ACS 5.x: Autenticación de TACACS+ y comando authorization basados en el ejemplo de configuración de la membresía del grupo AD

Contenido

Introducción

Este documento proporciona un ejemplo de configurar autenticación de TACACS+ y del comando authorization basado en la membresía del grupo AD de un usuario con el Cisco Secure Access Control System (ACS) 5.x y posterior. ACS utiliza Microsoft Active Directory (AD) como almacén de identidades externo para guardar recursos como usuarios, equipos, grupos y atributos.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El ACS 5.x se integra completamente al dominio deseado AD. Si el ACS no se integra con el dominio deseado AD, refiera a ACS 5.x y posterior: Integración con el ejemplo de configuración del Microsoft Active Directory para más información para realizar la tarea de la integración.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure ACS 5.3

- Versión 12.2(44)SE6 del Cisco IOS ® Software.**Nota:** Esta configuración se puede hacer en todos los dispositivos Cisco IOS.
- Dominio 2003 del Microsoft Windows server

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

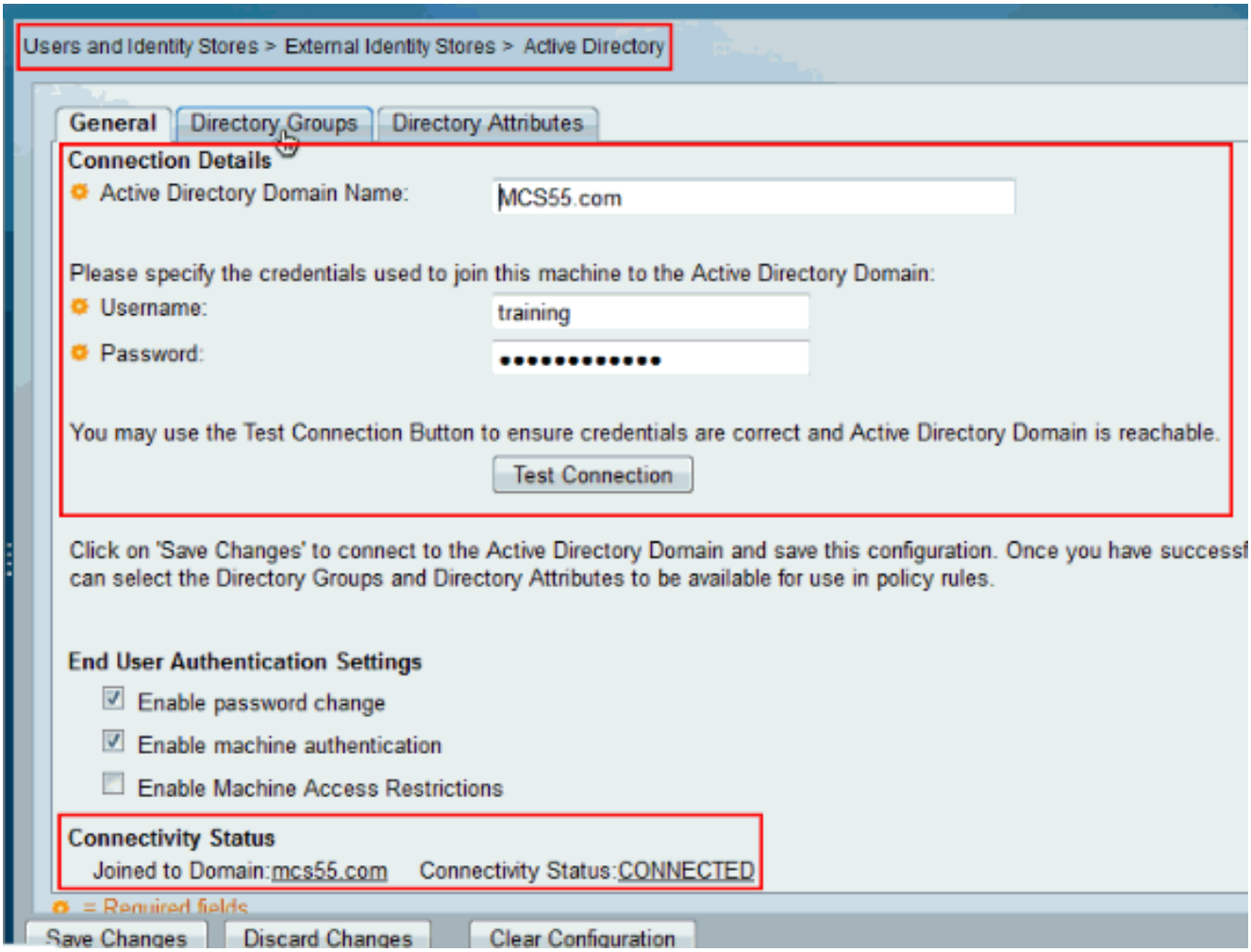
Configuración

Configuración ACS 5.x para la autenticación y autorización

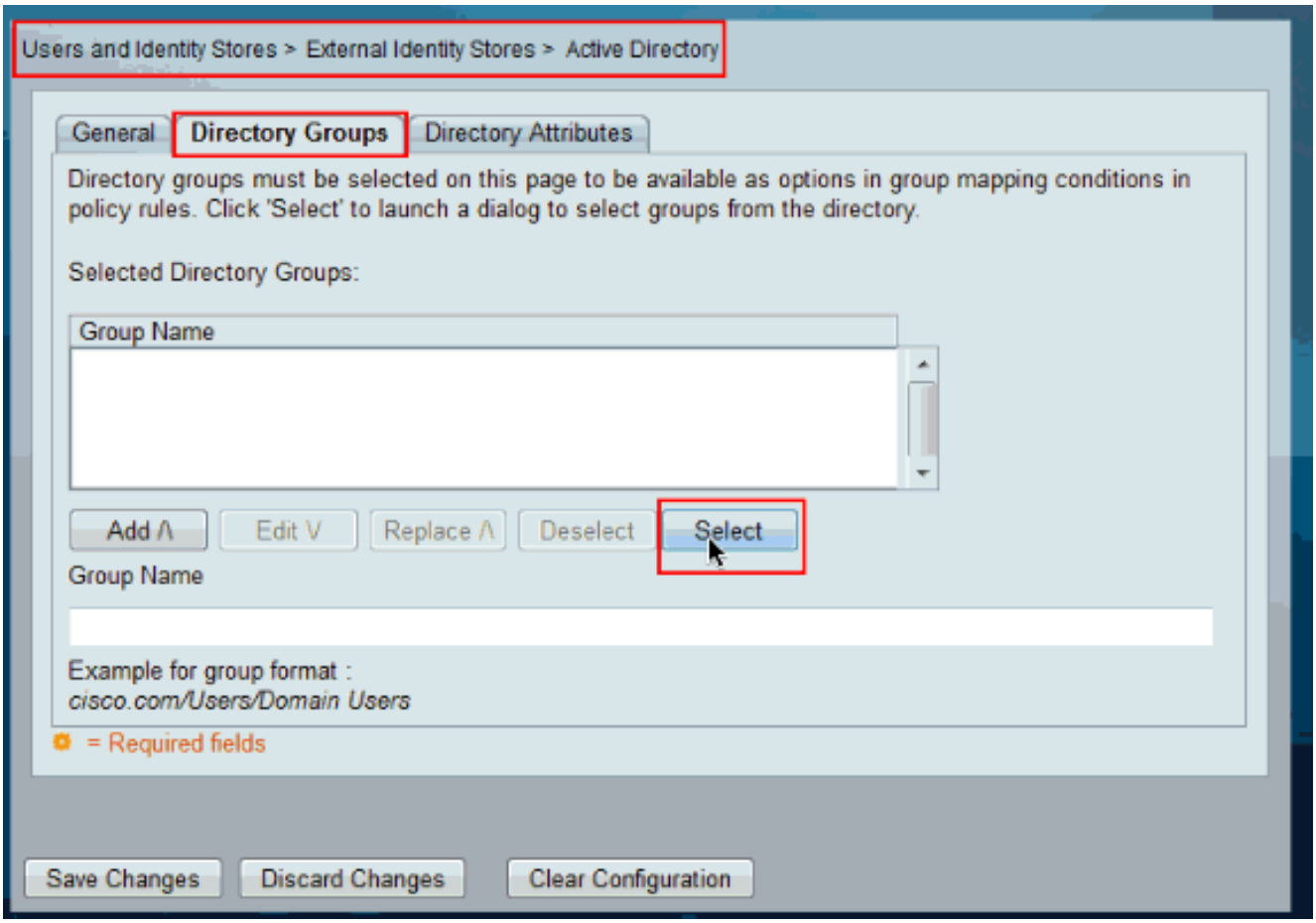
Antes de que usted comience la configuración del ACS 5.x para la autenticación y autorización, el ACS se debe haber integrado con éxito con Microsoft AD. Si el ACS no se integra con el dominio deseado AD, refiera a ACS 5.x y posterior: Integración con el ejemplo de configuración del Microsoft Active Directory para más información para realizar la tarea de la integración.

En esta sección, usted asocia dos grupos AD a dos diversos comandos estableces y dos perfiles del shell, uno con de total acceso y el otro con el limitado-acceso en los dispositivos Cisco IOS.

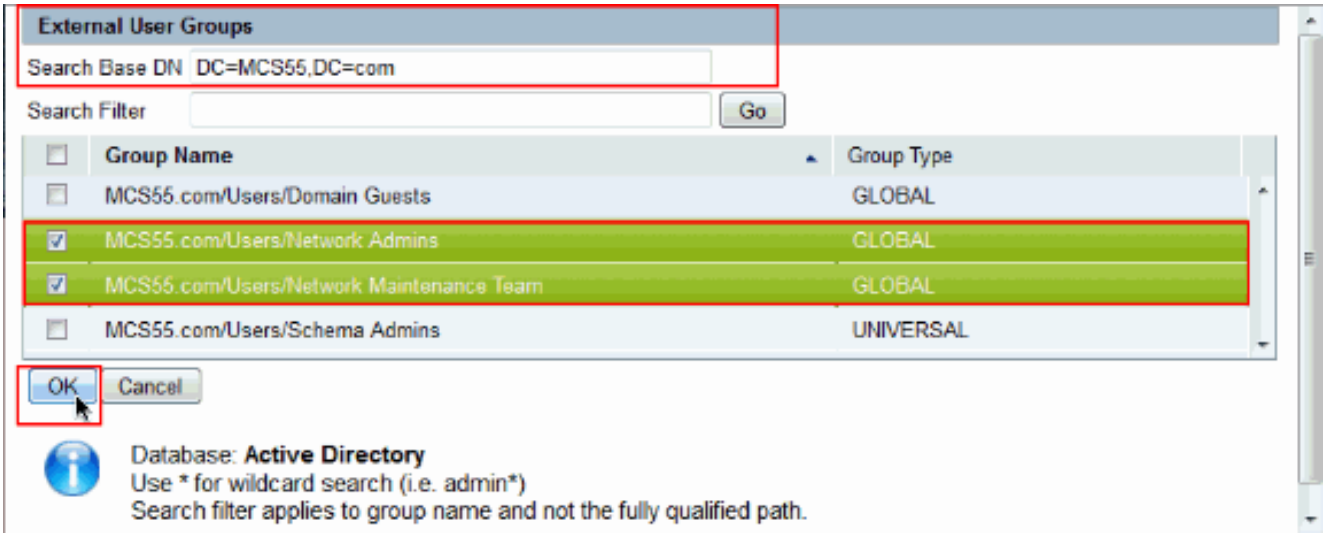
1. Registro en el ACS GUI usando las credenciales Admin.
2. Elija a los **usuarios y la identidad salva > identidad externa salva > Active Directory** y verifica que el ACS se ha unido al dominio deseado y también que el **estatus de la Conectividad** está mostrado según lo **conectado**.Haga clic en la lengueta de los **grupos del directorio**.



