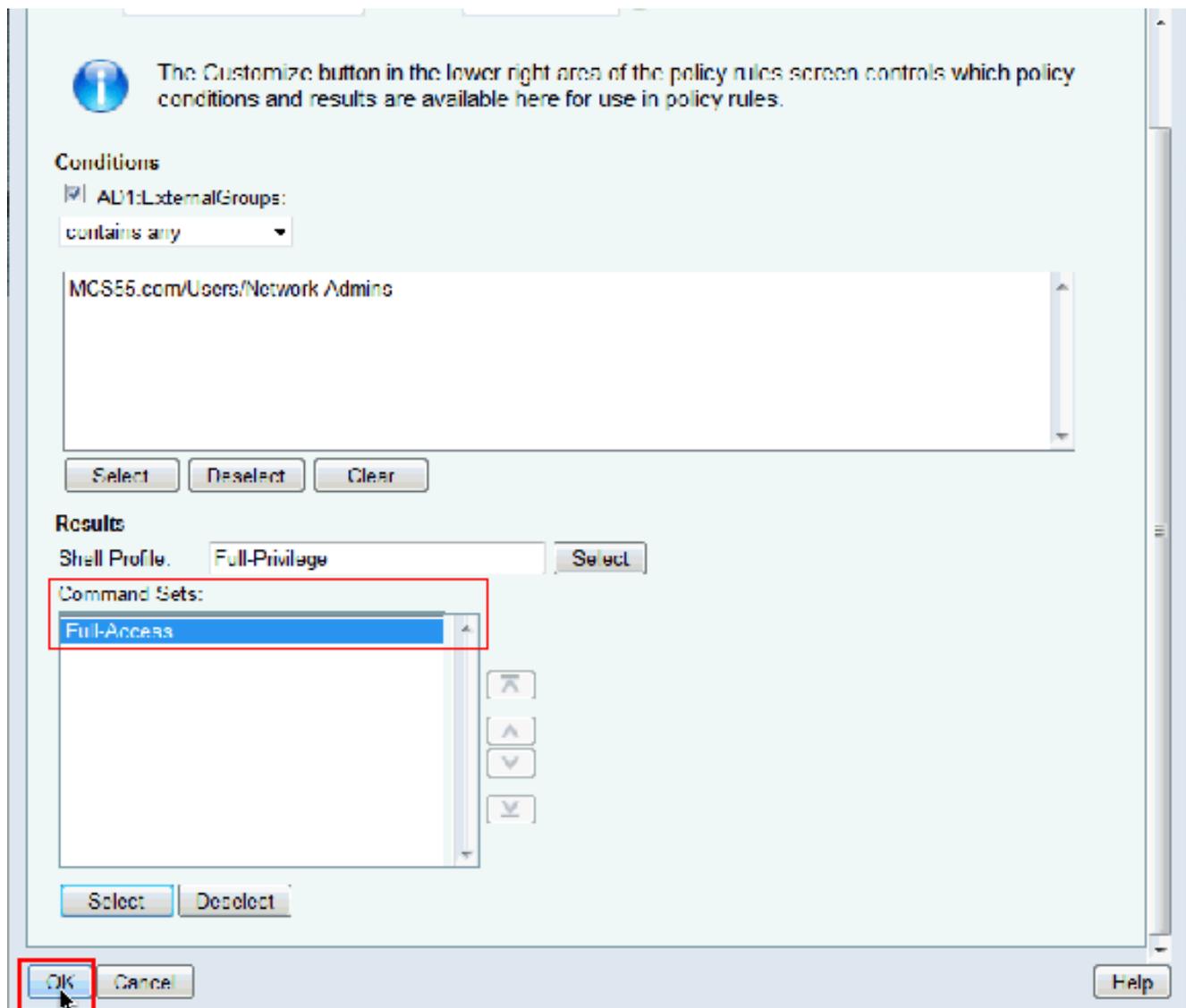
Command Sets

Filter: Match if:

