

ACS 5. x: TACACS + Аутентификация и Авторизация для выполнения команд на основе AD Примера конфигурации состава группы

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[!--- конфигурацию](#)

[Настройте ACS 5.x для проверки подлинности и авторизация](#)

[Настройте устройство Cisco IOS для Проверки подлинности и авторизация](#)

[Проверка](#)

[Дополнительные сведения](#)

[Введение](#)

Этот документ предоставляет пример настройки TACACS + Аутентификация и Авторизация для выполнения команд на основе AD состава группы пользователя с системой управления доступом Cisco Secure Access Control System (ACS) 5.x и позже. ACS использует Microsoft Active Directory (AD) в качестве внешнего хранилища идентификационных данных для хранения информации о таких ресурсах, как пользователи, машины, группы и атрибуты.

[Предварительные условия](#)

[Требования](#)

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- ACS 5.x полностью интегрирован к желаемому AD Домену. Если ACS не интегрирован с желаемым AD Доменом, обратитесь к [ACS 5.x и позже: Интеграция с Примером конфигурации Microsoft Active Directory](#) для получения дополнительной информации для выполнения задачи интеграции.

[Используемые компоненты](#)

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Secure ACS 5.3
- Релиз 12.2 программного обеспечения Cisco IOS (44) SE6. **Примечание:** Эта конфигурация может быть реализована на всех устройствах Cisco IOS.
- Домен Microsoft Windows server 2003 года

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

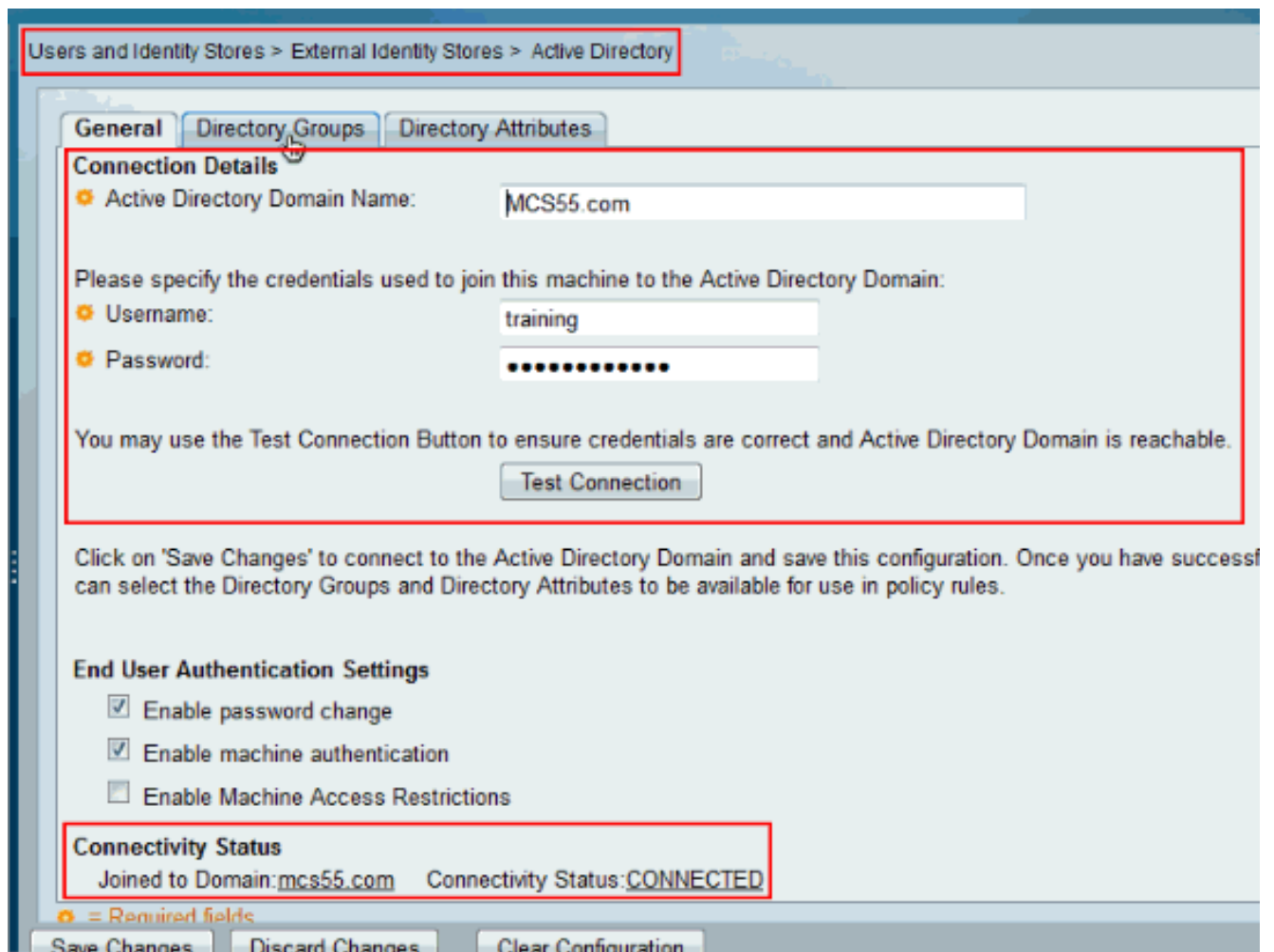
!--- конфигурацию

Настройте ACS 5.x для проверки подлинности и авторизация

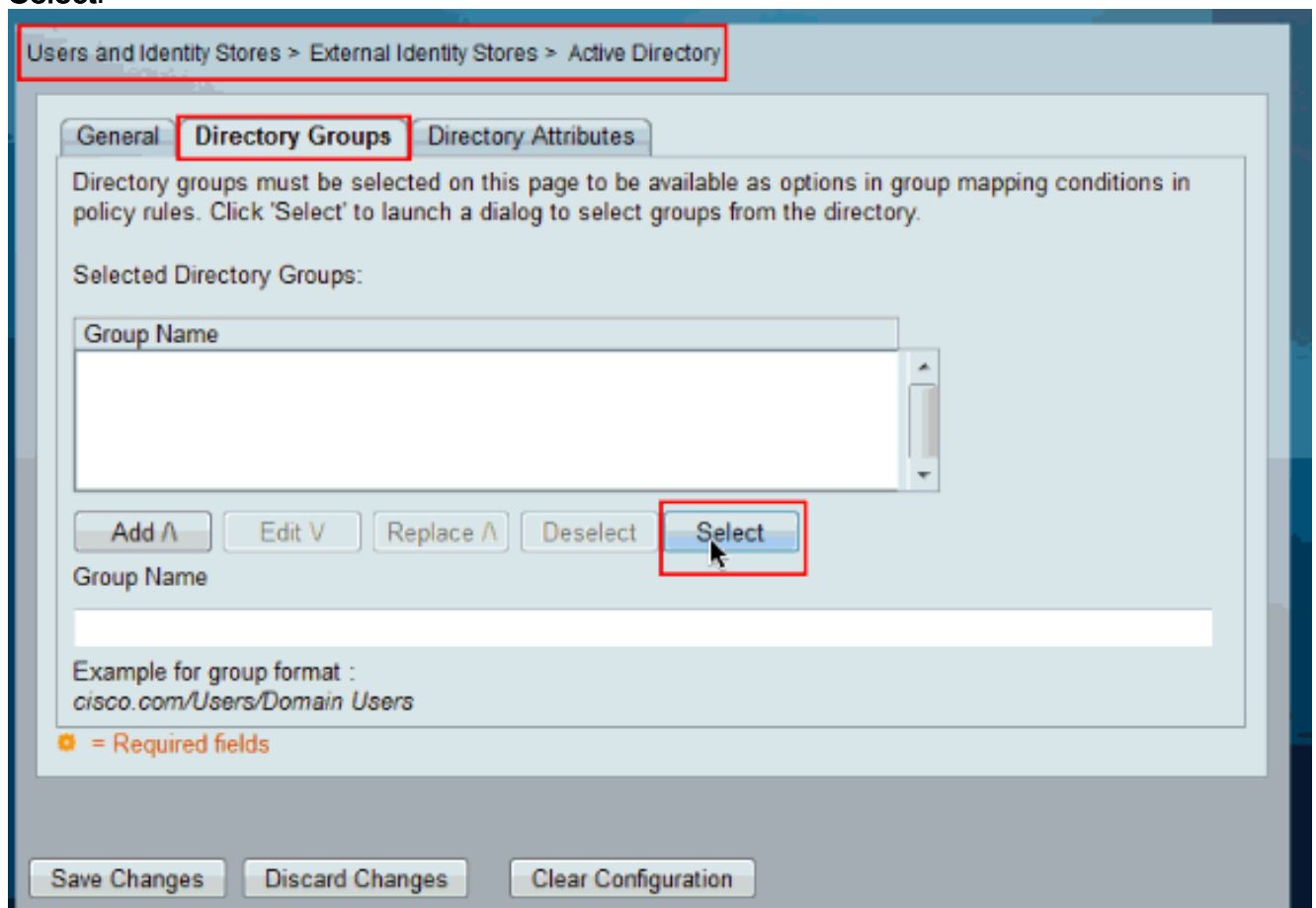
Перед началом конфигурации ACS 5.x для Проверки подлинности и авторизация ACS должен был быть интегрирован успешно с Microsoft AD. Если ACS не интегрирован с желаемым AD Доменом, обратитесь к [ACS 5.x и позже: Интеграция с Примером конфигурации Microsoft Active Directory](#) для получения дополнительной информации для выполнения задачи интеграции.

В этом разделе вы сопоставляете две AD группы с двумя другими наборами команд и двумя профилями Shell, один с полным доступом и другим с ограниченным доступом на устройствах Cisco IOS.

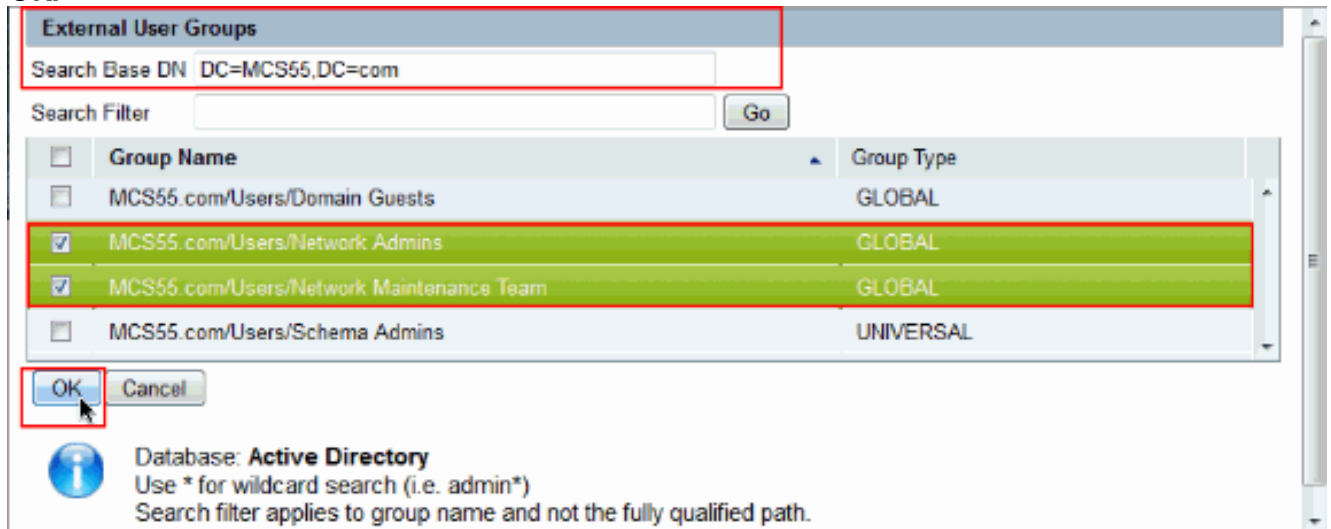
1. Войдите в учетные данные Admin использования GUI ACS.
2. Выберите **Users и Identity Stores> External Identity Stores> Active Directory** и проверьте, что ACS присоединился к желаемому домену и также что **статус подключения** показывают, как **связано**. Щелкните по **Directory Groups Tab**.