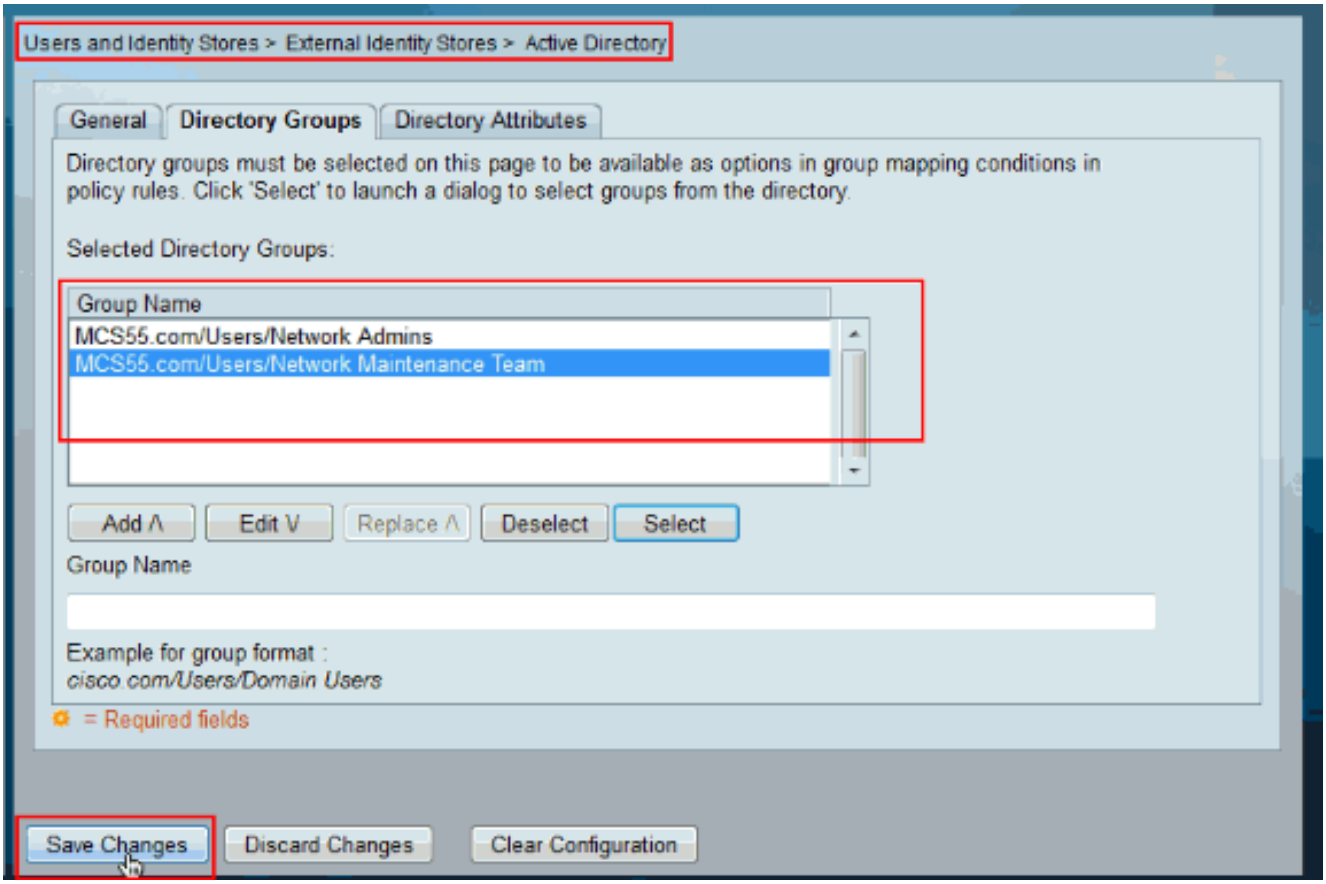
3. Haga clic
selecto.



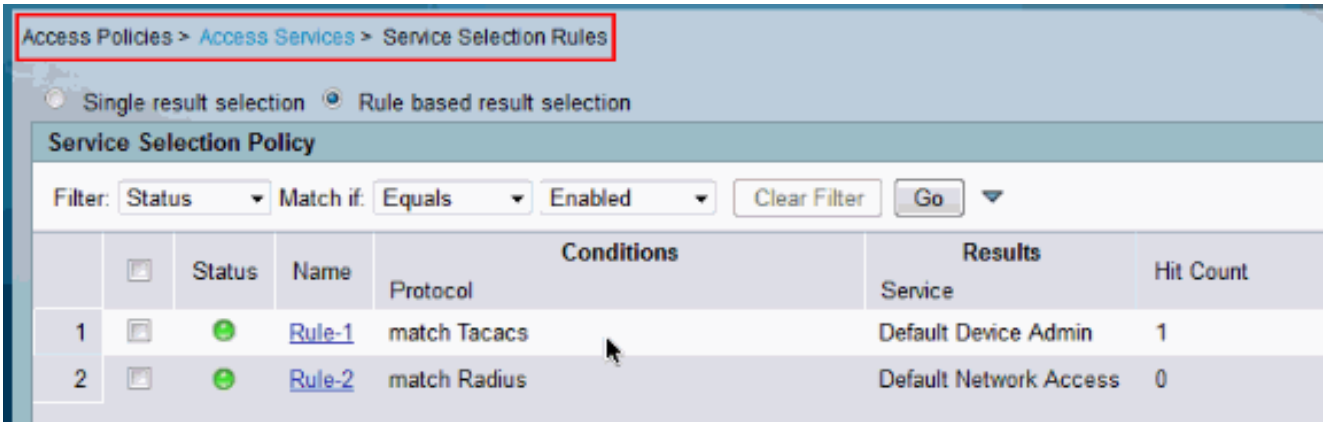
4. Elija a los grupos que necesitan ser asociados a los perfiles y a los comandos estableces del shell en la parte de posterior la configuración. Haga clic en OK.



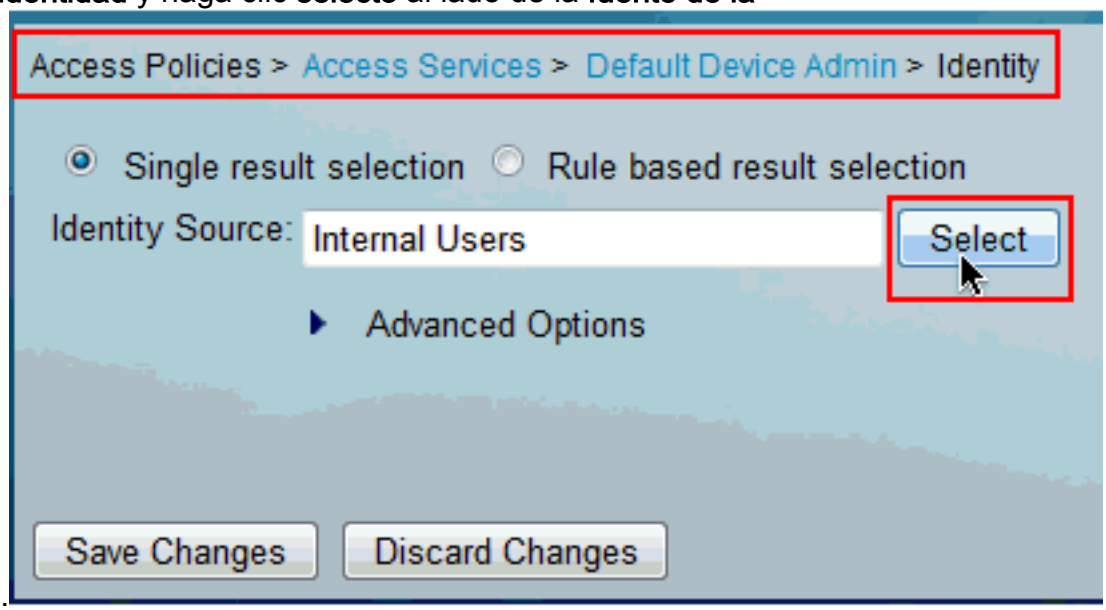
5. **Cambios de la salvaguardia del** tecleo.



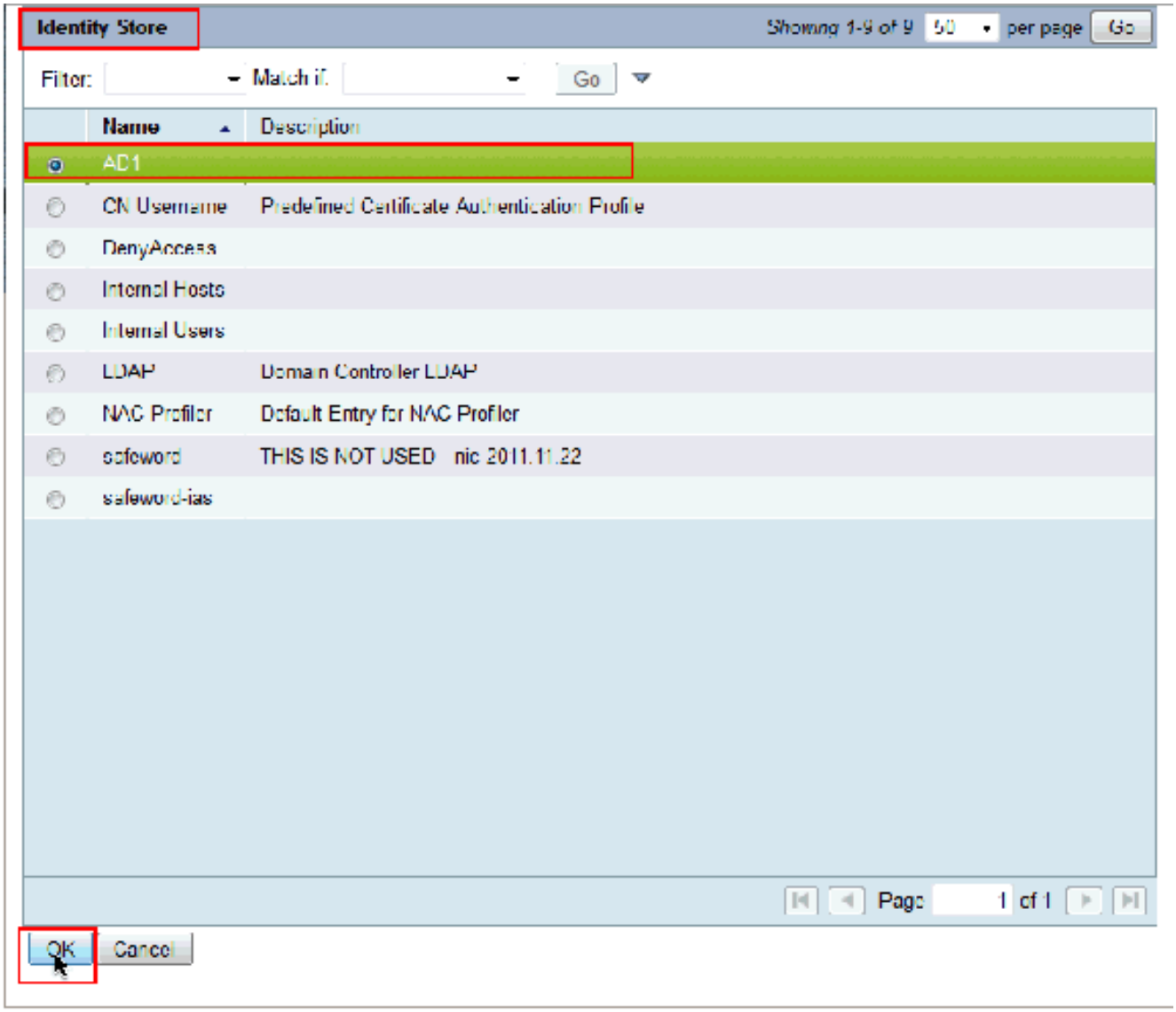
6. Elija las **políticas de acceso > el acceso mantiene > las reglas de selección del servicio** e identifica el servicio del acceso, que procesa autenticación de TACACS+. En este ejemplo, es el **dispositivo predeterminado Admin**.



