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

Содержание

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.

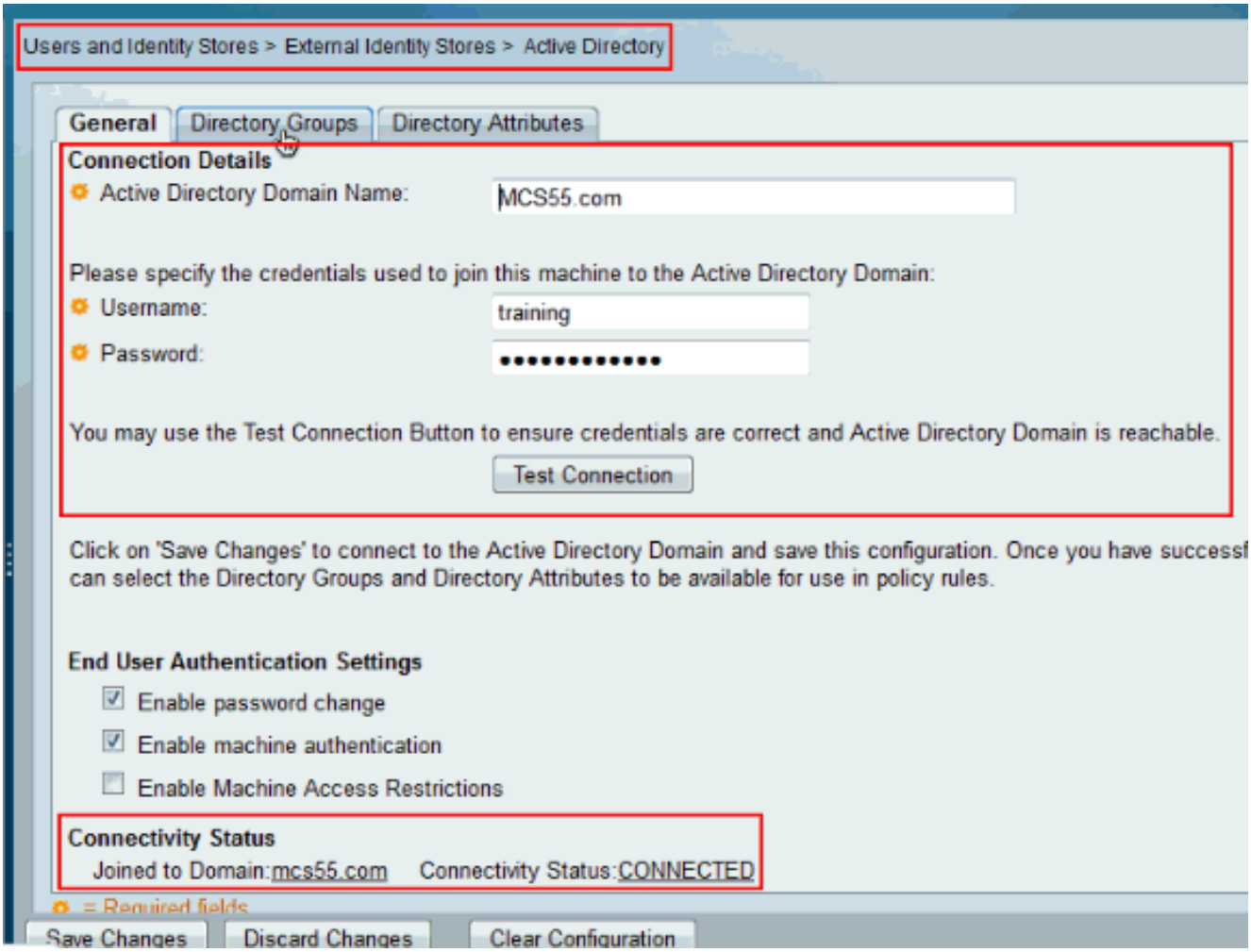
!--- конфигурацию

Настройте ACS 5.x для проверки подлинности и авторизация

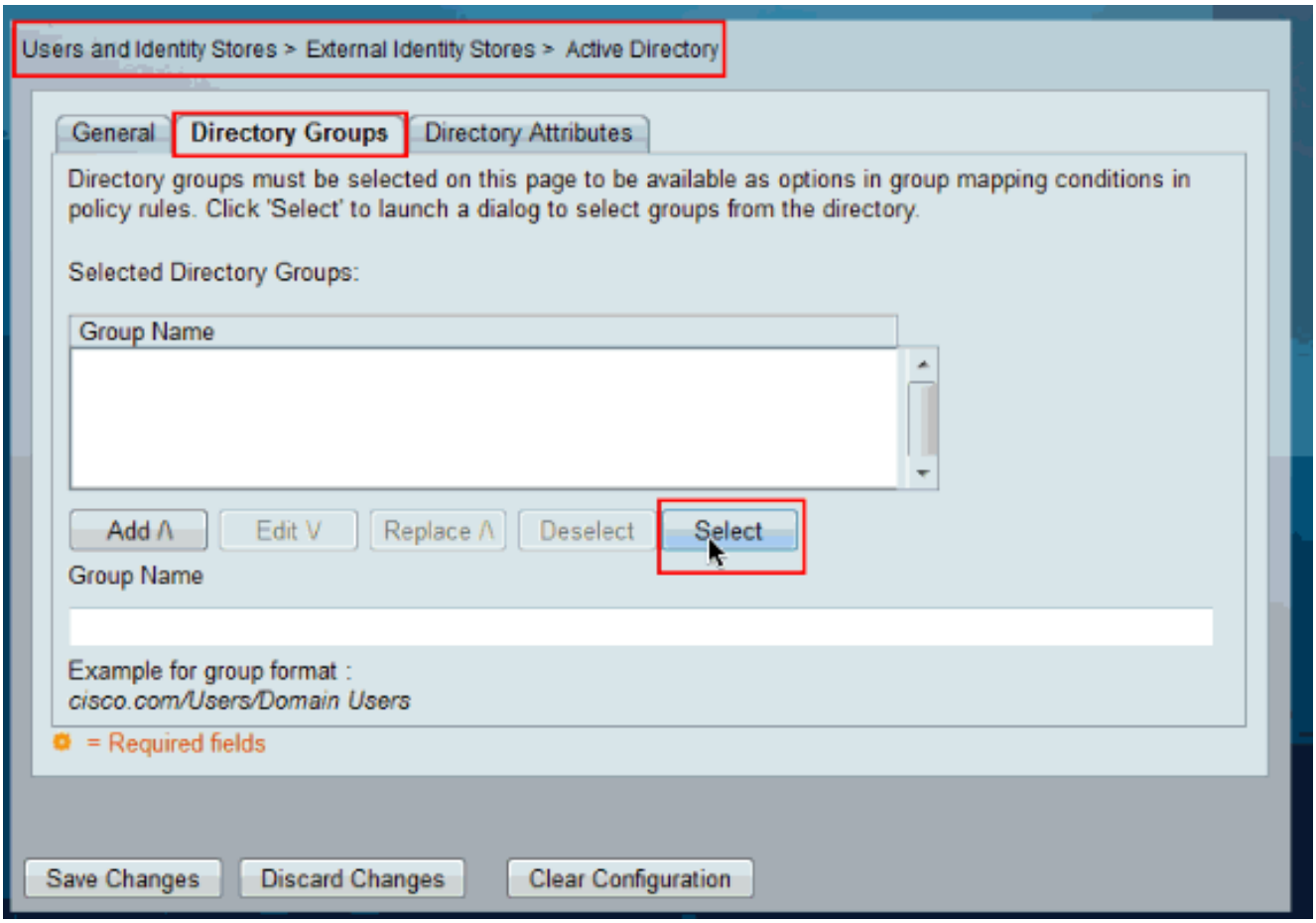
Перед началом конфигурации ACS 5.x для Проверки подлинности и авторизация ACS должен был быть интегрирован успешно с Microsoft AD. Если ACS не интегрирован с желаемым AD Доменом, обратитесь к ACS 5.x и позже: Интеграция с Примером конфигурации Microsoft Active Directory для получения дополнительной информации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

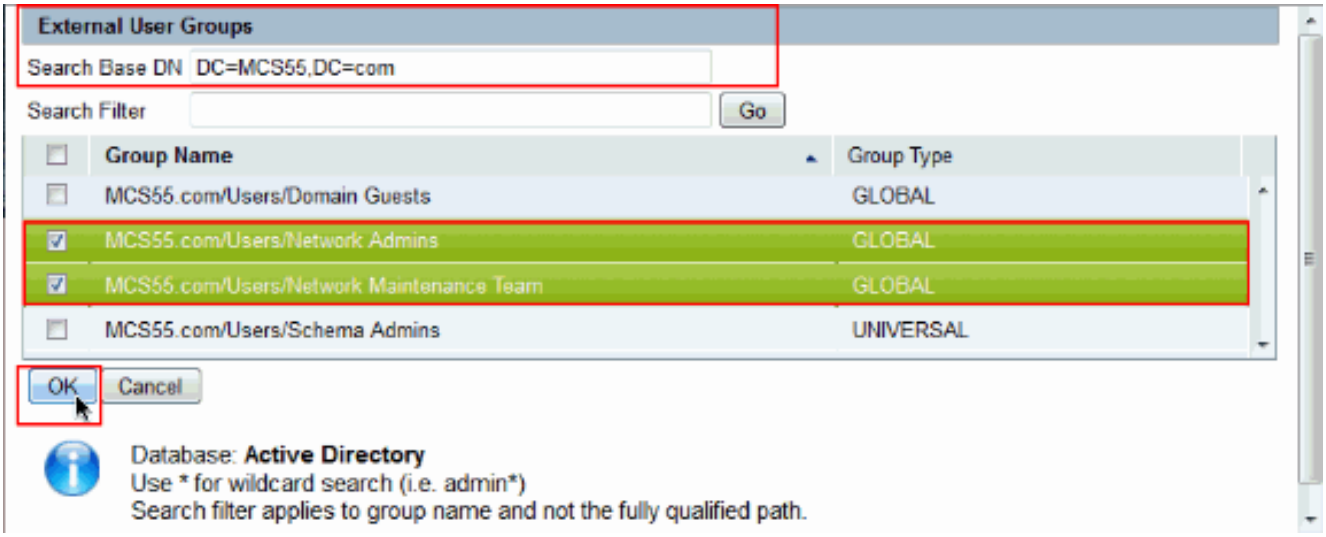
1. Войдите в учетные данные Admin использования GUI ACS.
2. Выберите **Users и Identity Stores> External Identity Stores> Active Directory** и проверьте, что ACS присоединился к желаемому домену и также что **статус подключения** показывают, как **связано**.Щелкните **по Directory Groups Tab**.



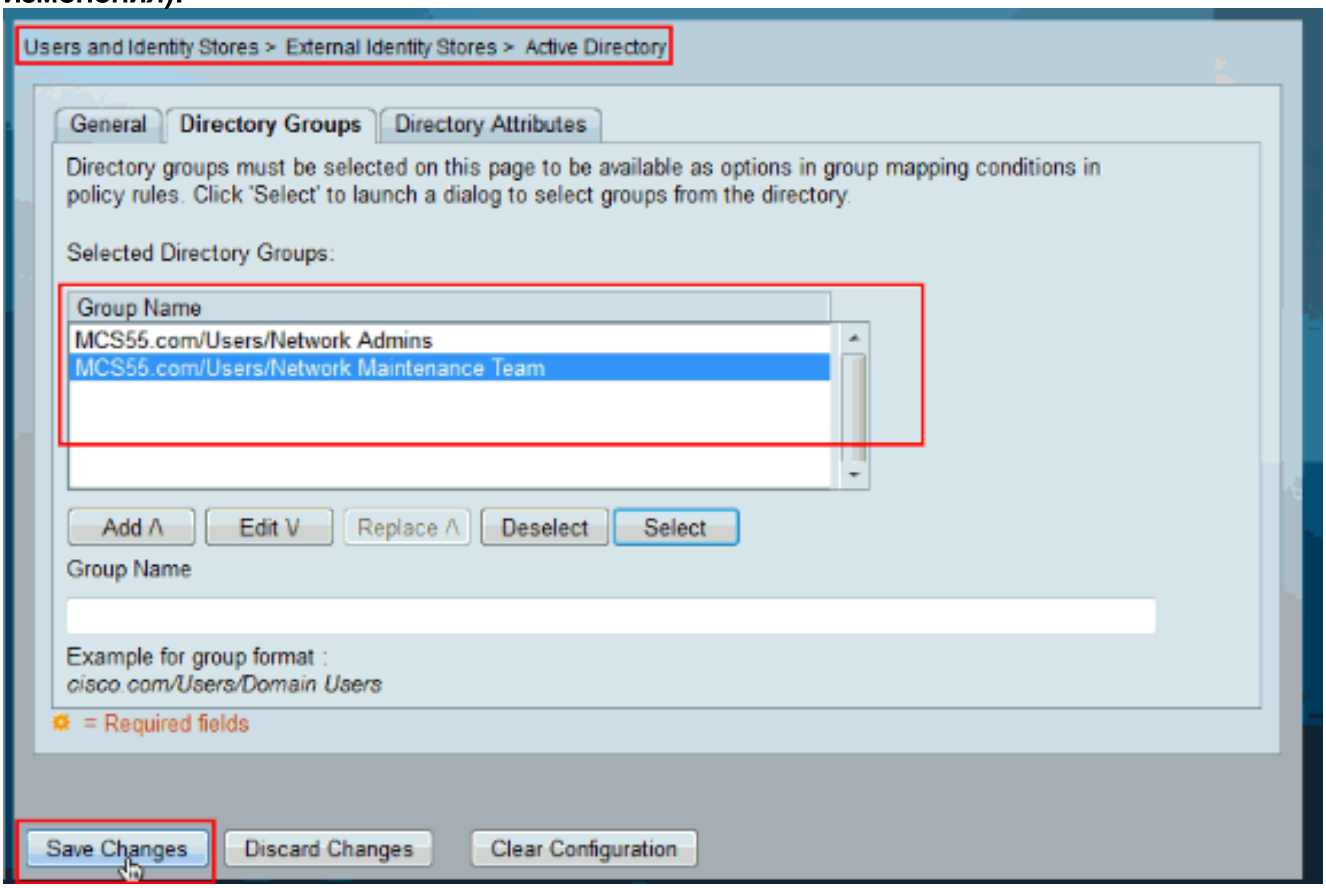
3. Нажмите **Select**.



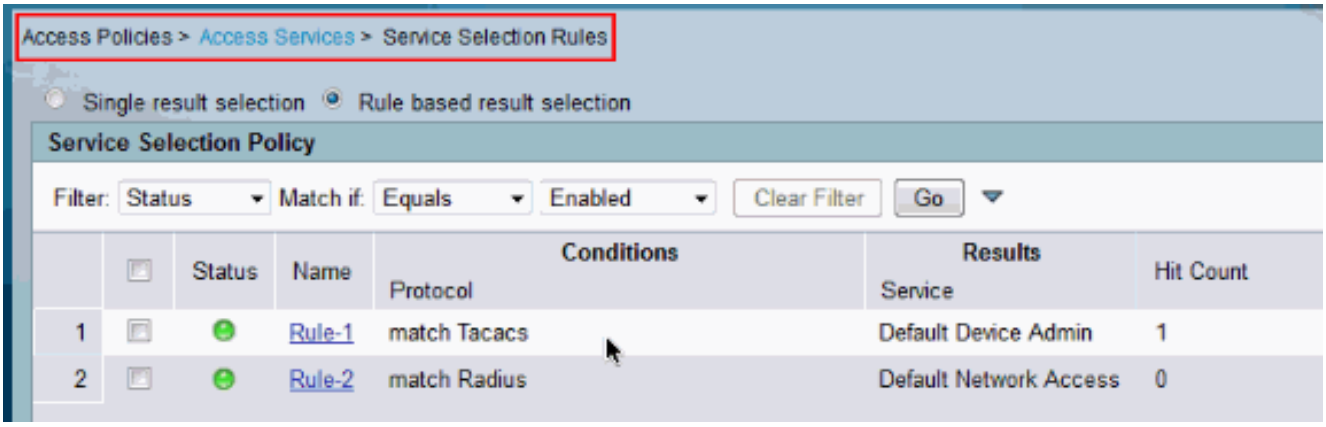
4. Выберите группы, которые должны быть сопоставлены с профилями Shell и наборами команд в более поздней части конфигурации. **Нажмите кнопку ОК.**



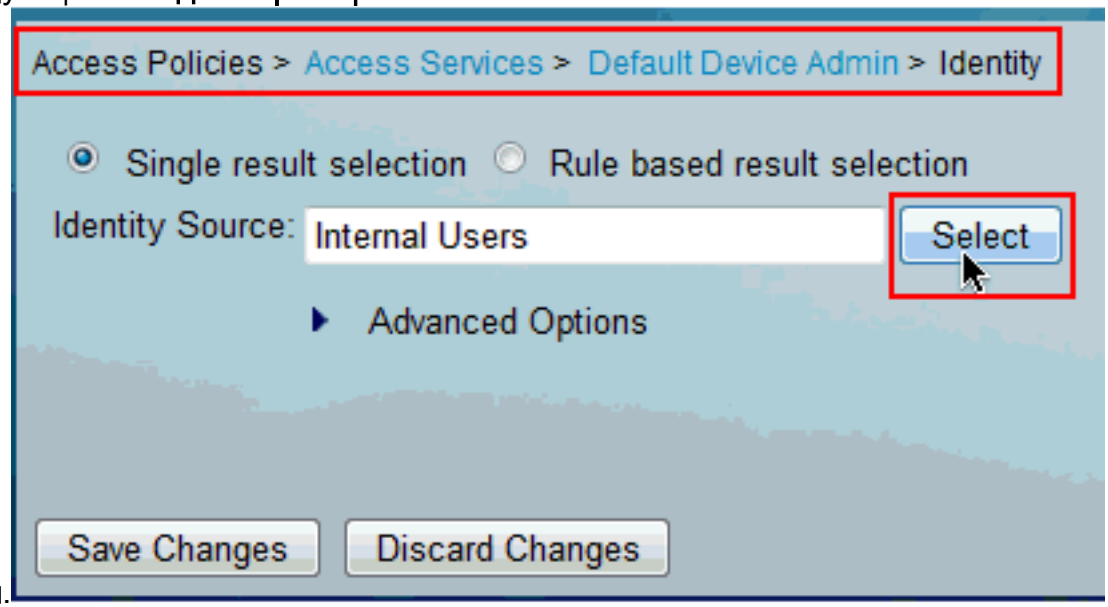
5. **Нажмите кнопку Save Changes (Сохранить изменения).**



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**.