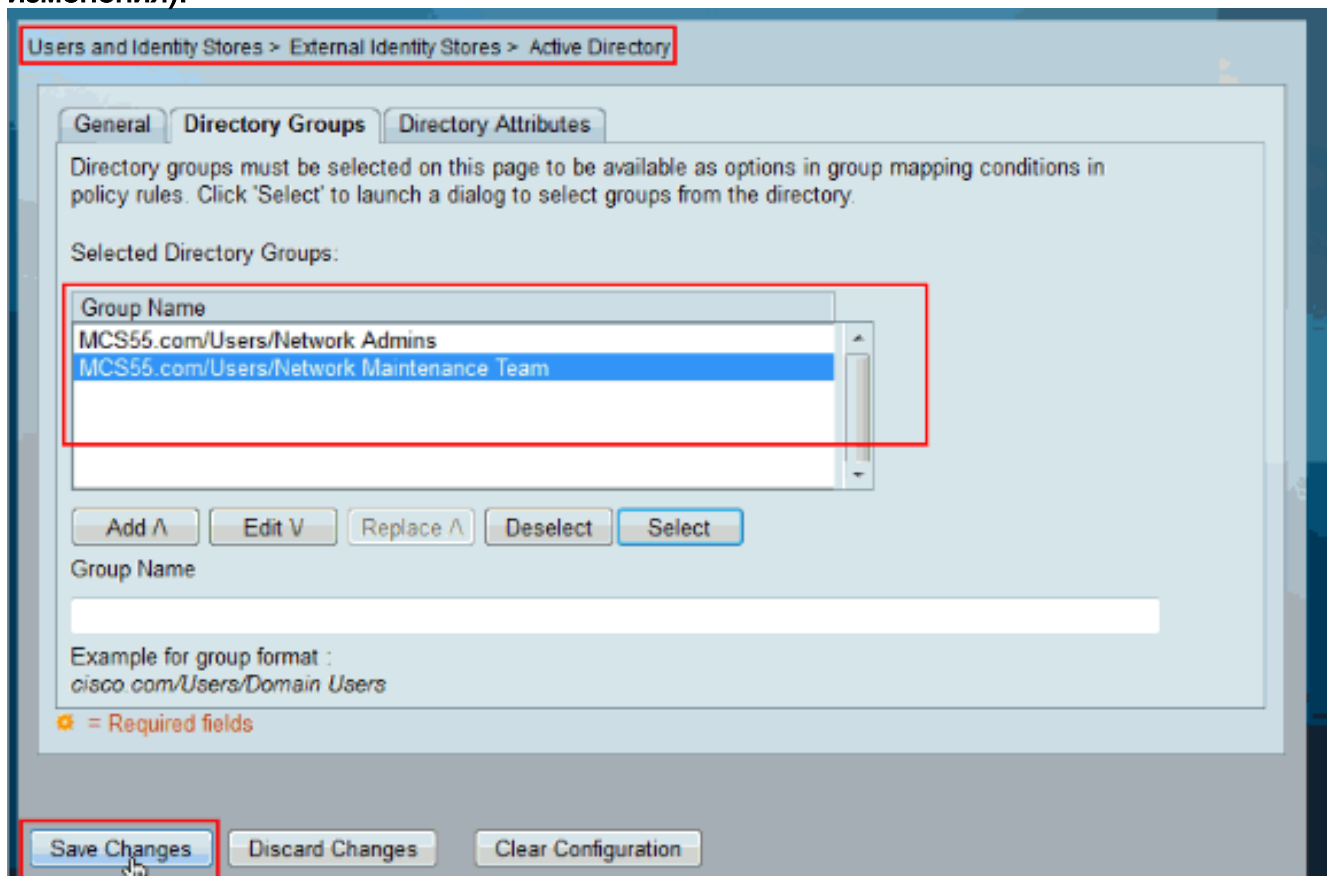
3. Нажмите Select.



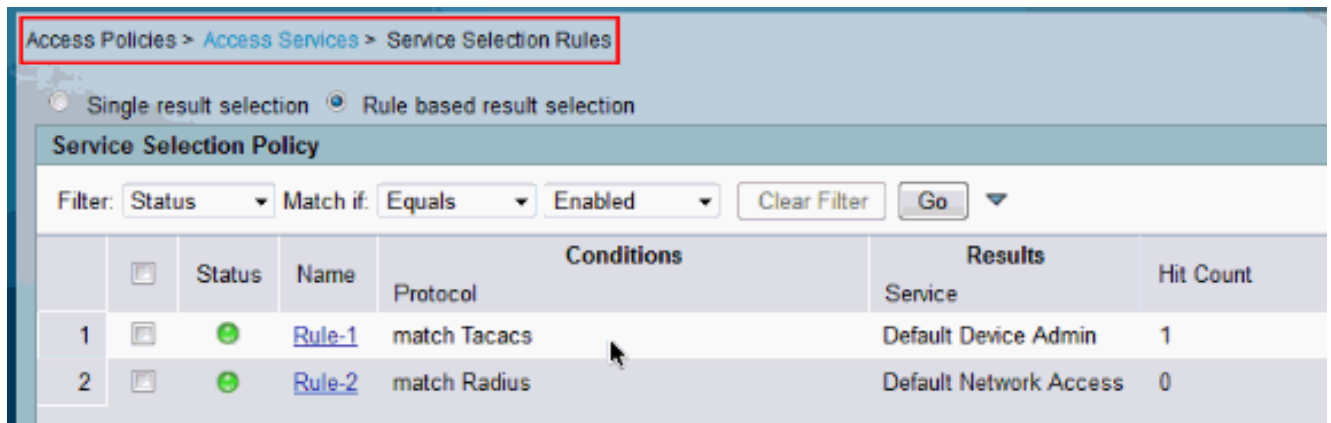
4. Выберите группы, которые должны быть сопоставлены с профилями Shell и наборами команд в более поздней части конфигурации. **Нажмите кнопку ОК.**



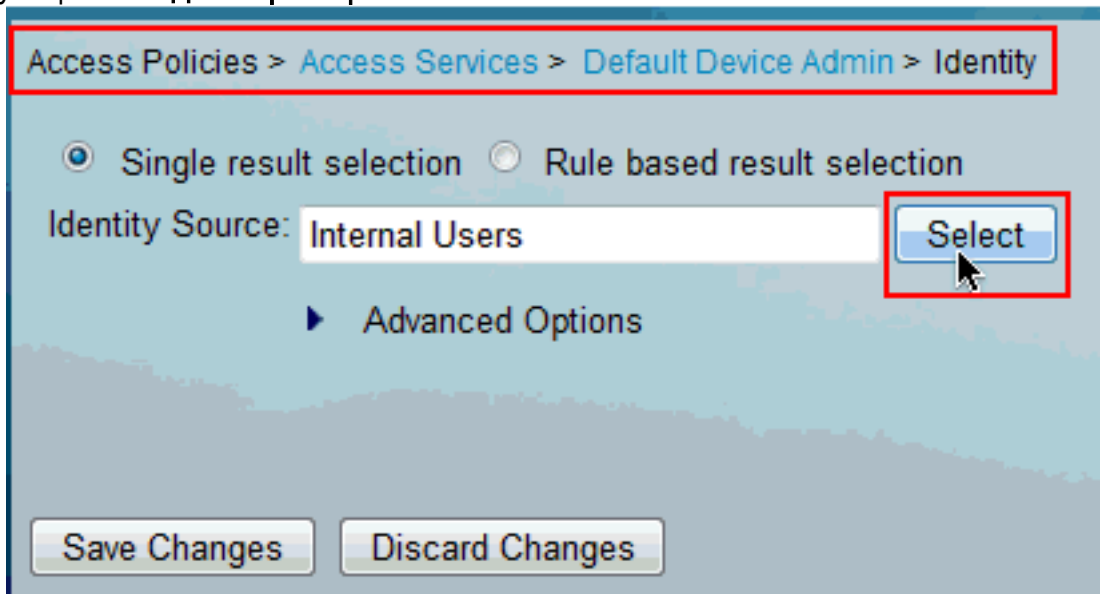
5. Нажмите кнопку **Save Changes (Сохранить изменения)**.



6. Выберите **Access Policies > Access Services > Service Selection Rules** и определите службу доступа, которая обрабатывает TACACS + Аутентификация. В данном примере это - **Администратор устройства по умолчанию**.

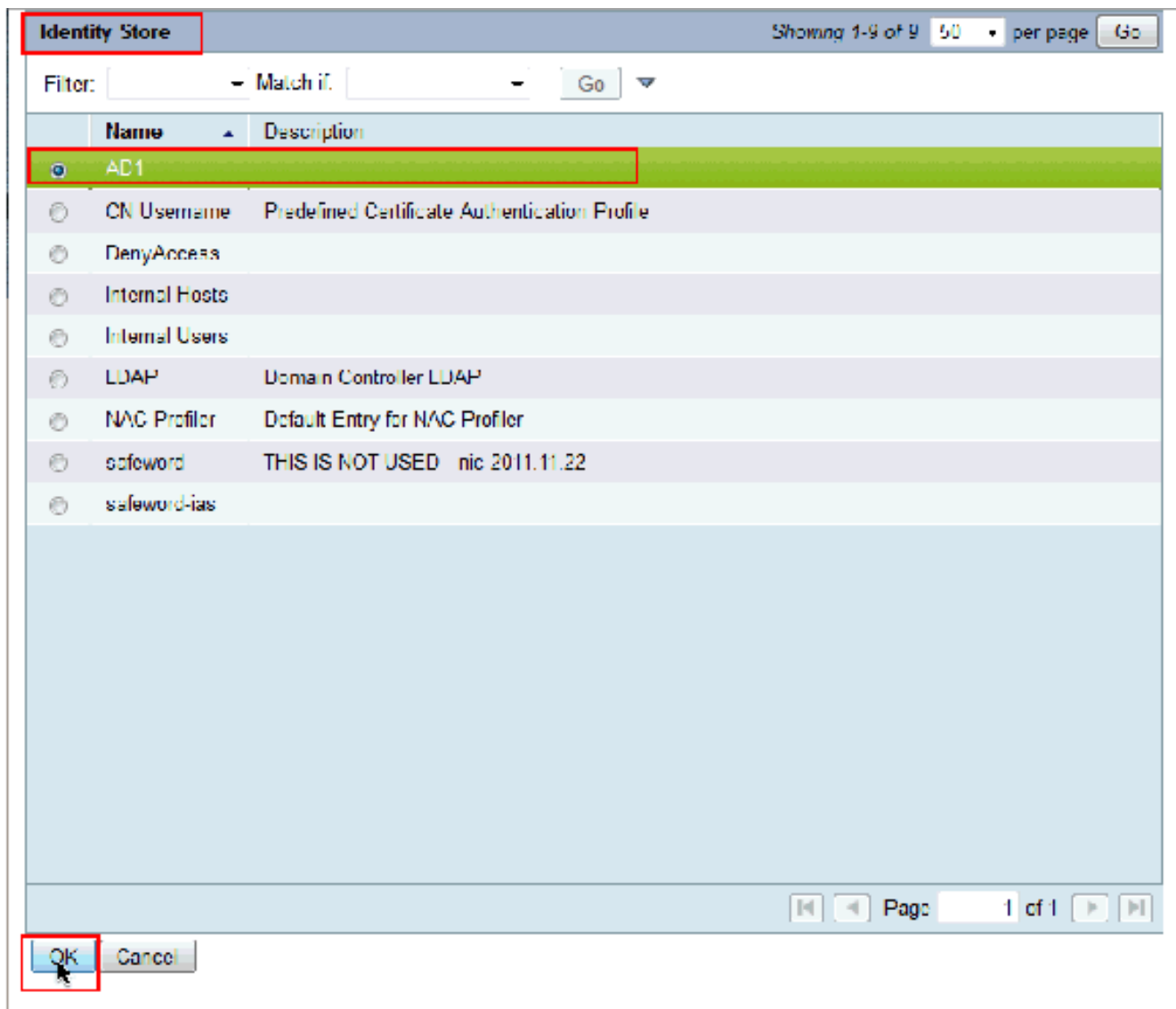


7. Выберите **Access Policies> Access Services> Default Device Admin> Identity** и нажмите **Select**, следующий за **Идентификационным**