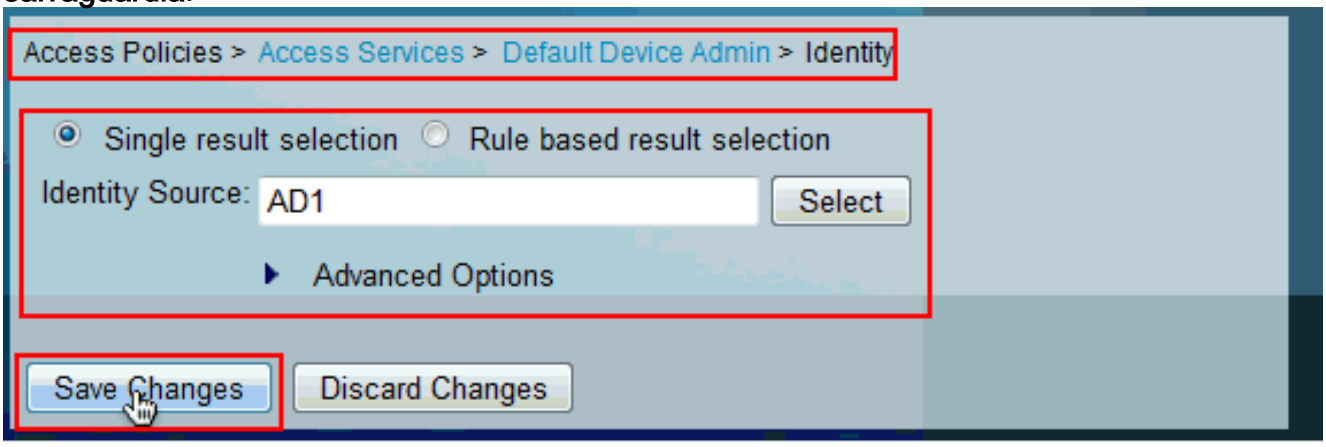
7. Elija las **políticas de acceso > los servicios del acceso > el dispositivo del valor por defecto Admin > identidad** y haga clic **selecto** al lado de la **fuente de la identidad**.



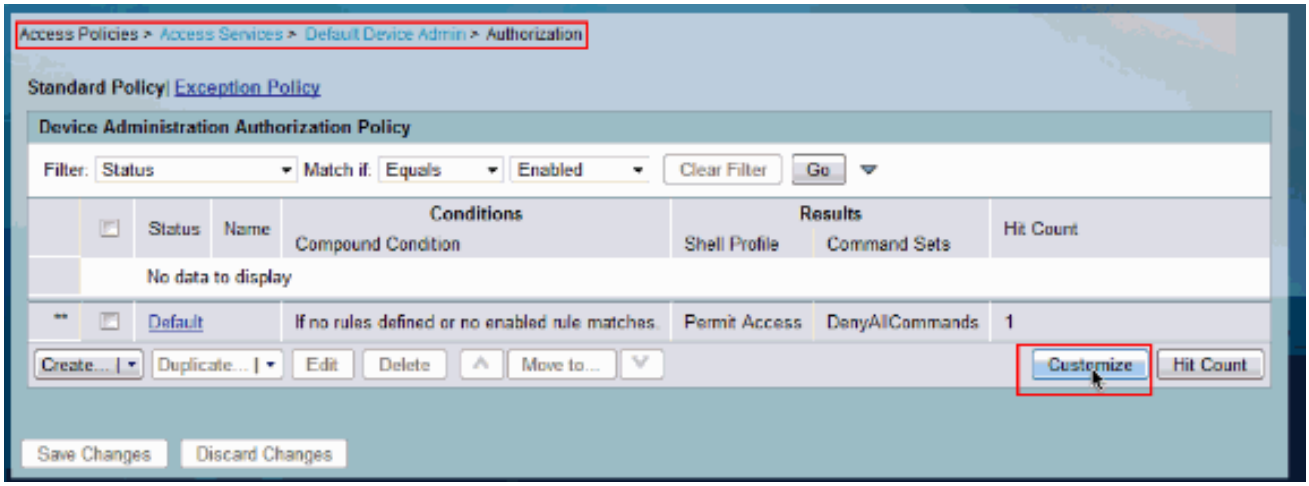
8. Elija **AD1** y haga clic la **AUTORIZACIÓN**.



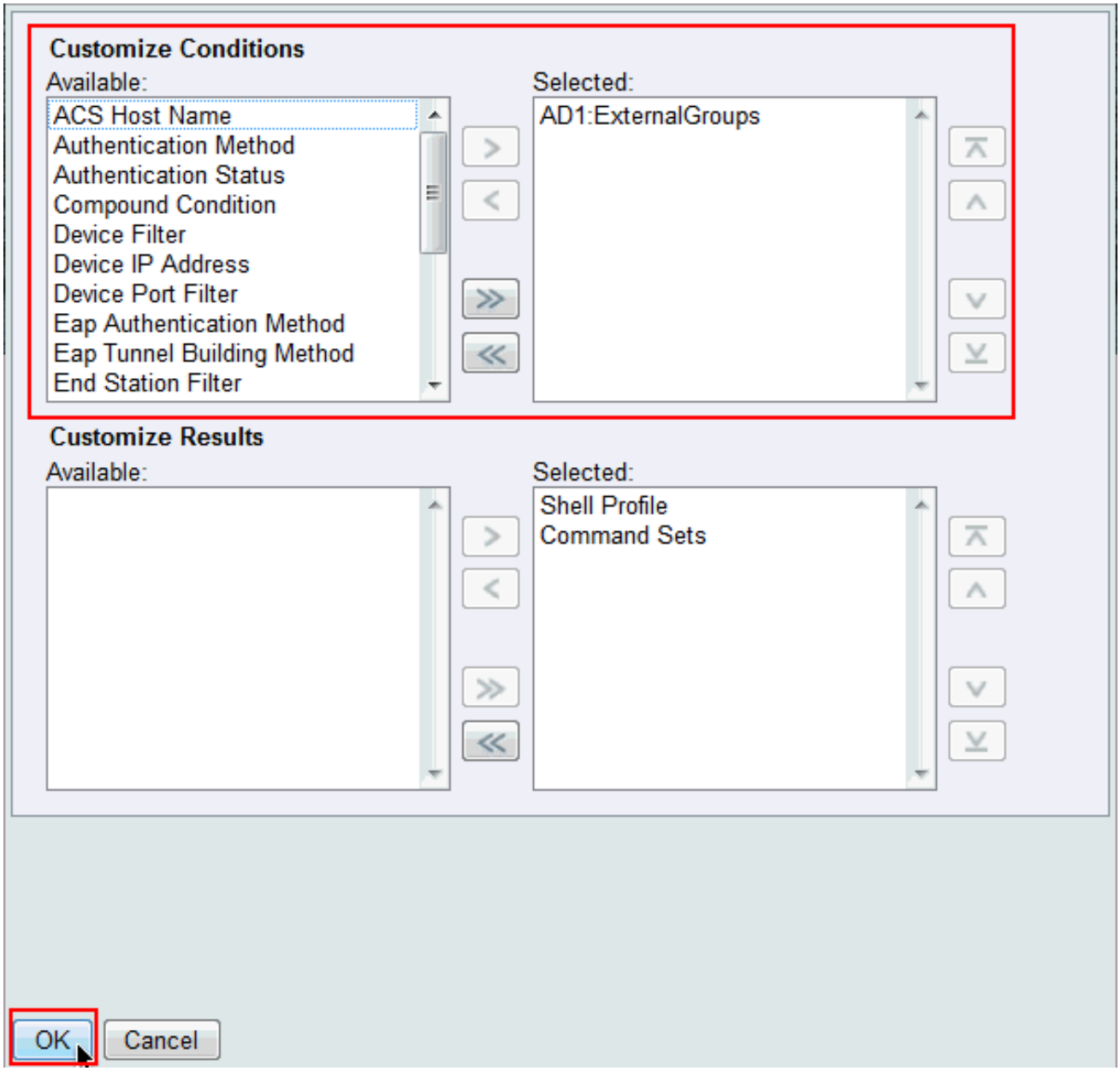
9. Haga clic los **cambios de la salvaguardia**.



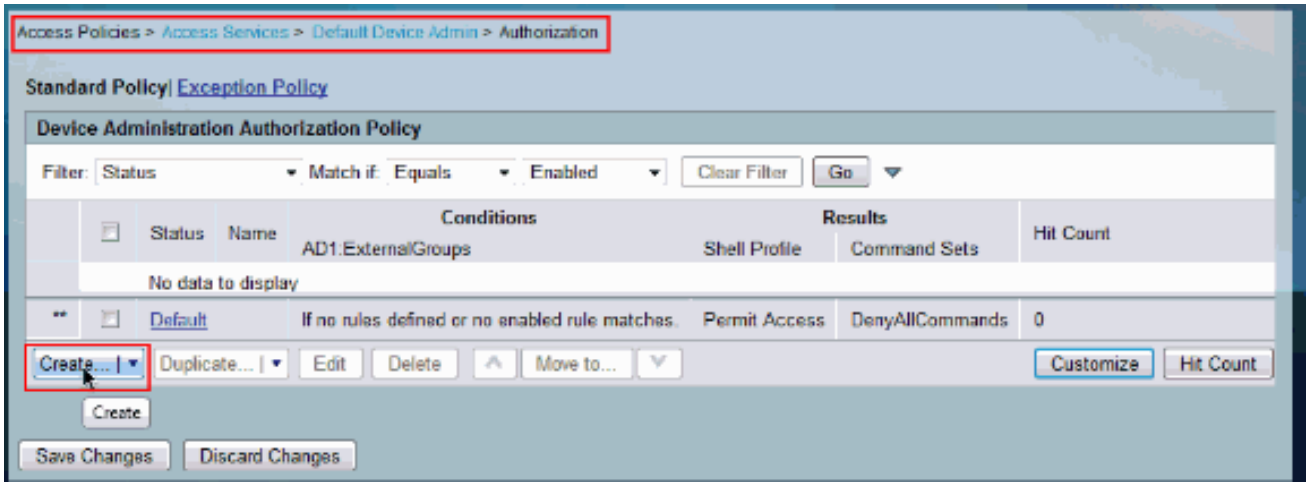
10. Elija las **políticas de acceso > los servicios del acceso > el dispositivo del valor por defecto Admin > autorización** y haga clic en **personalizan**.