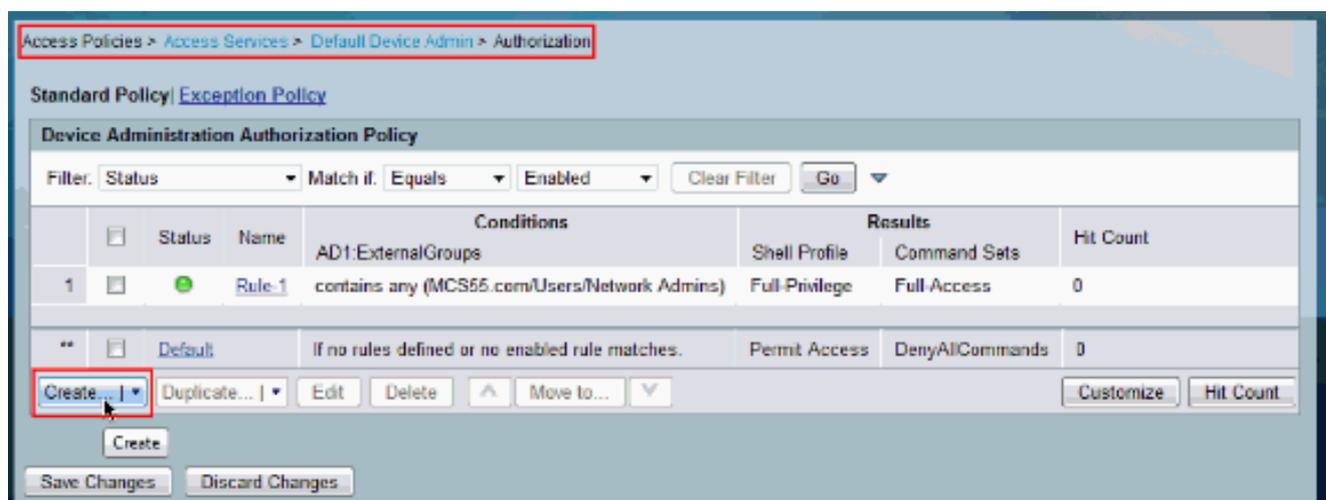
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

|

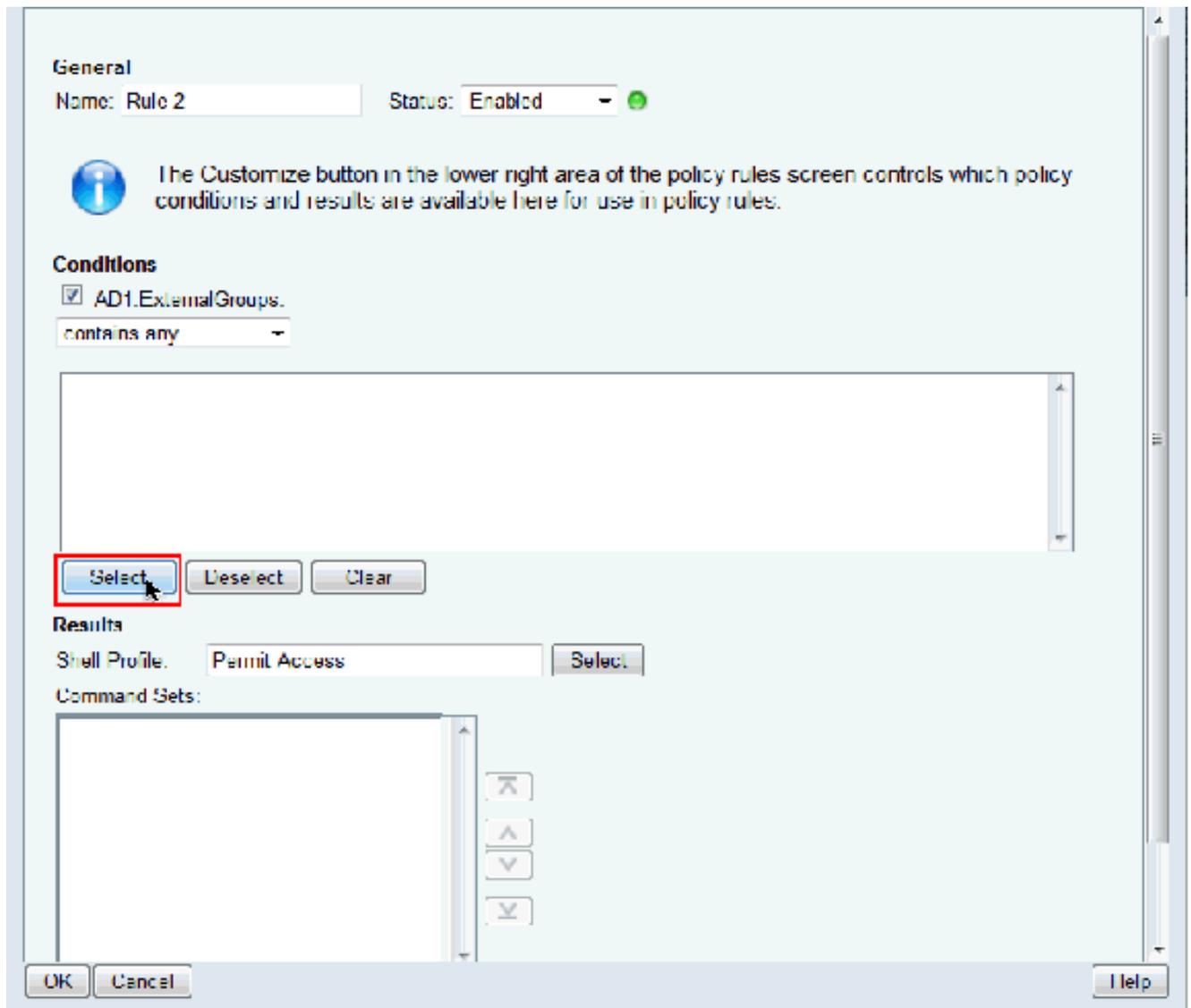
24. Click OK. Isso conclui a configuração da Regra-1.