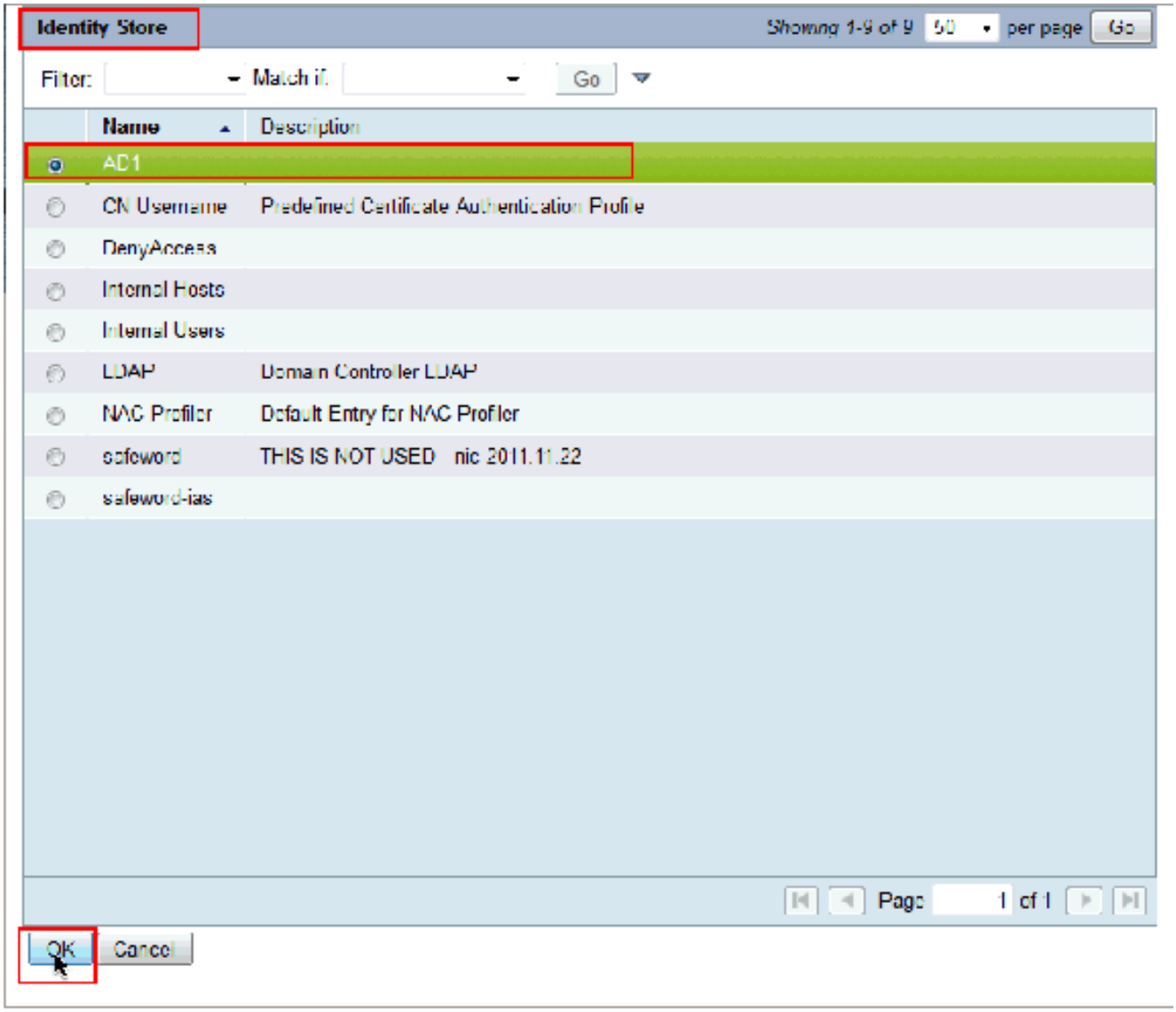


7. Выберите **Access Policies> Access Services> Default Device Admin> Identity** и нажмите **Select**, следующий за **Идентификационным**

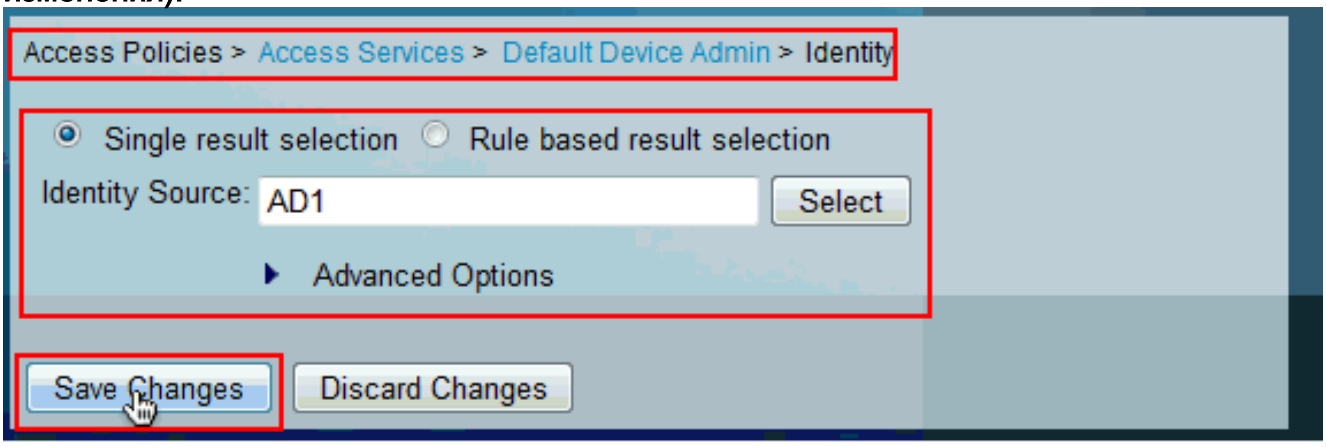


Источником.

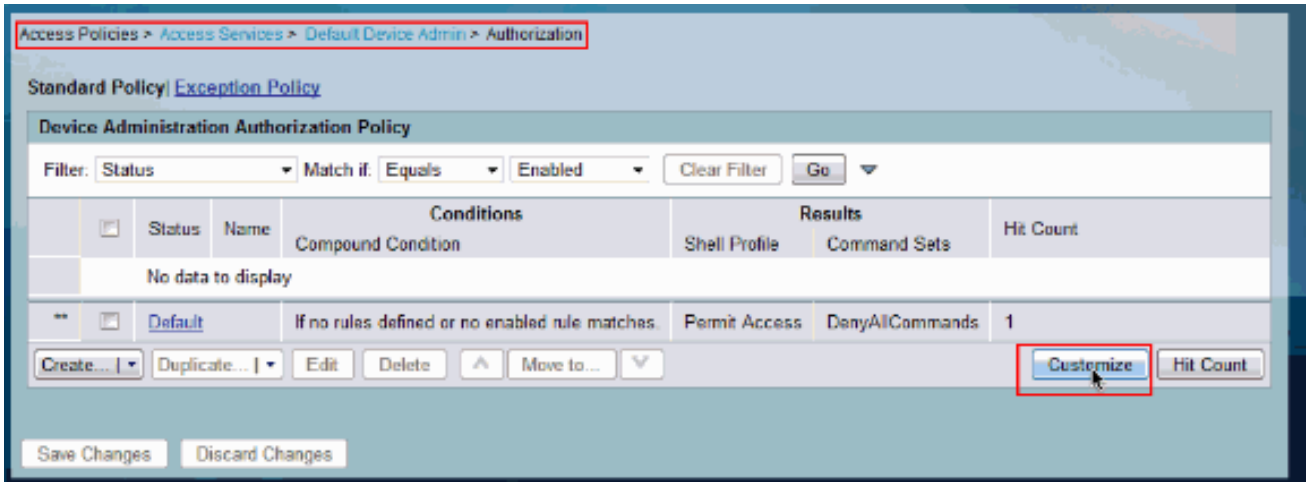
8. Выберите **AD1** и нажмите **OK**.



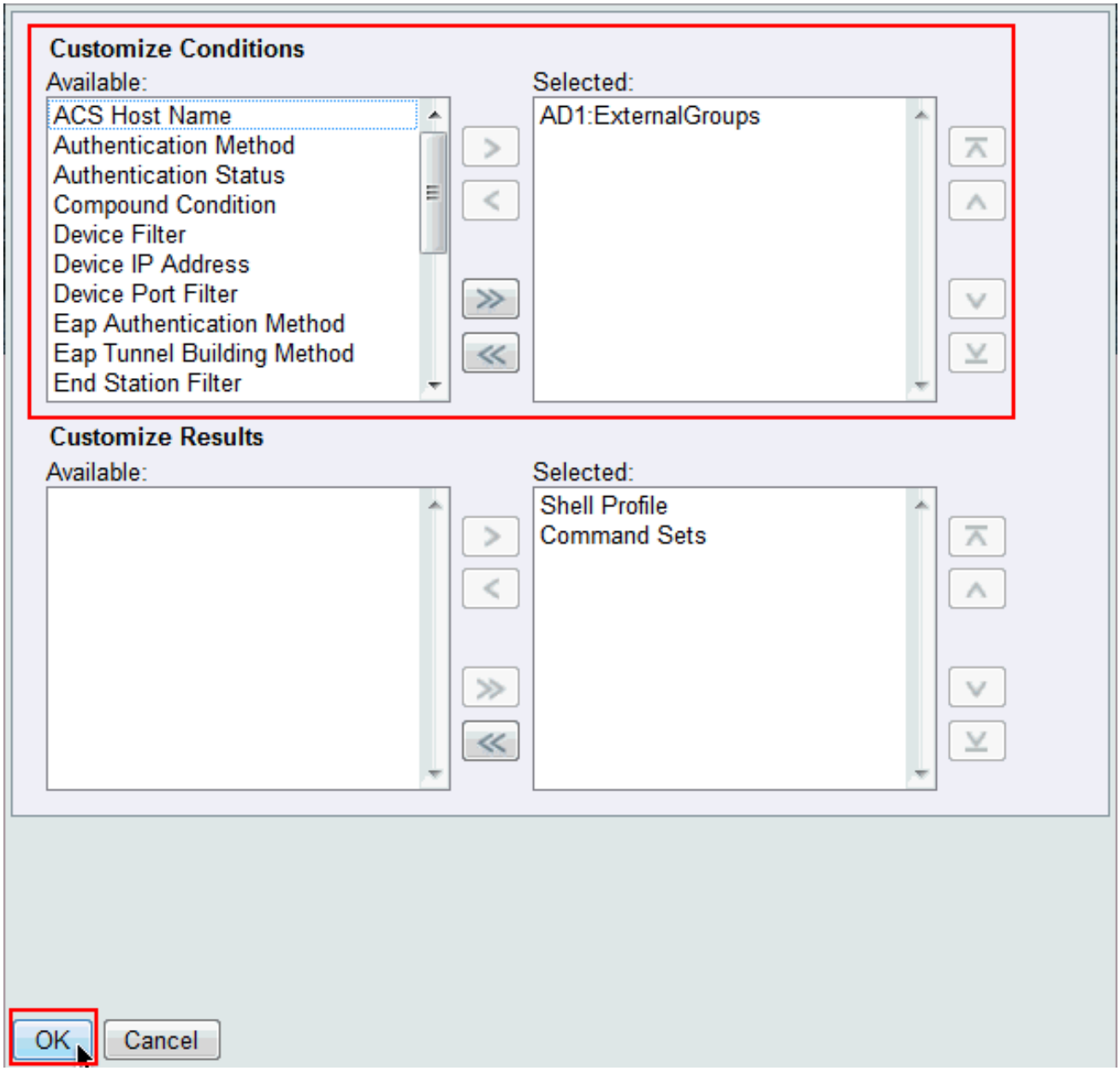
9. **Нажмите кнопку Save Changes (Сохранить изменения).**



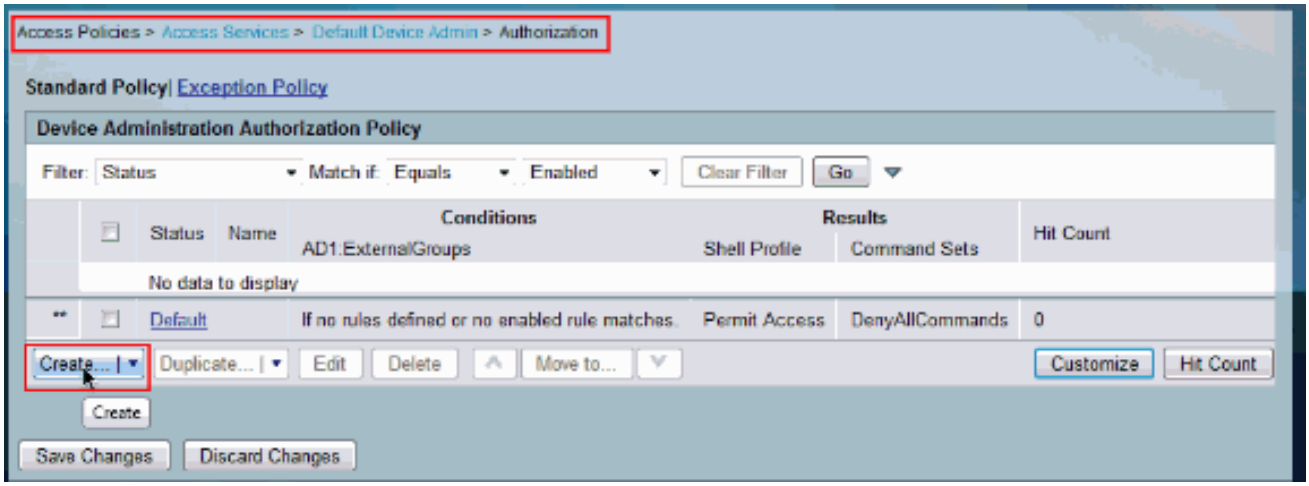
10. Выберите **Access Policies> Access Services> Default Device Admin> Authorization** и щелкните **по Customize**.