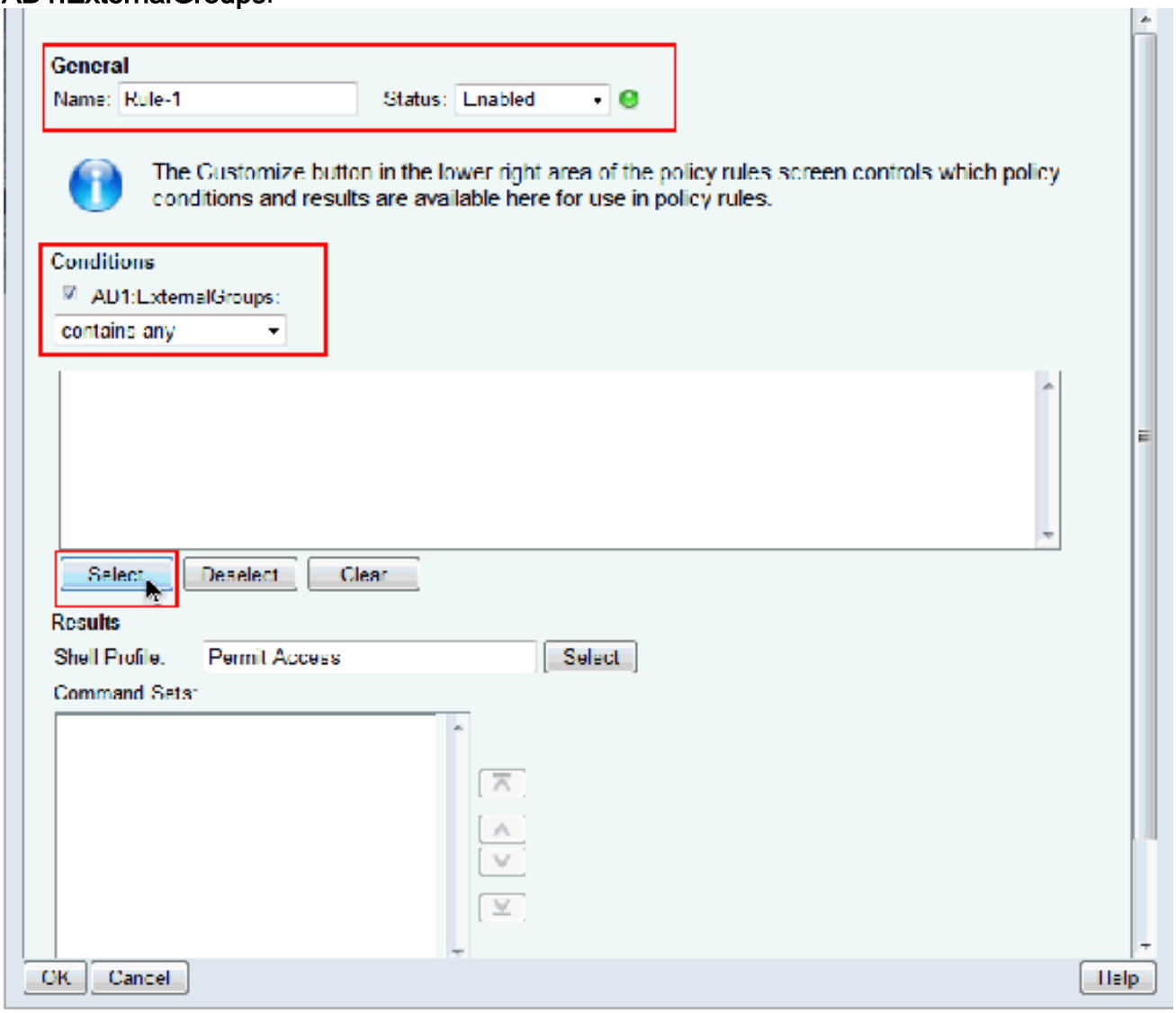
11. Copie **AD1:ExternalGroups de disponible a la sección seleccionada de las condiciones Customize** y después mueva el **perfil** y a los **comandos estableces del shell** desde **disponible a la sección seleccionada de los resultados Customize**. Ahora haga clic la **AUTORIZACIÓN**.



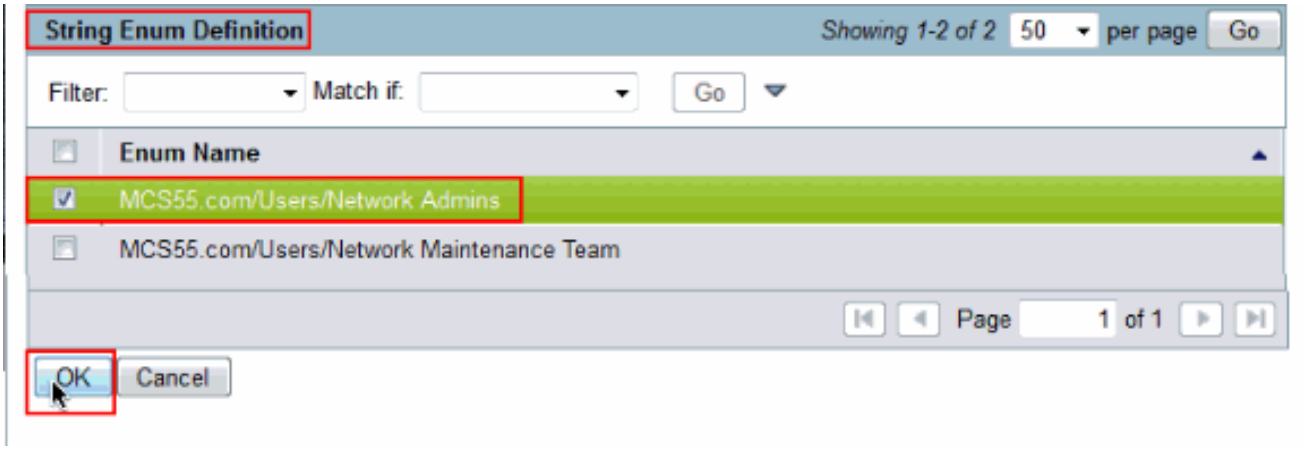
12. El tecleo **crea** para crear una nueva regla.



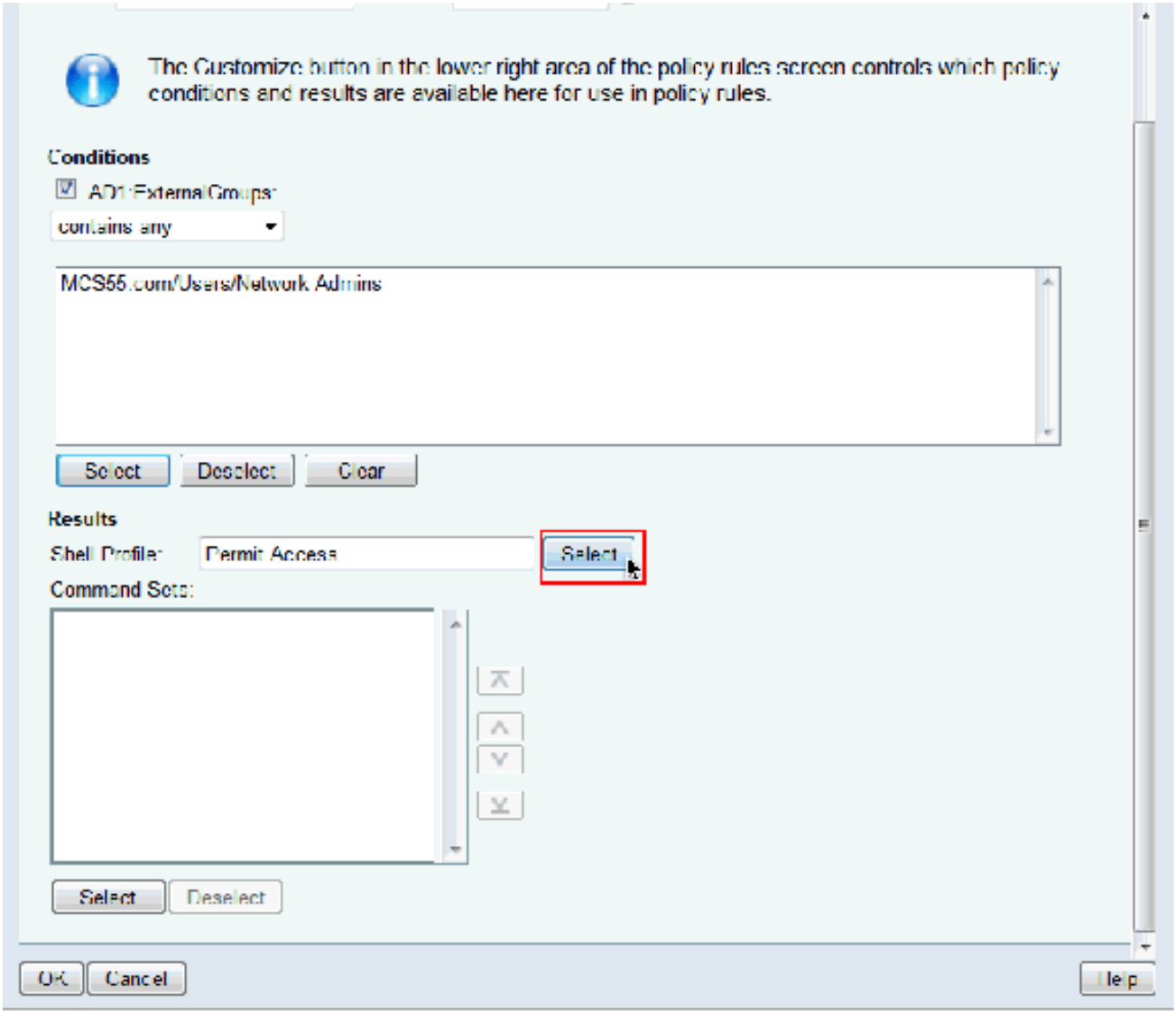
13. Tecleo **selecto** en la condición **AD1:ExternalGroups**.



