

ACS 5.x:AD 그룹 멤버십 컨피그레이션 예제에 따른 TACACS+ 인증 및 명령 권한 부여

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[인증 및 권한 부여를 위해 ACS 5.x 구성](#)

[인증 및 권한 부여를 위해 Cisco IOS 디바이스 구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ACS(Secure Access Control System) 5.x 이상을 사용하는 사용자의 AD 그룹 멤버십을 기반으로 TACACS+ 인증 및 명령 권한 부여를 구성하는 예를 제공합니다.ACS는 Microsoft AD(Active Directory)를 외부 ID 저장소로 사용하여 사용자, 시스템, 그룹 및 특성과 같은 리소스를 저장합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ACS 5.x는 원하는 AD 도메인에 완벽하게 통합됩니다.ACS가 원하는 AD 도메인과 통합되지 않은 경우 [ACS 5.x 이상](#)을 참조하십시오.통합 작업을 수행하기 위한 자세한 내용은 [Microsoft Active Directory 구성](#) 예와 통합하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS 5.3
- Cisco IOS[®] Software 릴리스 12.2(44)SE6.참고: 이 컨피그레이션은 모든 Cisco IOS 디바이스에서 수행할 수 있습니다.
- Microsoft Windows Server 2003 도메인

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

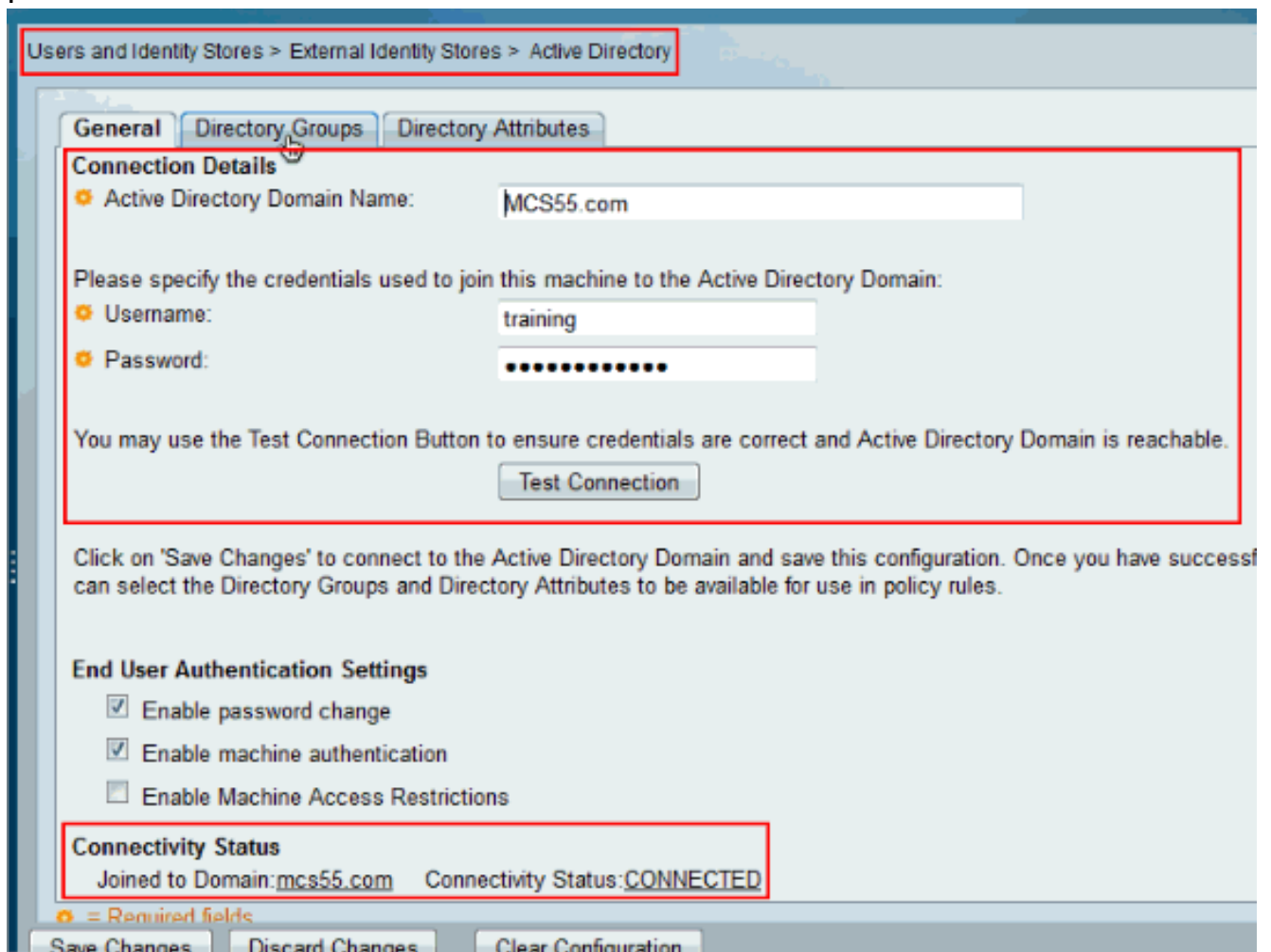
구성

인증 및 권한 부여를 위해 ACS 5.x 구성

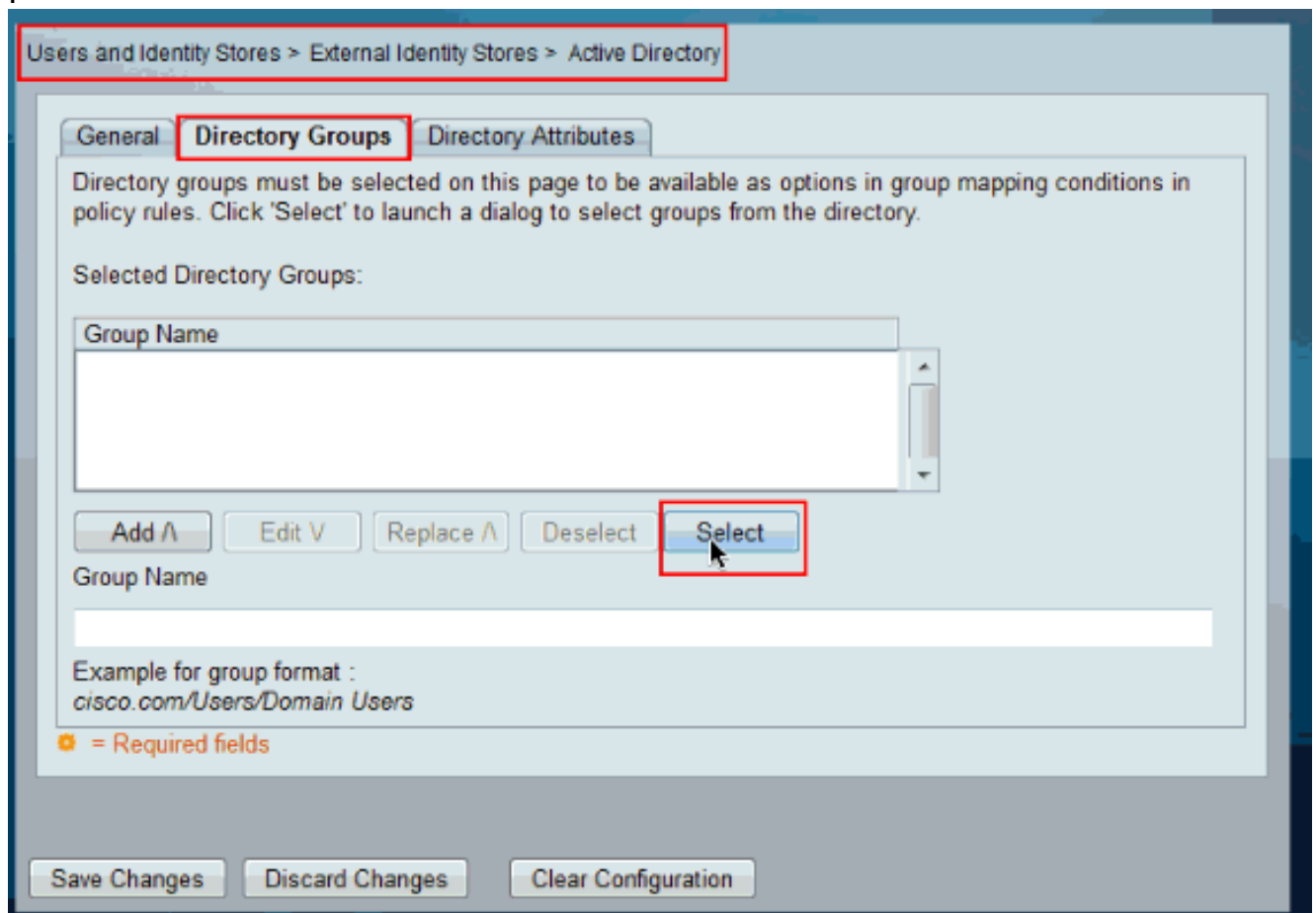
인증 및 권한 부여를 위한 ACS 5.x 구성을 시작하기 전에 ACS가 Microsoft AD와 성공적으로 통합되어야 합니다.ACS가 원하는 AD 도메인과 통합되지 않은 경우 [ACS 5.x 이상](#)을 참조하십시오.통합 작업을 수행하기 위한 자세한 내용은 [Microsoft Active Directory 구성](#) 예와 통합하십시오.

이 섹션에서는 두 개의 AD 그룹을 두 개의 서로 다른 명령 세트와 두 개의 셸 프로파일(하나는 전체 액세스 권한이 있고 다른 하나는 Cisco IOS 디바이스에서 제한된 액세스)에 매핑합니다.

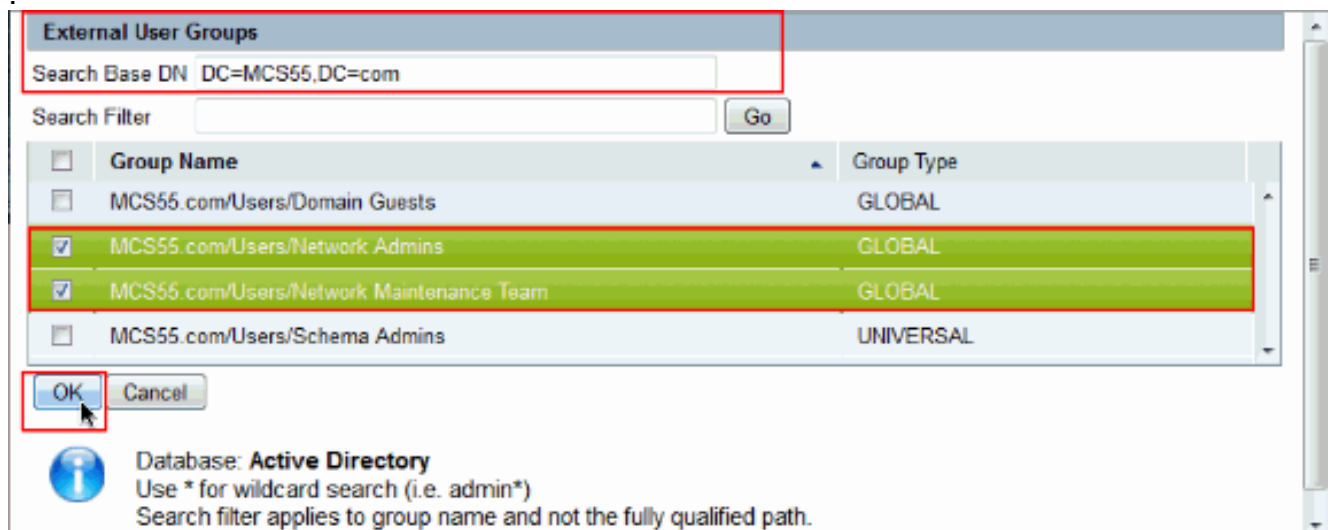
1. 관리자 자격 증명을 사용하여 ACS GUI에 로그인합니다.
2. **Users and Identity Stores(사용자 및 ID 저장소) > External Identity Stores(외부 ID 저장소) > Active Directory**를 선택하고 ACS가 원하는 도메인에 가입되어 있는지, **연결 상태가 연결된 것**으로 표시되는지 **확인**합니다.**Directory Groups(디렉토리 그룹)** 탭을 클릭합니다