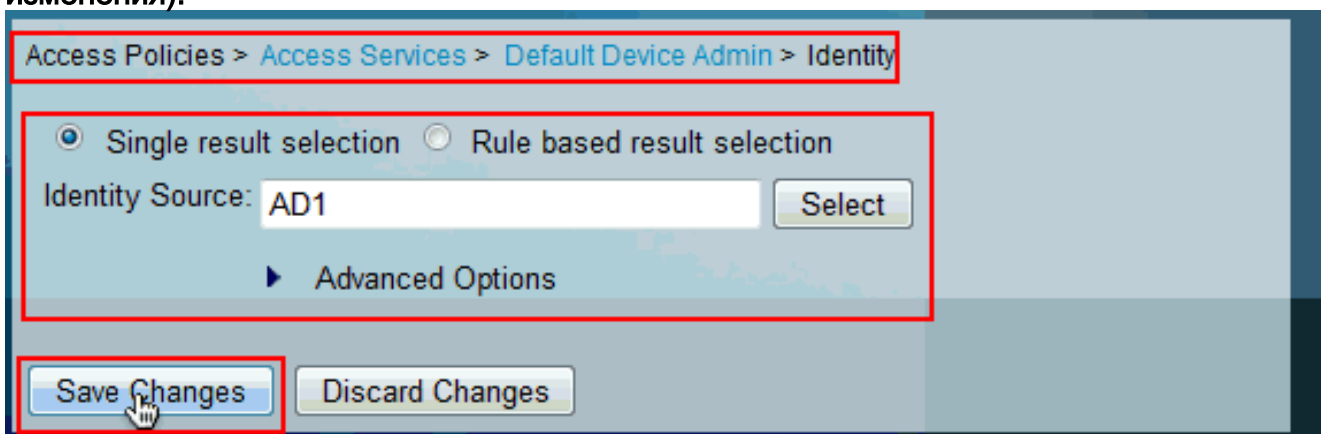


Источником.

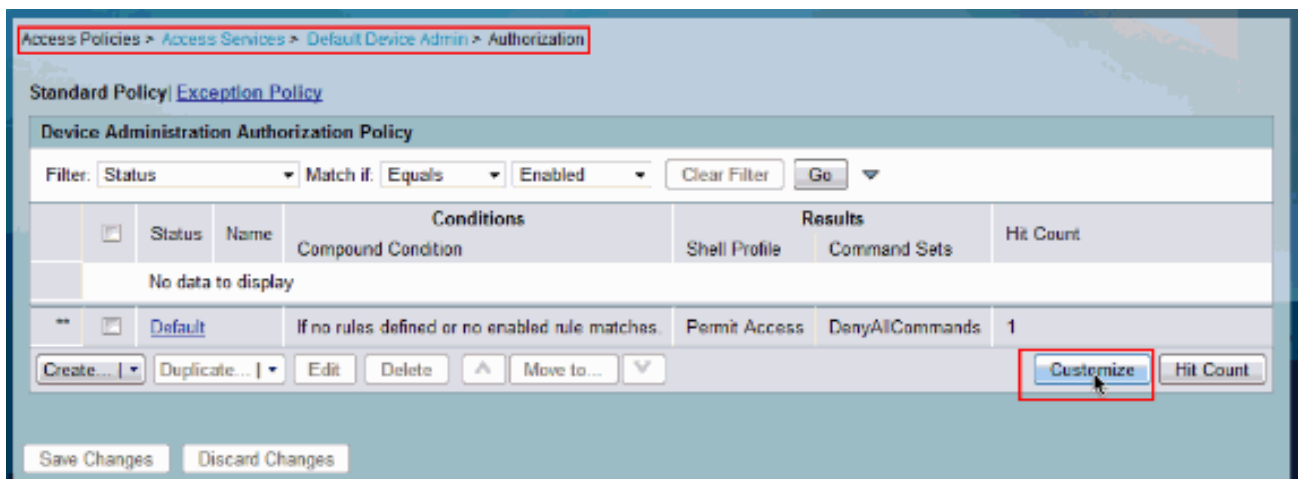
8. Выберите **AD1** и нажмите **ОК**.



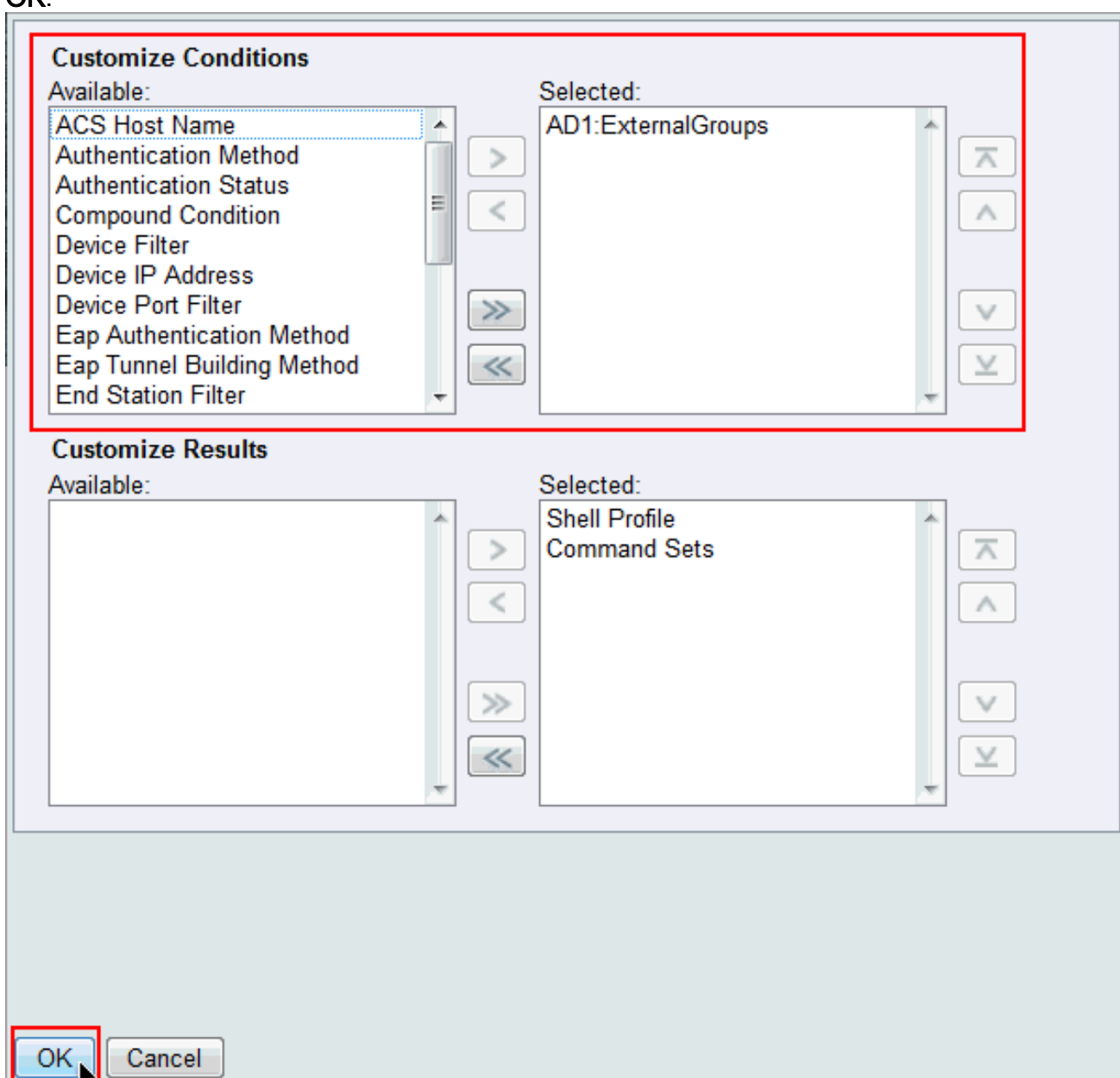
9. Нажмите кнопку **Save Changes** (Сохранить изменения).



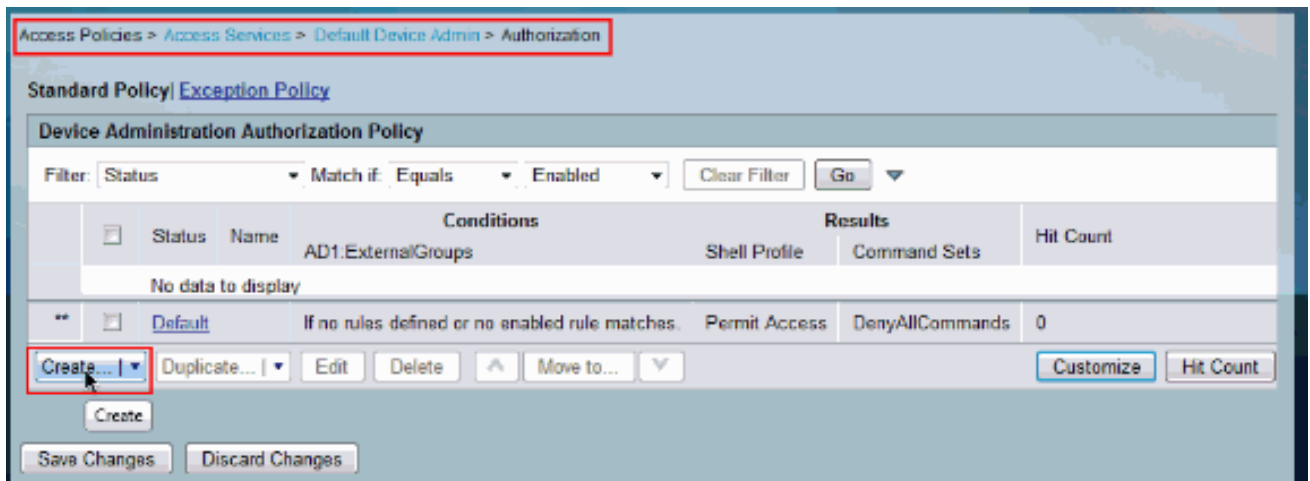
10. Выберите **Access Policies > Access Services > Default Device Admin > Authorization** и щелкните по **Customize**.