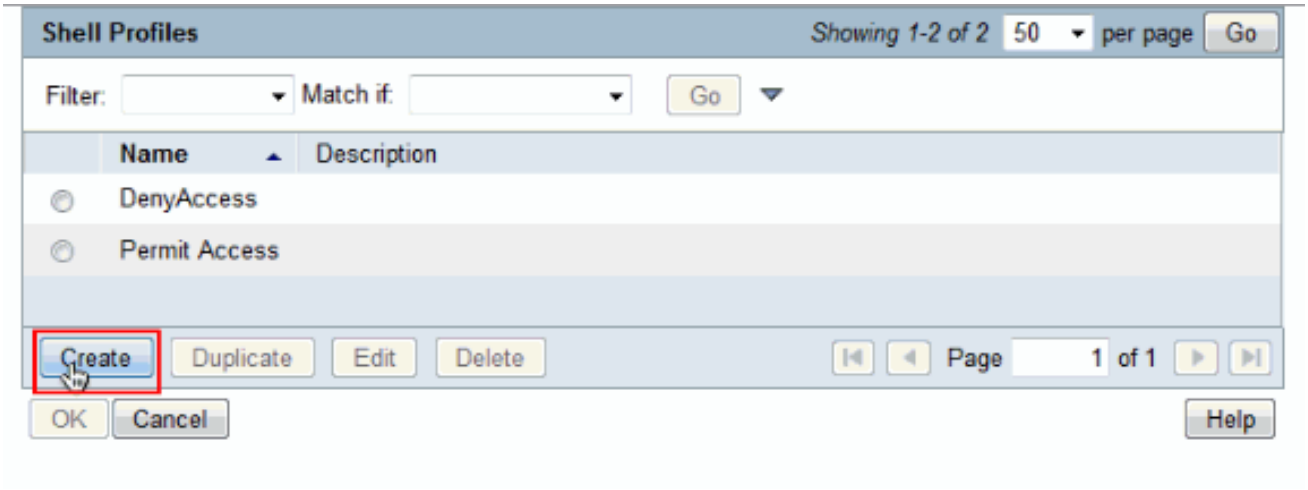
14. Elija al grupo que usted quiere para proporcionar el acceso total en el dispositivo Cisco IOS. Haga clic en **OK**.



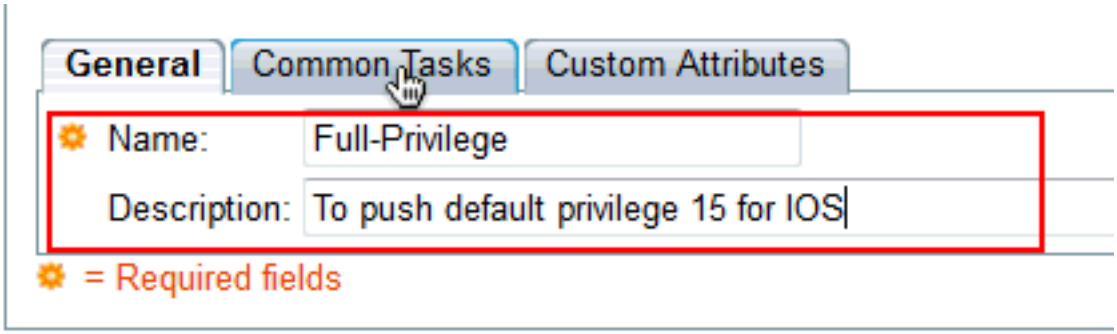
15. Tecleo **selecto** en el campo del perfil del shell.



16. El tecleo **crea** para crear un nuevo **perfil del shell** para los usuarios de total acceso.

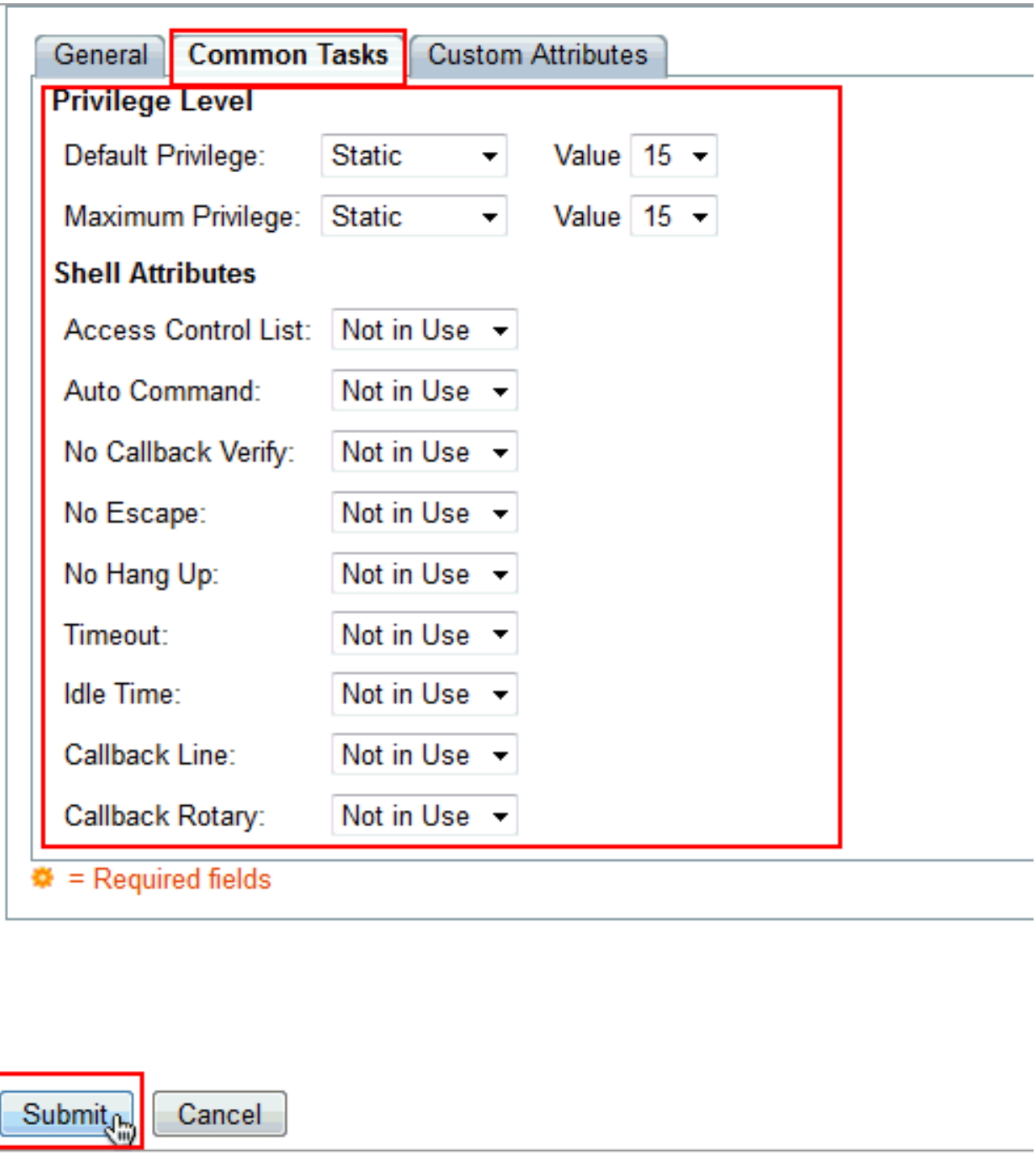


17. Proporcione un **nombre** y un **Description(optional)** en la **ficha general** y haga clic en la lengueta **común de las**

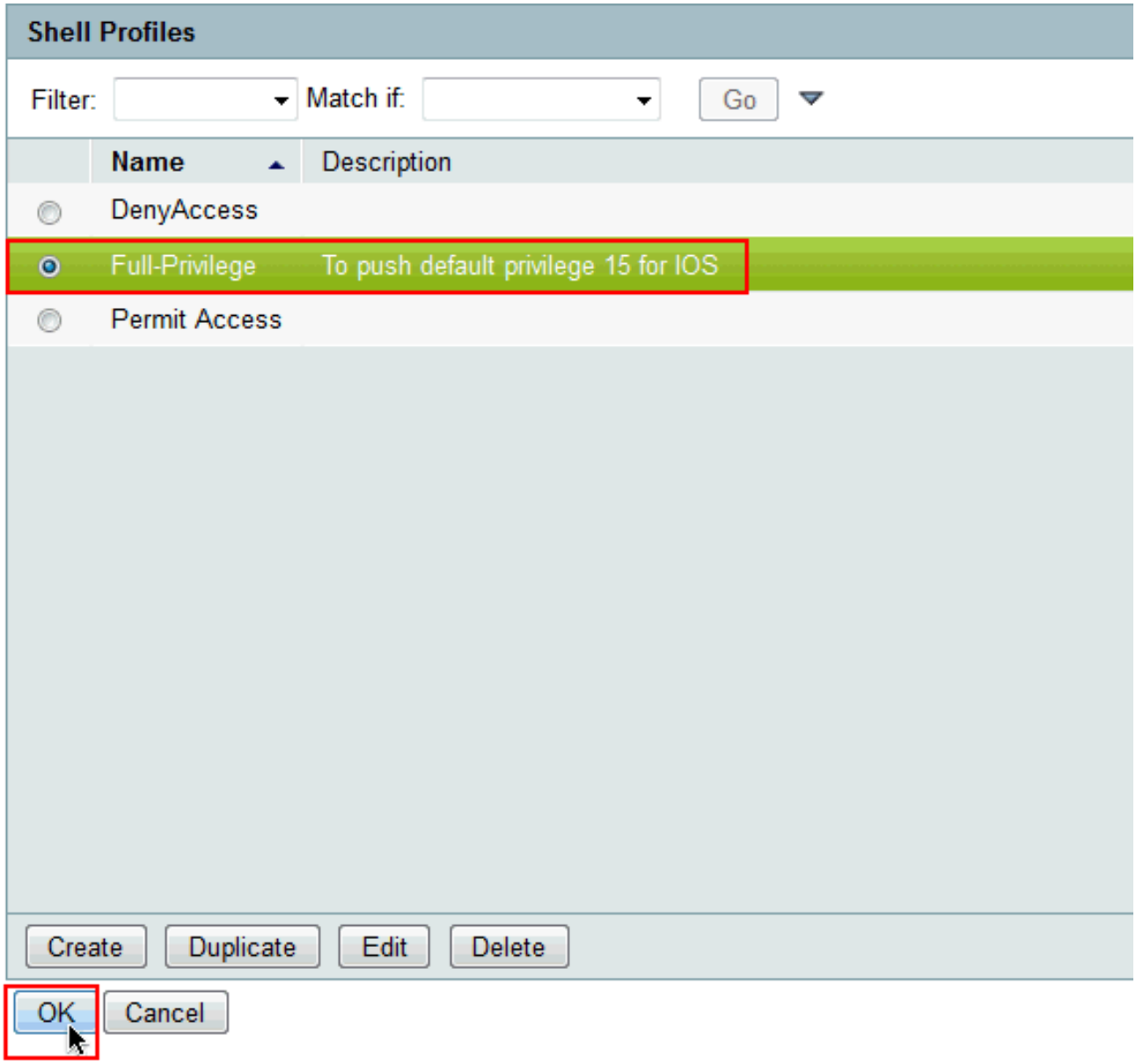


tareas.