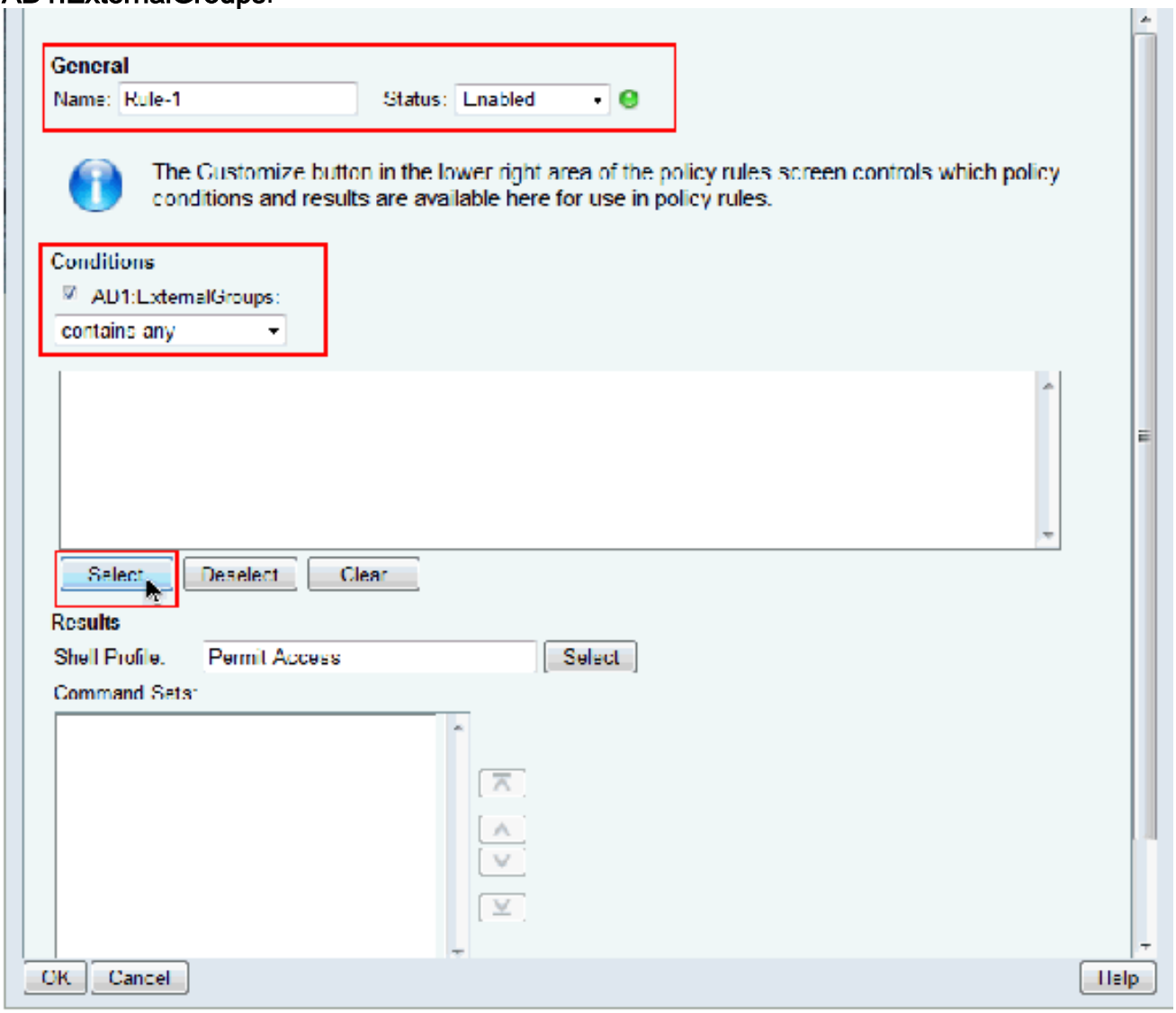
11. **Копия AD1:ExternalGroups** от **Доступного** до **Выбранного раздела Настраивает Условия** и затем перемещает **Профиль Shell**, и **Наборы команд** от **Доступного** до **Выбранного раздела Настраивают Результаты**. Теперь нажмите **OK**.



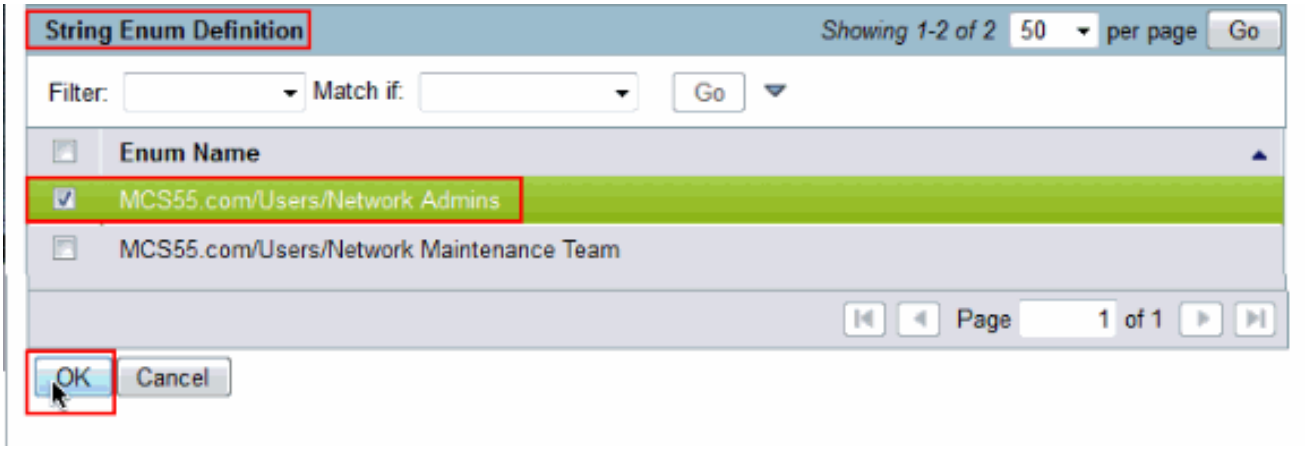
12. Нажмите **Create** для создания нового Правила.



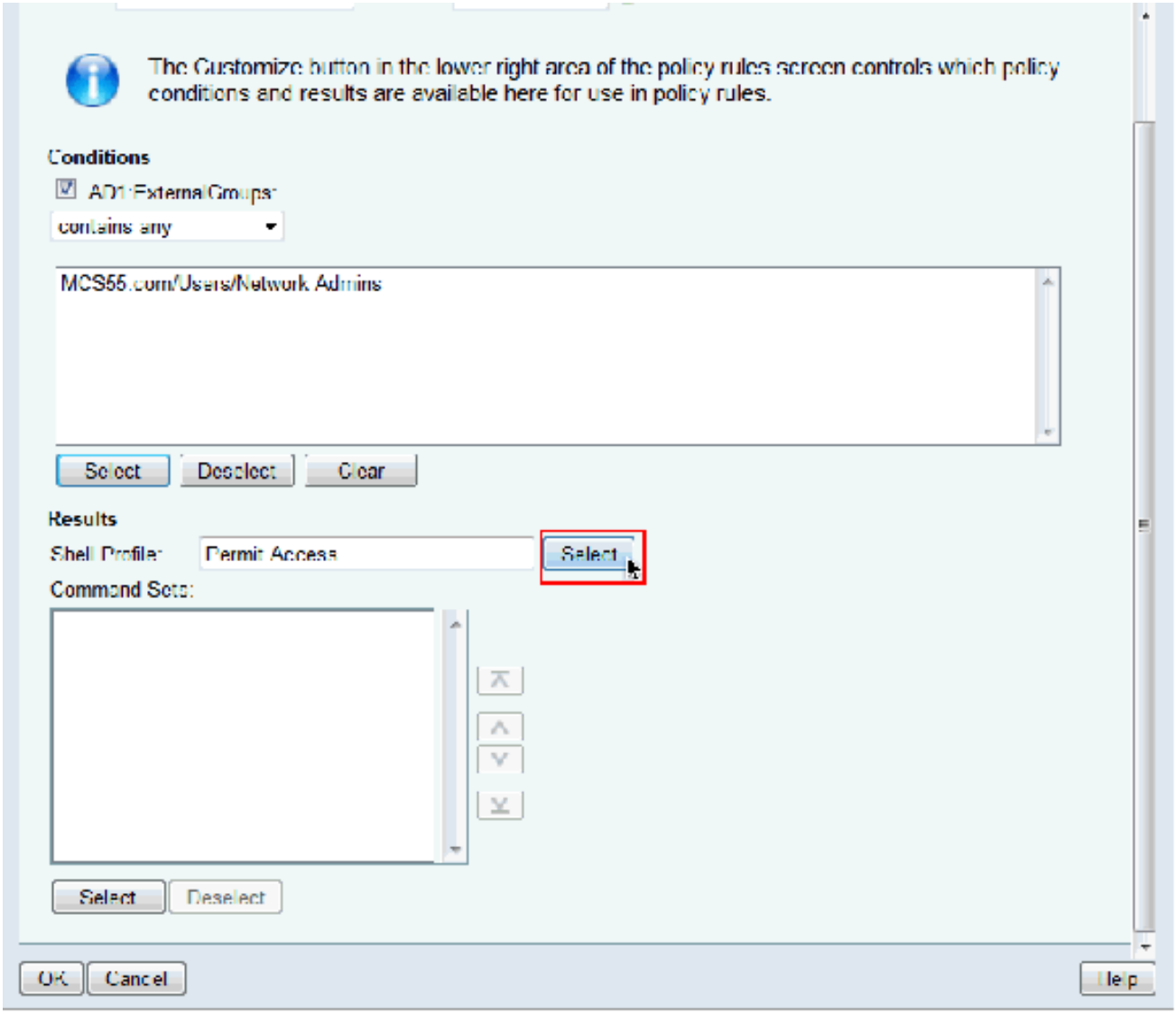
13. Нажмите **Select** в условии **AD1:ExternalGroups**.



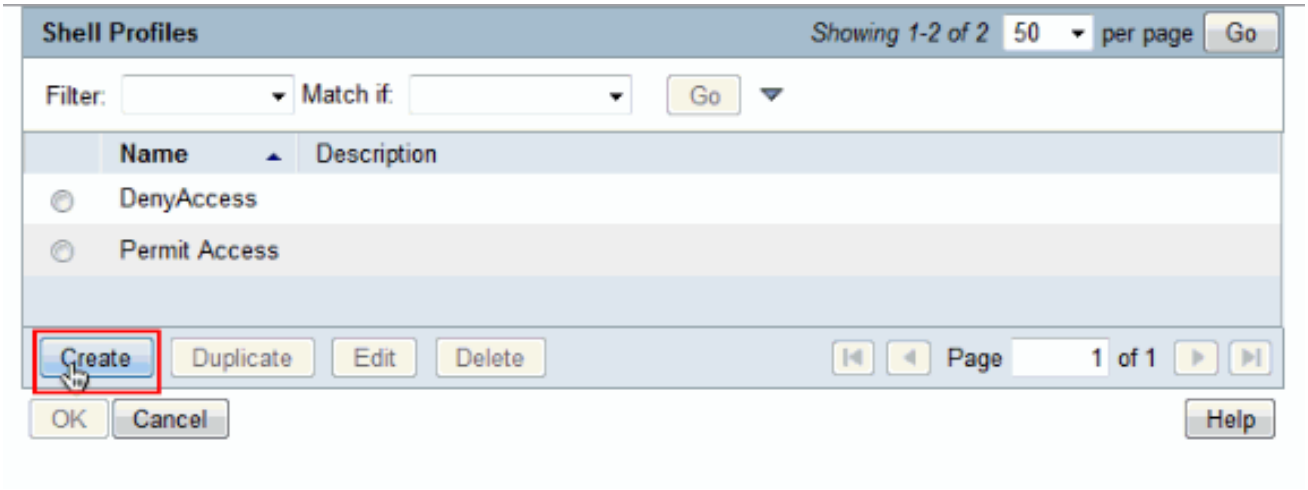
14. Выберите группу, что вы хотите предоставить полный доступ на устройстве Cisco IOS. **Нажмите кнопку ОК.**



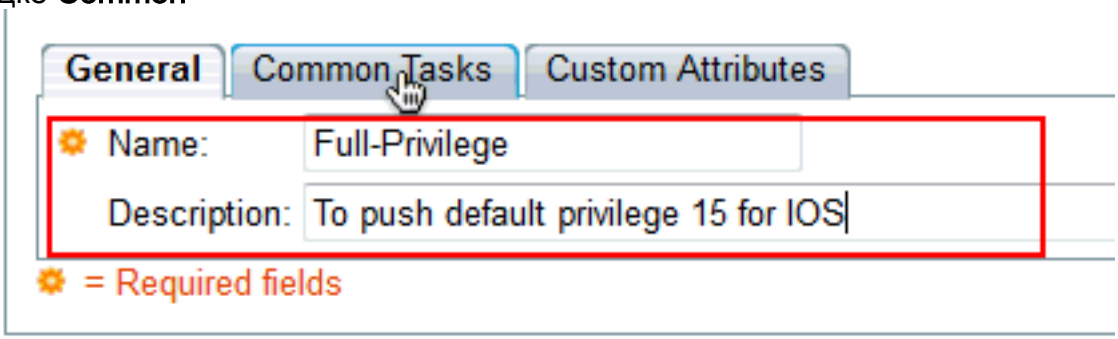
15. Нажмите **Select** в поле Shell Profile.



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

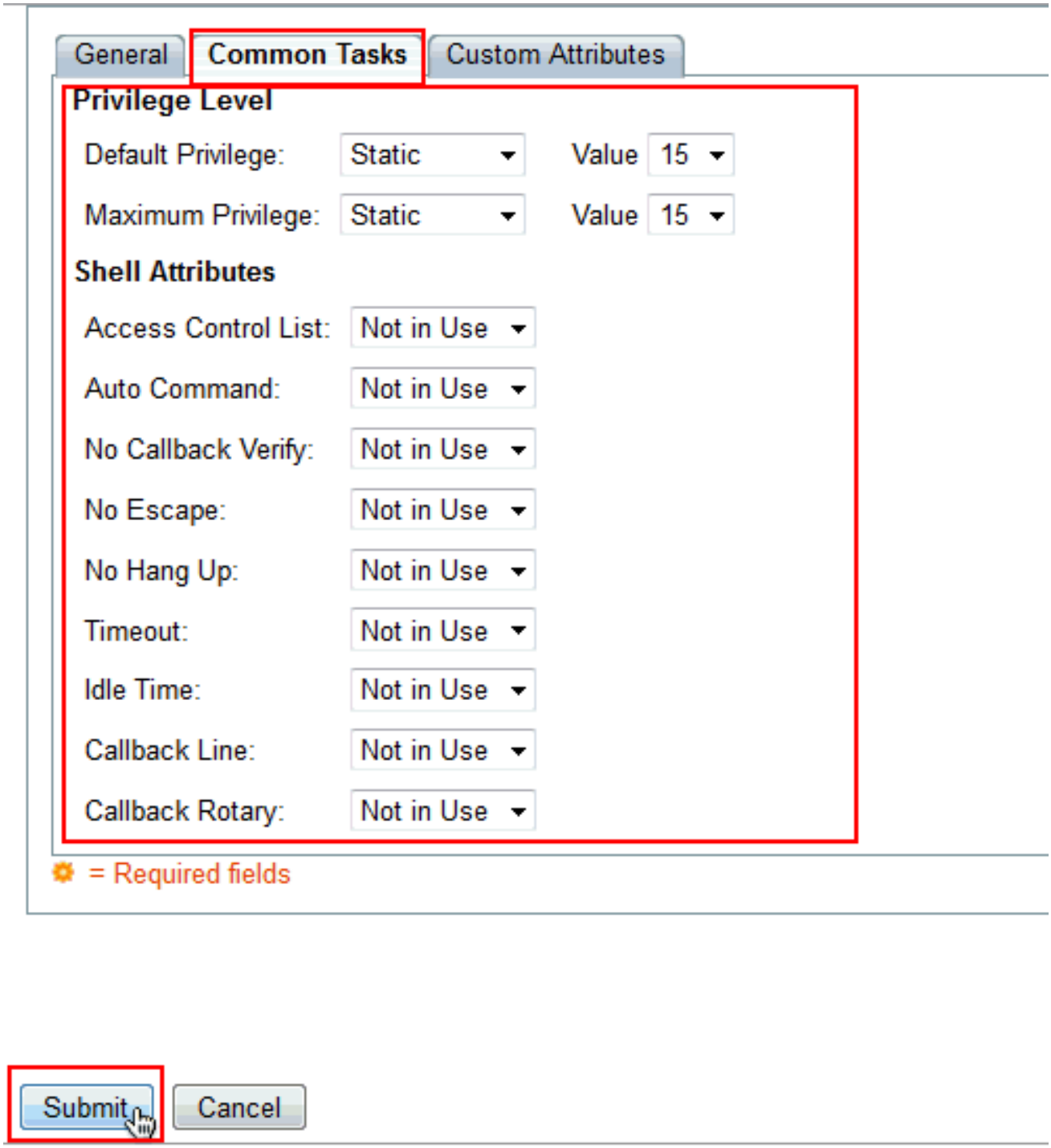


17. Предоставьте **Название** и **Описание** (дополнительное) во **Вкладке Общие**, и щелкните по вкладке **Common**