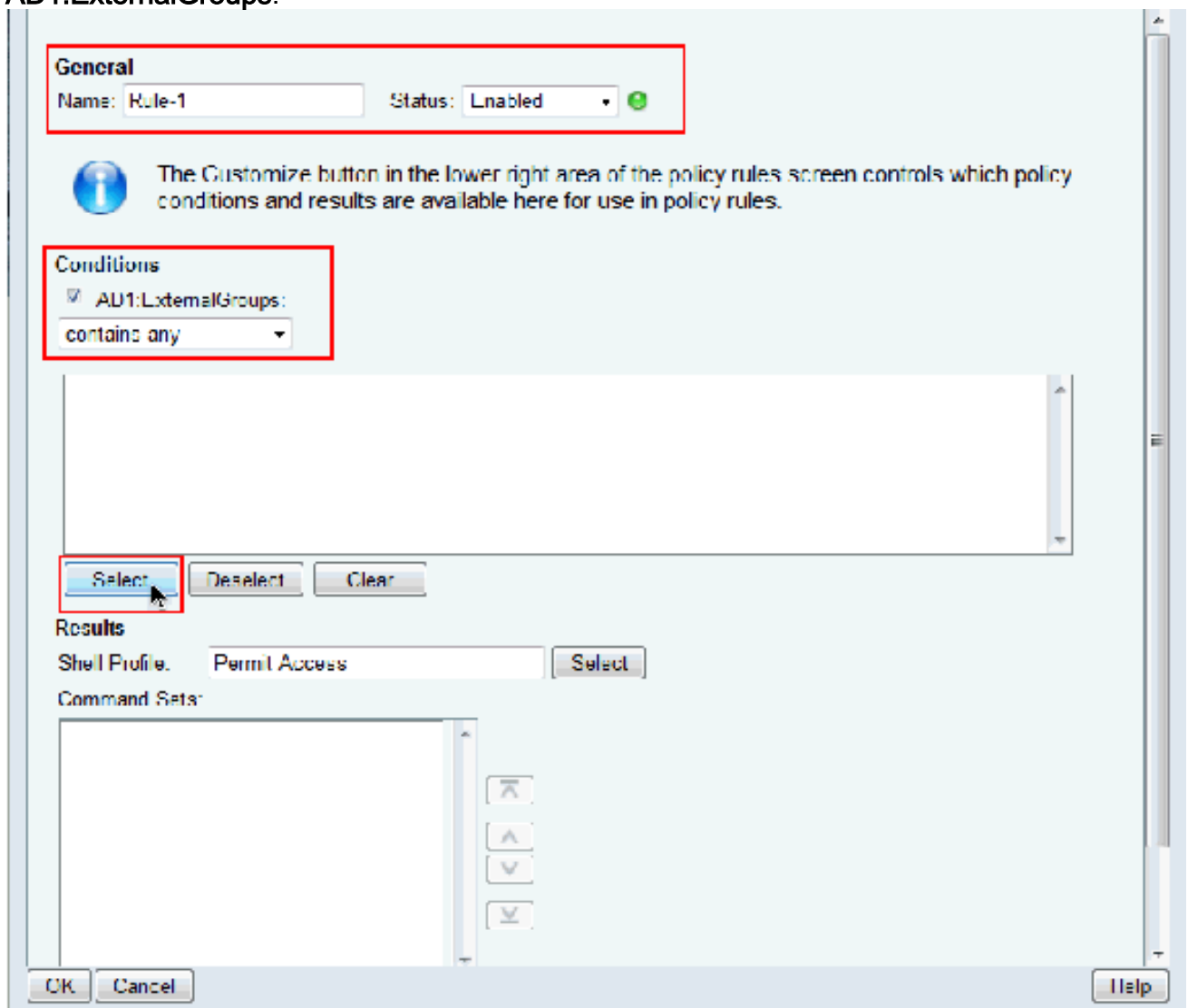
11. Копия AD1:ExternalGroups от Доступного до Выбранного раздела Настраивает Условия и затем перемещает Профиль Shell, и Наборы команд от Доступного до Выбранного раздела Настраивают Результаты. Теперь нажмите ОК.



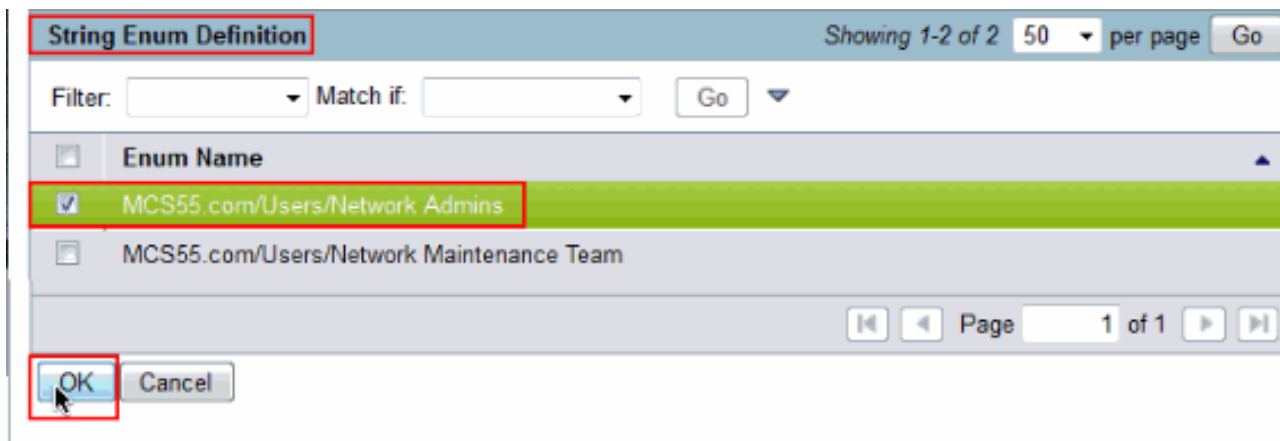
12. Нажмите **Create** для создания нового Правила.



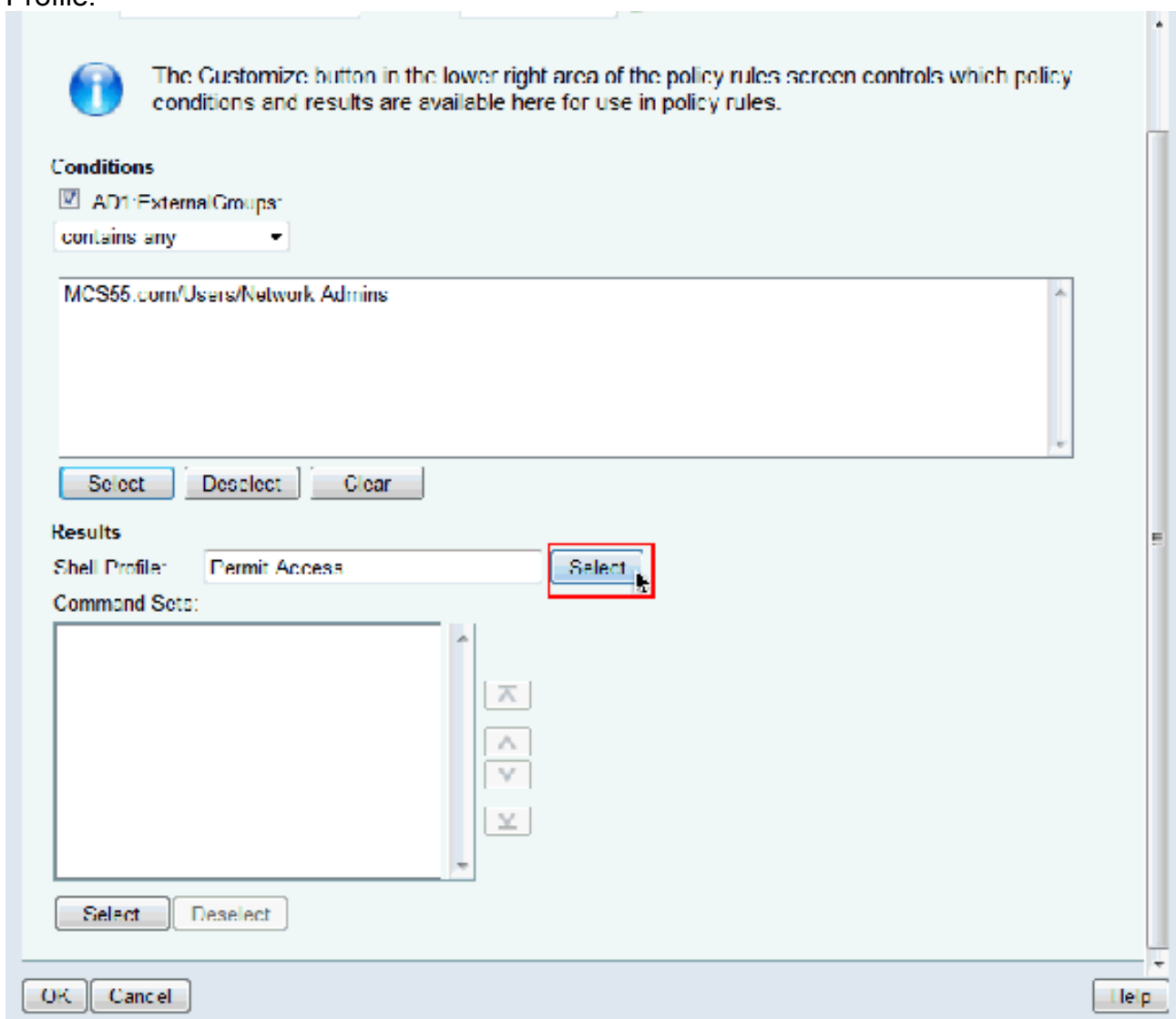
13. Нажмите **Select** в условии **AD1:ExternalGroups**.



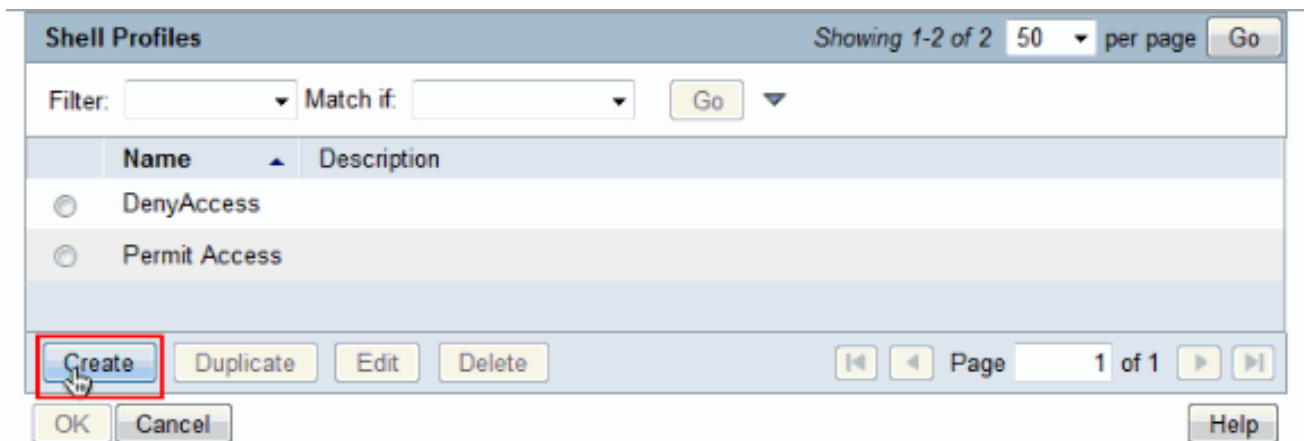
14. Выберите группу, что вы хотите предоставить полный доступ на устройстве Cisco IOS. Нажмите кнопку **OK**.



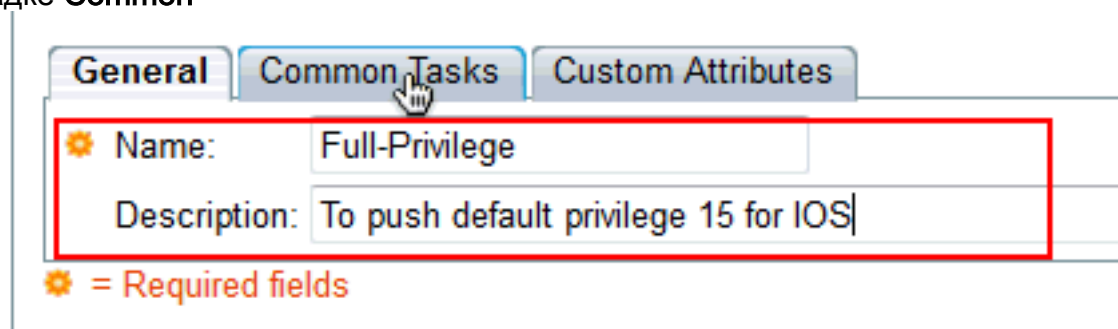
15. Нажмите **Select** в поле Shell Profile.



16. Нажмите **Create** для создания нового Профиля Shell для пользователей полного доступа.



17. Предоставьте **Название** и **Описание** (дополнительное) во **Вкладке Общие**, и щелкните по вкладке **Common**



Tasks. _____

18. Измените привилегии по умолчанию и максимальную привилегию к статическому со значением 15. Нажмите кнопку Submit (Отправить).