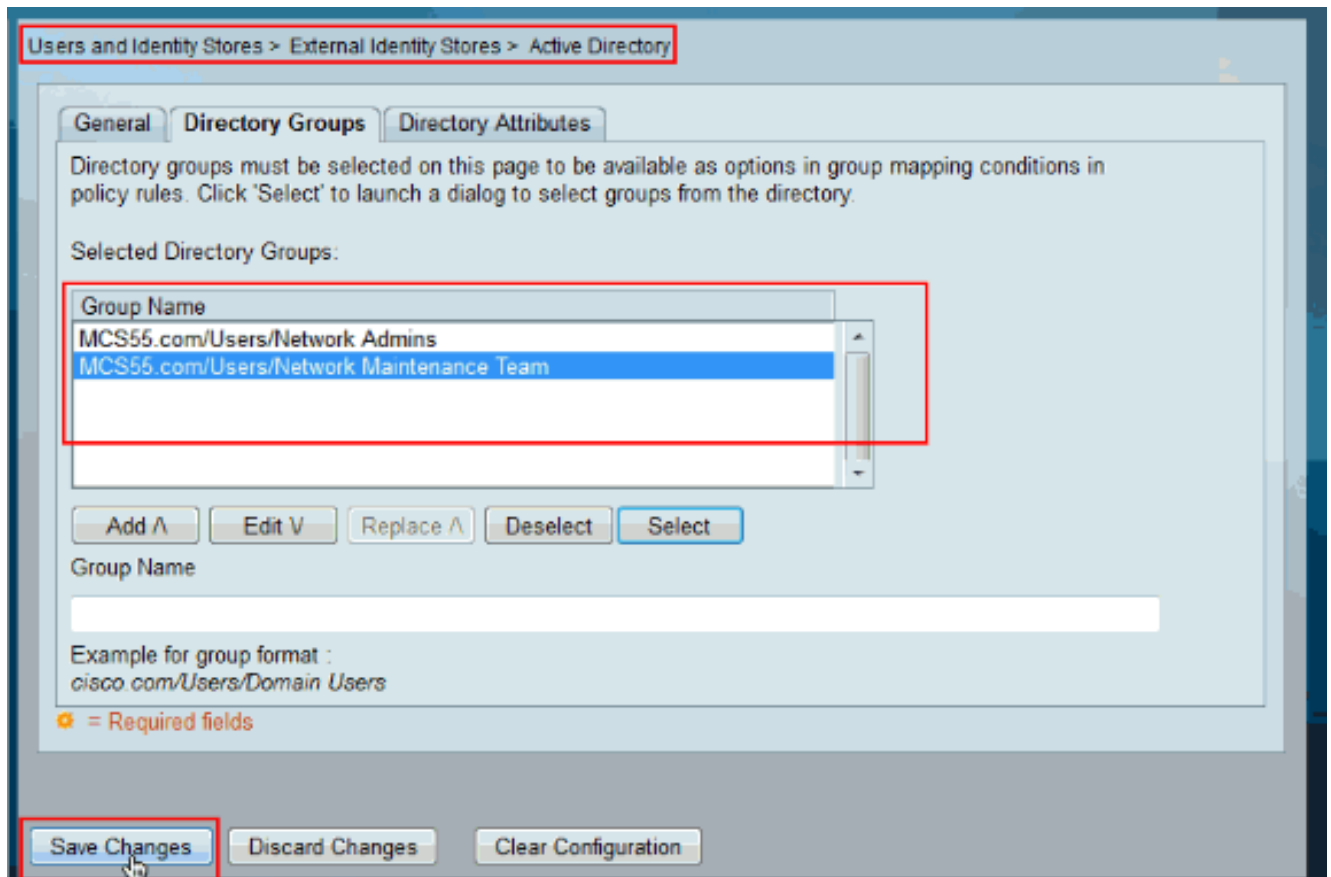
3. 선택을 클릭합니다



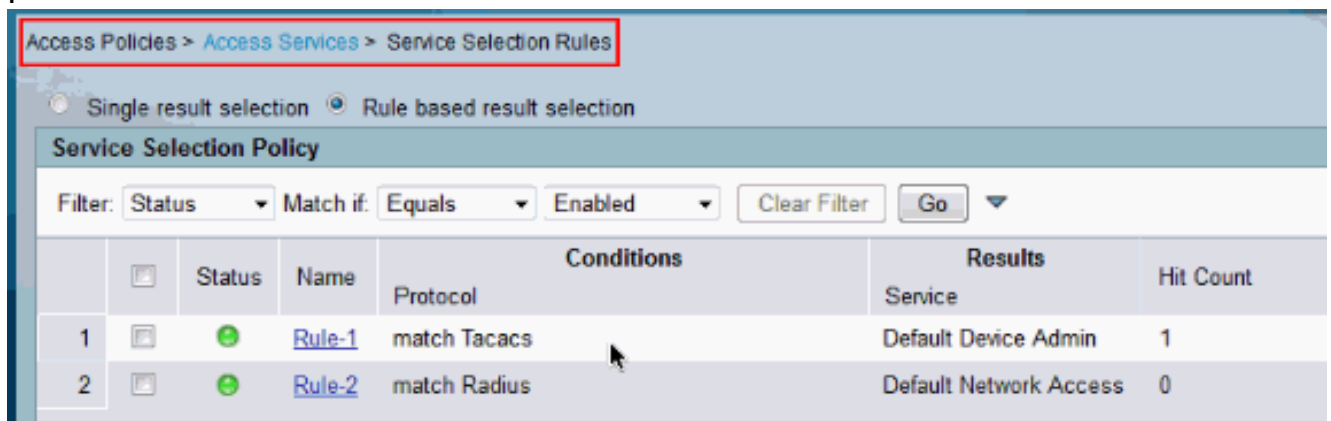
4. 컨피그레이션의 윗부분에 있는 셀 프로필 및 명령 집합에 매핑해야 하는 그룹을 선택합니다.
.확인을 클릭합니다



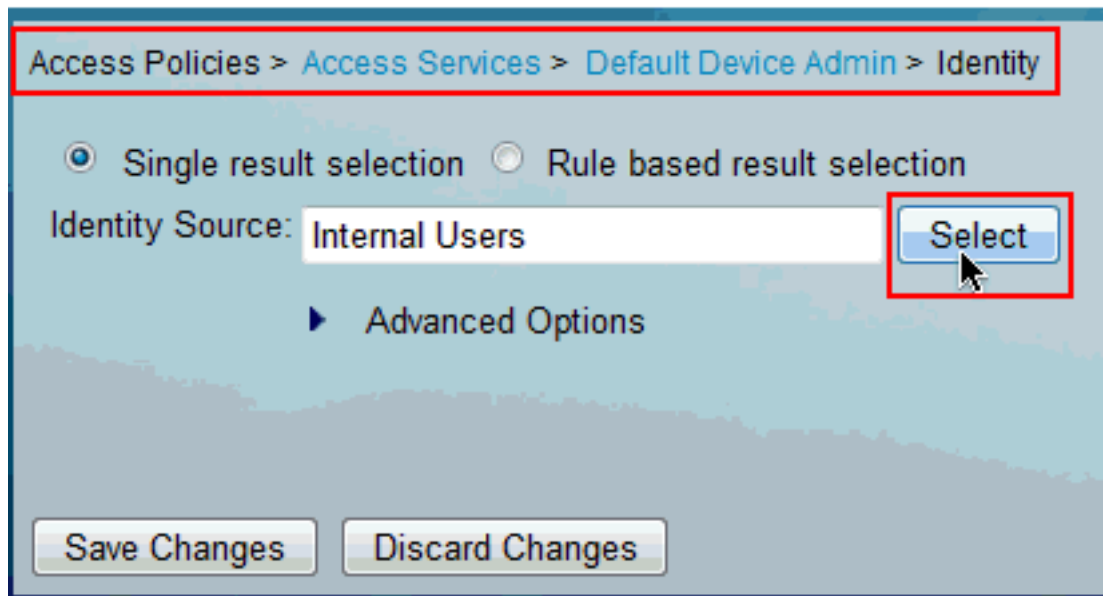
5. Save Changes를 클릭합니다



6. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Service Selection Rules(서비스 선택 규칙)를 선택하고 액세스 서비스를 식별하며, 이는 TACACS+ 인증을 처리합니다.이 예에서는 기본 디바이스 관리입니다

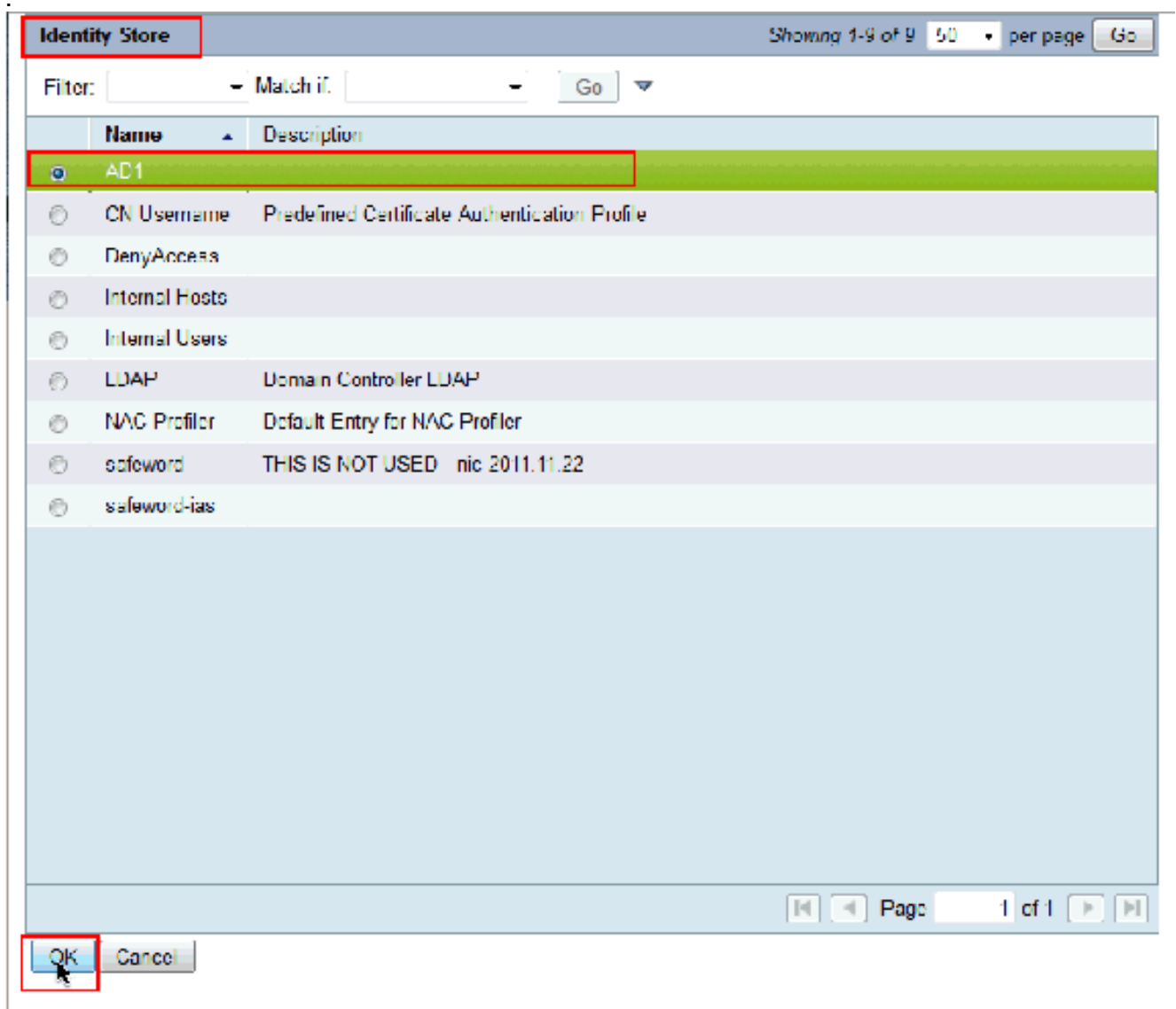


7. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Device Admin(기본 디바이스 관리자) > Identity(ID)를 선택하고 Identity Source(ID 소스) 옆에 있는 Select(선택