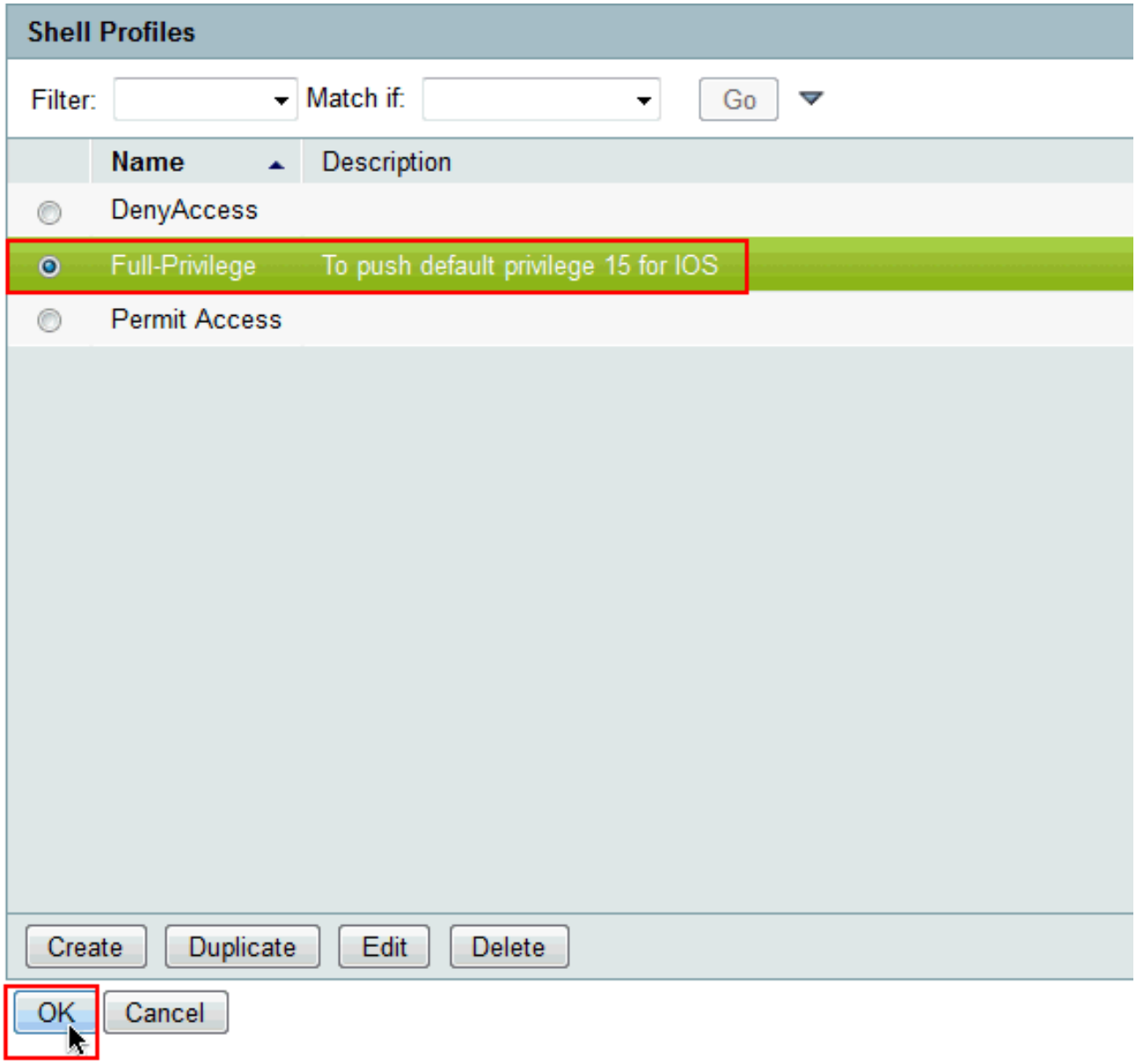


Tasks.

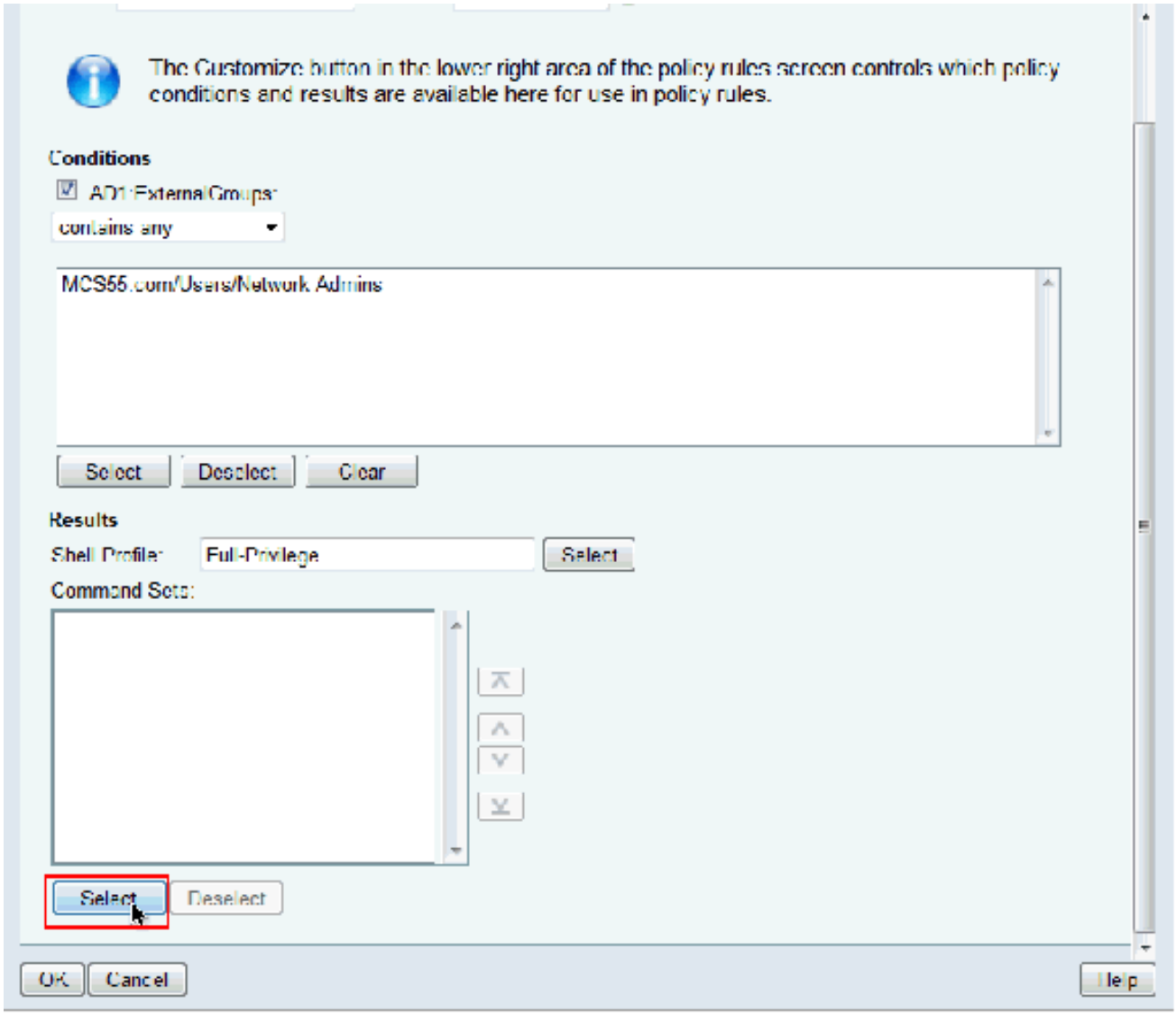
18. Измените **привилегии по умолчанию** и **максимальную привилегию** к **статическому** со **значением 15**. **Нажмите кнопку Submit (Отправить).**



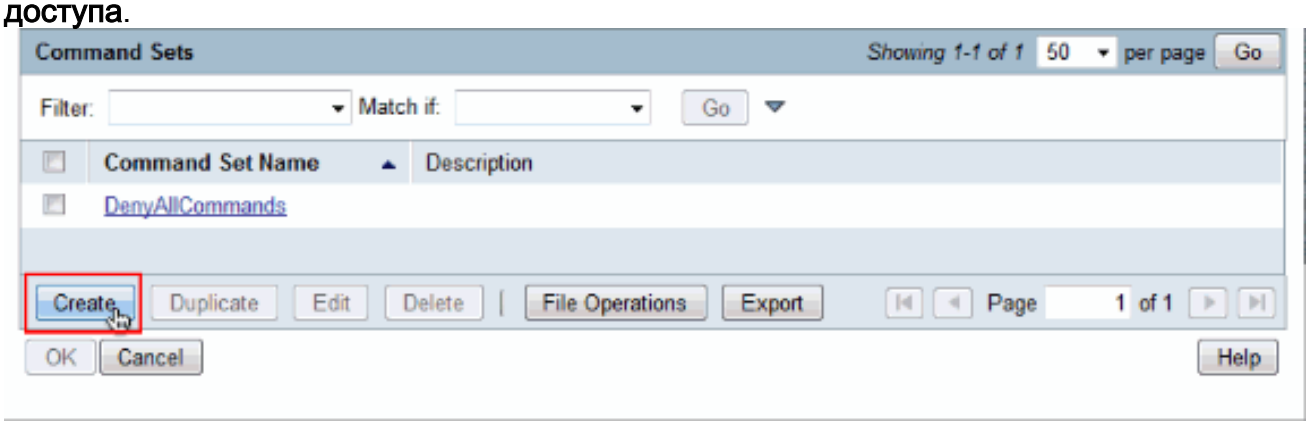
19. Теперь выберите недавно созданный полный доступ **Профиль Shell** (Полные полномочия в данном примере) и нажмите **OK**.



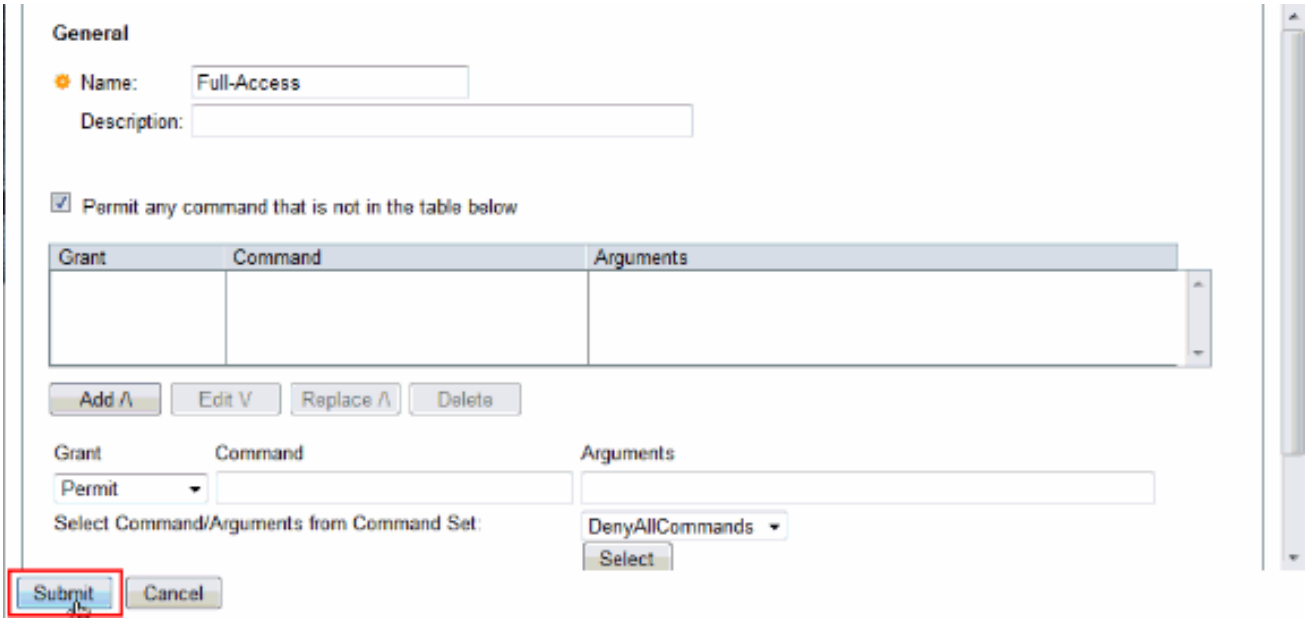
20. Нажмите **Select** в поле Command Sets.



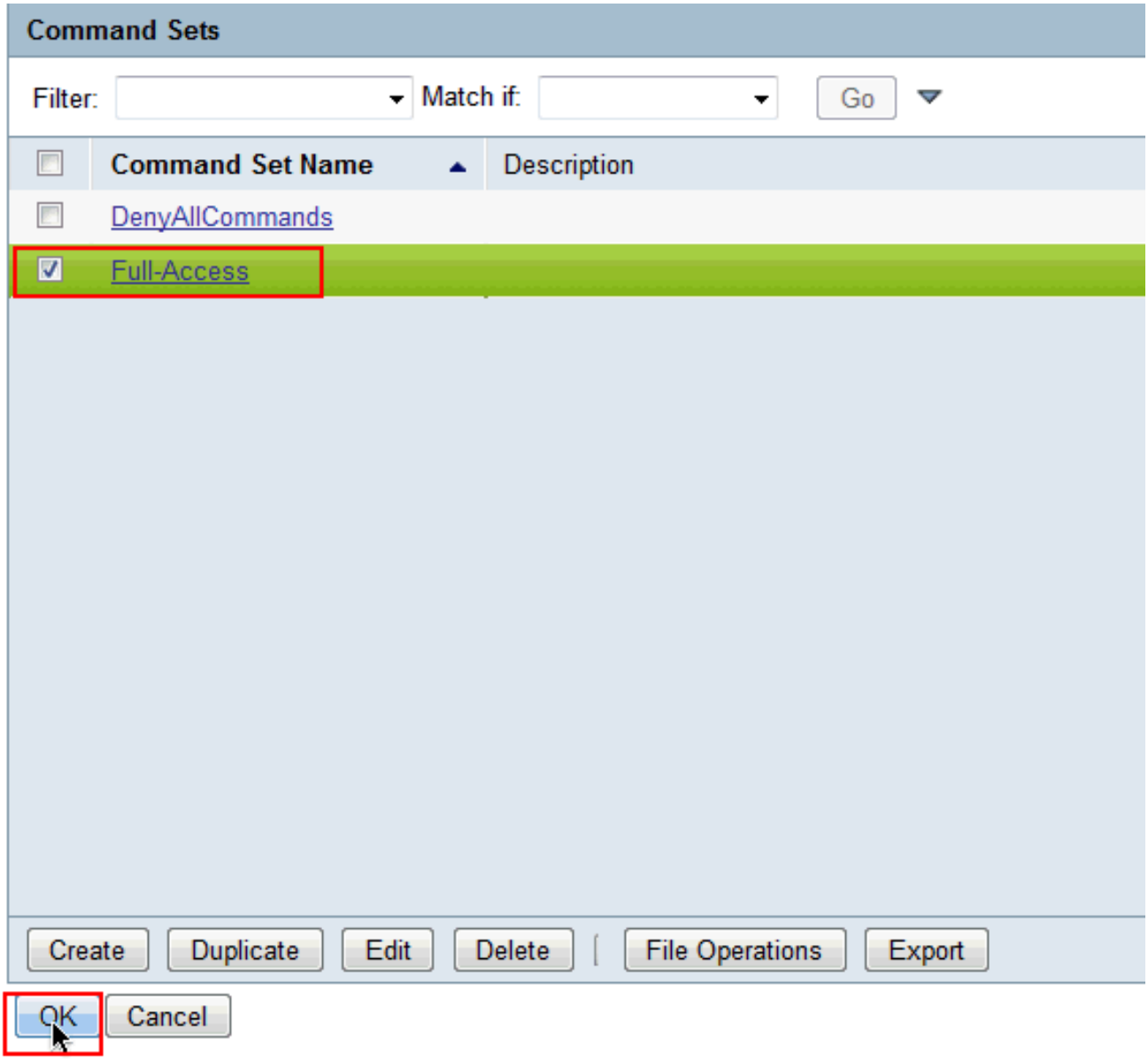
21. Нажмите **Create** для создания нового **Набора команд** для пользователей **Полного доступа**.