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

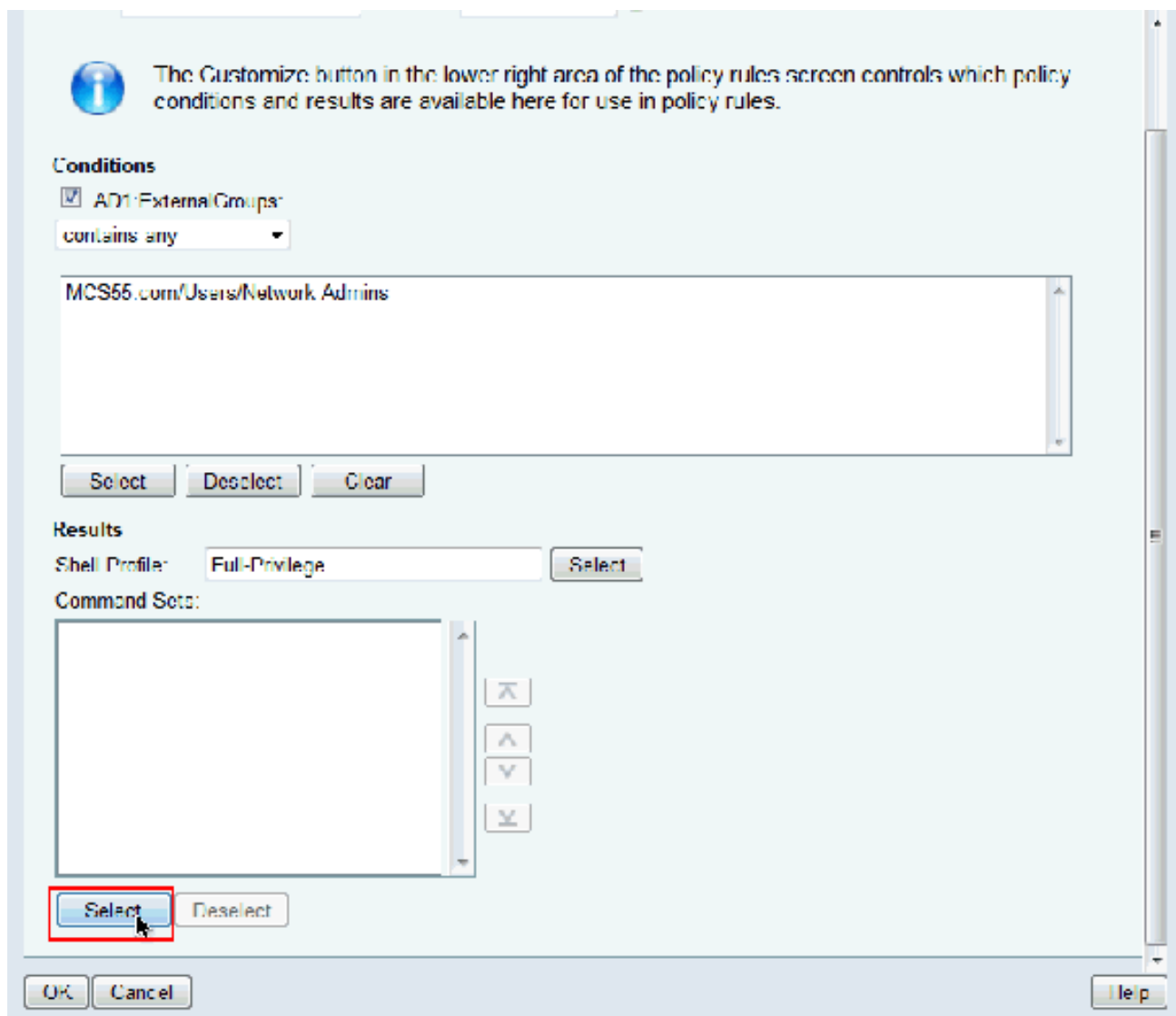
19. Теперь выберите недавно созданный полный доступ **Профиль Shell** (Полные полномочия в данном примере) и нажмите **OK**.

Shell Profiles

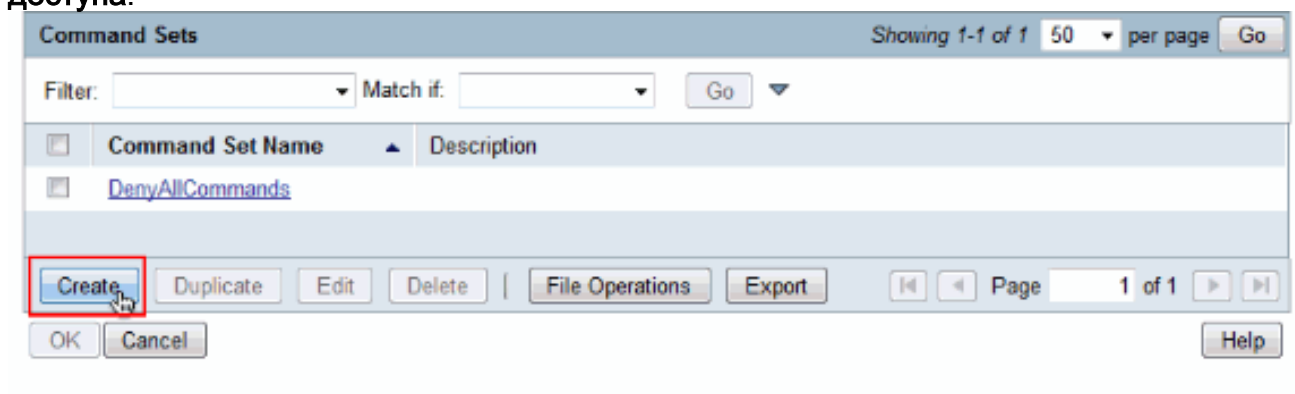
Filter: Match if:

	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. Нажмите **Select** в поле Command Sets.



21. Нажмите **Create** для создания нового **Набора команд** для пользователей **Полного доступа**.



22. Предоставьте **Название** и гарантируйте, что **ниже**, проверен флажок затем для **Разрешения любой команды**, которая не находится в таблице. Нажмите кнопку **Submit** (Отправить). Примечание: См. [Создание, Дублирование и Редактирование Наборов команд для Администрирования устройств](#) для получения дополнительной информации о Наборх команд.

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. Нажмите кнопку
OK.

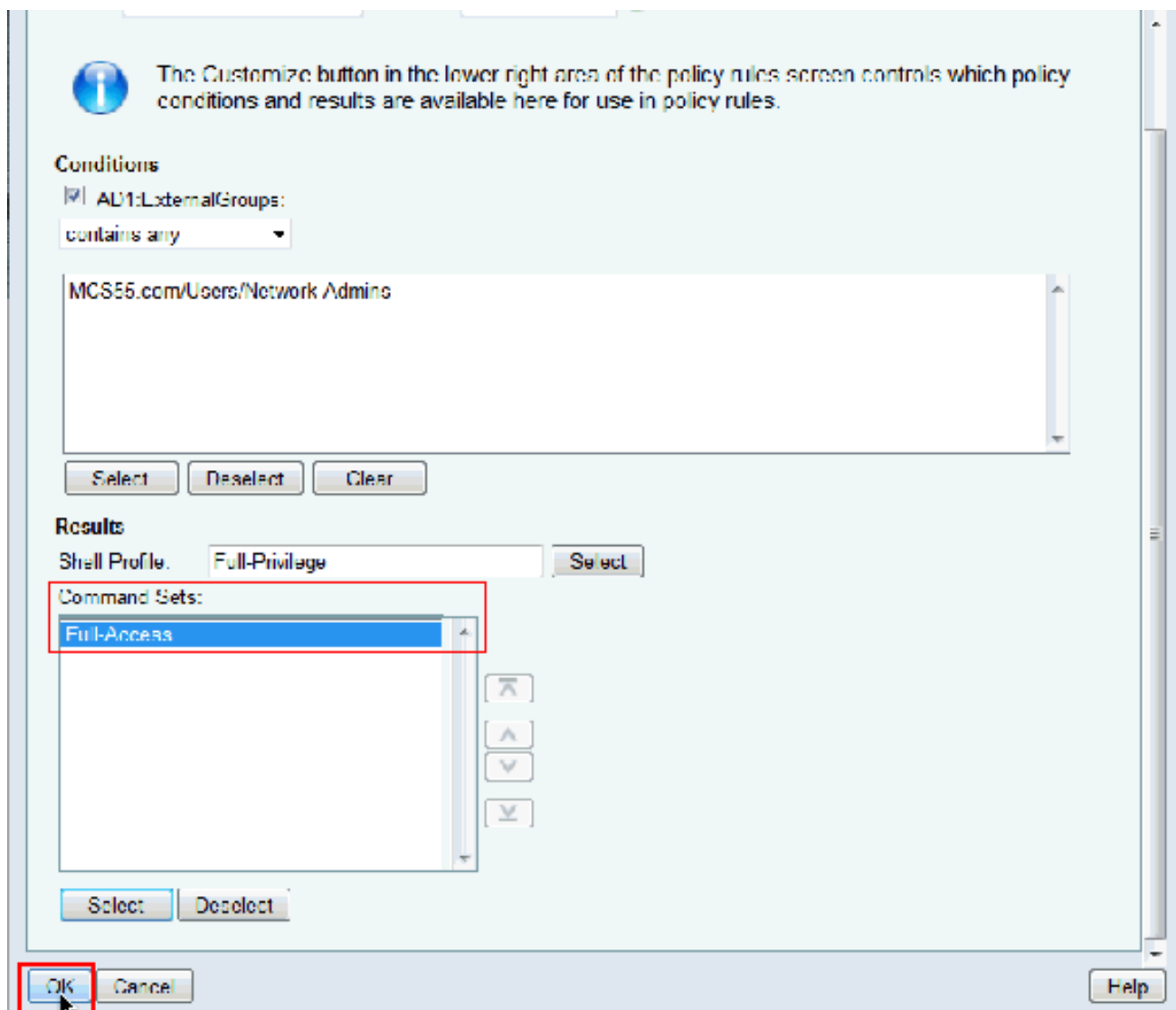
Command Sets

Filter: Match if:

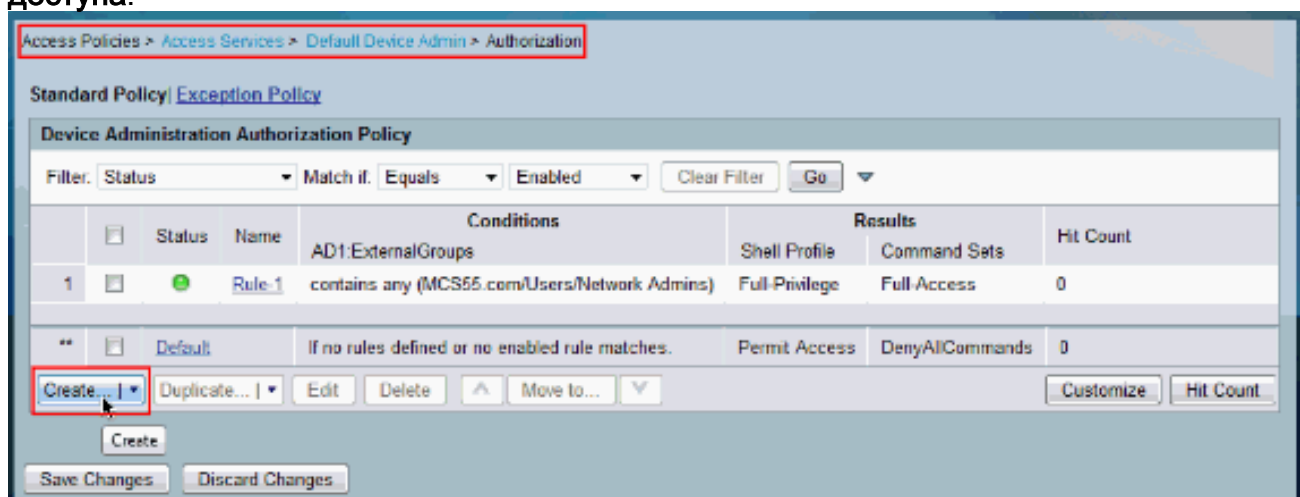
<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