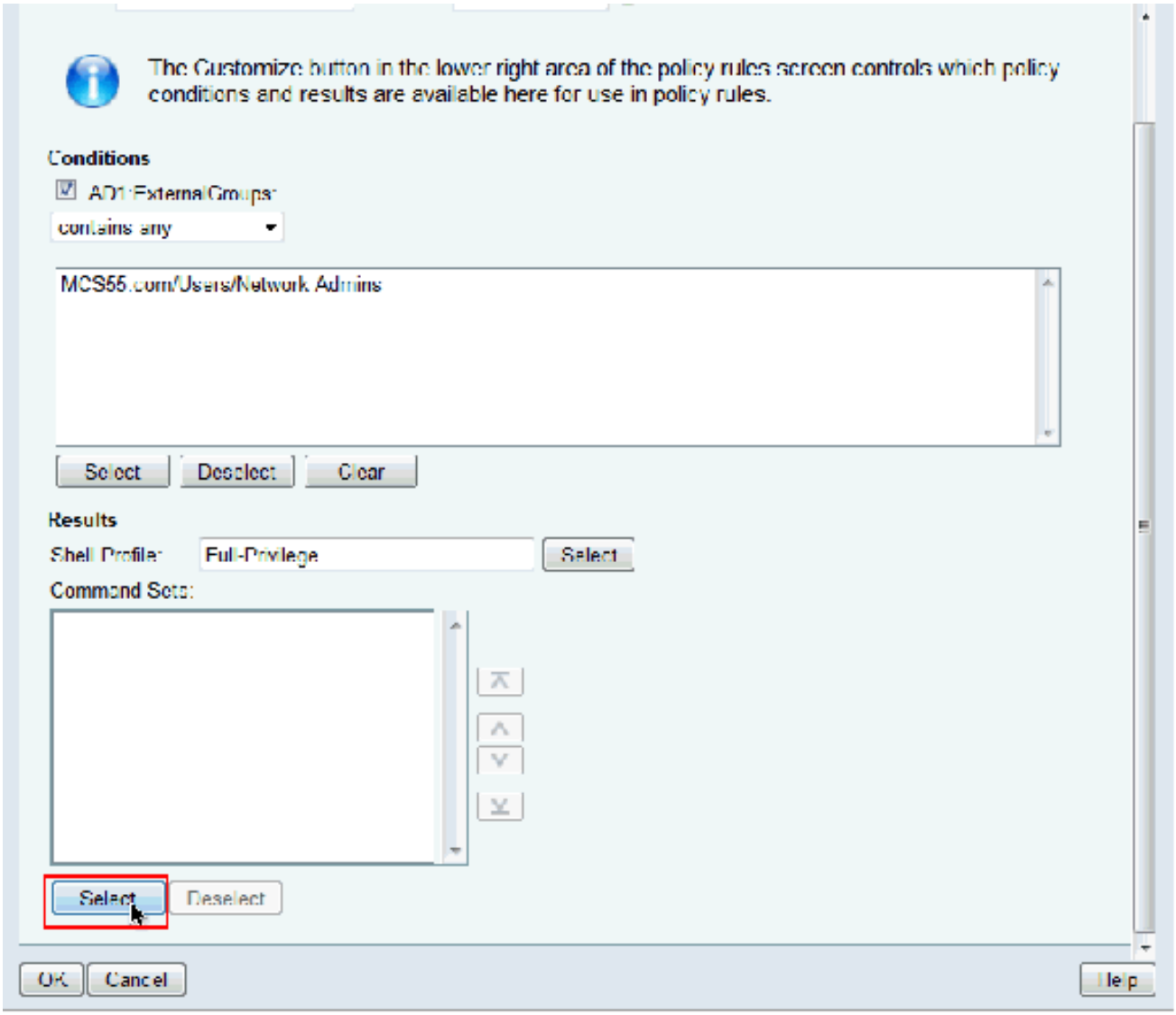
18. Cambie el **privilegio predeterminado** y el **privilegio del máximo a los parásitos atmosféricos** con el **valor 15**. Haga clic en Submit (Enviar).



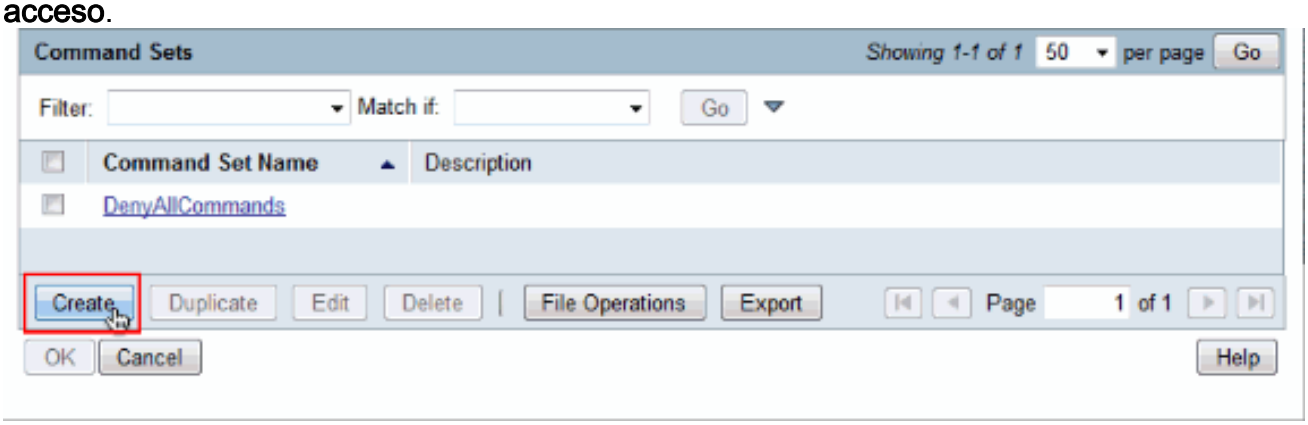
19. Ahora elija el **perfil** de total acceso creado recientemente del **shell** (FULL-privilegio en este ejemplo) y haga clic la **AUTORIZACIÓN**.



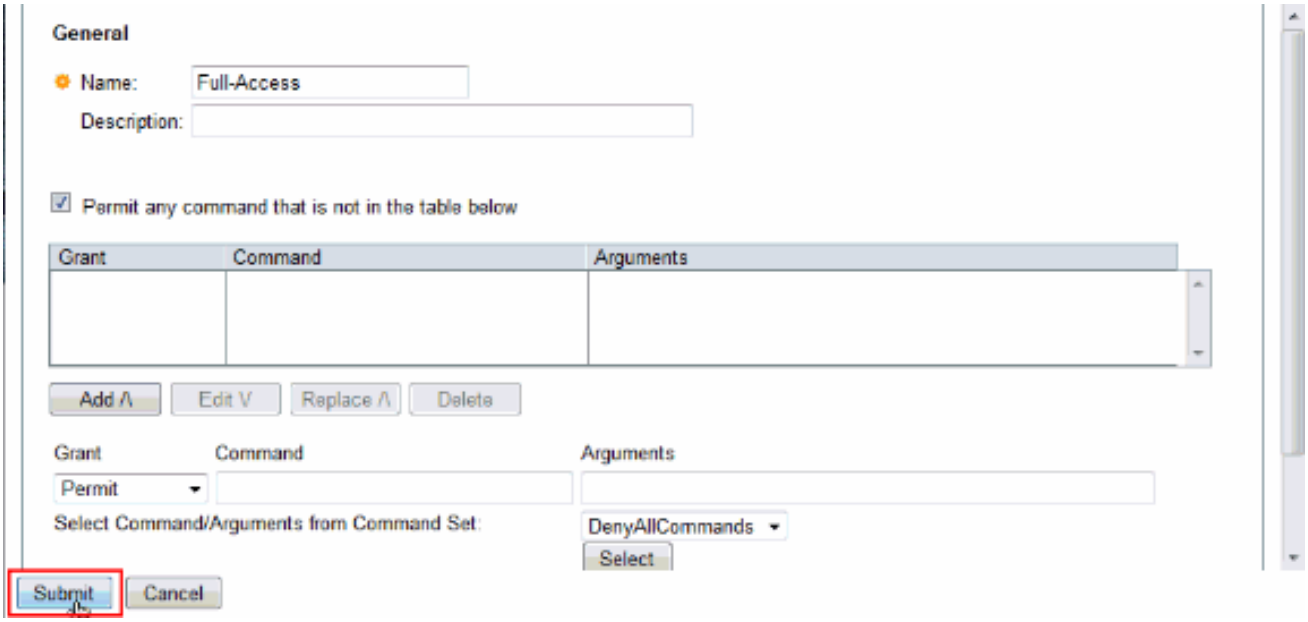
20. Haga clic **selecto** en el campo de los comandos estableces.



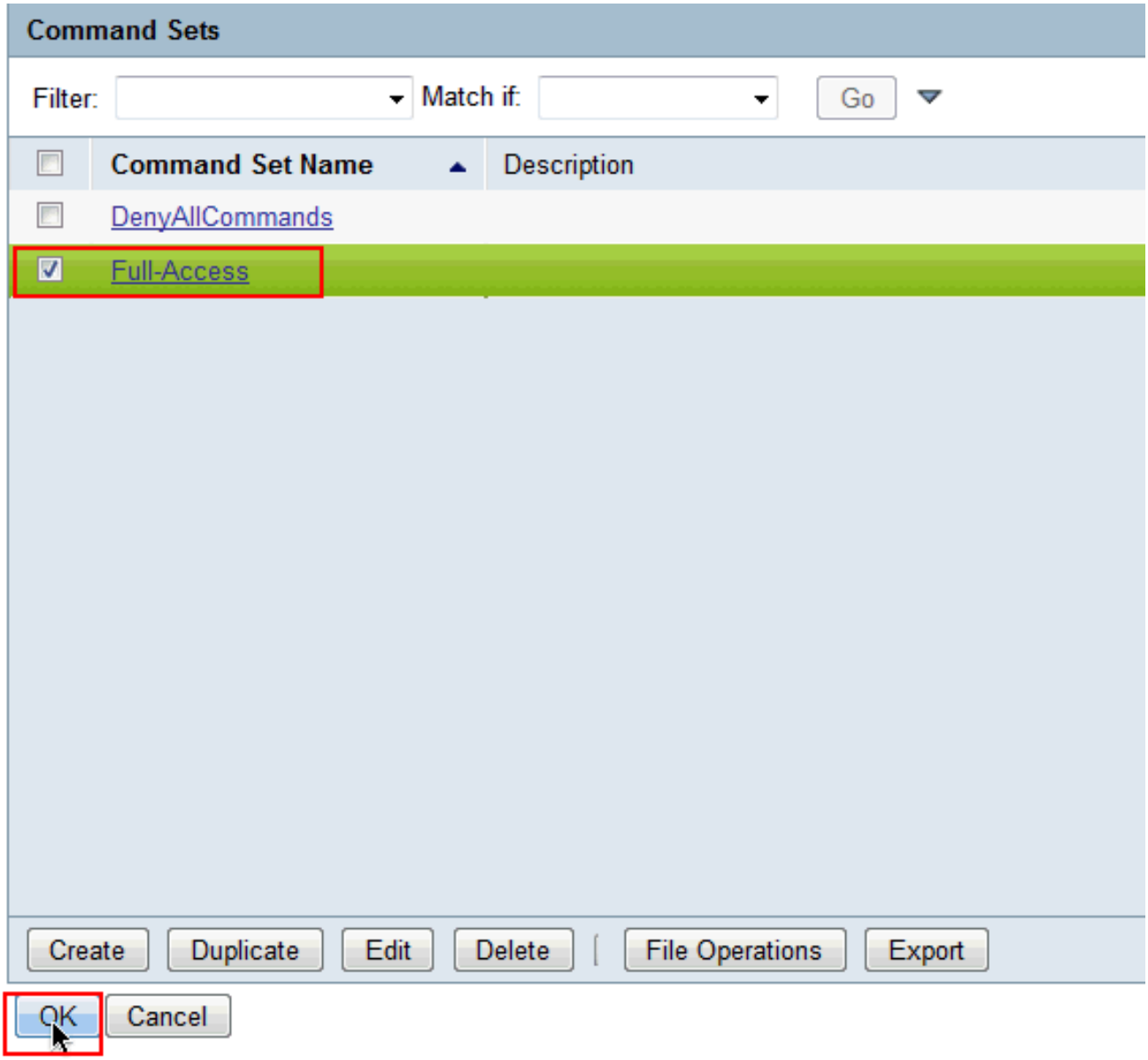
21. El tecleo **crea** para crear un comando new **fijado** para los usuarios **de total acceso**.