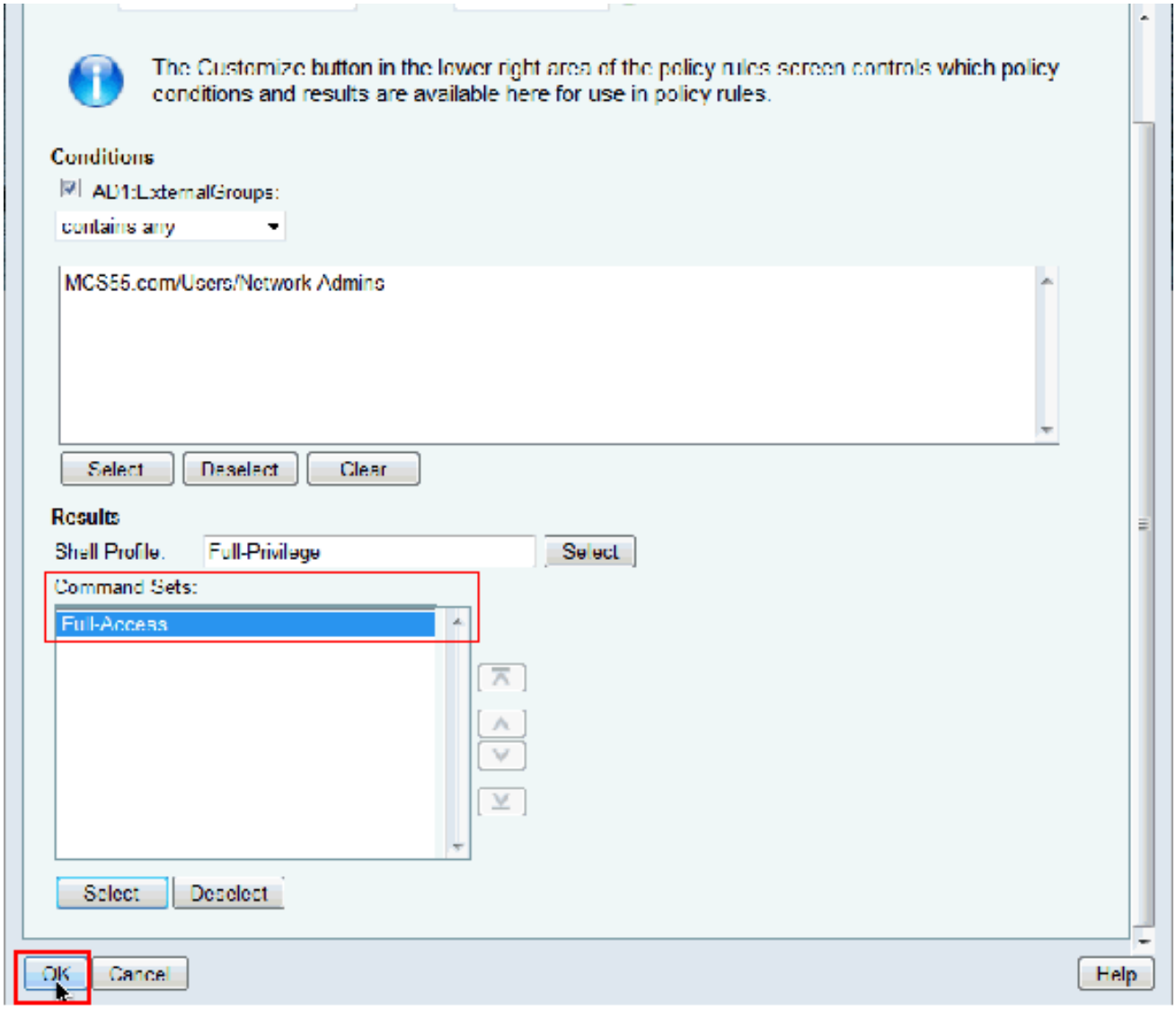
22. Предоставьте **Название** и гарантируйте, что **ниже**, проверен флажок затем для **Разрешения любой команды, которая не находится в таблице**. **Нажмите кнопку Submit (Отправить).Примечание:** См. Создание, Дублирование и Редактирование Наборов команд для Администрирования устройств для получения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



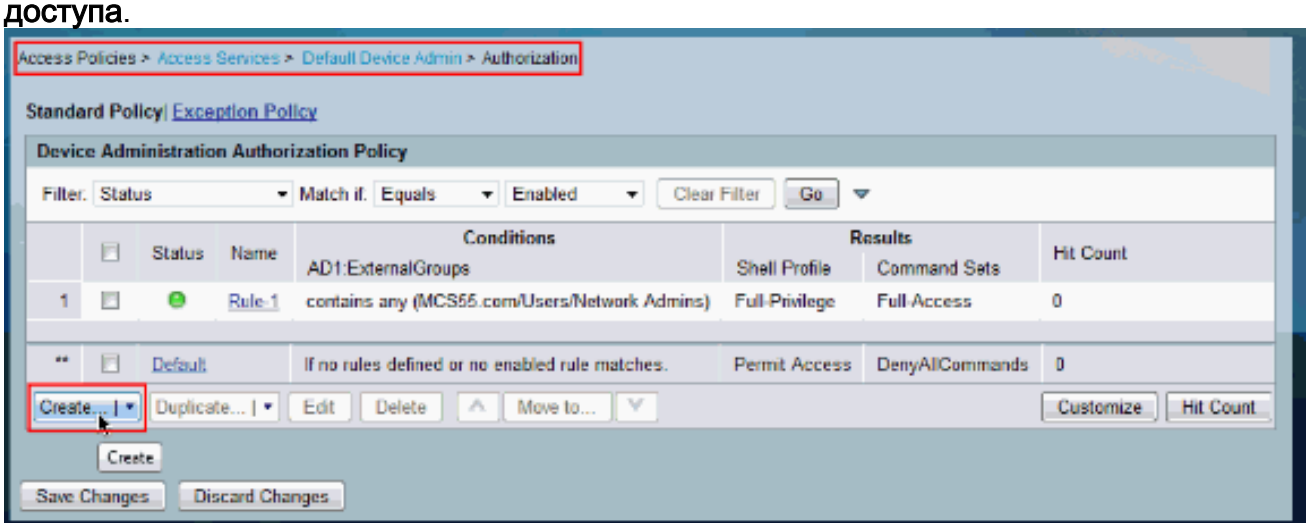
23. **Нажмите кнопку OK.**



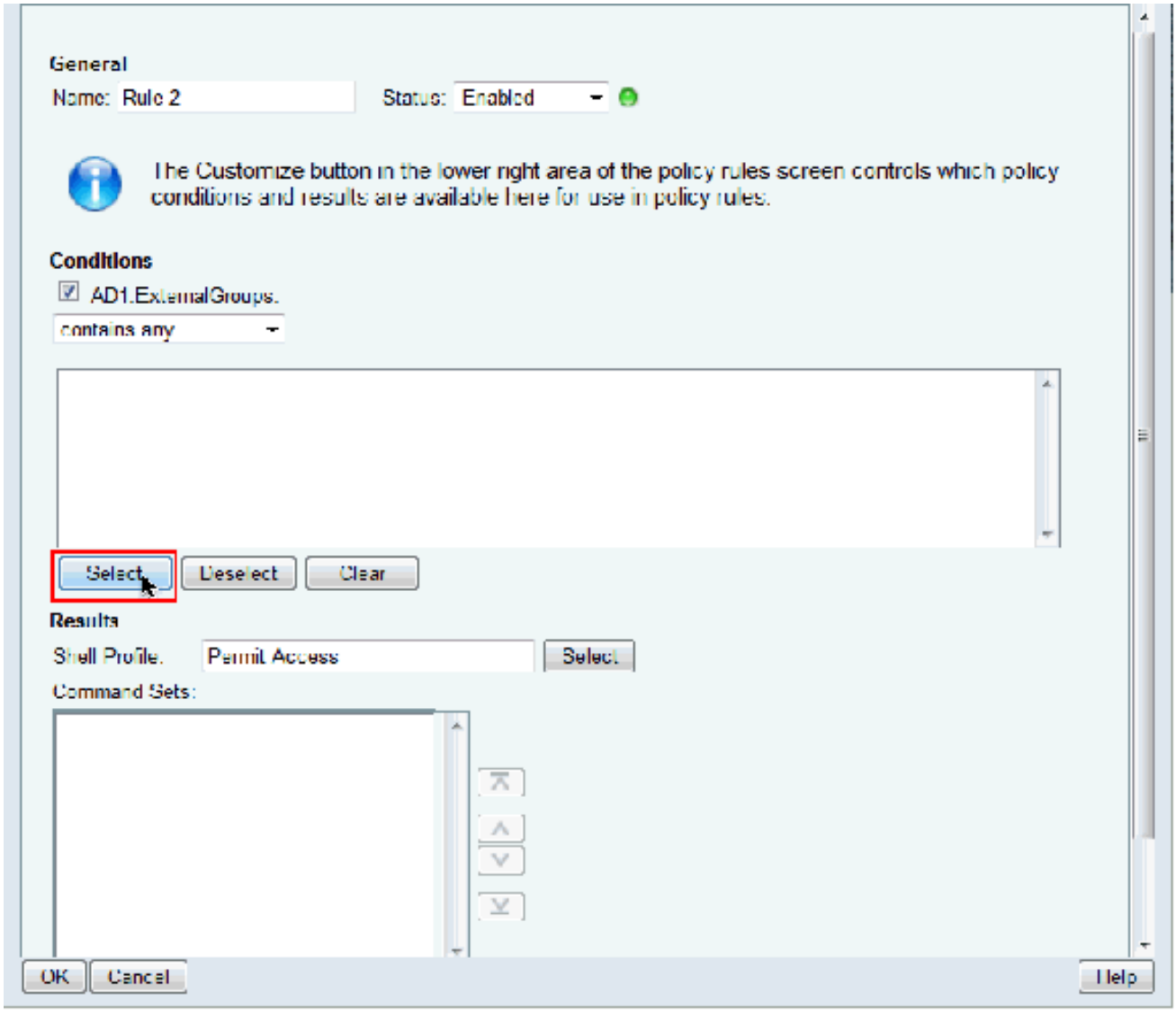
24. **Нажмите кнопку OK.** Это завершает конфигурацию **Правила 1**.



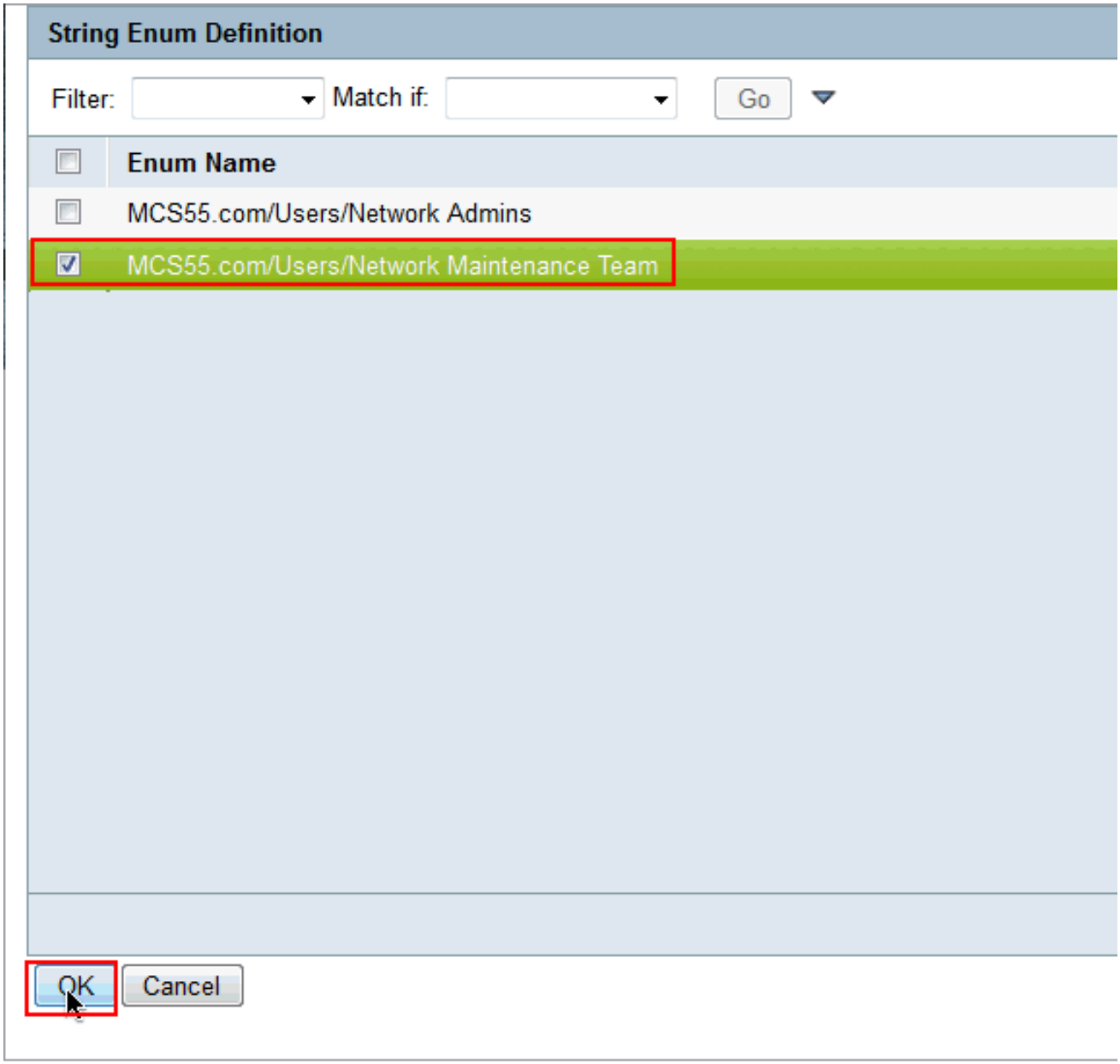
25. Нажмите **Create** для создания нового Правила для пользователей **ограниченного доступа**.



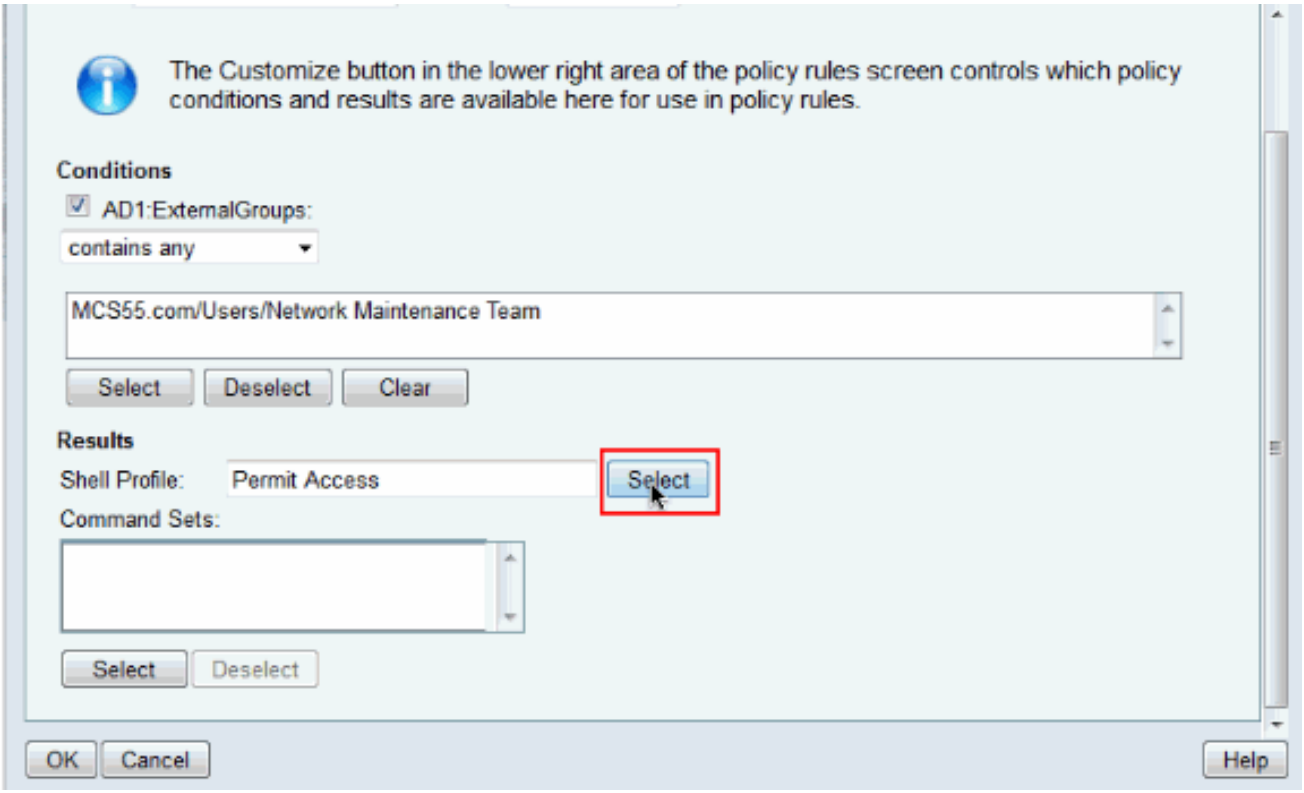
26. Выберите **AD1:ExternalGroups** и нажмите **Select**.