|

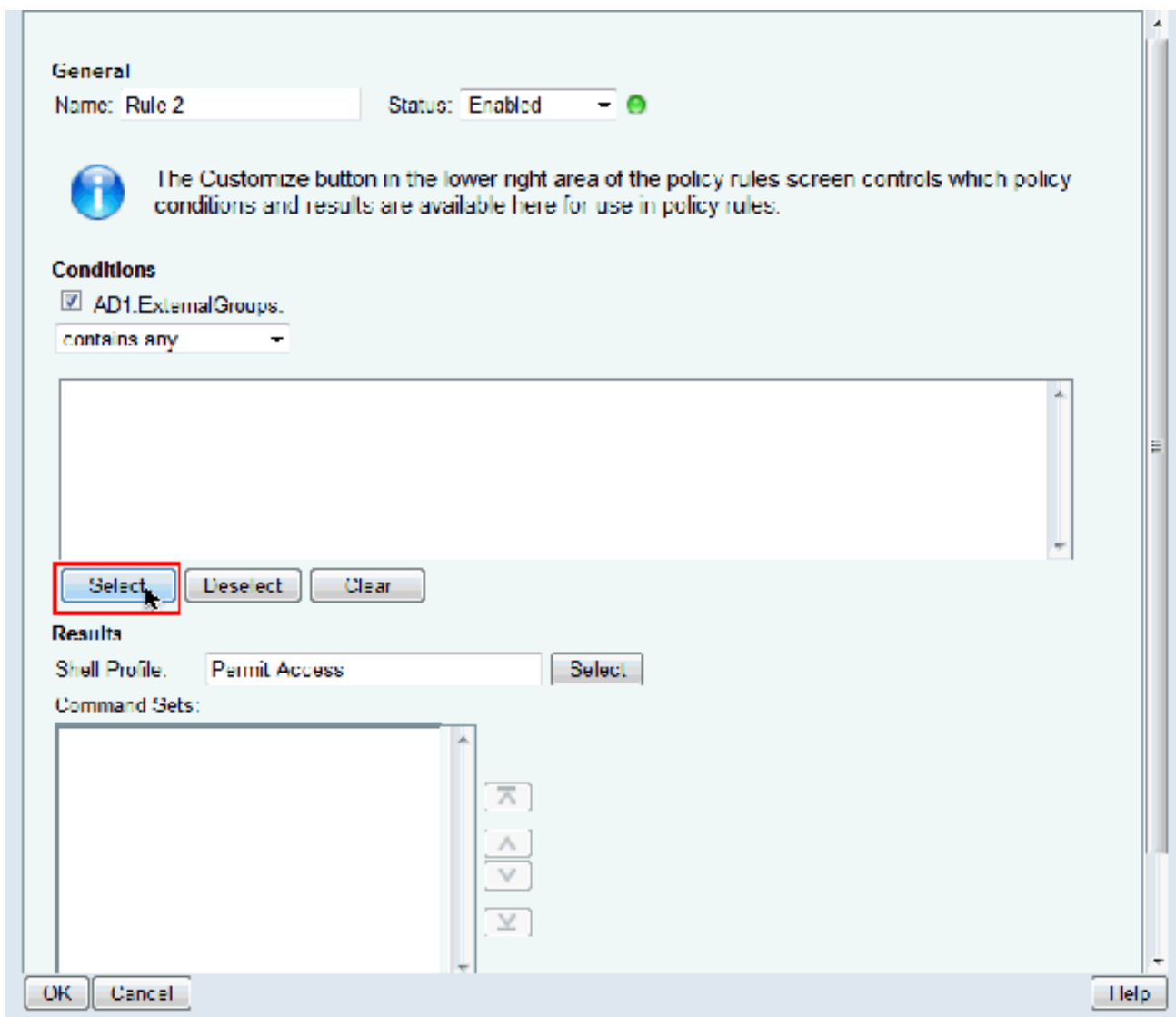
24. Нажмите кнопку OK. Это завершает конфигурацию Правила
1.



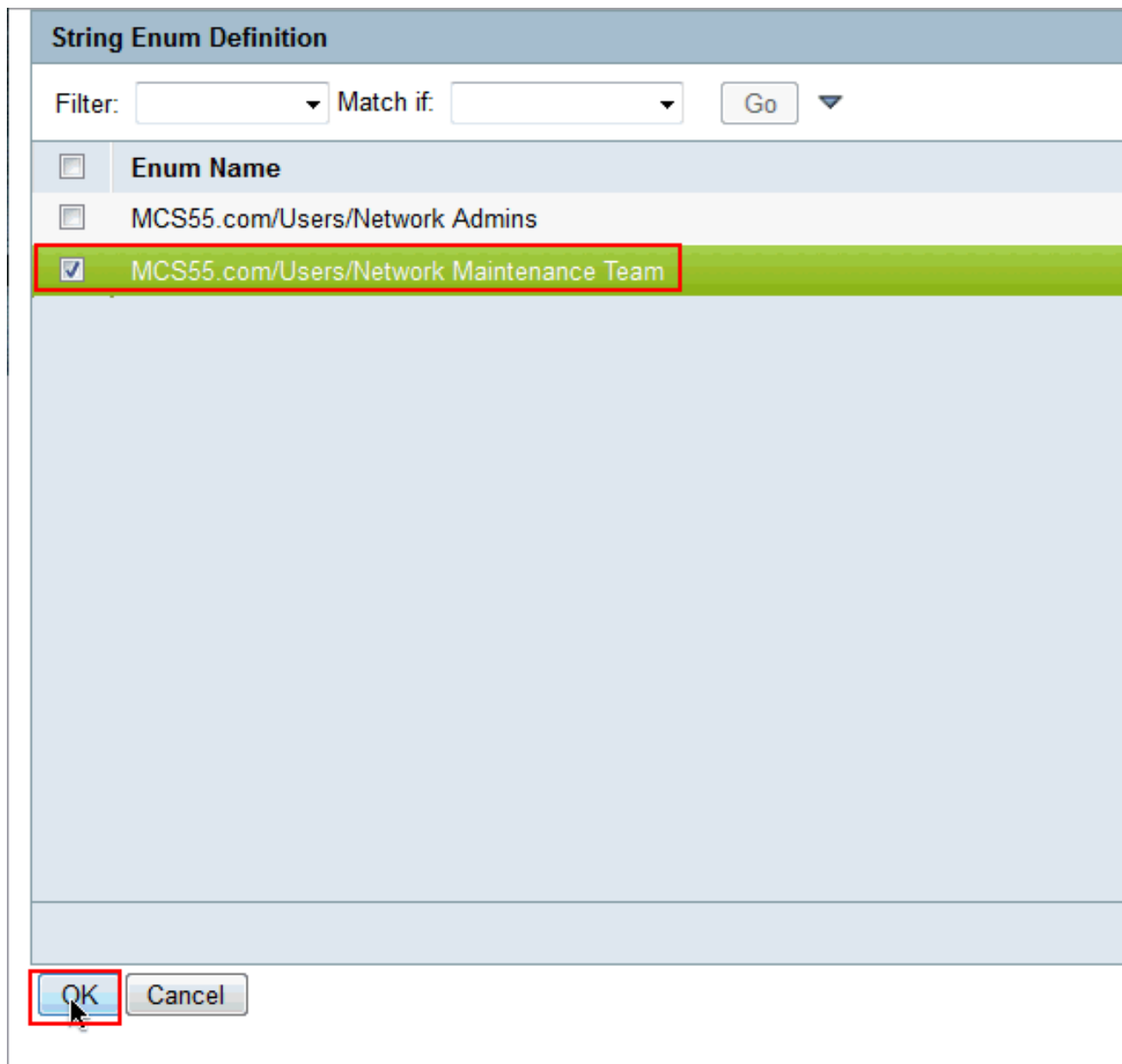
25. Нажмите **Create** для создания нового Правила для пользователей **ограниченного доступа**.



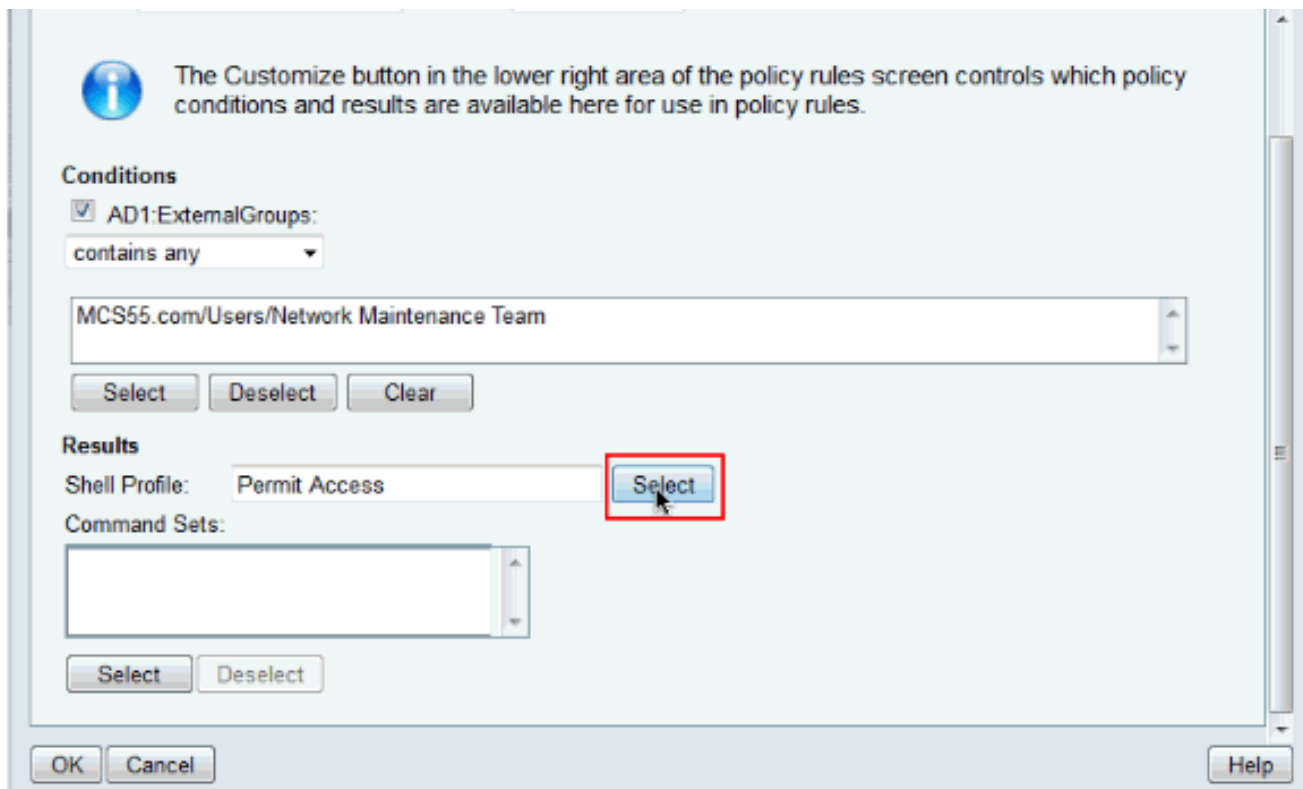
26. Выберите **AD1:ExternalGroups** и нажмите **Select**.



27. Выберите группу (или) группы, к которым вы хотите предоставить ограниченный доступ и нажать **OK**.



28. Нажмите **Select** в поле Shell Profile.



29. Нажмите **Create** для создания нового **Профиля Shell** для ограниченного доступа.

Shell Profiles

Filter: Match if:

<input type="radio"/>	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input type="radio"/>	Permit Access	

30. Предоставьте **Название** и **Описание** (дополнительное) во **Вкладке Общие**, и щелкните по вкладке **Common Tasks**.

General Common Tasks Custom Attributes

Name: Limited-Privilege

Description: To push default privilege 1 for IOS

⚙ = Required fields

31. Измените Привилегии по умолчанию и Максимальную Привилегию к Статическому со значениями 1 и 15 соответственно. Нажмите кнопку Submit (Отправить).