25. Clique em Criar para criar uma nova Regra para usuários com acesso limitado.



26. Escolha AD1:ExternalGroups e clique em Select.



27. Escolha o(s) grupo(s) ao(s) qual(is) você deseja conceder acesso limitado e clique em OK.

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. Clique em Select no campo Shell Profile.



29. Clique em Create para criar um novo Shell Profile para acesso limitado.

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. Forneça um Nome e Descrição (opcional) na guia Geral e clique na guia Tarefas comuns.

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

⚙ = Required fields

31. Altere o Privilégio padrão e o Privilégio máximo para Estático com valores 1 e 15 respectivamente. Clique em Submit.

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. Click OK.

Shell Profiles

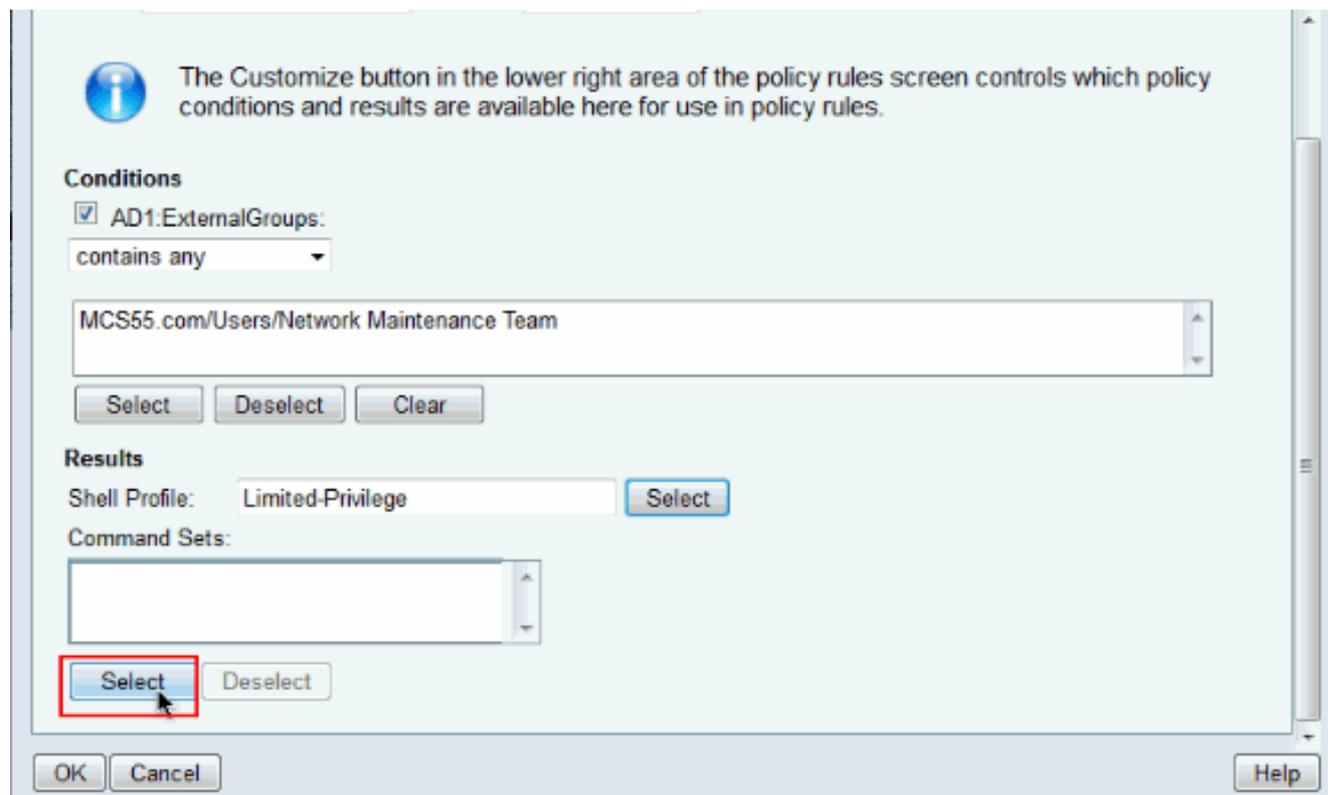
Filter: Match if: Go

	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	

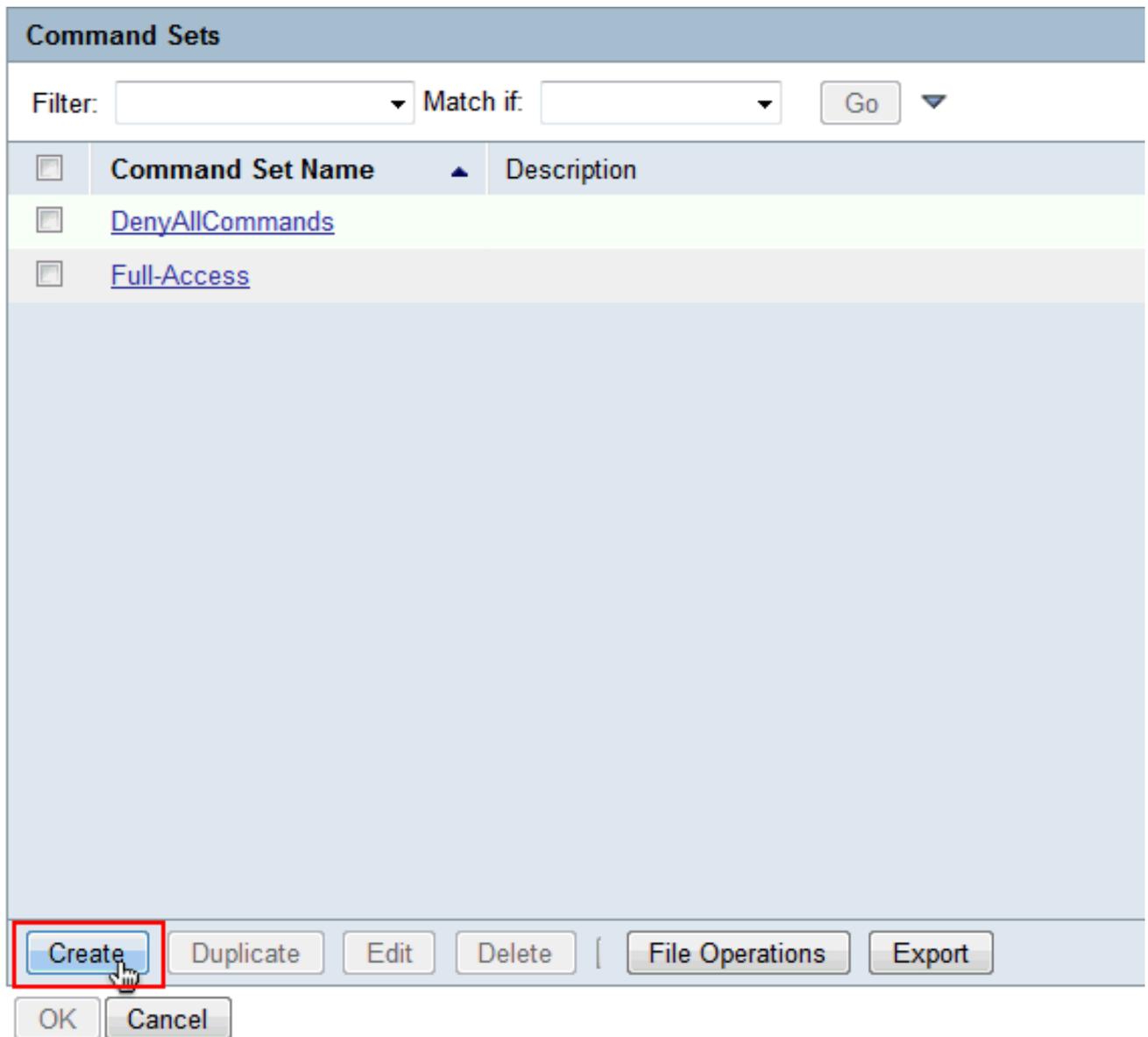
Create Duplicate Edit Delete

OK Cancel

33. Clique em Selecionar no campo Conjuntos de Comandos.



34. Clique em Criar para criar um novo Conjunto de Comandos para o grupo de acesso limitado.



35. Forneça um Nome e verifique se a caixa de seleção ao lado de Permitir qualquer comando que não esteja na tabela abaixo não está marcada. Clique em Adicionar depois de