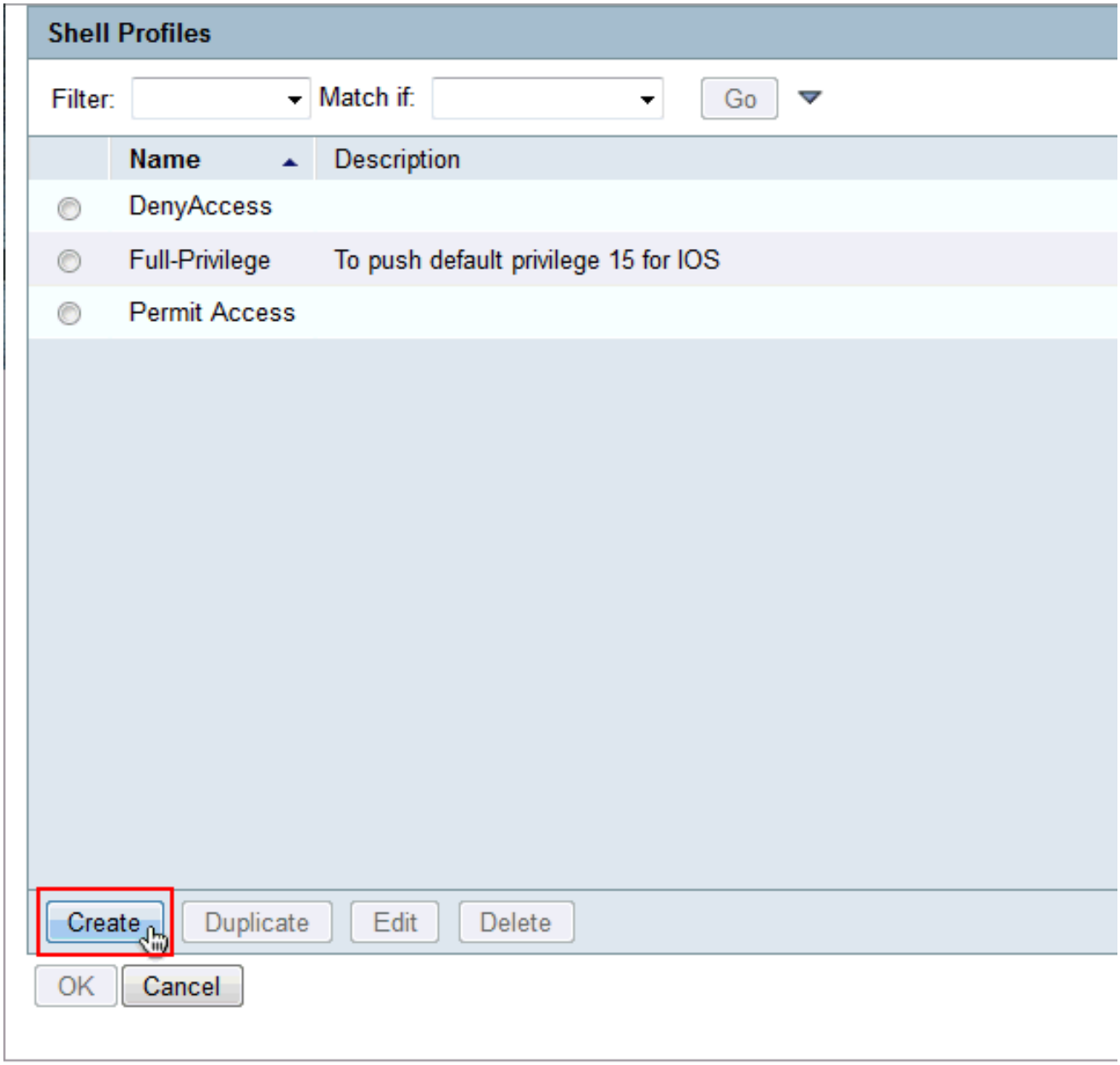
27. Выберите группу (или) группы, к которым вы хотите предоставить ограниченный доступ и нажать
OK.



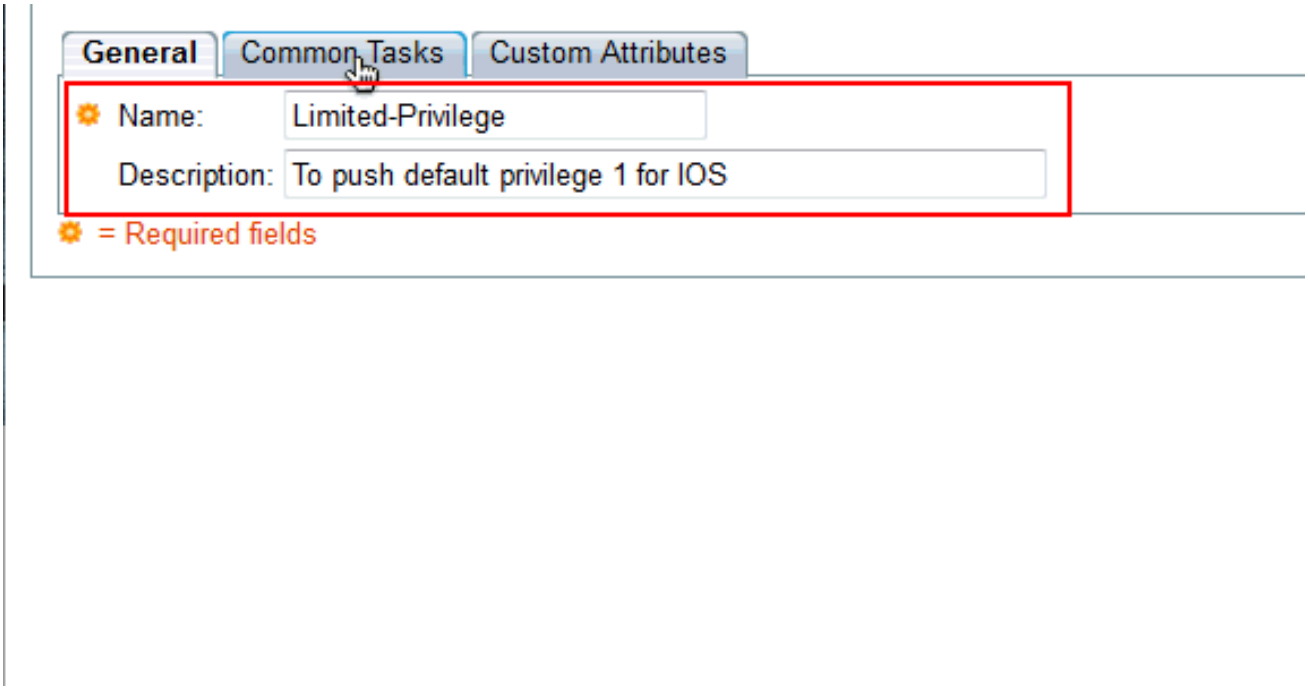
28. Нажмите **Select** в поле Shell Profile.



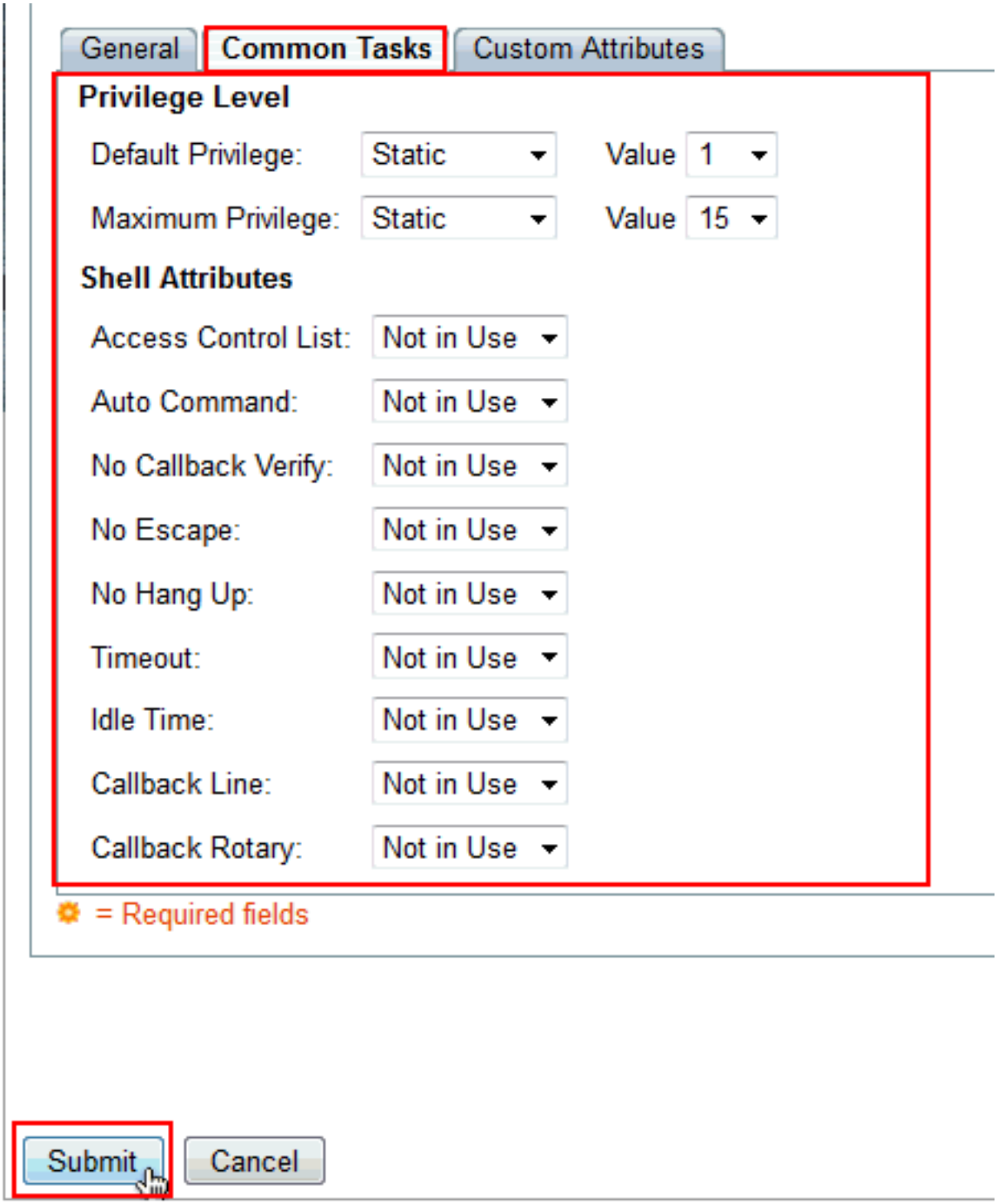
29. Нажмите **Create** для создания нового **Профиля Shell** для ограниченного доступа.



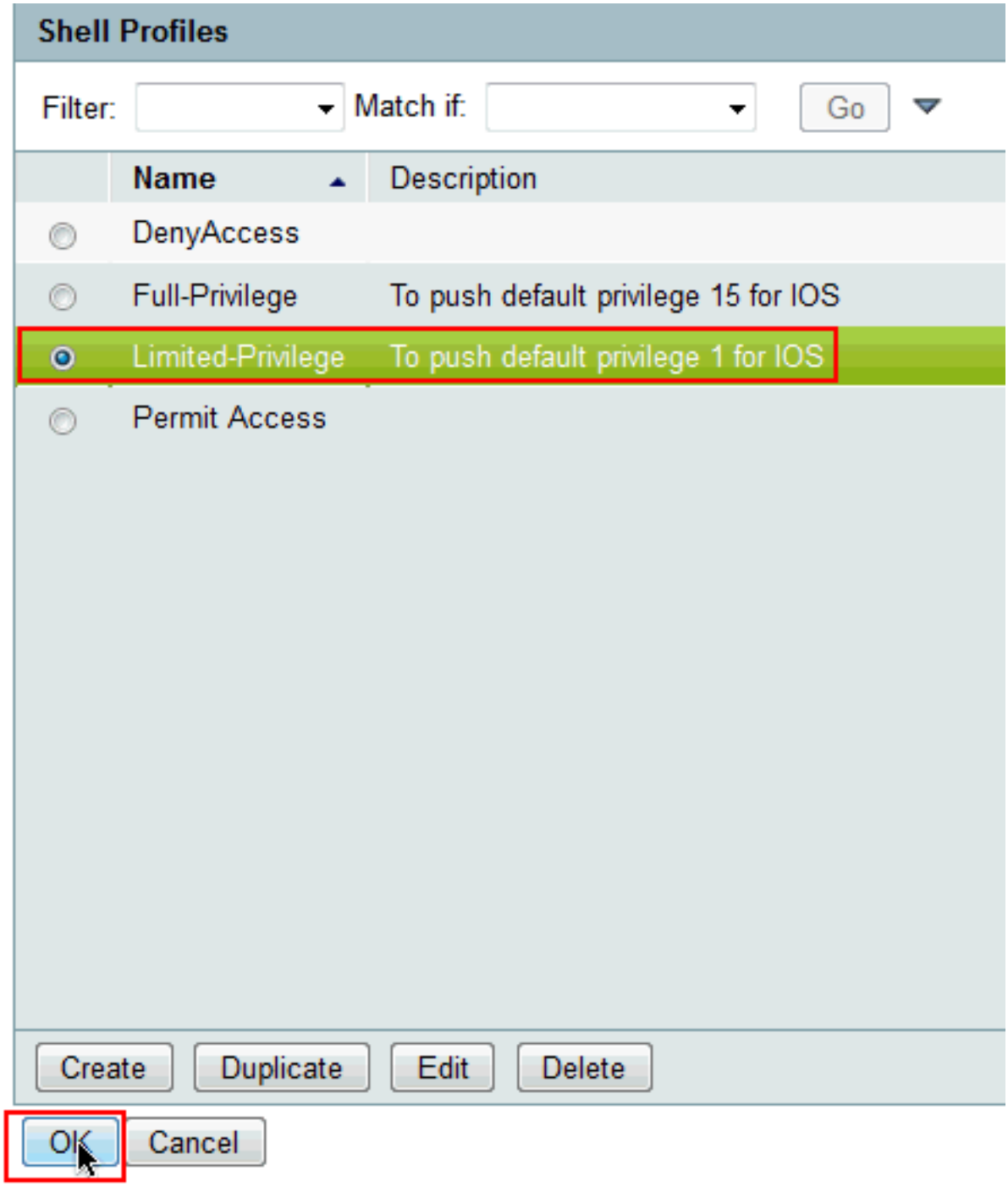
30. Предоставьте **Название** и **Описание** (дополнительное) во **Вкладке Общие**, и щелкните по вкладке **Common Tasks**.