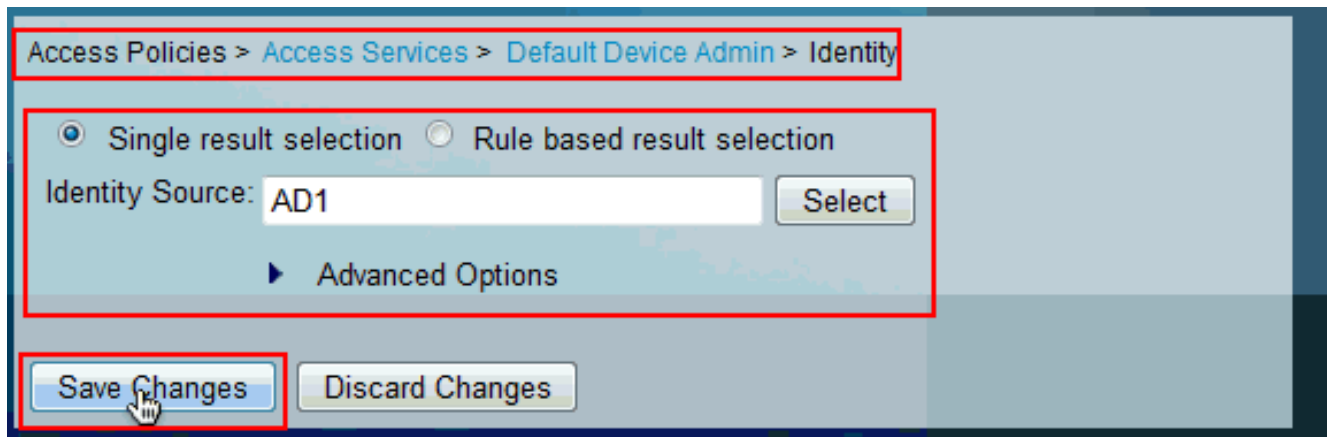


)를 클릭합니다.

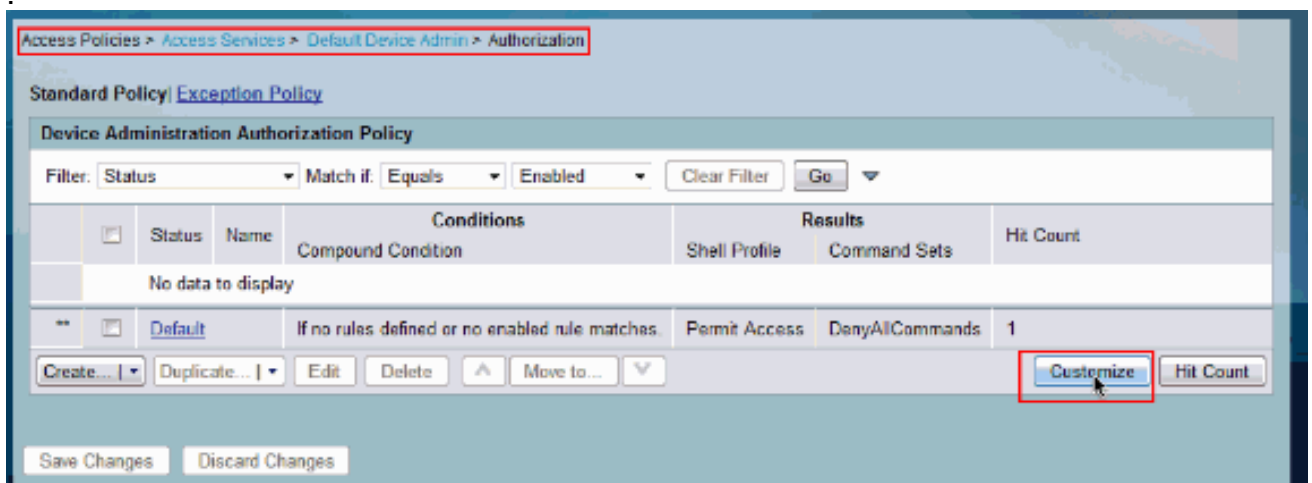
8. AD1을 선택하고 OK를 클릭합니다



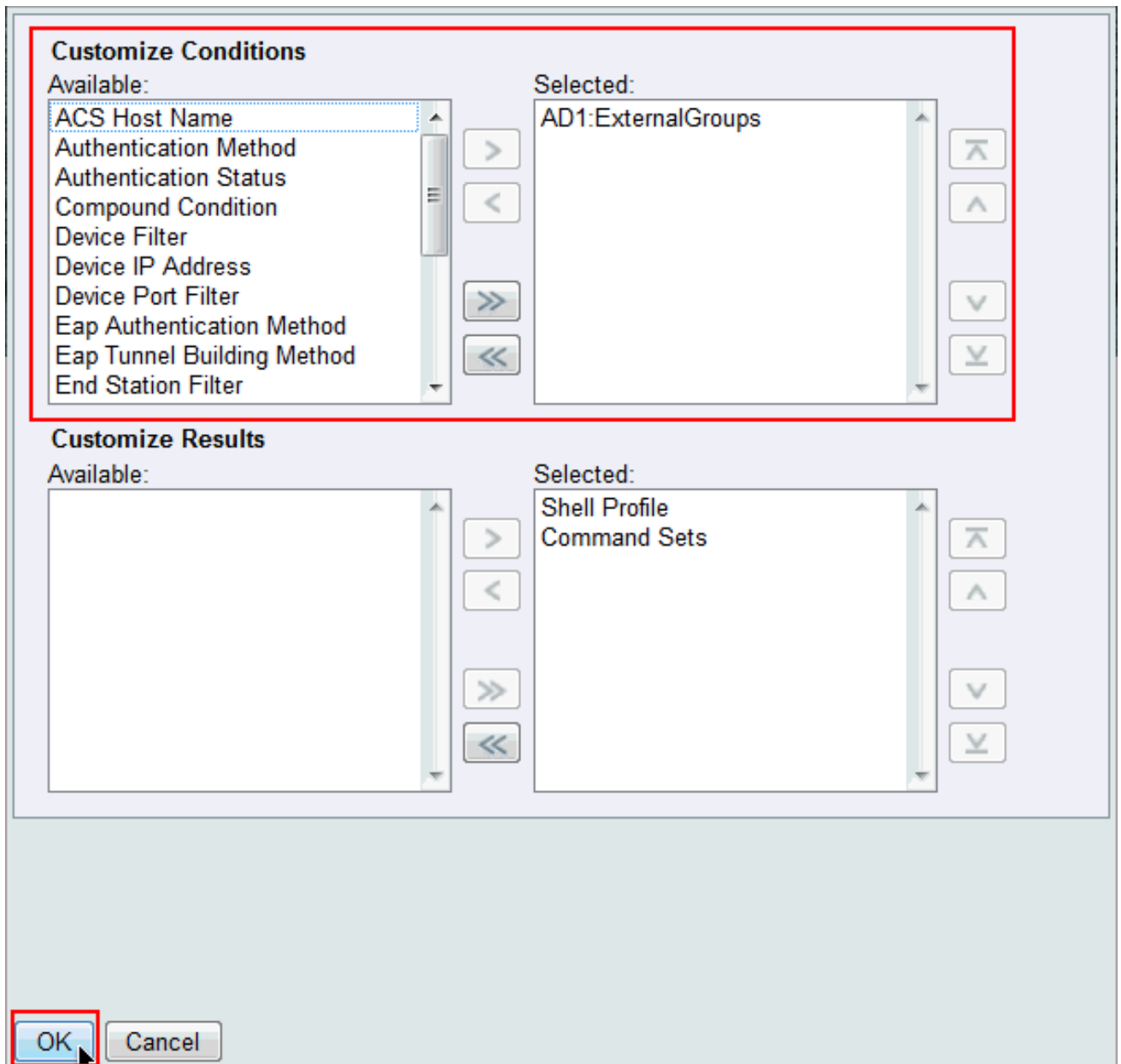
9. Save Changes를 클릭합니다



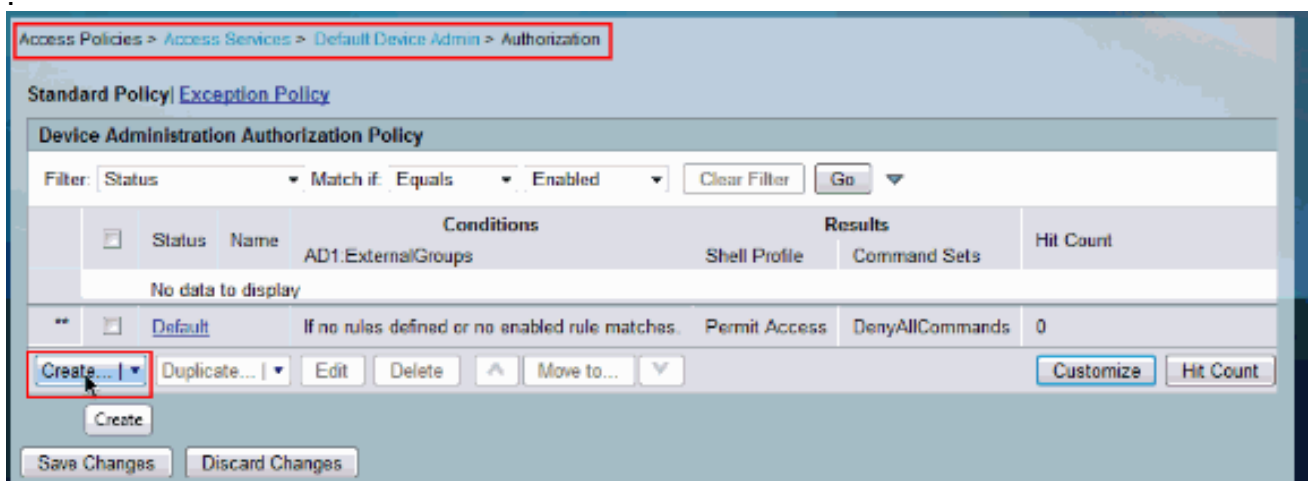
10. Access Policies(액세스 정책) > Access Services(액세스 서비스) > Default Device Admin(기본 디바이스 관리자) > Authorization(권한 부여)을 선택하고 Customize(사용자 지정)를 클릭합니다