digitar show no espaço fornecido na seção command e escolha Permit na seção Grant para que somente os comandos show sejam permitidos para os usuários no grupo de acesso limitado.

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. Da mesma forma, adicione outros comandos a serem permitidos para os usuários em um grupo de acesso limitado com o uso de Add. Clique em Submit.

Observação: consulte [Criação, Duplicação e Edição de Conjuntos de Comandos para Administração de Dispositivos](#) para obter mais informações sobre Conjuntos de Comandos.

General

Name:

Description:

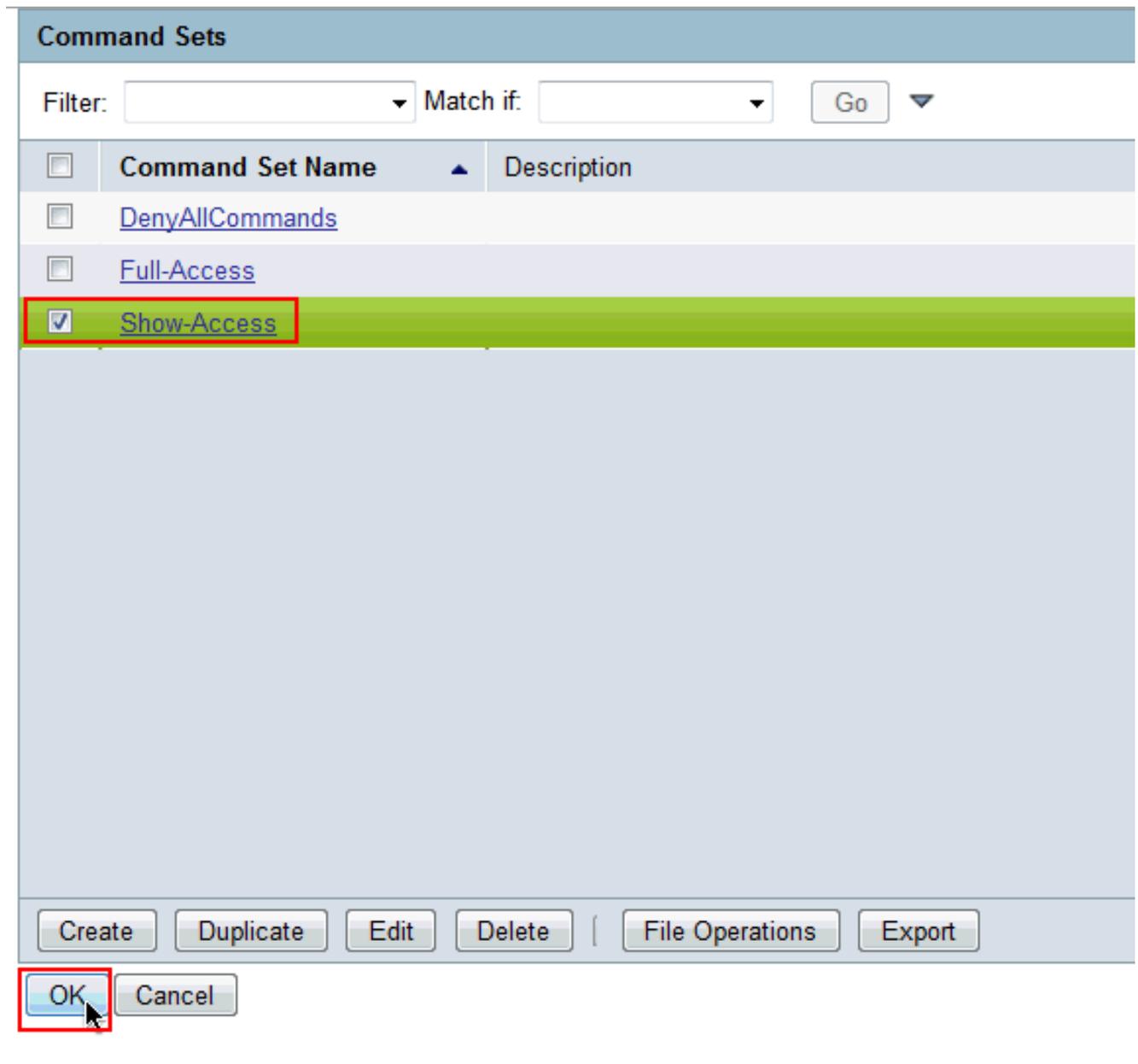
Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