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

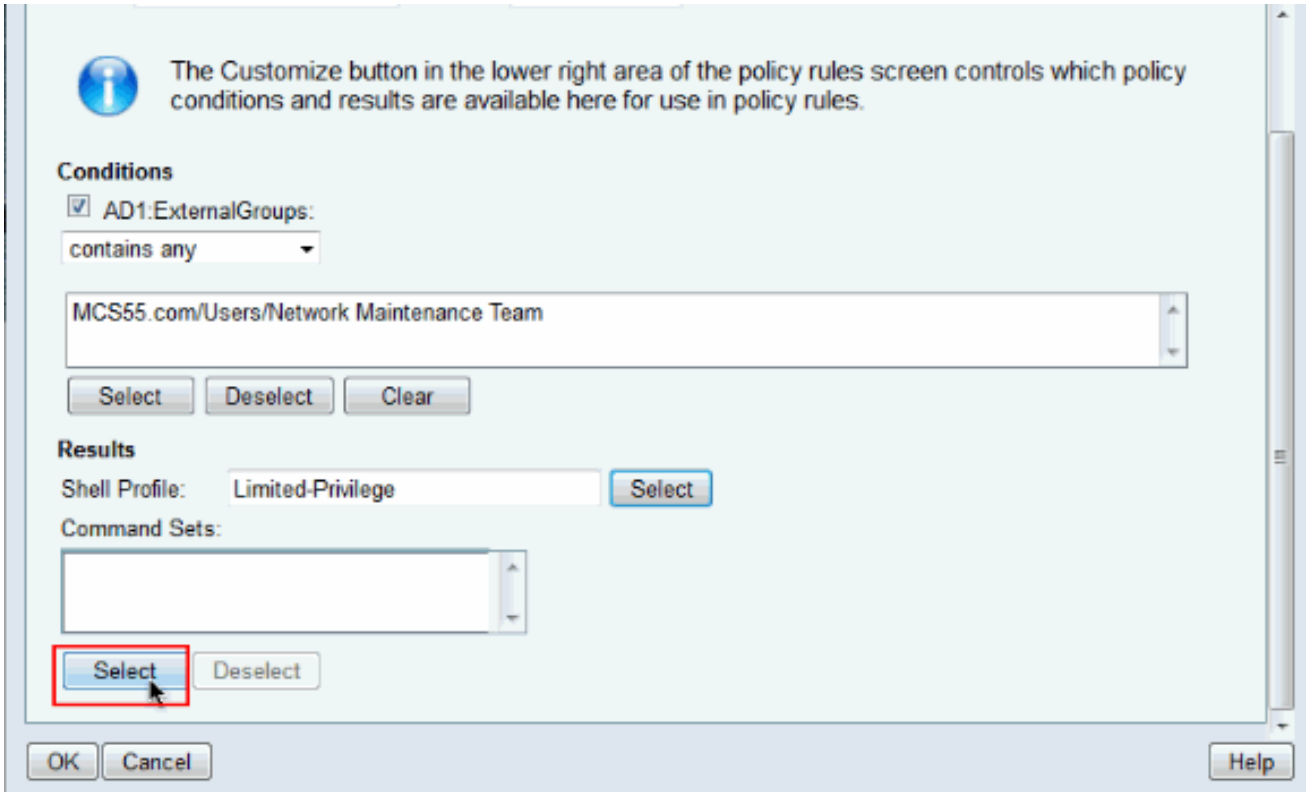


32. Нажмите кнопку

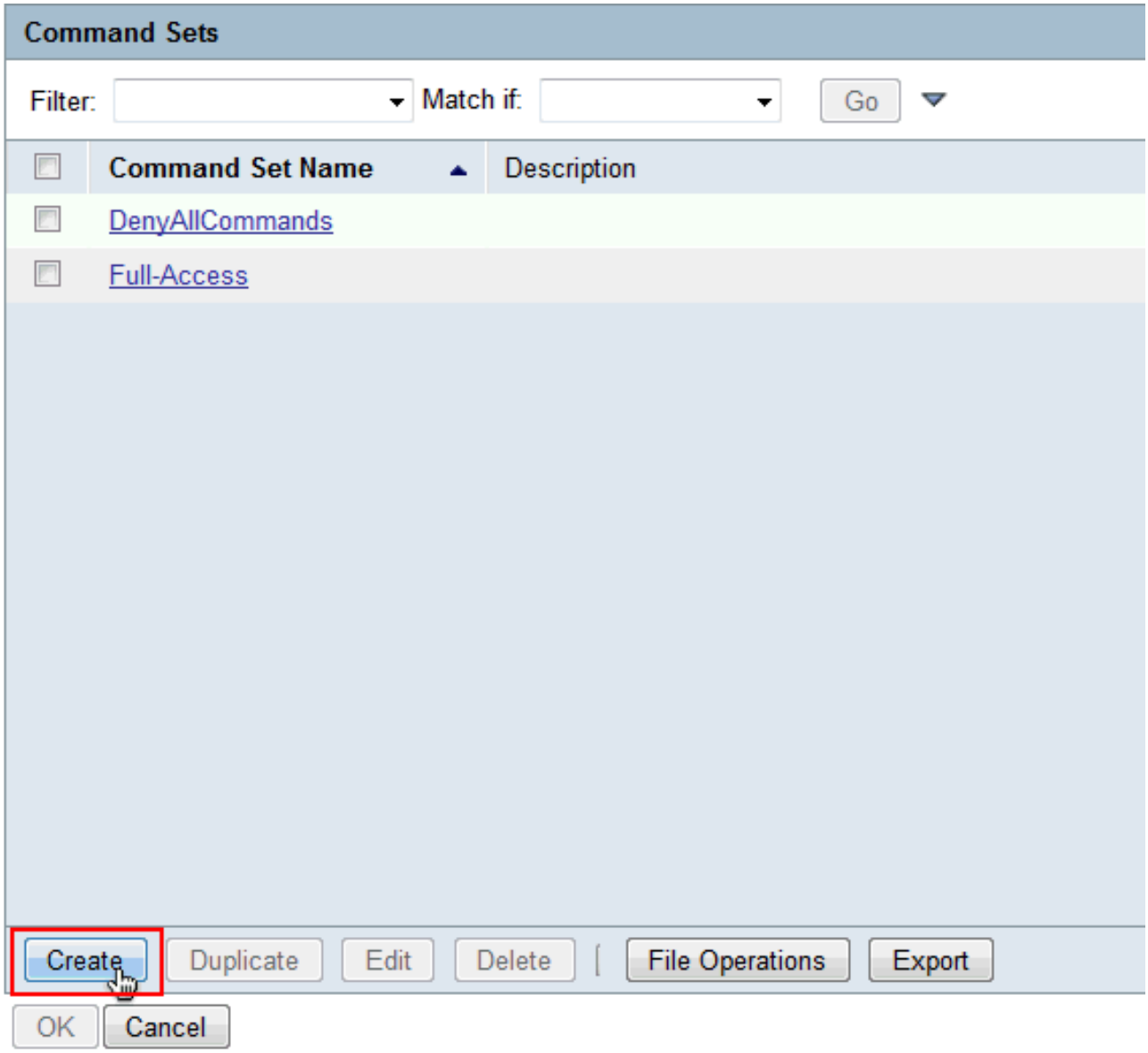


OK.

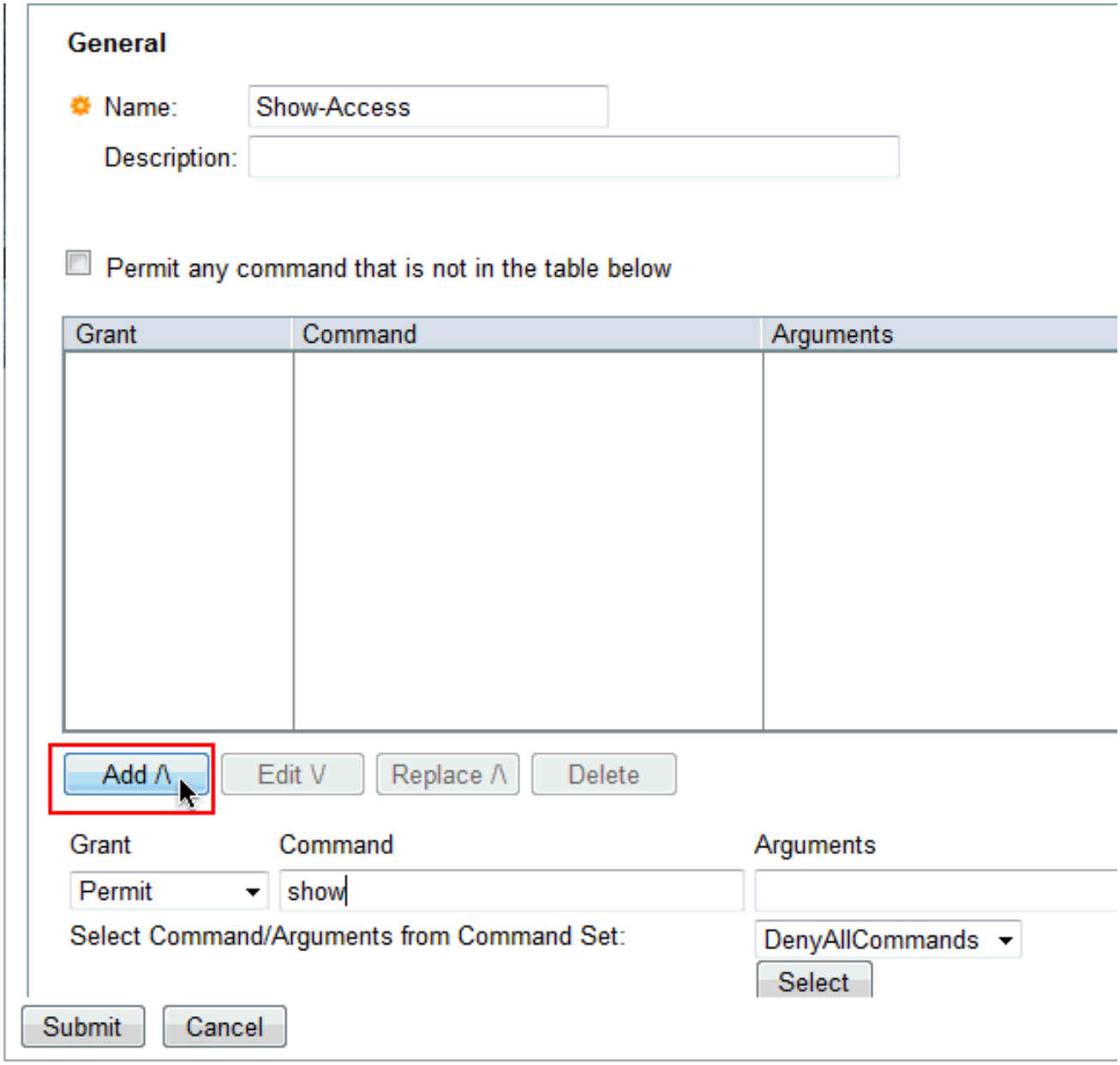
33. Нажмите **Select** в поле Command Sets.



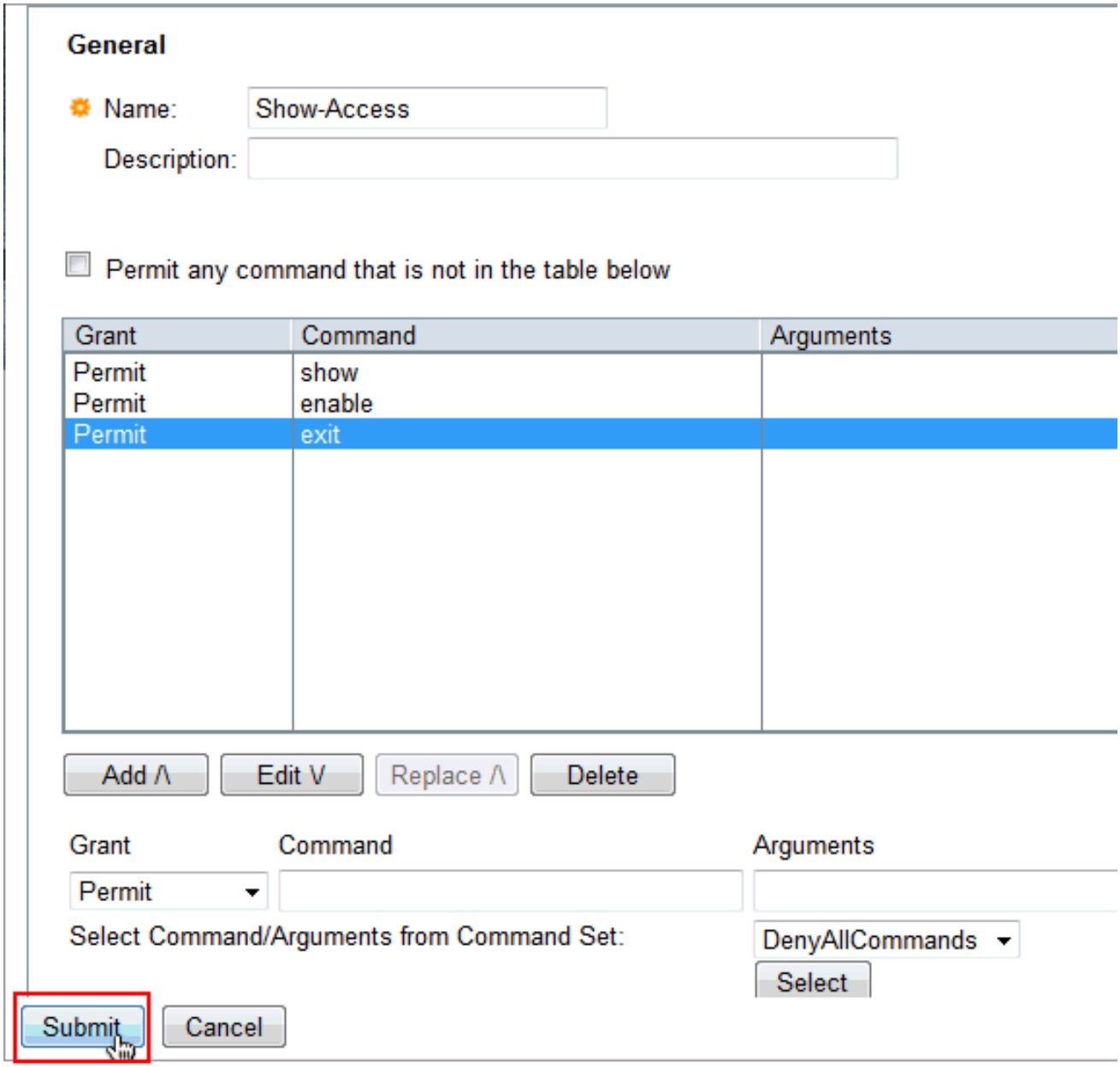
34. Нажмите **Create** для создания нового **Набора команд** для группы ограниченного доступа.



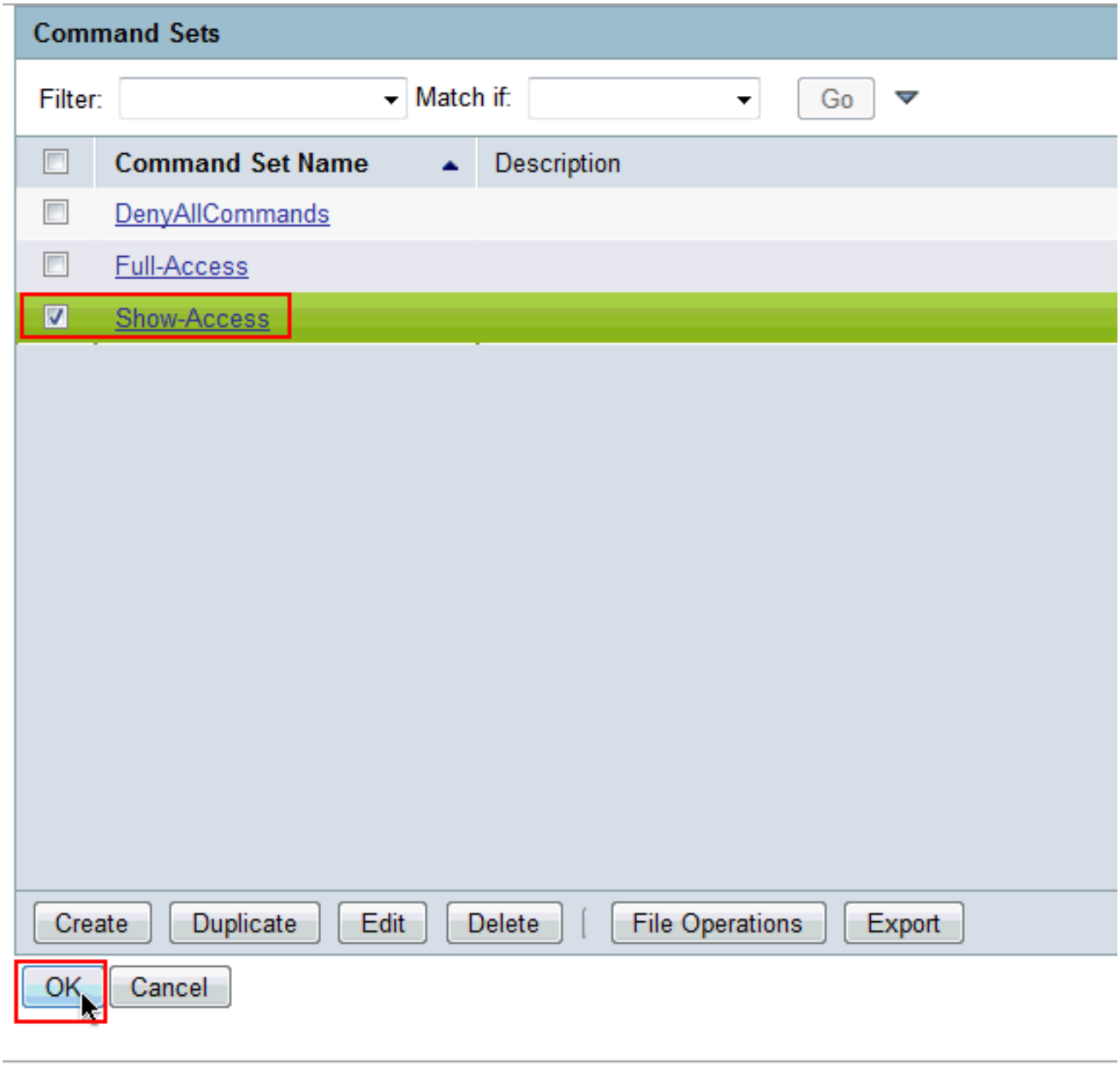
35. Предоставьте **Название** и гарантируйте, что **ниже**, не установлен флажок затем для **Разрешения любой команды, которая не находится в таблице**. **Нажмите Add** после ввода **показывают** в пространстве, предоставленном в **разделе команд**, и выбирают **Permit** в разделе **Предоставления**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



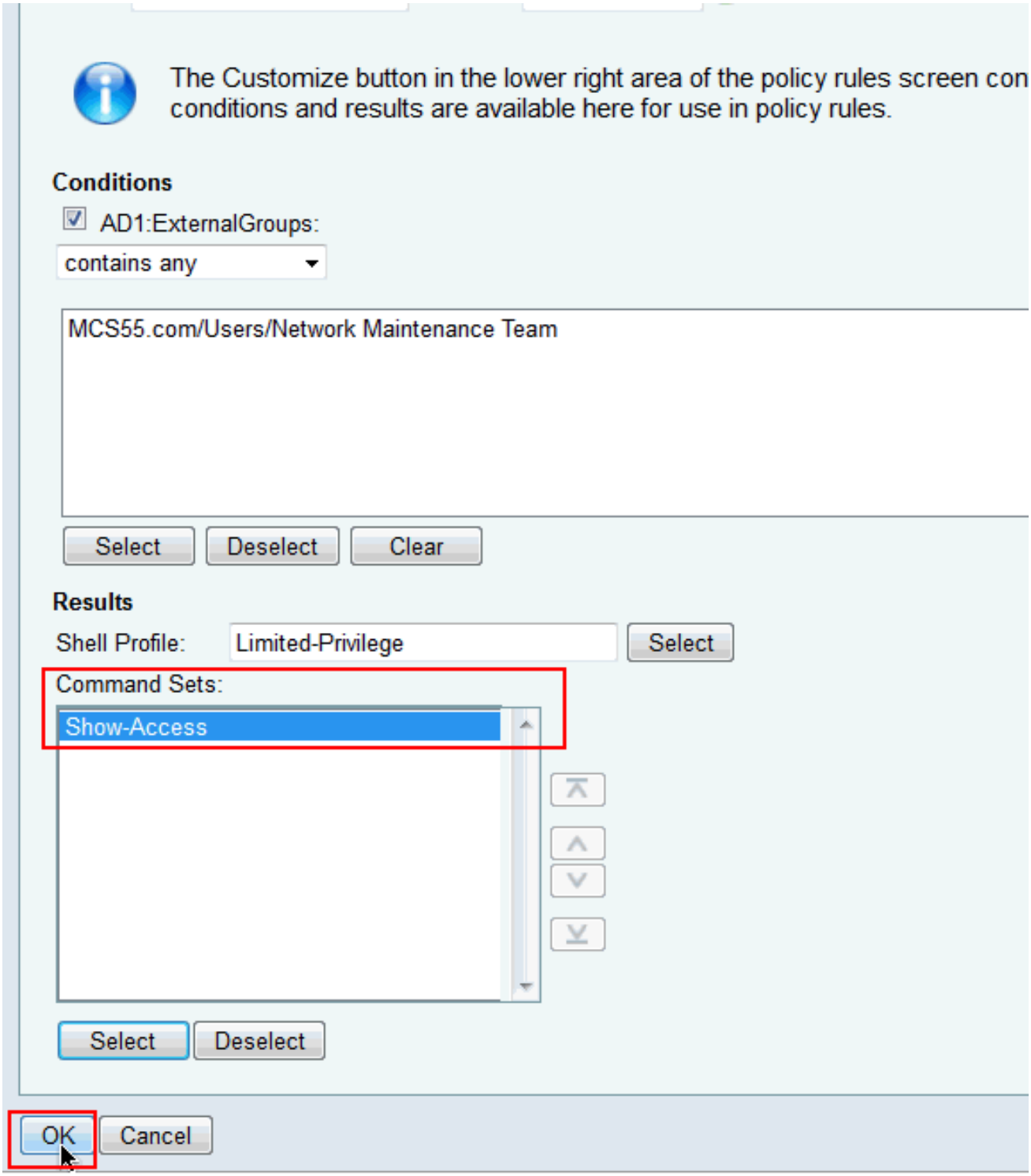
36. Так же добавьте**, что Добавляют** любые другие команды, которые будут разрешены для пользователей в группе ограниченного доступа с использованием. **Нажмите кнопку Submit (Отправить).Примечание:** См. Создание, Дублирование и Редактирование Наборов команд для Администрирования устройств для получения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