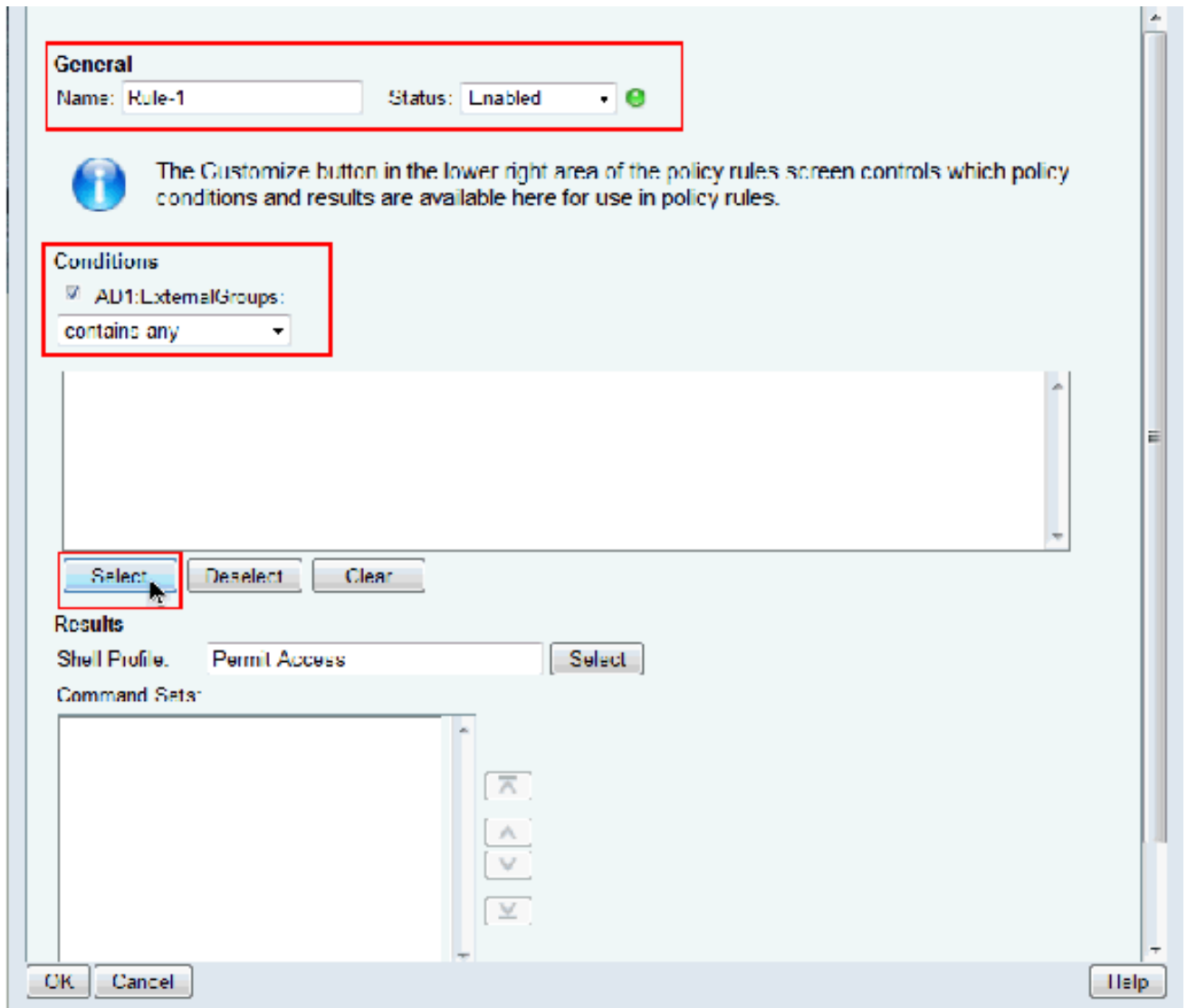
11. AD1:ExternalGroups를 Available from Customize Conditions(사용 가능) 섹션에서 Selected(선택한)로 복사한 다음 Available(사용 가능)에서 Customize Results(사용자 지정 결과)의 Selected(선택한) 섹션으로 셸 프로파일 및 명령 세트를 이동합니다.이제 OK(확인)를 클릭합니다



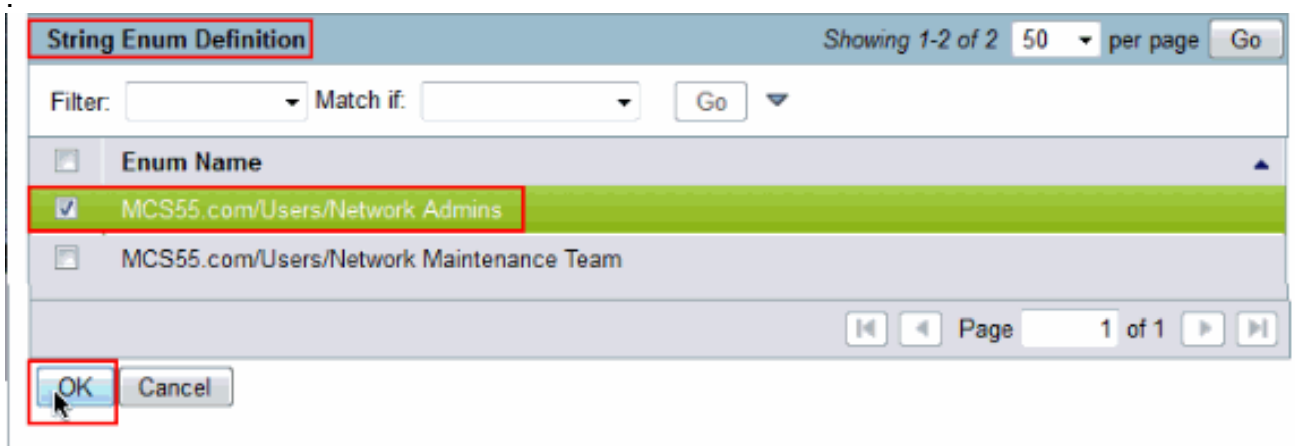
12. 새 규칙을 생성하려면 Create를 클릭합니다



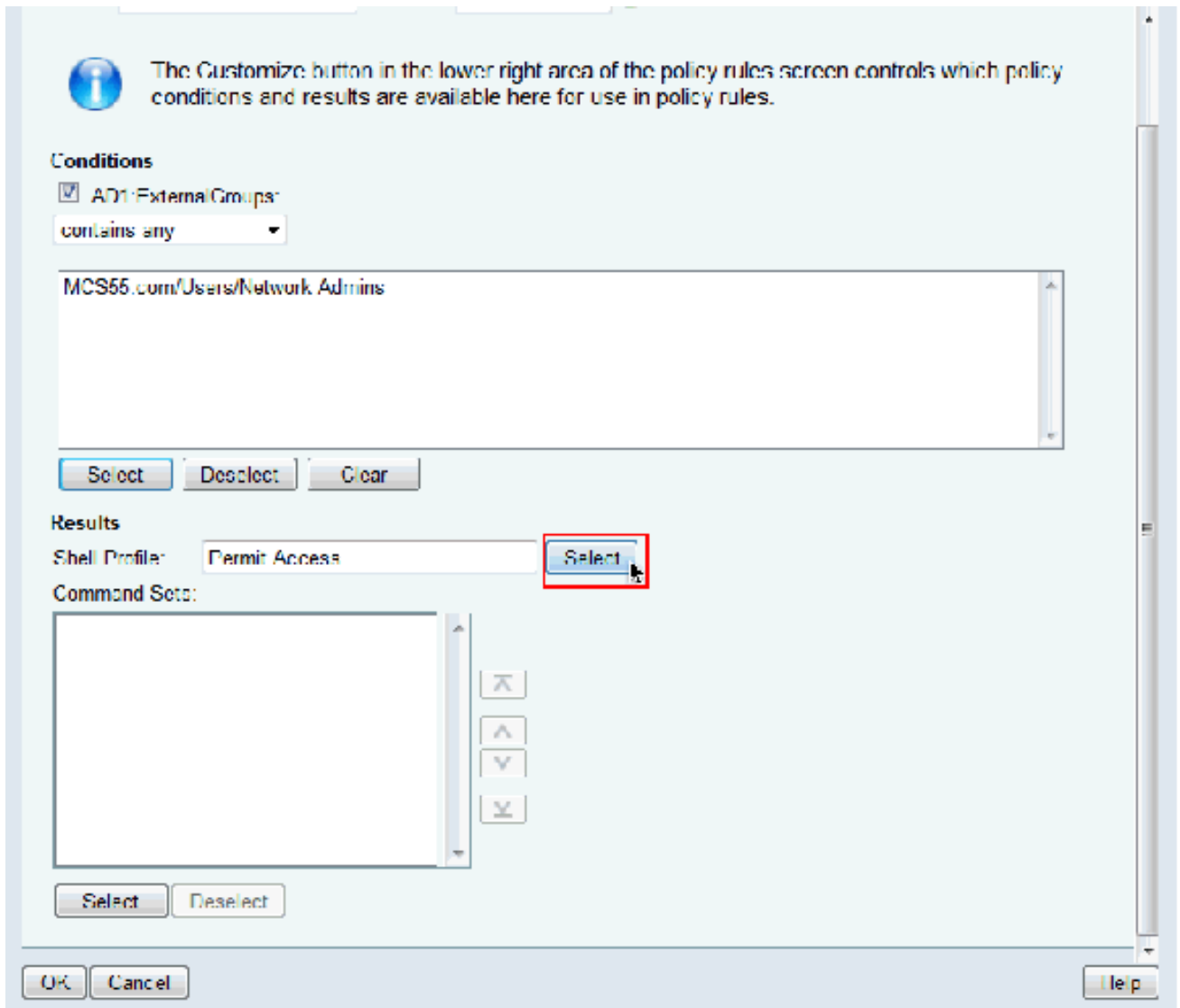
13. AD1:ExternalGroups Condition에서 Select(선택)를 클릭합니다



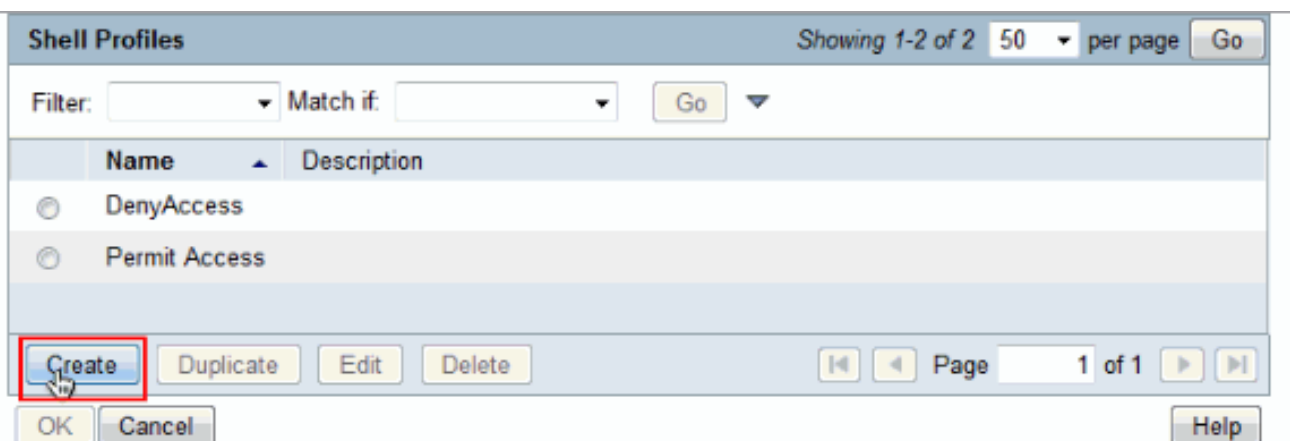
14. Cisco IOS 디바이스에서 전체 액세스를 제공할 그룹을 선택합니다. 확인을 클릭합니다