37. Click OK.



38. Click 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

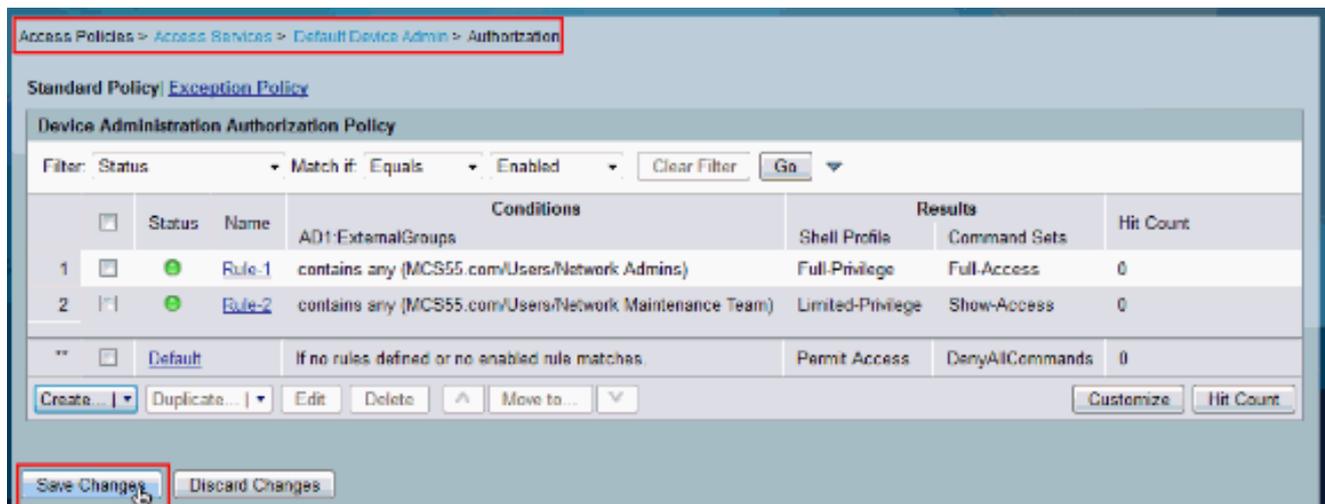
Select

Deselect

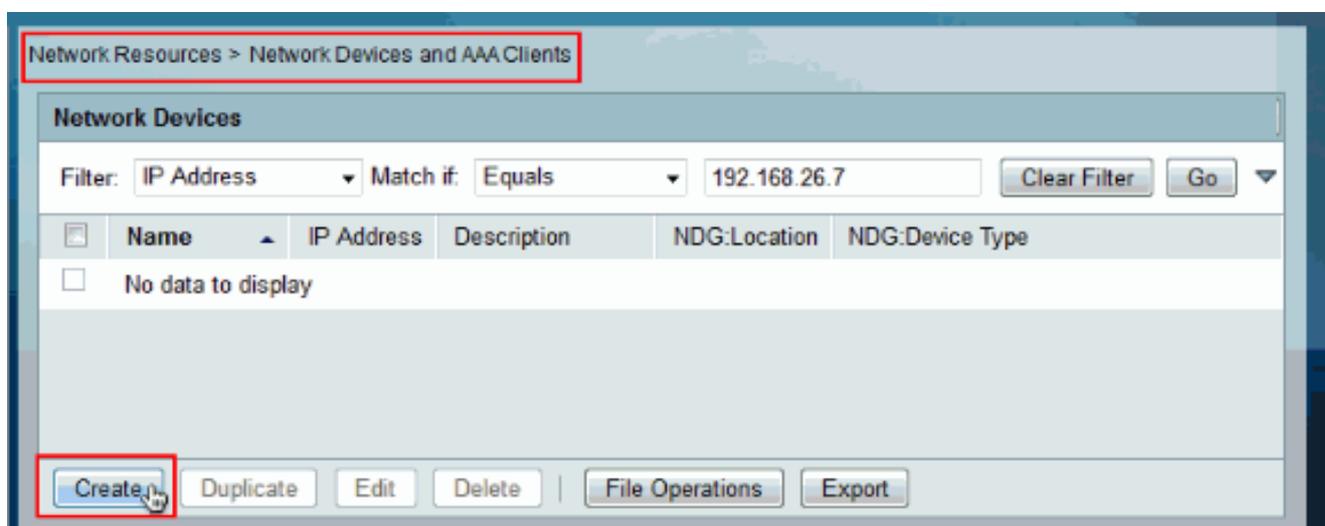
OK

Cancel

39. Clique em Save Changes.



40. Clique em Create para adicionar o dispositivo Cisco IOS como um AAA Client no ACS.



41. Forneça um nome, endereço IP, segredo compartilhado para TACACS+ e clique em Enviar.

Configurar o dispositivo IOS Cisco para autenticação e autorização

Conclua estas etapas para configurar o dispositivo Cisco IOS e o ACS para Autenticação e Autorização.

1. Crie um usuário local com privilégio total para fallback com o comando `username`, como mostrado aqui:

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

2. Forneça o endereço IP do ACS para habilitar o AAA e adicionar o ACS 5.x como servidor TACACS.

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

Observação: a chave deve corresponder ao segredo compartilhado fornecido no ACS para este dispositivo IOS Cisco.

3. Teste a alcançabilidade do servidor TACACS com o comando `test aaa` como mostrado.

```
test aaa group tacacs+ user1 xxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+
```

User was successfully authenticated.

A saída do comando anterior mostra que o servidor TACACS está acessível e que o usuário foi autenticado com êxito.

Observação: User1 e a senha xxx pertencem ao AD. Se o teste falhar, verifique se o segredo compartilhado fornecido na etapa anterior está correto.

4. Configure o login e habilite as autenticações e use as autorizações de execução e de comando como mostrado aqui:

```
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
```

Observação: as palavras-chave Local e Enable são usadas para fallback para o usuário local do Cisco IOS e enable secret, respectivamente, se o servidor TACACS estiver inacessível.