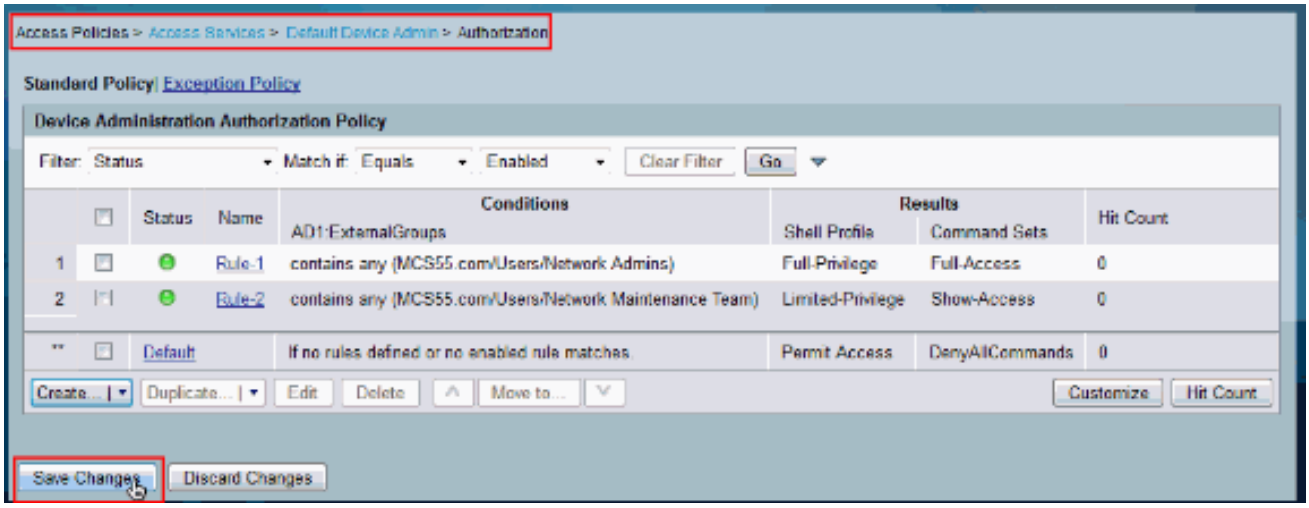
37. Нажмите кнопку **OK**.



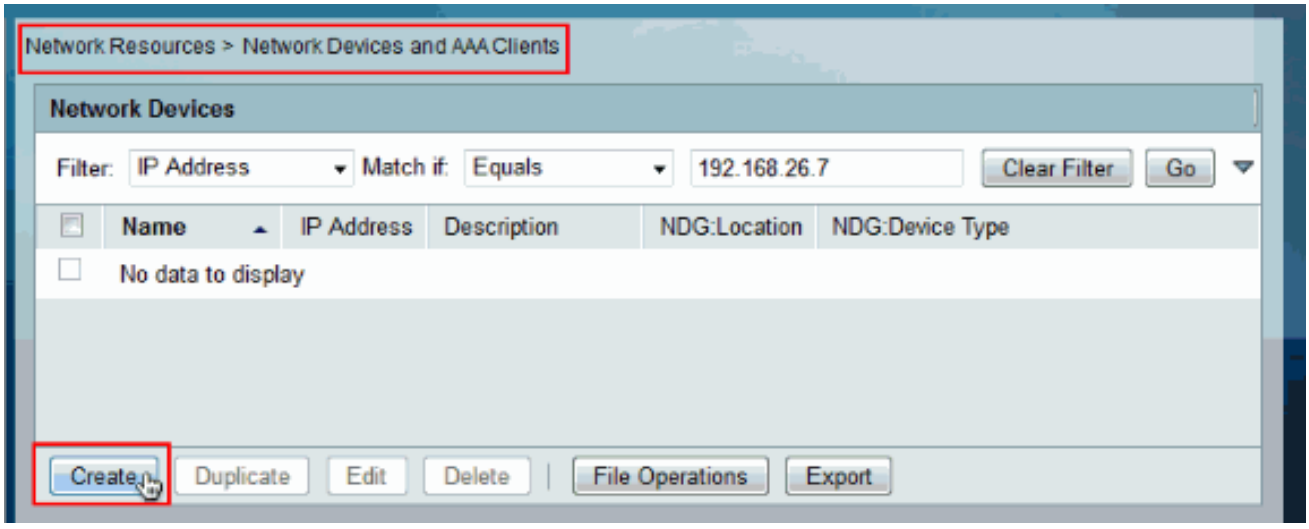
38. Нажмите кнопку **OK**.



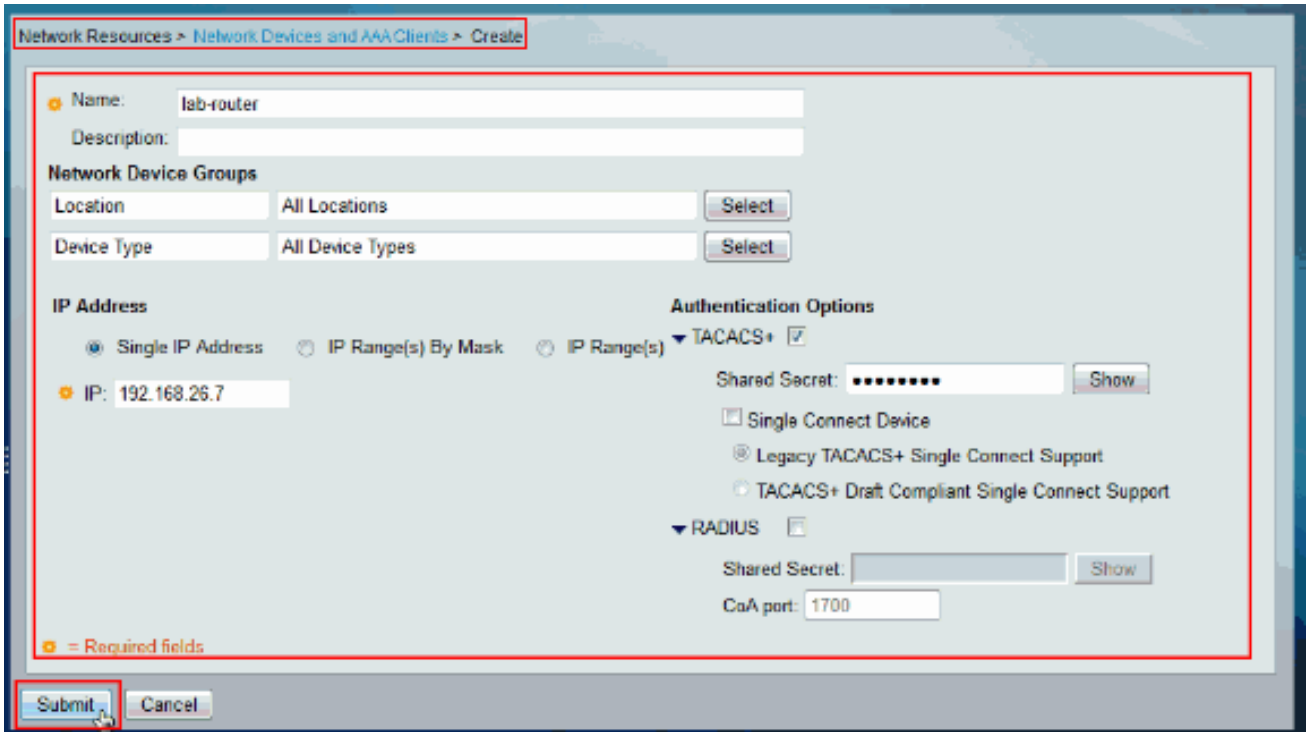
39. **Нажмите кнопку Save Changes (Сохранить изменения).**



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

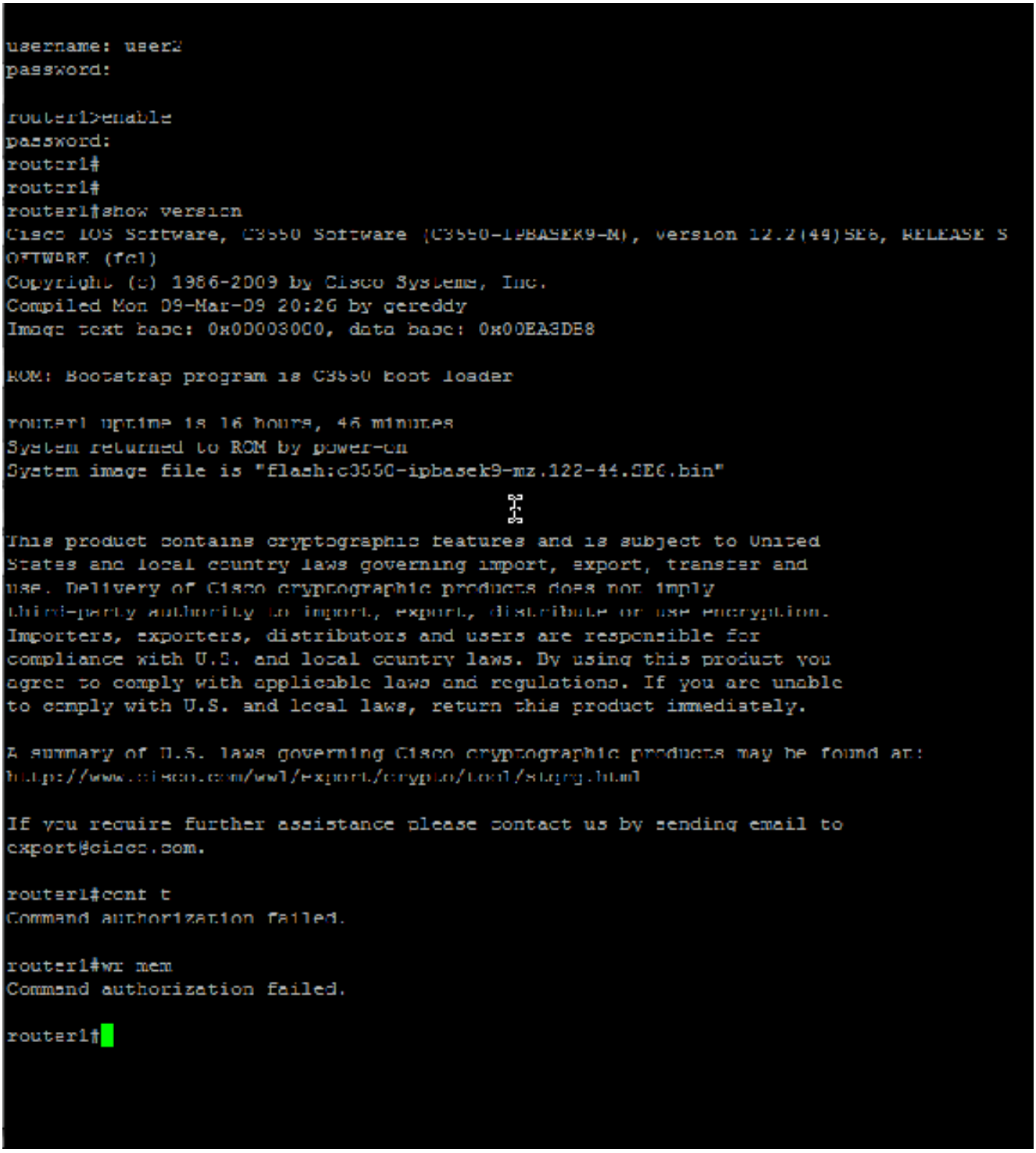
Чтобы проверить, что проверка подлинности и авторизация входит к устройству Cisco IOS через Telnet.

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. Попытайтесь выполнить любую команду, чтобы гарантировать, что у вас есть полный доступ.

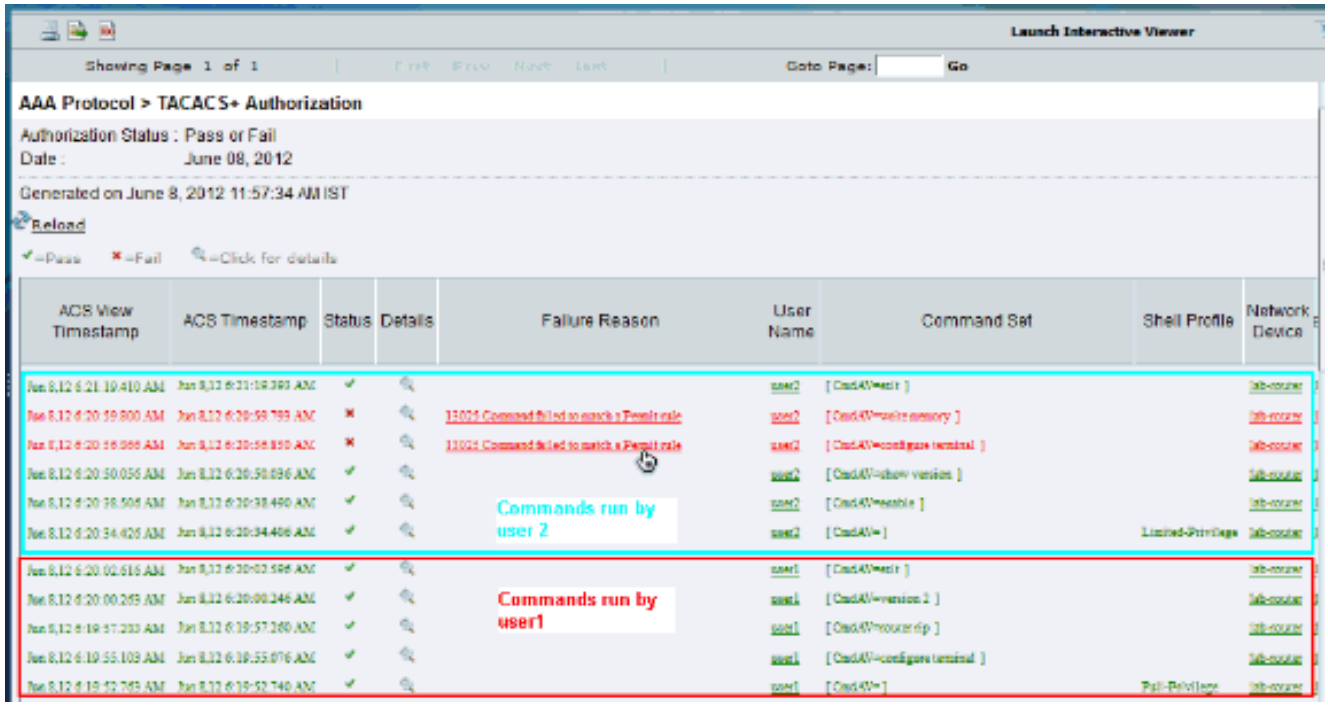
```
username: user1
password:

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.



3. Вход в систему к GUI ACS и **средству просмотра Отслеживающего и сообщающего** запуска. Выберите **AAA Protocol> TACACS+Authorization** для проверки действий, выполненных user1 и
user2.



Дополнительные сведения

- Система управления доступом Cisco Secure Access Control System
- Cisco Systems – техническая поддержка и документация