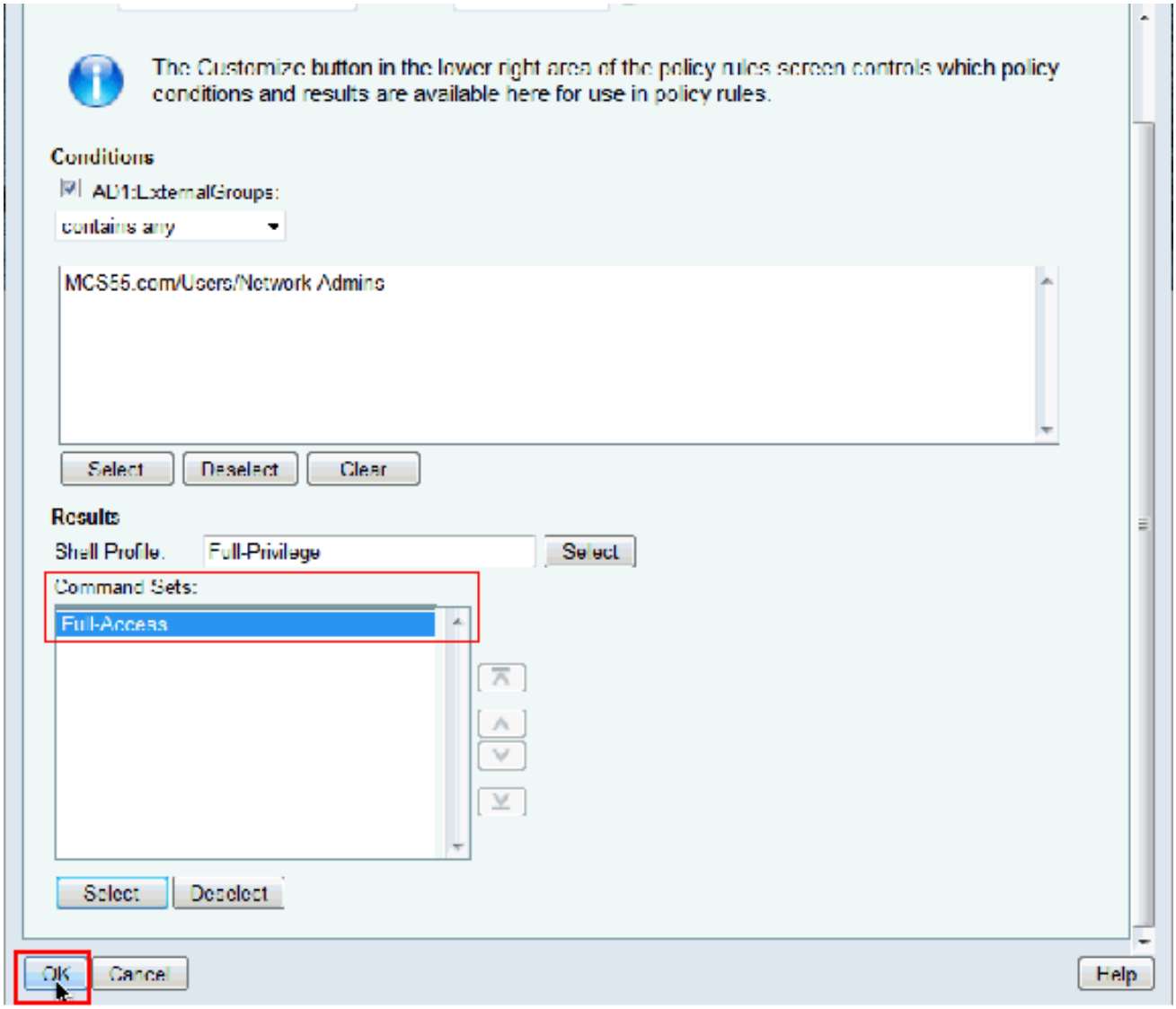
22. Proporcione un **nombre** y asegúrese de que la casilla de verificación al lado del **comando permit any que no está en la tabla abajo** está marcada. Haga clic en Submit (Enviar).**Nota:** Refiera a crear, a duplicación, y a los conjuntos del comando editing para Device Administration (Administración del dispositivo) para más información sobre los comandos
estableces.



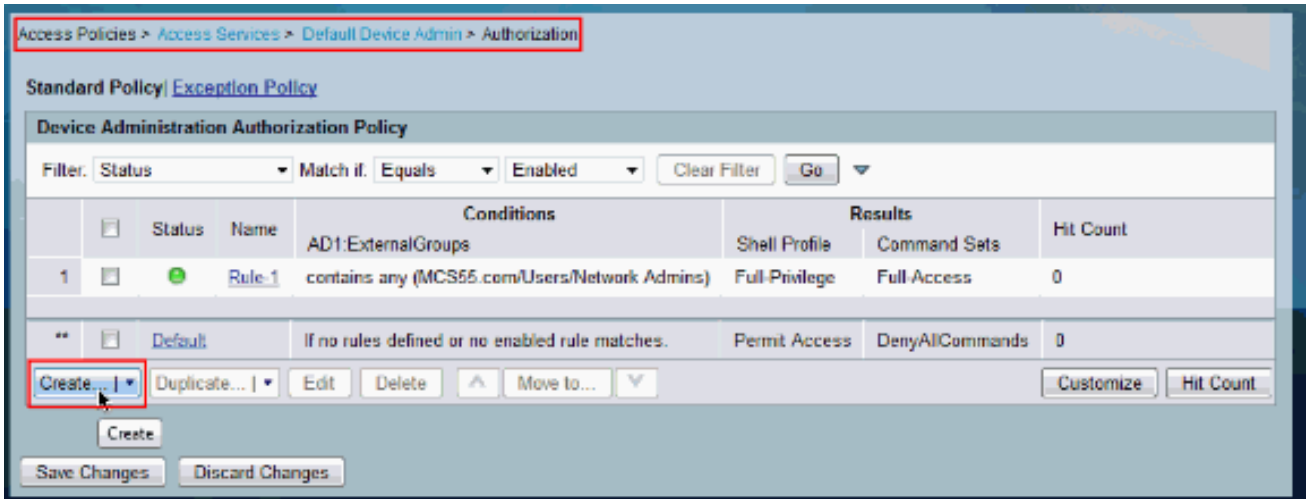
23. Haga clic en OK.



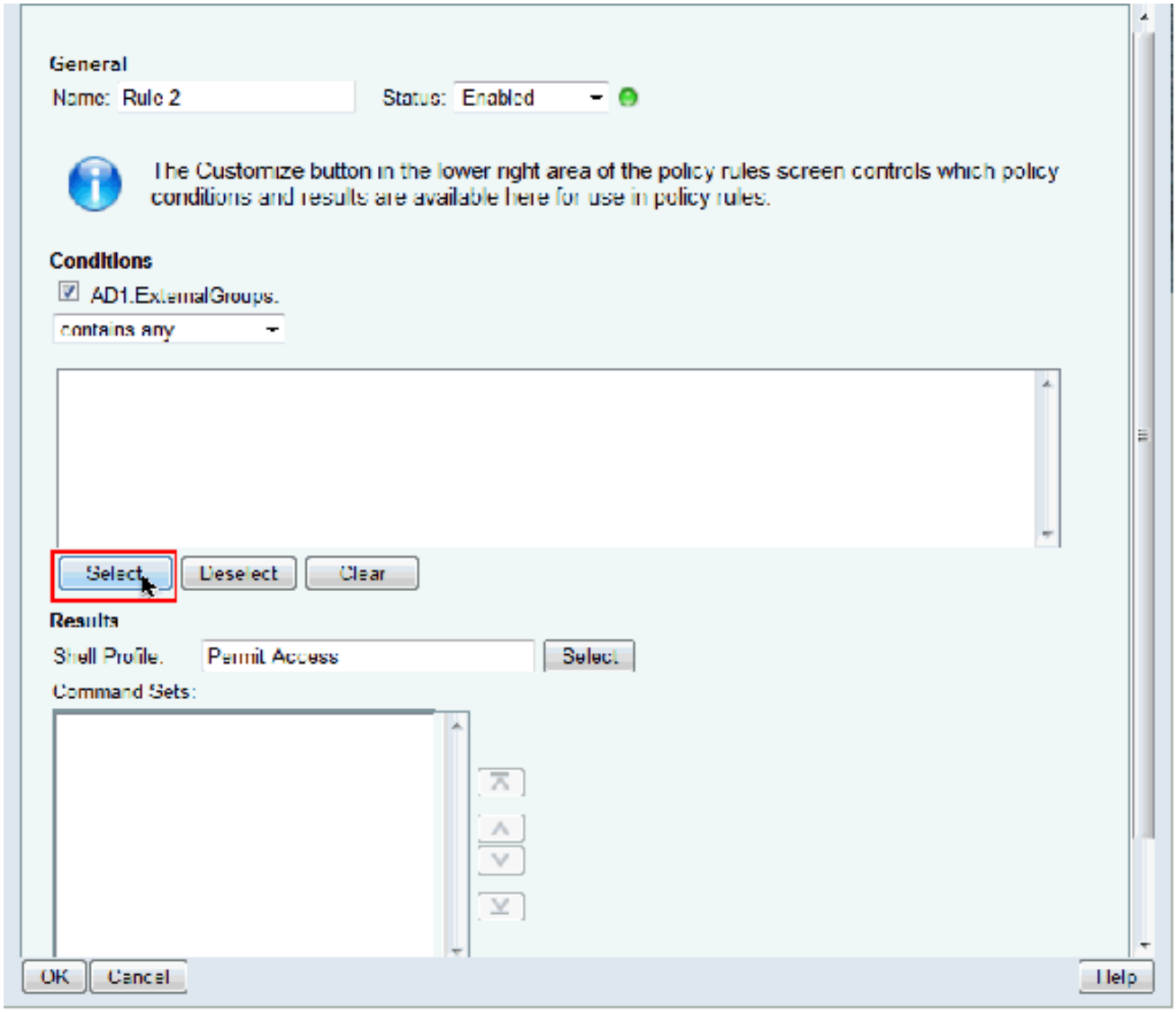
24. Haga clic en OK. Esto completa la configuración de **Rule-1**.