Verificar

Para verificar a autenticação e o login de autorização no dispositivo IOS Cisco através de Telnet.

1. Faça Telnet para o dispositivo Cisco IOS como user1 que pertence ao grupo de acesso completo no AD. O grupo Administradores de Rede é o grupo no AD que é mapeado para Perfil do Shell de Privilégio Completo e Comando de Acesso Completo no ACS. Tente executar qualquer comando para garantir que você tenha acesso total.

```
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. Execute Telnet para o dispositivo Cisco IOS como o usuário2 que pertence ao grupo de acesso limitado no AD. (O grupo Network Maintenance Team é o grupo no AD que é mapeado para Limited-Privilege Shell Profile e Show-Access Command set no ACS). Se você tentar executar qualquer comando diferente dos mencionados no conjunto de comandos Show-Access, receberá um erro Command Authorization Failed, que mostra que o usuário2 tem acesso limitado.

```
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
FTWARE (fc1)
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, 46 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-44.SE6.bin"

          55
          55
          55

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/qa/slsrpg.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. Faça login na GUI do ACS e inicie o Monitoring and Reports viewer. Escolha AAA Protocol > TACACS+Authorization para verificar as atividades executadas por user1 e user2.

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=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=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

Informações Relacionadas

- [Cisco Secure Access Control System](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.