15. 셸 프로필 필드에서 선택을 클릭합니다



16. 전체 액세스 사용자에게 대한 새 셸 프로파일을 생성하려면 Create(생성)를 클릭합니다



17. General(일반) 탭에서 Name(이름) 및 Description(설명)(선택 사항)을 제공하고 Common Tasks(공통 작업) 탭을 클릭합니다

General Common Tasks Custom Attributes

☀ Name: Full-Privilege

Description: To push default privilege 15 for IOS

☀ = Required fields

18. 기본 권한 및 최대 권한을 값 15의 정적으로 변경하고 제출을 누릅니다

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

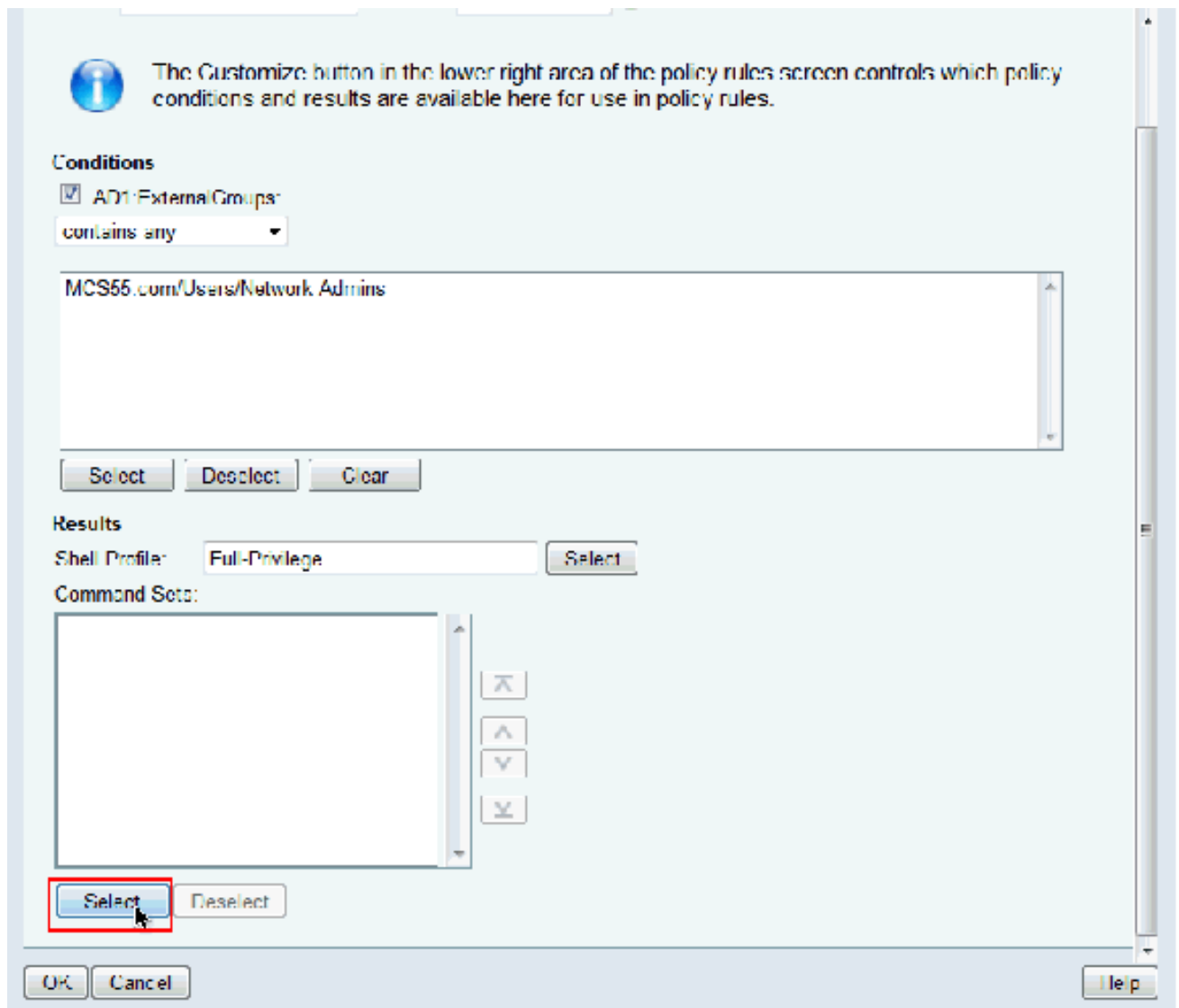
- 이제 새로 생성된 전체 액세스 셸 프로파일(이 예에서는 전체 권한)을 선택하고 확인을 클릭합니다

Shell Profiles

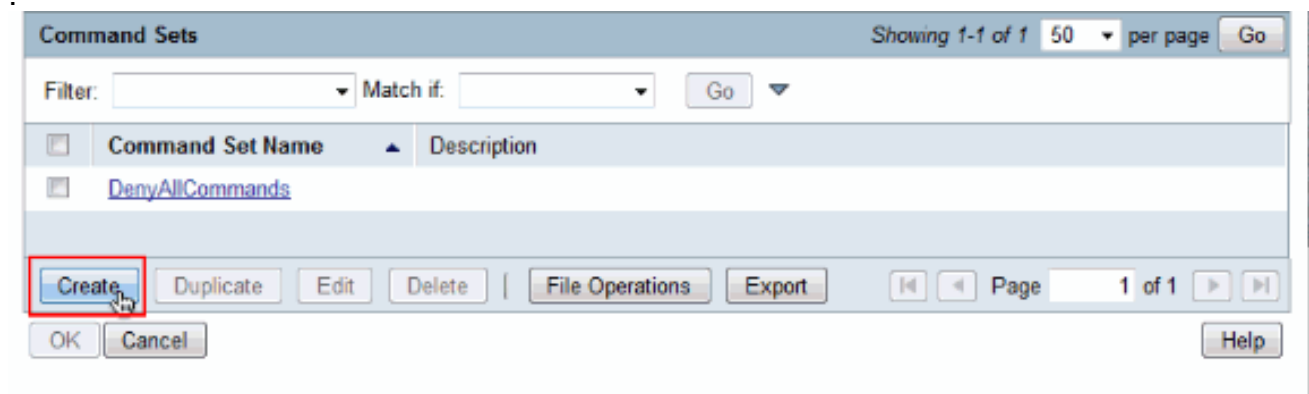
Filter: Match if:

	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** 필드에서 Select를 클릭합니다



21. Create(생성)를 클릭하여 전체 액세스 사용자에게 대한 새 명령 세트를 생성합니다



22. 이름을 제공하고 아래 표에 없는 명령 허용 옆의 확인란이 선택되어 있는지 확인합니다 .Submit(제출)을 클릭합니다.참고: 명령 세트에 대한 자세한 내용은 [디바이스 관리를 위한 명령 세트 생성, 복제 및 편집](#)을 참조하십시오

General

Name:
 Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Add Edit Replace Delete

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

23. 확인을 클릭합니다

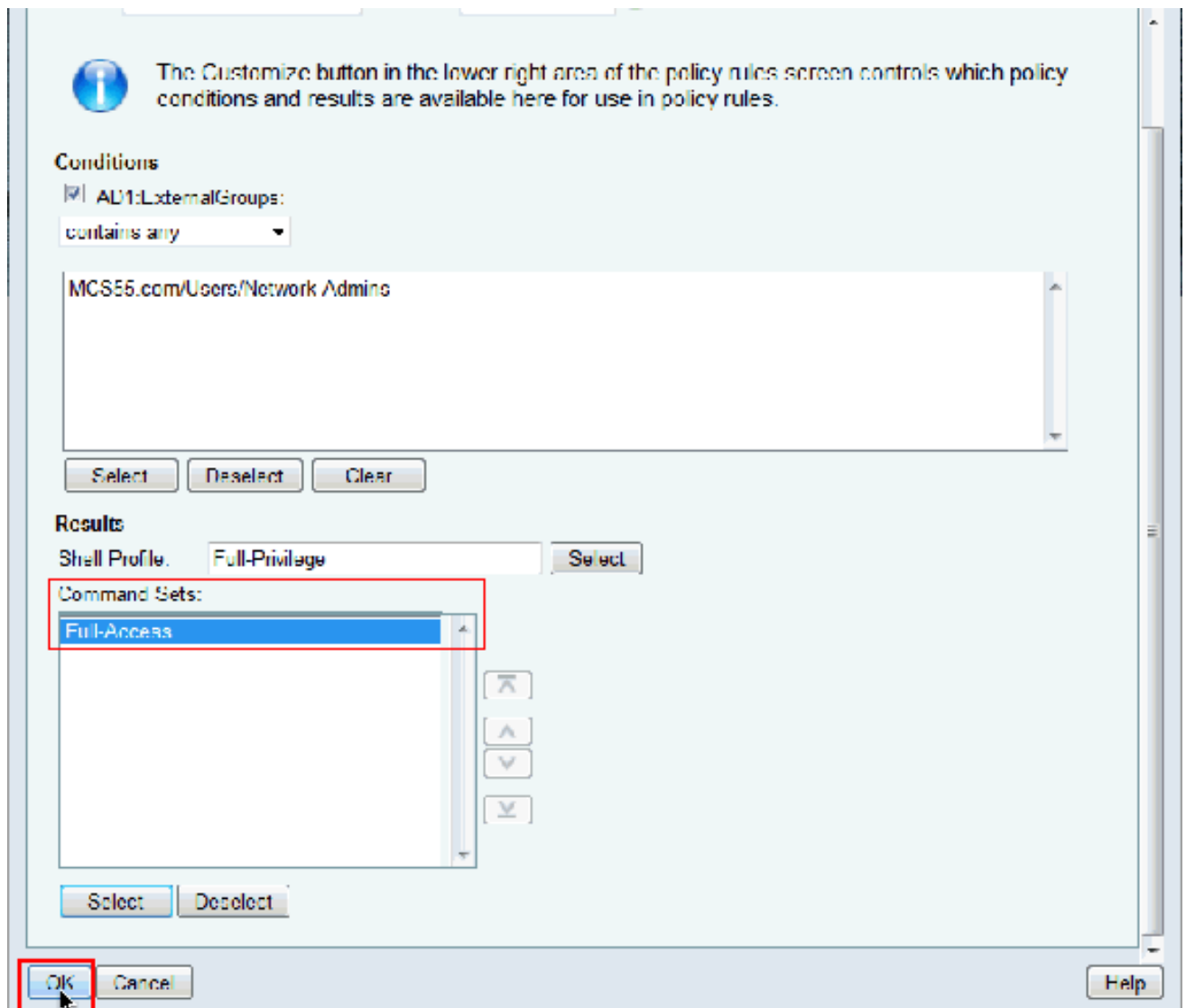
Command Sets

Filter: Match if:

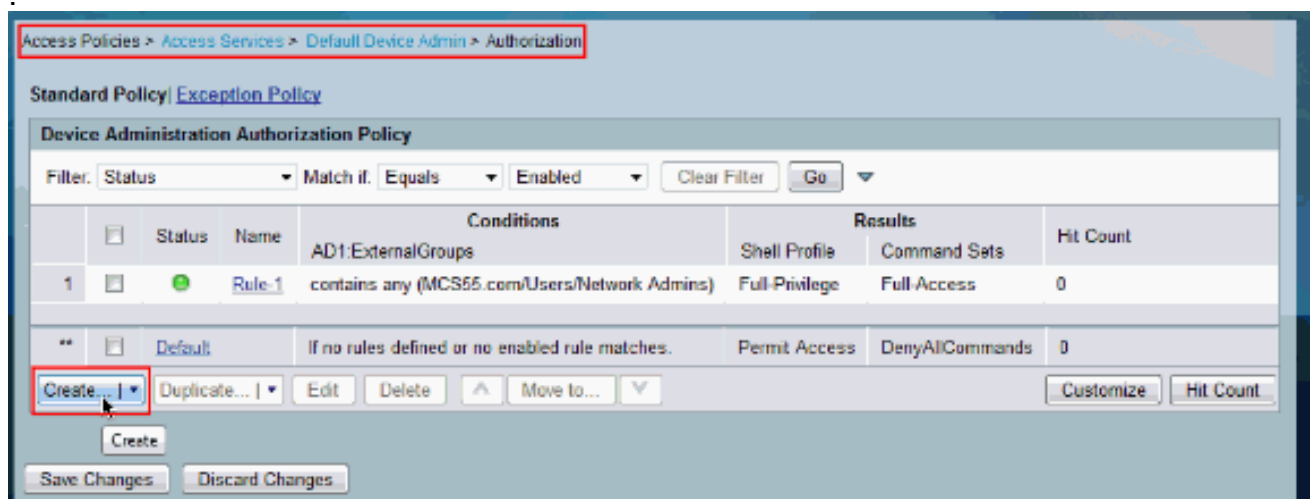
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