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. Нажмите кнопку

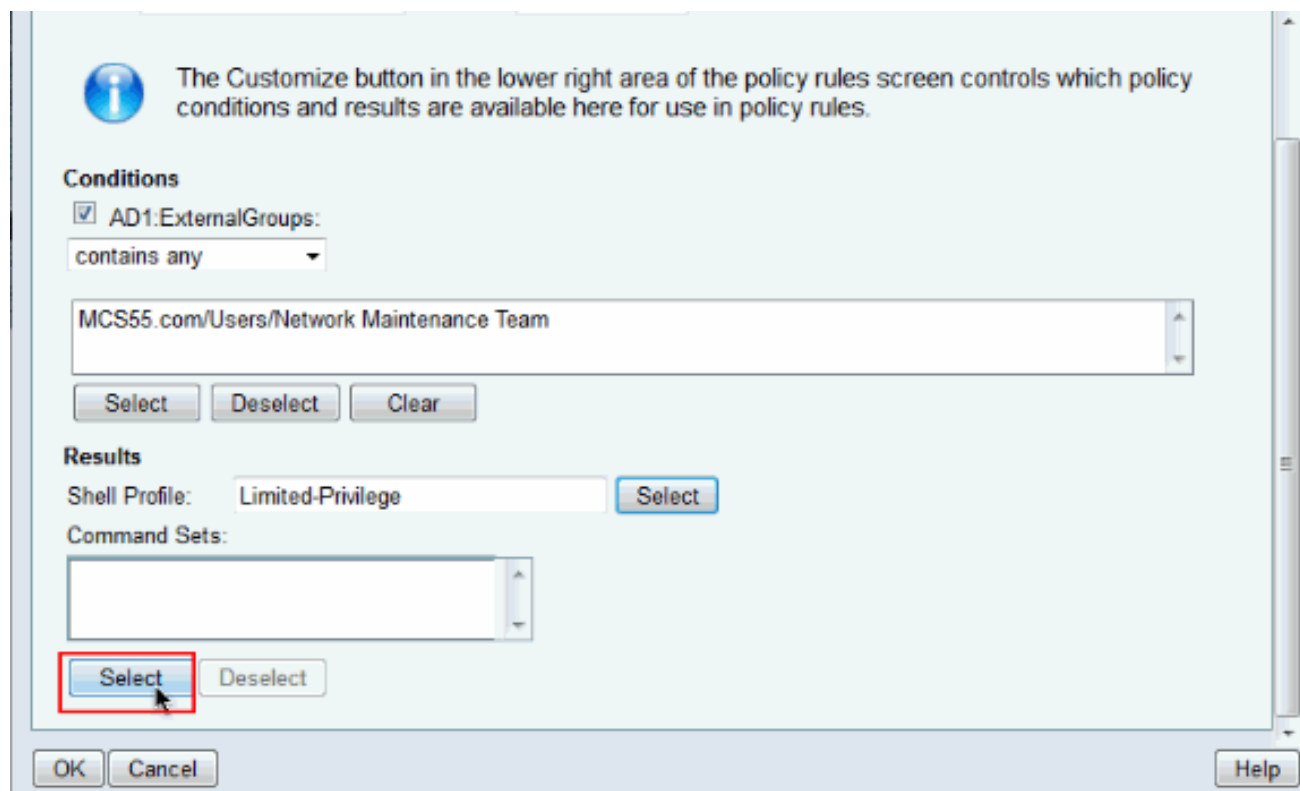
Shell Profiles

Filter: Match if: Go

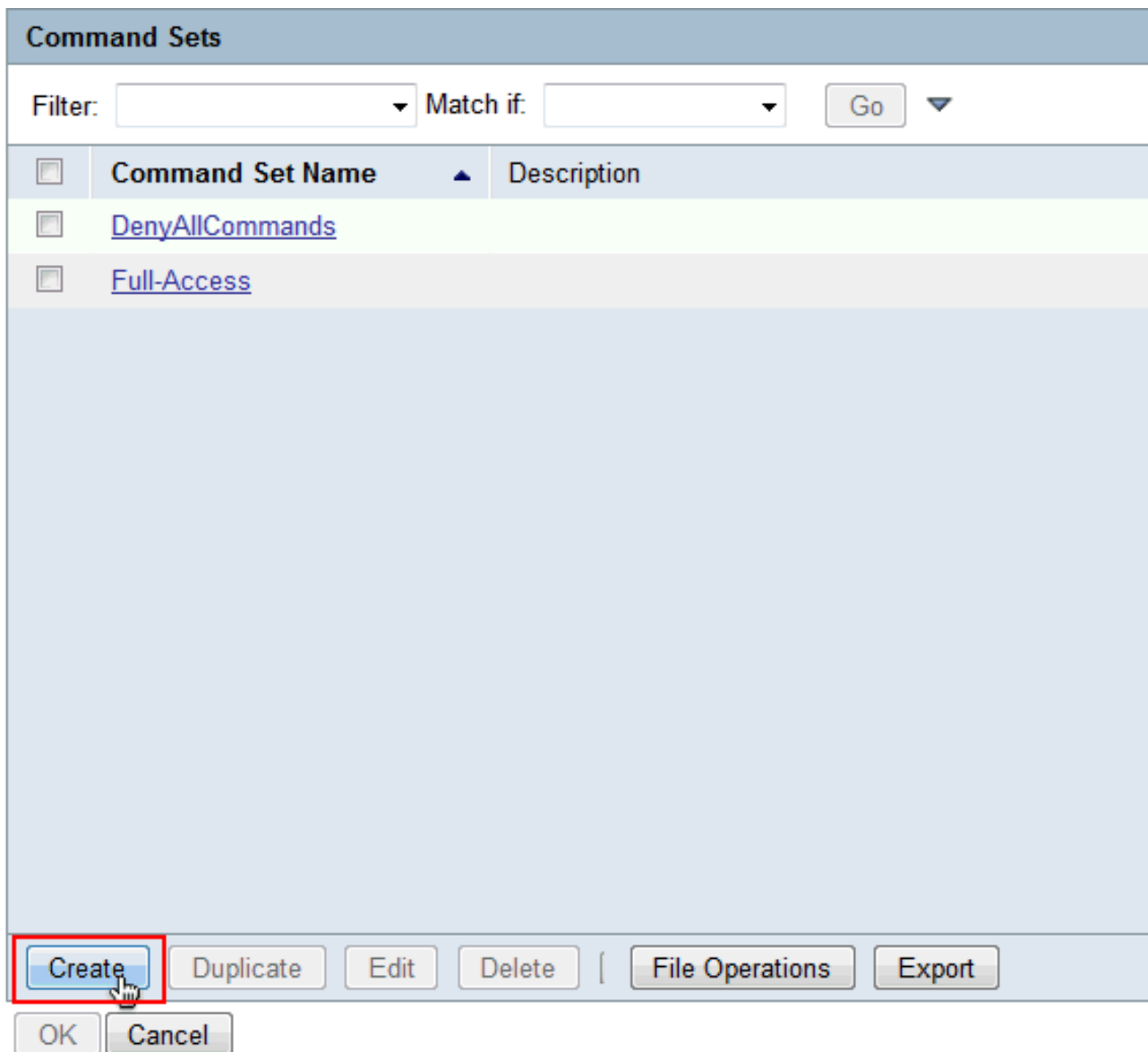
	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input checked="" type="radio"/>	Limited-Privilege	To push default privilege 1 for IOS
<input type="radio"/>	Permit Access	

OK.

33. Нажмите **Select** в поле Command Sets.



34. Нажмите **Create** для создания нового **Набора команд** для группы ограниченного доступа.



35. Предоставьте **Название** и гарантируйте, что **ниже**, не установлен флажок затем для **Разрешения** любой команды, которая не находится в таблице. Нажмите **Add** после ввода **показывают** в пространстве, предоставленном в **разделе команд**, и выбирают **Permit** в разделе **Предоставления** так, чтобы только команды показа были разрешены для пользователей в группе ограниченного доступа.

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. Так же добавьте, что **Добавляют** любые другие команды, которые будут разрешены для пользователей в группе ограниченного доступа с использованием. **Нажмите** кнопку **Submit** (Отправить).Примечание: См. [Создание, Дублирование и Редактирование Наборов команд для Администрирования устройств](#) для получения дополнительной информации о Наборах команд.

General

Name:

Description:

Permit any command that is not in the table below

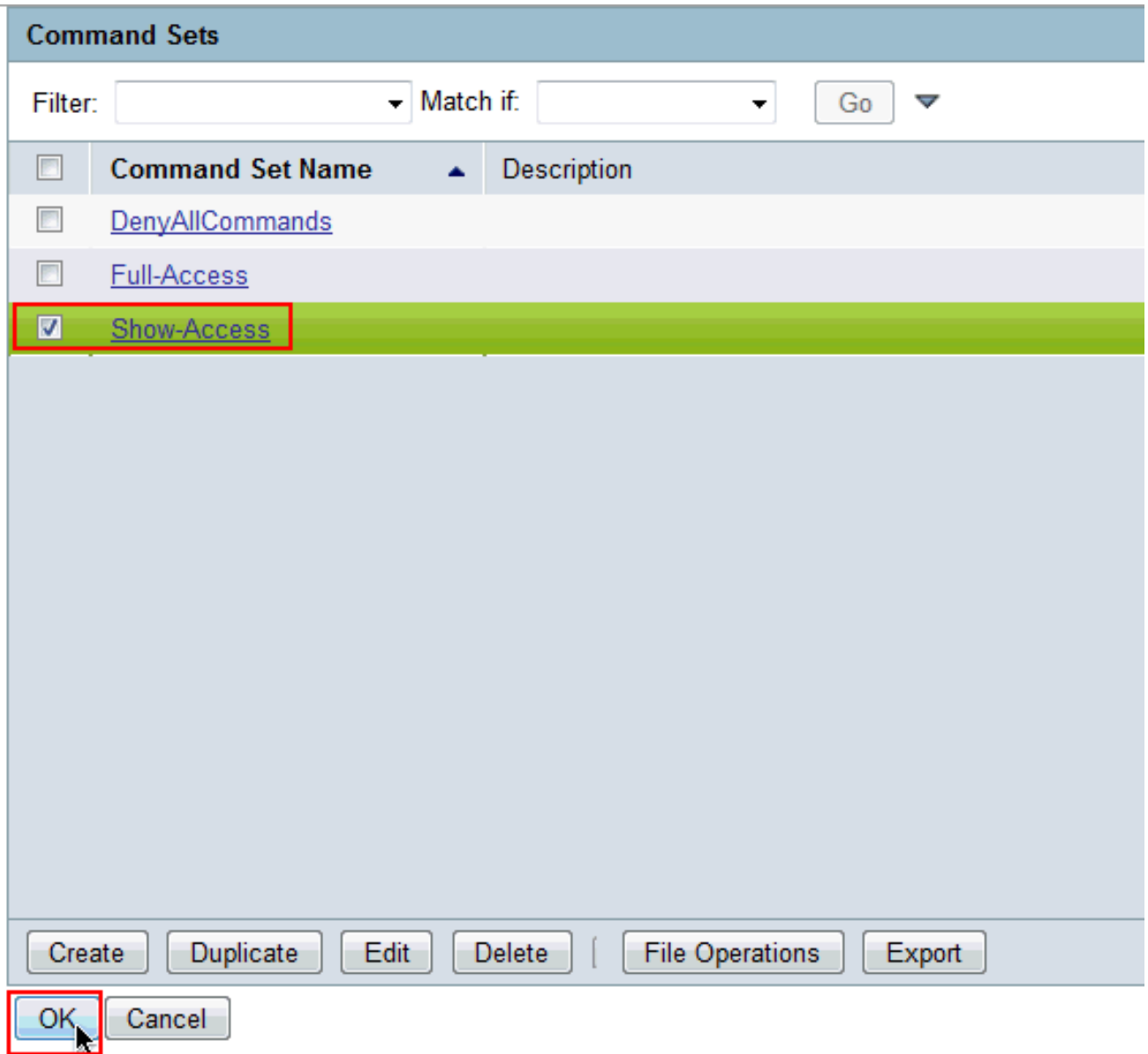
Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command:

Arguments:

Select Command/Arguments from Command Set:

37. Нажмите кнопку
OK.