|

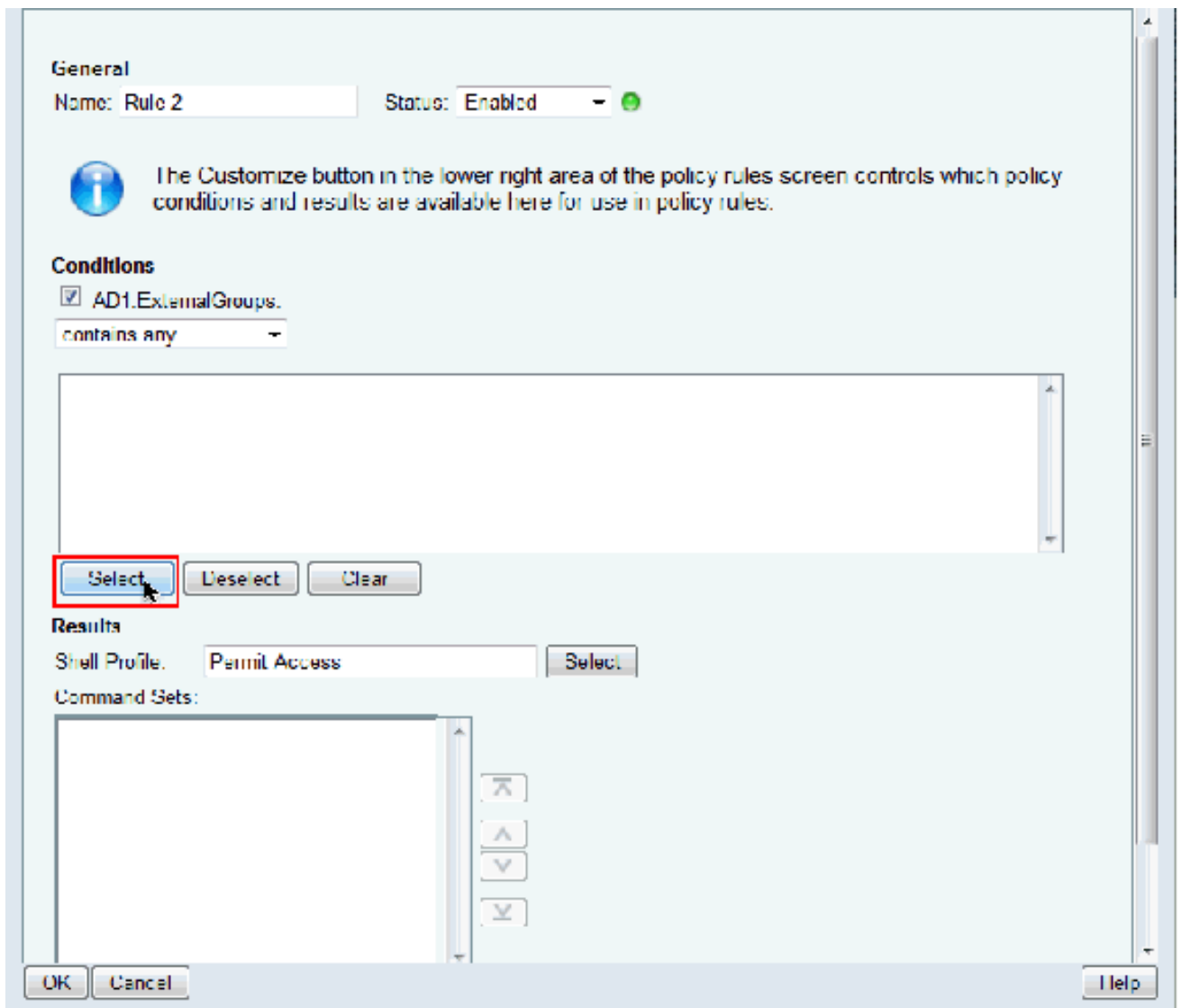
24. 확인을 클릭합니다. 이렇게 하면 Rule-1의 컨피그레이션이 완료됩니다



25. 제한된 액세스 사용자에게 대한 새 규칙을 생성하려면 Create를 클릭합니다



26. AD1:ExternalGroups를 선택하고 Select를 클릭합니다



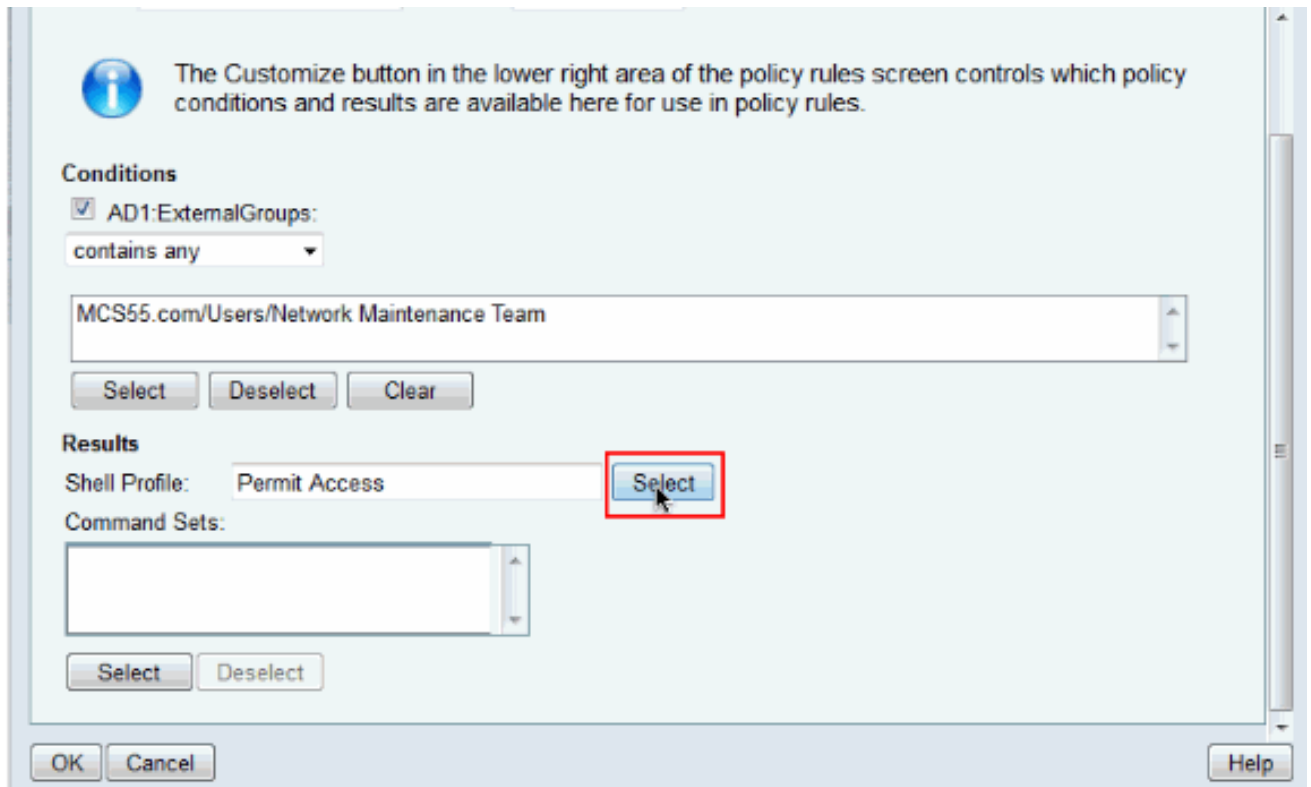
27. 제한된 액세스를 제공할 그룹 또는 그룹을 선택하고 **확인**을 클릭합니다

String Enum Definition

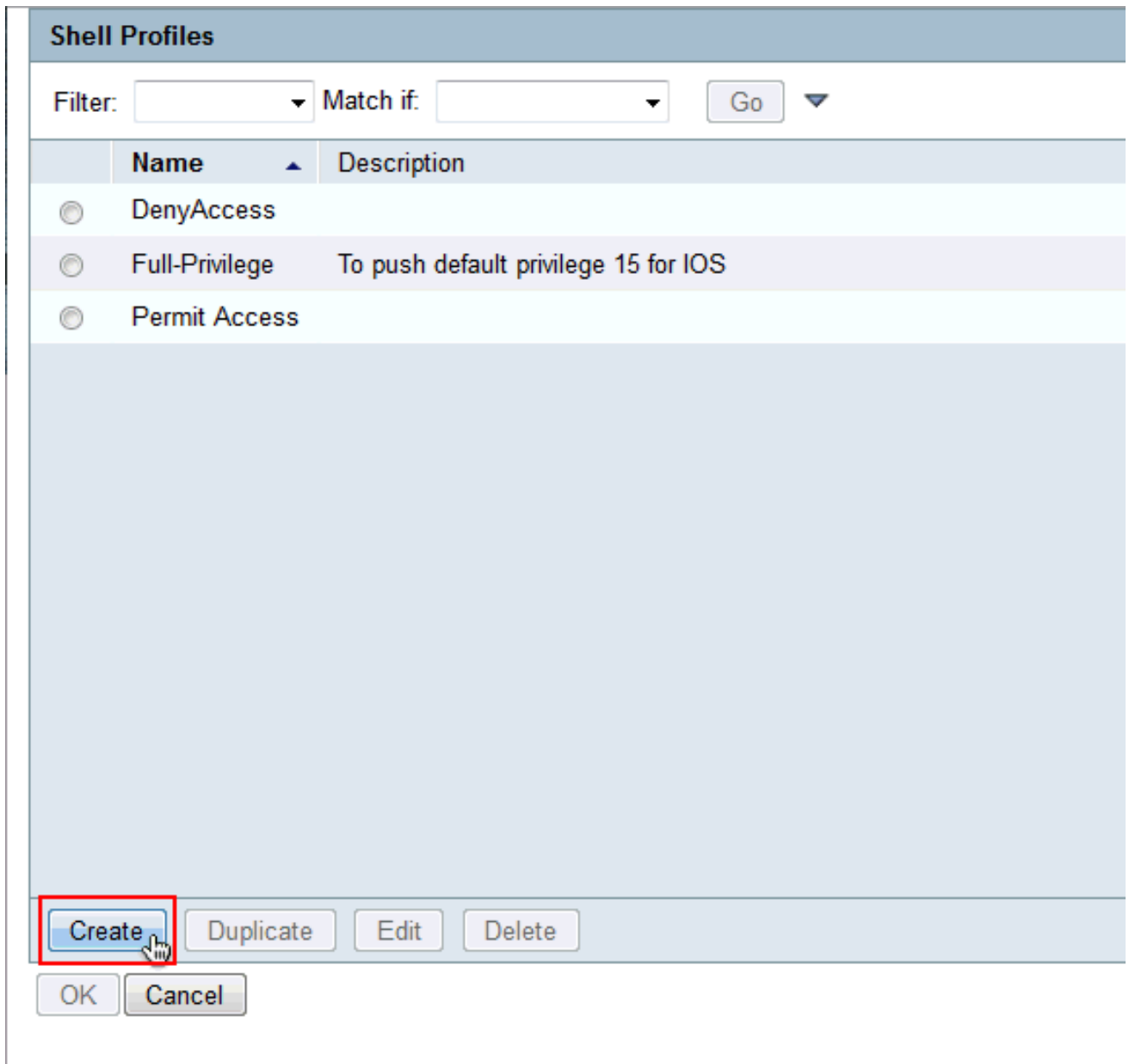
Filter: Match if: Go

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

28. 셀 **프로필** 필드에서 선택을 클릭합니다



29. Create(생성)를 클릭하여 제한된 액세스를 위한 새 셸 프로파일을 생성합니다



30. General(일반) 탭에서 Name 및 Description(선택 사항)을 제공하고 Common Tasks(공통 작업) 탭을 클릭합니다

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

☛ = Required fields

31. Default Privilege(기본 권한) 및 Maximum Privilege(최대 권한)를 Static with Values 1(값 1 및 15)로 변경합니다.Submit(제출)을 클릭합니다

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

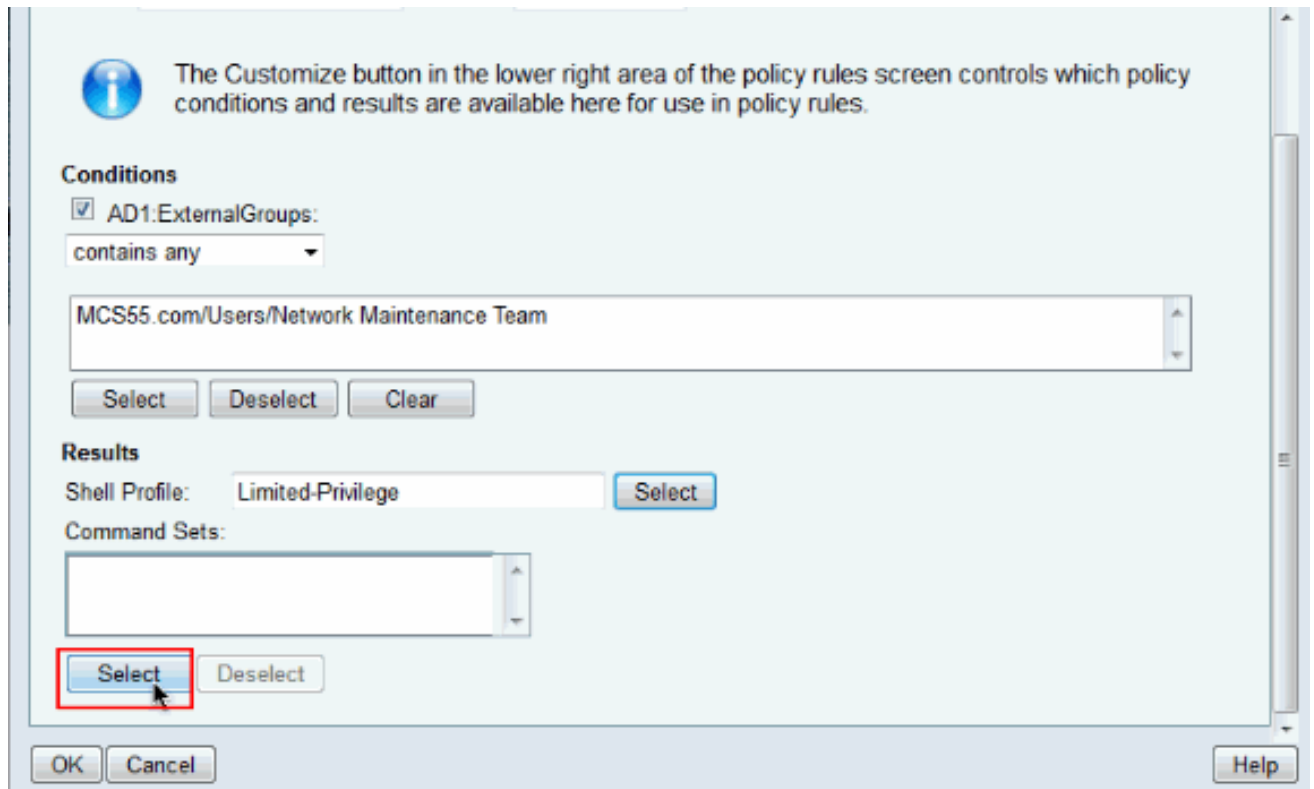
32. 확인을 클릭합니다

Shell Profiles

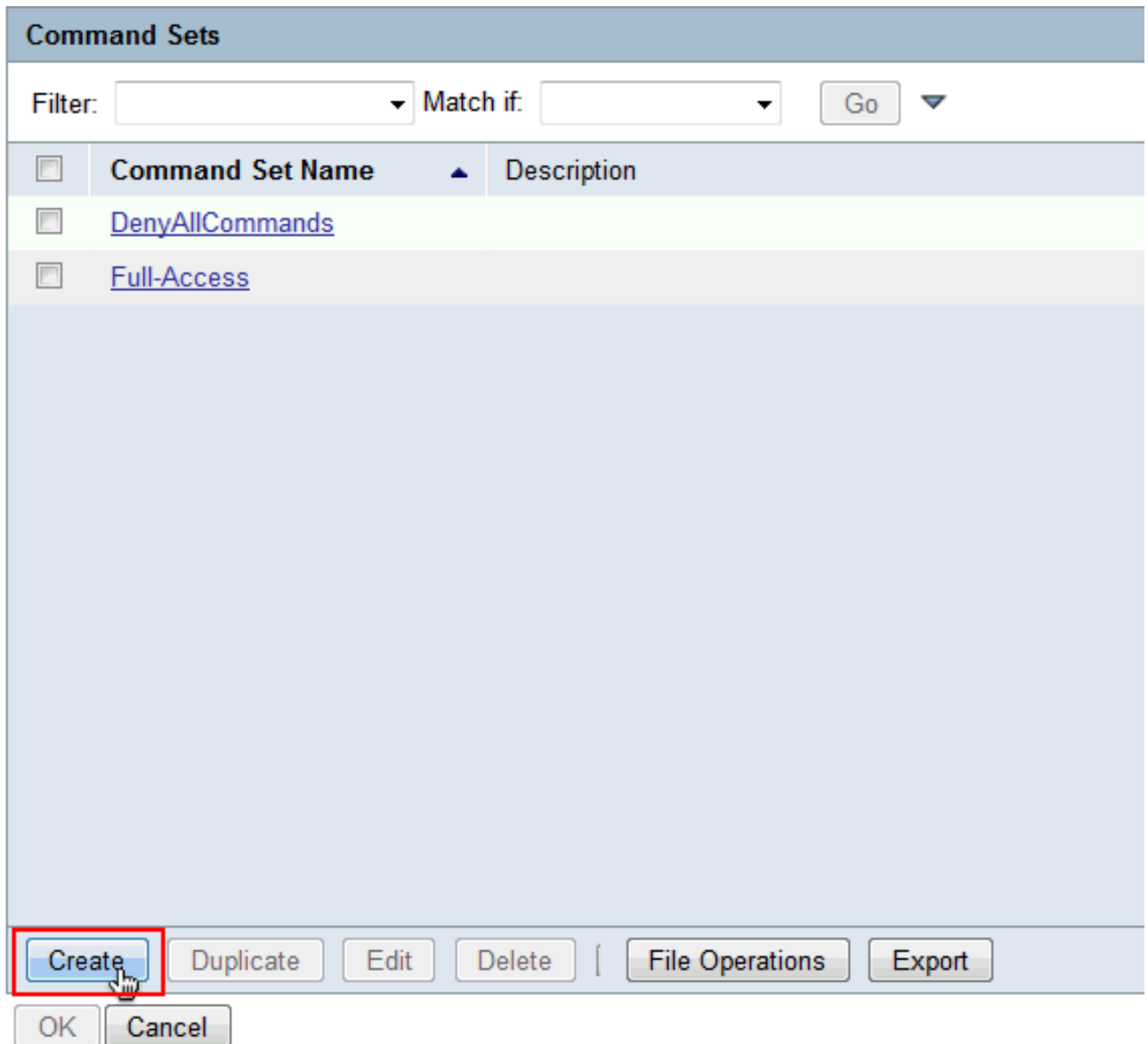
Filter: Match if:

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	

33. Command **Sets** 필드에서 Select를 클릭합니다



34. Create(생성)를 클릭하여 제한된 액세스 그룹에 대한 새 명령 세트를 생성합니다



35. 이름을 제공하고 아래 표에 없는 명령 허용 옆의 확인란이 선택되지 않았는지 확인합니다. 명령 섹션에 제공된 공간에 **show**를 입력한 후 **Add**를 클릭하고 Grant 섹션에서 Permit을 선택하여 제한된 액세스 그룹의 사용자에게 show 명령만 허용하도록 합니다

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. 마찬가지로 Add를 사용하여 제한된 액세스 그룹의 사용자에게 허용할 다른 모든 명령을 추가합니다. Submit(제출)을 클릭합니다. 참고: 명령 [세트에](#) 대한 자세한 내용은 [디바이스 관리를 위한 명령 세트 생성, 복제 및 편집](#)을 참조하십시오

General

Name:

Description:

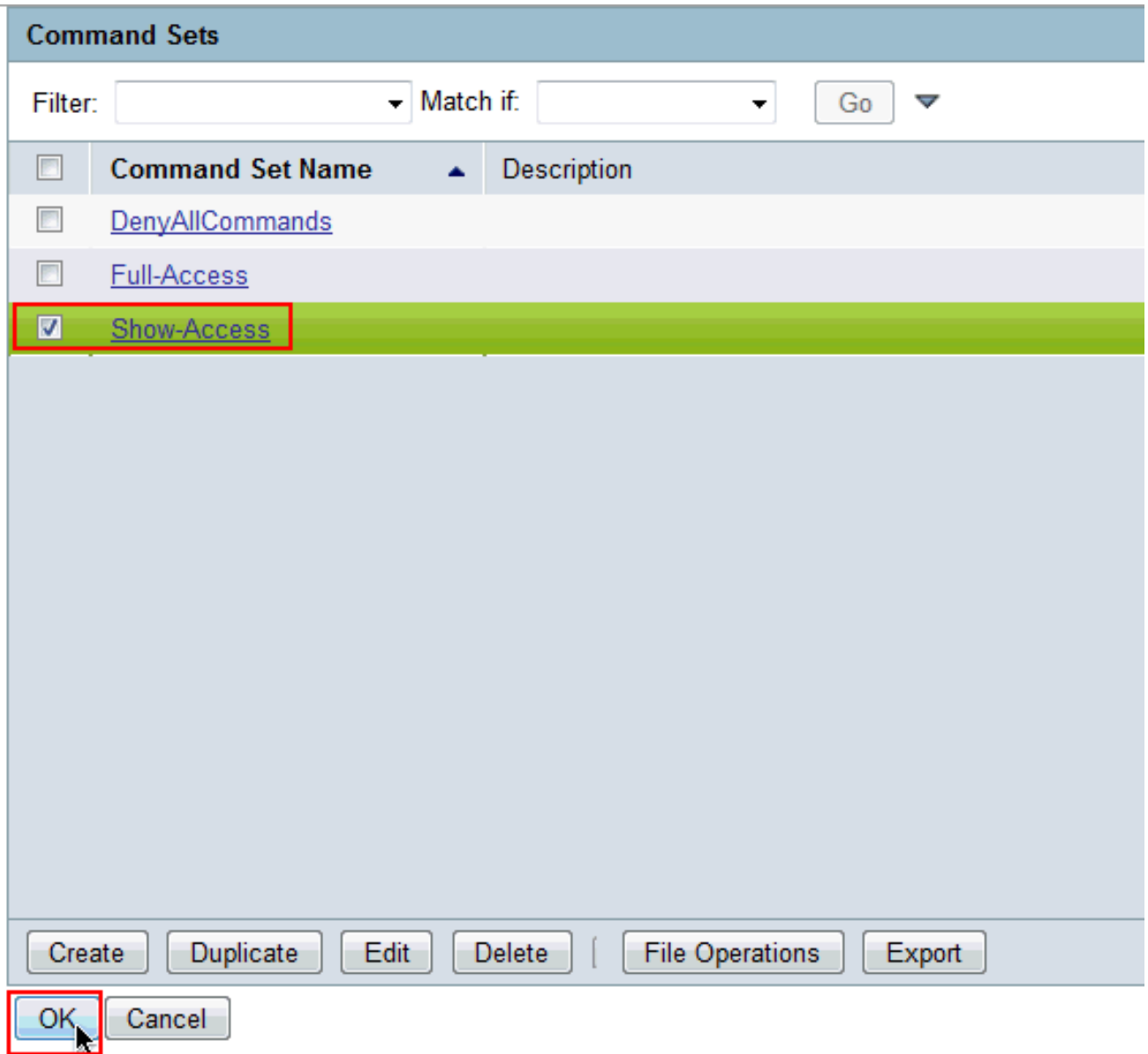
Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