38. Нажмите кнопку
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

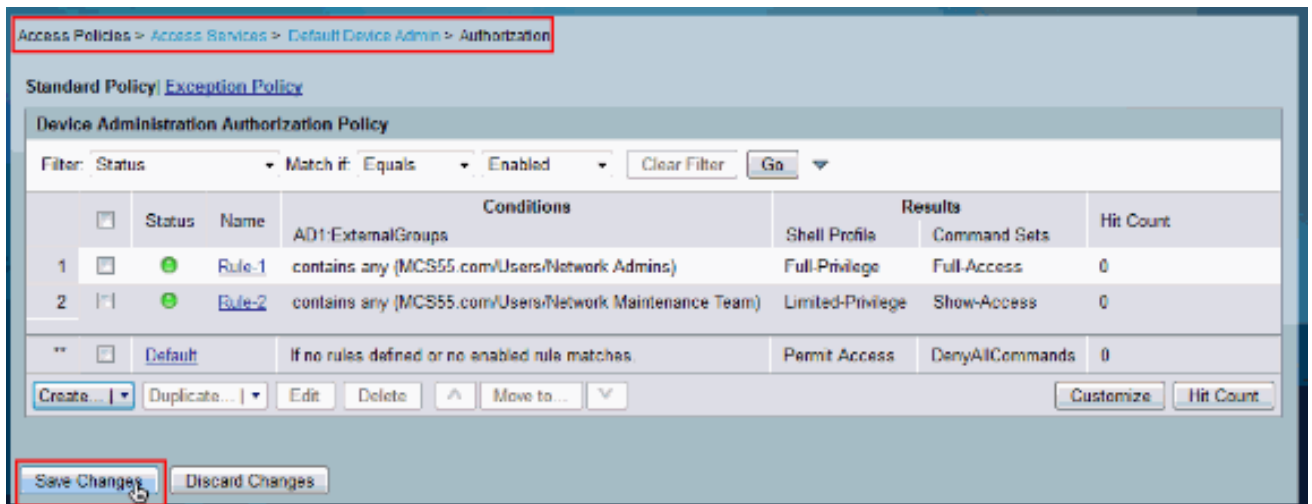
Select

Deselect

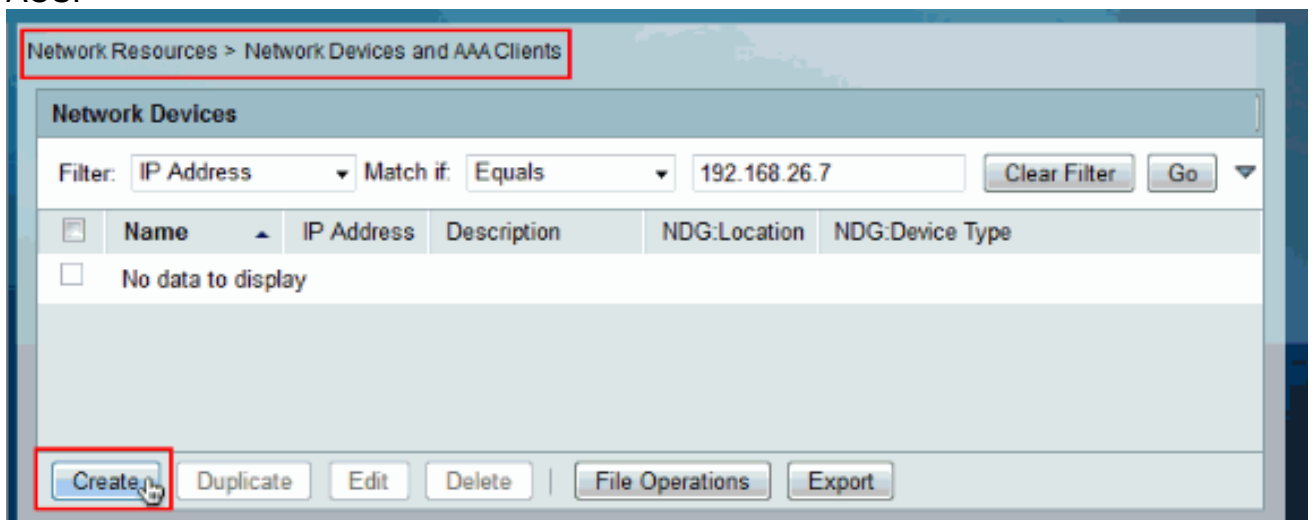
OK

Cancel

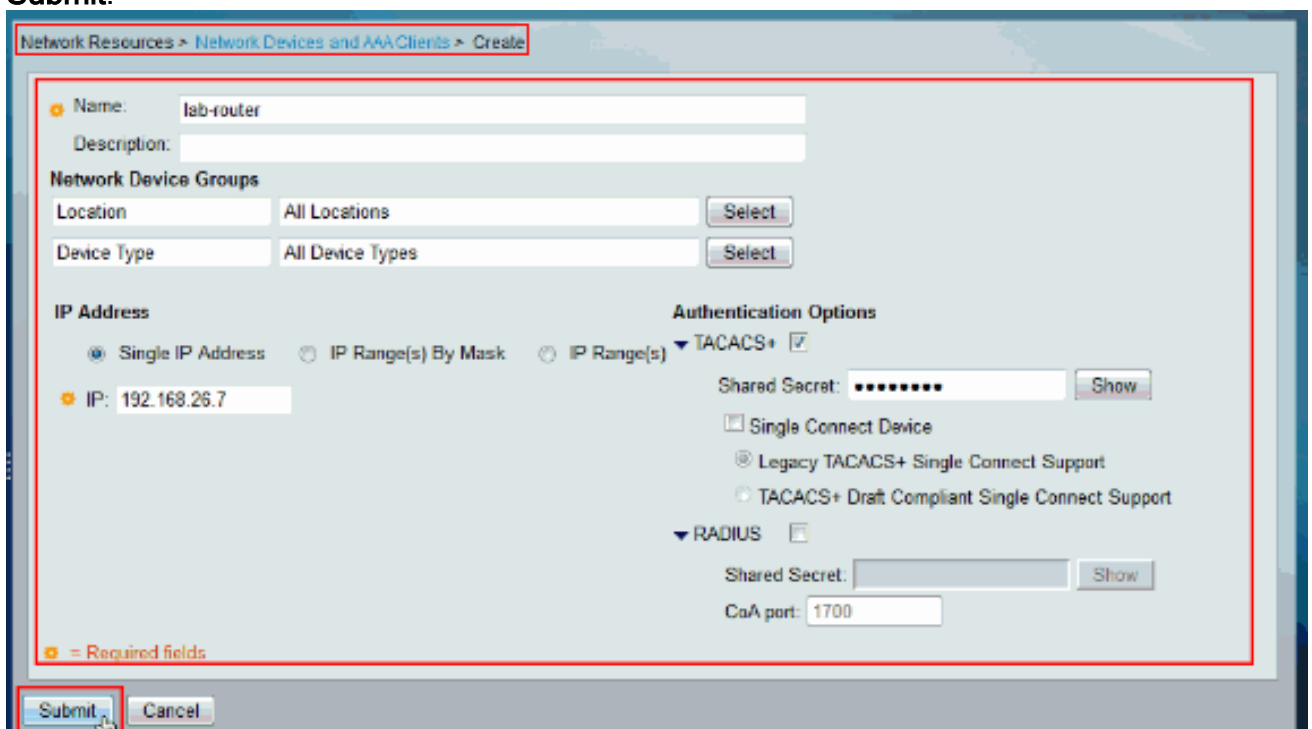
39. Нажмите кнопку Save Changes (Сохранить изменения).



40. Нажмите **Create** для добавления устройства Cisco IOS как Клиент AAA на ACS.



41. Предоставьте **Название**, **IP-адрес**, **Общий секретный ключ для TACACS +** и нажмите **Submit**.



[Настройте устройство Cisco IOS для Проверки подлинности и авторизация](#)

Выполните эти шаги для настройки устройства Cisco IOS и ACS для Проверки подлинности и авторизация.

1. Создайте локального пользователя с полными полномочиями для нейтрализации с командой **имени пользователя** как показано здесь:

```
username admin privilege 15 password 0 cisco123!
```
2. Предоставьте IP-адрес ACS, чтобы включить AAA и добавить ACS 5.x как Сервер tacacs.

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

Примечание: Ключ должен совпасть с Общим секретным ключом, предоставленным на ACS для этого устройства Cisco IOS.
3. Протестируйте достижимость Сервера tacacs с **командой test aaa** как показано.

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

Выходные данные предыдущей команды показывают, что Сервер tacacs достижим, и пользователь успешно аутентифицировался.**Примечание:** User1 и пароль xxx принадлежат AD. Если тестовые сбои гарантируйте, что Общий секретный ключ, предоставленный в предыдущем шаге, корректен.
4. Настройте вход в систему и включите аутентификации и затем используйте Exec и авторизации для выполнения команд как показано здесь:

```
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
```

Примечание: Если Сервер tacacs недостижим, Локальная переменная и Ключевые слова enable используются для нейтрализации к локальному пользователю Cisco IOS и enable secret соответственно.

Проверка

Чтобы проверить, что проверка подлинности и авторизация входит к устройству Cisco IOS через Telnet.

1. Telnet к устройству Cisco IOS как user1, кто принадлежит группе полного доступа в AD. Сетевая группа Admin является группой в AD, который сопоставлен с Полными полномочиями Профиль Shell и Набор команд Полного доступа на ACS. Попробуйте выполнить любую команду, чтобы гарантировать, что у вас есть полный доступ.

```
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 к устройству Cisco IOS как user2, кто принадлежит группе ограниченного доступа в AD. (Группа **Команды Обслуживания сети** является группой в AD, который сопоставлен с **Ограниченной Привилегией Профиль Shell** и **Набор команд Показывать-доступа** на ACS). При попытке выполнить какую-либо команду кроме тех упомянутых в наборе команд **Показывать-доступа**, необходимо получить ошибку `Command Authorization Failed`, которая показывает, что user2 имеет ограниченный доступ.

```

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"

          5
          5

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/stipng.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. Вход в систему к GUI ACS и средству просмотра Отслеживающего и сообщаемого запуски. Выберите AAA Protocol> TACACS+Authorization для проверки действий, выполненных user1 и 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 6:21:19.390 AM	✔			user2	[CmdA]write		lab-cosmos
Jun 8,12 6:20:59.800 AM	Jun 8,12 6:20:59.799 AM	✖		11025 Command failed to match a Permit rule	user2	[CmdA]write memory		lab-cosmos
Jun 8,12 6:20:59.999 AM	Jun 8,12 6:20:59.899 AM	✖		11024 Command failed to match a Permit rule	user2	[CmdA]configure terminal		lab-cosmos
Jun 8,12 6:20:50.056 AM	Jun 8,12 6:20:50.056 AM	✔			user2	[CmdA]show version		lab-cosmos
Jun 8,12 6:20:38.506 AM	Jun 8,12 6:20:38.499 AM	✔			user2	[CmdA]enable		lab-cosmos
Jun 8,12 6:20:34.426 AM	Jun 8,12 6:20:34.406 AM	✔			user2	[CmdA]=	Limited-Privilege	lab-cosmos
Jun 8,12 6:20:02.616 AM	Jun 8,12 6:20:02.596 AM	✔			user1	[CmdA]write		lab-cosmos
Jun 8,12 6:20:00.265 AM	Jun 8,12 6:20:00.246 AM	✔			user1	[CmdA]version 2		lab-cosmos
Jun 8,12 6:19:57.203 AM	Jun 8,12 6:19:57.200 AM	✔			user1	[CmdA]router rip		lab-cosmos
Jun 8,12 6:19:55.103 AM	Jun 8,12 6:19:55.076 AM	✔			user1	[CmdA]configure terminal		lab-cosmos
Jun 8,12 6:19:52.743 AM	Jun 8,12 6:19:52.740 AM	✔			user1	[CmdA]=	Full-Privilege	lab-cosmos

Commands run by user 2

Commands run by user1

Дополнительные сведения

- [Система управления доступом Cisco Secure Access Control System](#)
- [Cisco Systems – техническая поддержка и документация](#)