37. 확인을 클릭합니다



38. 확인을 클릭합니다



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

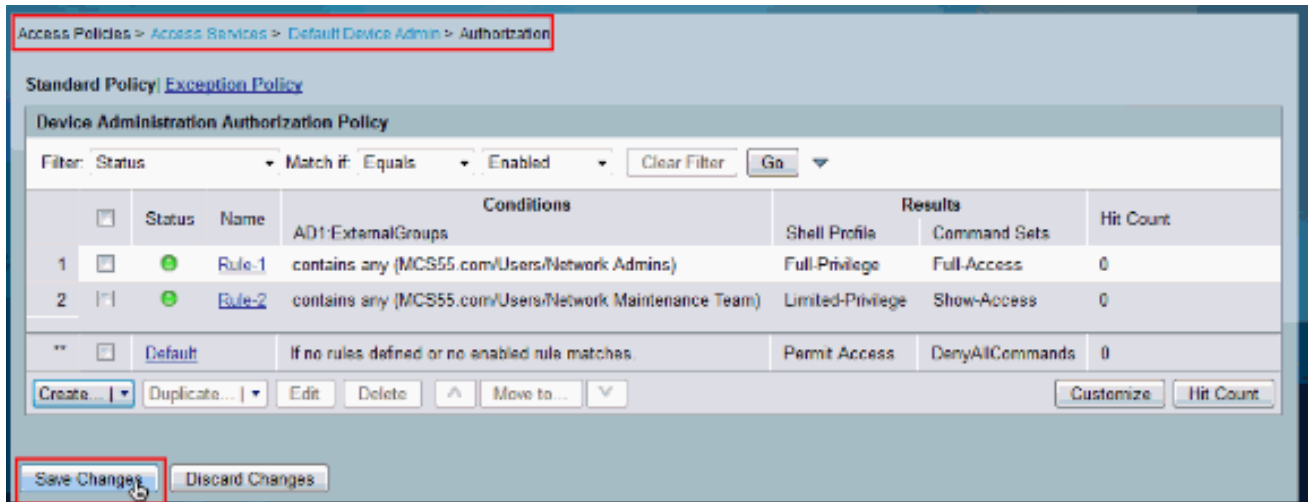
Select

Deselect

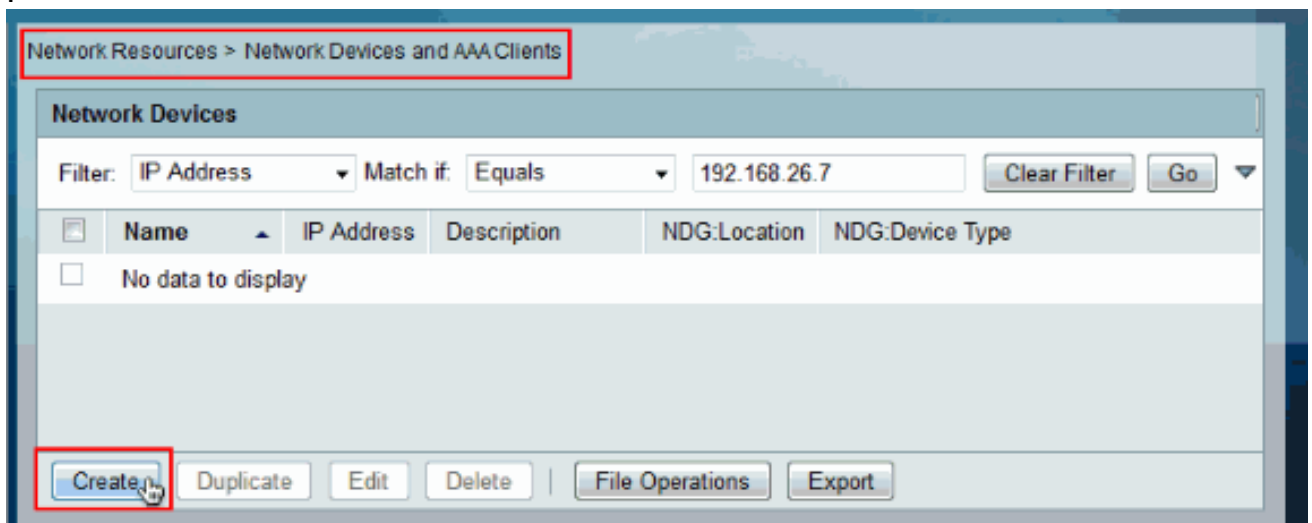
OK

Cancel

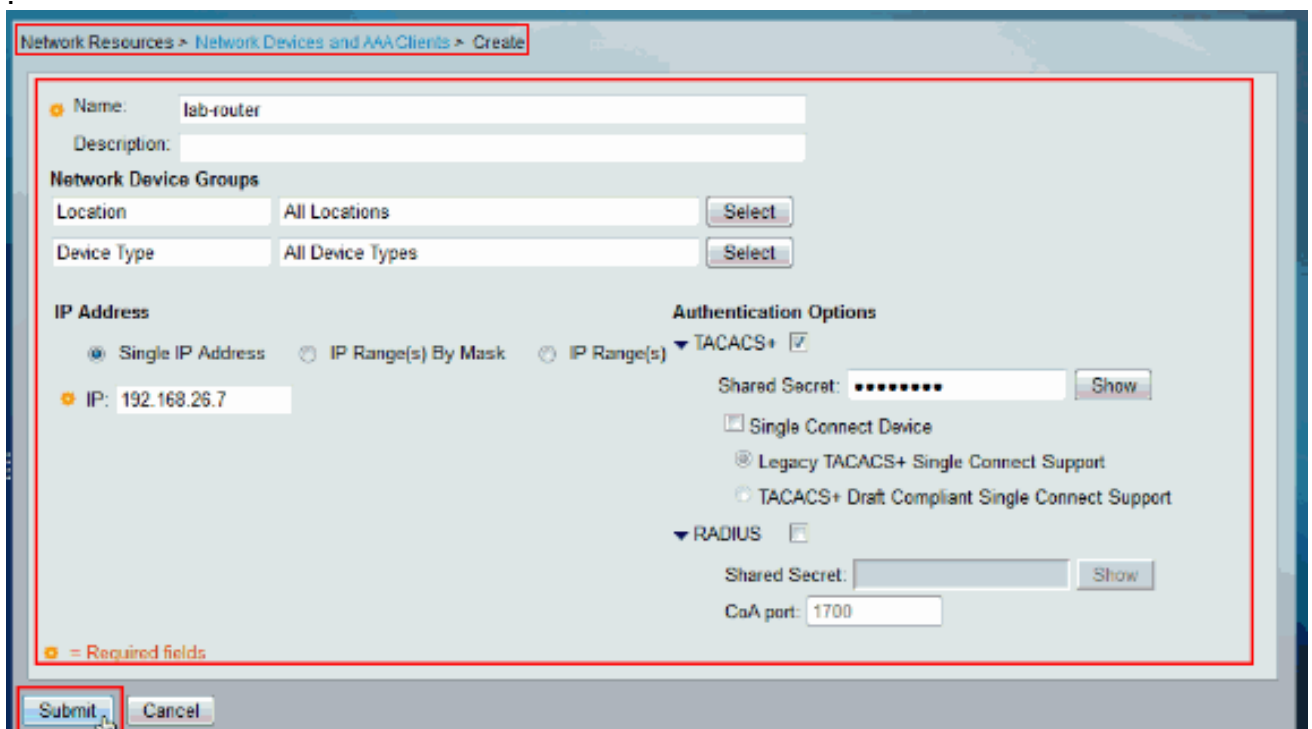
39. Save Changes를 클릭합니다



40. Create(생성)를 클릭하여 Cisco IOS 디바이스를 ACS에서 AAA 클라이언트로 추가합니다



41. TACACS용 이름, IP 주소, 공유 암호를 제공하고 Submit(제출)을 클릭합니다



인증 및 권한 부여를 위해 Cisco IOS 디바이스 구성

인증 및 권한 부여를 위해 Cisco IOS 디바이스 및 ACS를 구성하려면 다음 단계를 완료합니다.

1. 다음과 같이 `username` 명령을 사용하여 대체(fallback)할 전체 권한이 있는 로컬 사용자를 생성합니다.

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

2. AAA를 활성화하고 ACS 5.x를 TACACS 서버로 추가하려면 ACS의 IP 주소를 입력합니다.

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

참고: 키는 이 Cisco IOS 디바이스에 대해 ACS에 제공된 Shared-Secret과 일치해야 합니다.

3. 표시된 대로 `test aaa` 명령을 사용하여 TACACS 서버 연결성을 테스트합니다.

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

이전 명령의 출력에서는 TACACS 서버에 연결할 수 있으며 사용자가 성공적으로 인증되었음을 보여줍니다.**참고:** User1 및 password xxx는 AD에 속합니다. 테스트가 실패할 경우 이전 단계에서 제공한 공유 암호가 올바른지 확인하십시오.

4. 로그인을 구성하고 인증을 활성화한 다음 아래와 같이 Exec 및 명령 권한 부여를 사용합니다.

```
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
```

참고: Local 및 Enable 키워드는 Cisco IOS 로컬 사용자를 대체하기 위해 사용되며 TACACS 서버에 연결할 수 없는 경우 각각 비밀번호를 활성화합니다.

다음을 확인합니다.

텔넷을 통해 Cisco IOS 디바이스에 인증 및 권한 부여를 확인하려면

1. AD의 전체 액세스 그룹에 속하는 user1로 Cisco IOS 디바이스에 텔넷합니다. Network Admins 그룹은 ACS에서 설정된 Full-Privilege Shell Profile 및 Full-Access Command에 매핑된 AD의 그룹입니다. 모든 명령을 실행하여 전체 액세스 권한이 있는지 확인합니다

```
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. AD의 제한된 액세스 그룹에 속하는 user2로 Cisco IOS 디바이스에 텔넷합니다. (네트워크 유지 관리 팀 그룹은 ACS의 제한된 권한 셸 프로파일 및 Show-Access 명령에 매핑된 AD의 그룹입니다.) Show-Access 명령 집합에 언급된 명령 이외의 다른 명령을 실행하려고 하면

user2에 제한된 액세스 권한이 있음을 나타내는 오류가 발생합니다

```
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 (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/www/export/cryptolocal/stamp.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 GUI에 로그인하여 **Monitoring and Reports(모니터링 및 보고서) 뷰어**를 실행합니다
.user1 및 user2에서 수행한 활동을 확인하려면 **AAA Protocol(AAA 프로토콜) > TACACS+Authorization(TACACS+권한 부여)**을 선택합니다

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 6:21:19.393 AM	✔			user2	[CmdA]write		lab-cs02e
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.793 AM	✖		11025 Command failed to match a Permit rule	user2	[CmdA]write memory		lab-cs02e
Jun 8,12 6:20:59.999 AM	Jun 8,12 6:20:59.830 AM	✖		11024 Command failed to match a Permit rule	user2	[CmdA]config terminal		lab-cs02e
Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50.056 AM	✔			user2	[CmdA]show version		lab-cs02e
Jun 8,12 6:20:38.506 AM	Jun 8,12 6:20:38.490 AM	✔			user2	[CmdA]enable		lab-cs02e
Jun 8,12 6:20:34.426 AM	Jun 8,12 6:20:34.406 AM	✔			user2	[CmdA]=	Limited-Privilege	lab-cs02e
Jun 8,12 6:20:02.616 AM	Jun 8,12 6:20:02.596 AM	✔			user1	[CmdA]write		lab-cs02e
Jun 8,12 6:20:00.265 AM	Jun 8,12 6:20:00.246 AM	✔			user1	[CmdA]version 2		lab-cs02e
Jun 8,12 6:19:57.203 AM	Jun 8,12 6:19:57.200 AM	✔			user1	[CmdA]router rip		lab-cs02e
Jun 8,12 6:19:55.103 AM	Jun 8,12 6:19:55.076 AM	✔			user1	[CmdA]config terminal		lab-cs02e
Jun 8,12 6:19:52.743 AM	Jun 8,12 6:19:52.740 AM	✔			user1	[CmdA]=	Full-Privilege	lab-cs02e

Commands run by user 2

Commands run by user1

관련 정보

- [Cisco Secure Access Control System](#)
- [기술 지원 및 문서 - Cisco Systems](#)