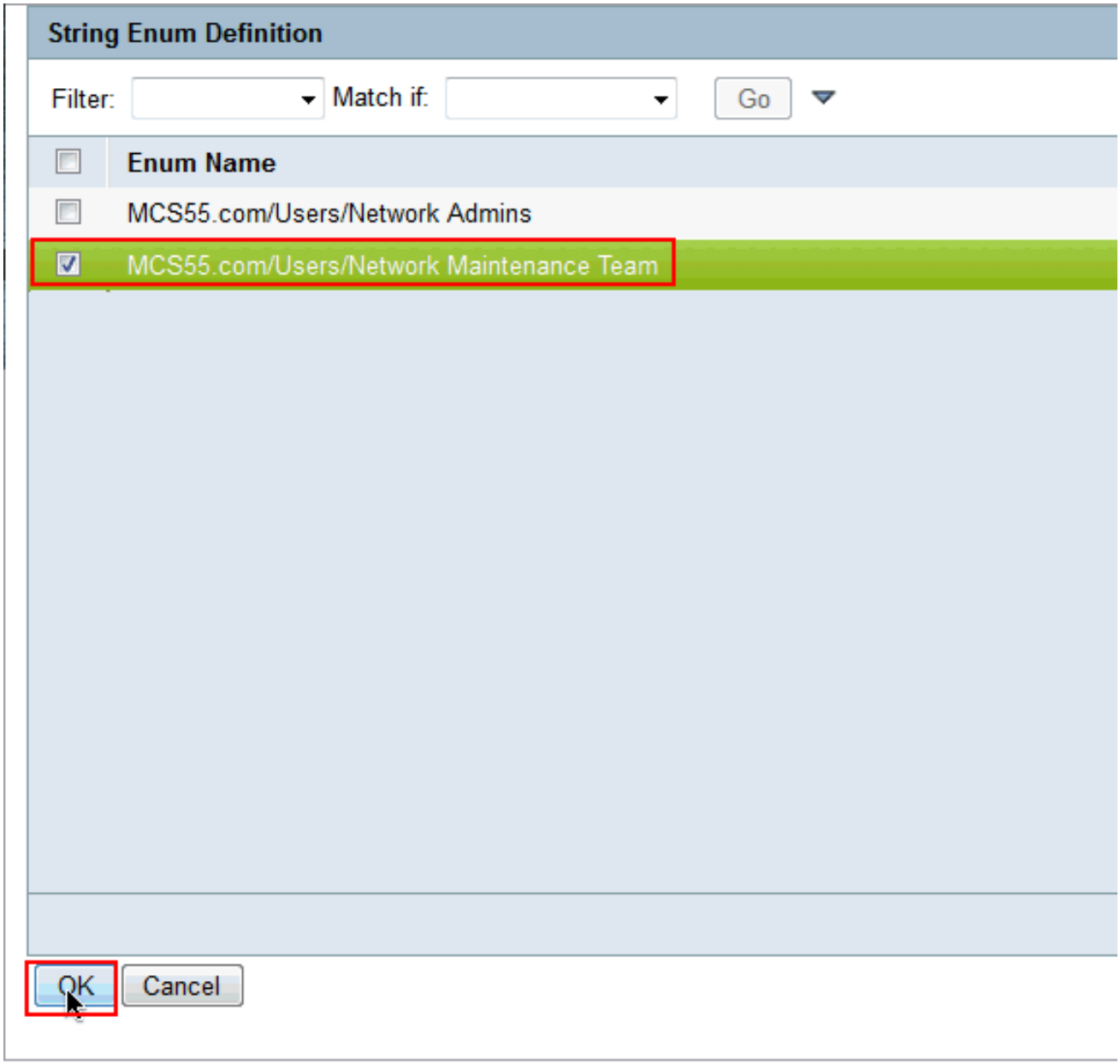
25. El tecleo **crea** para crear una nueva regla para los usuarios **limitados del acceso**.



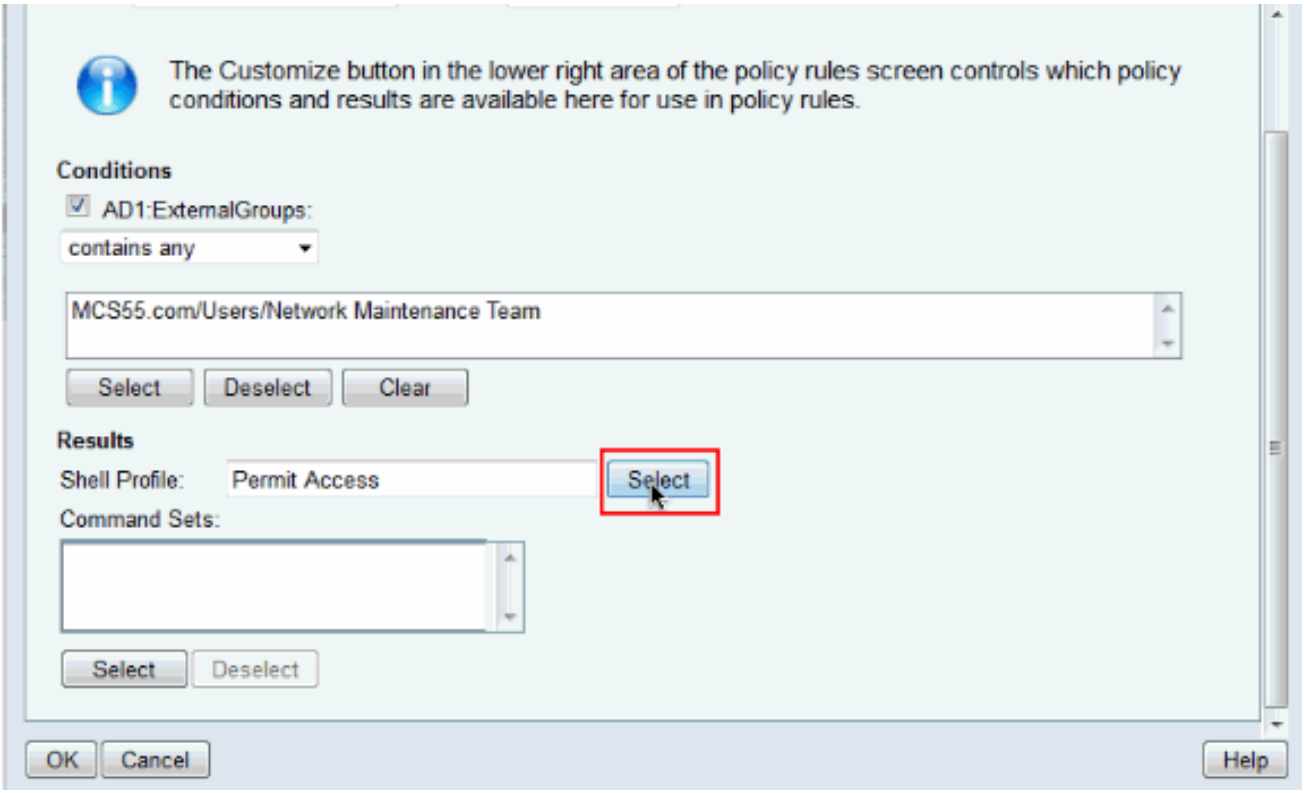
26. Elija **AD1:ExternalGroups** y haga clic **selecto**.



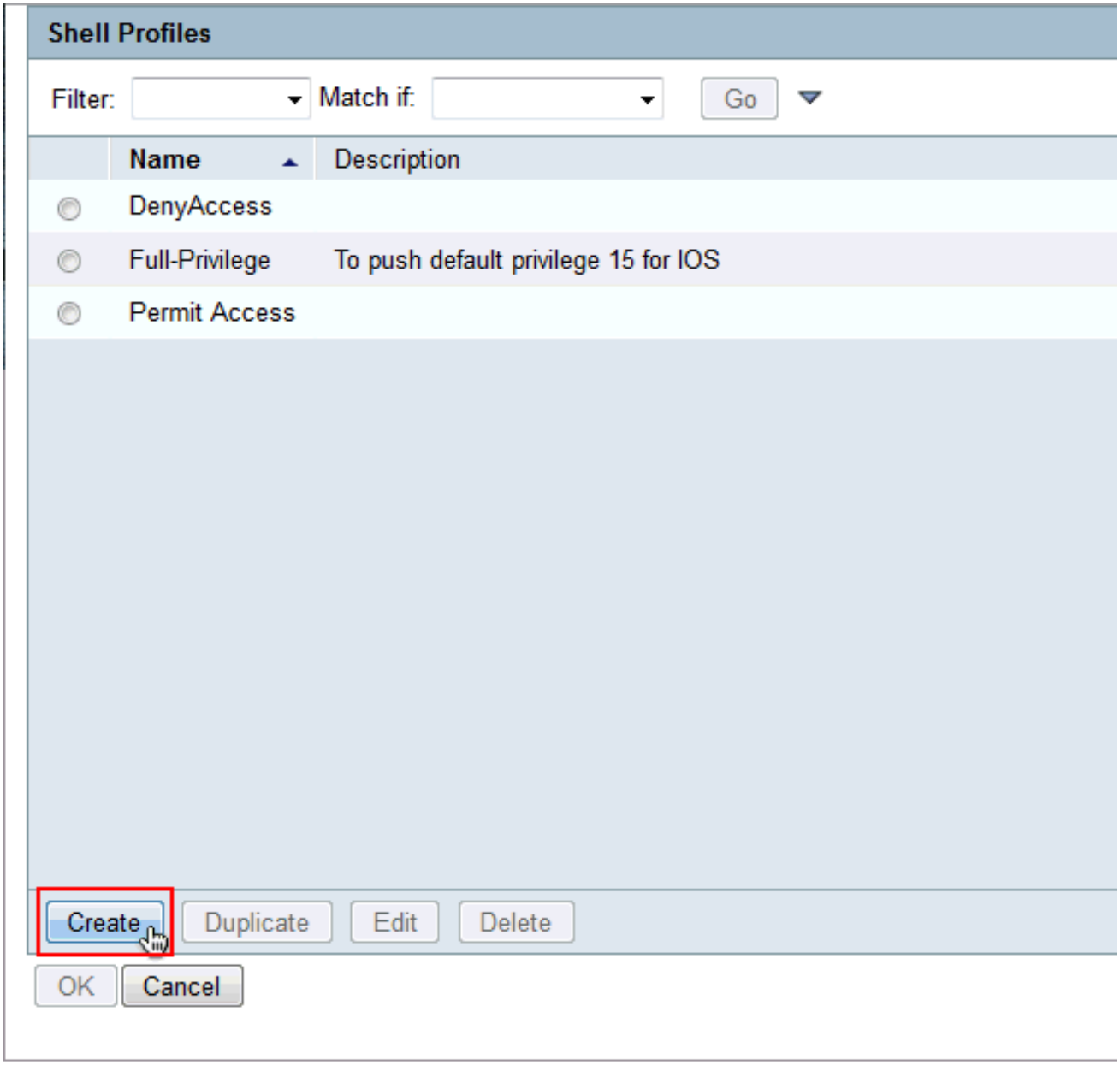
27. Elija a los grupos del grupo (o) a quienes usted quiere proporcionar el acceso limitado y hacer clic la
AUTORIZACIÓN.



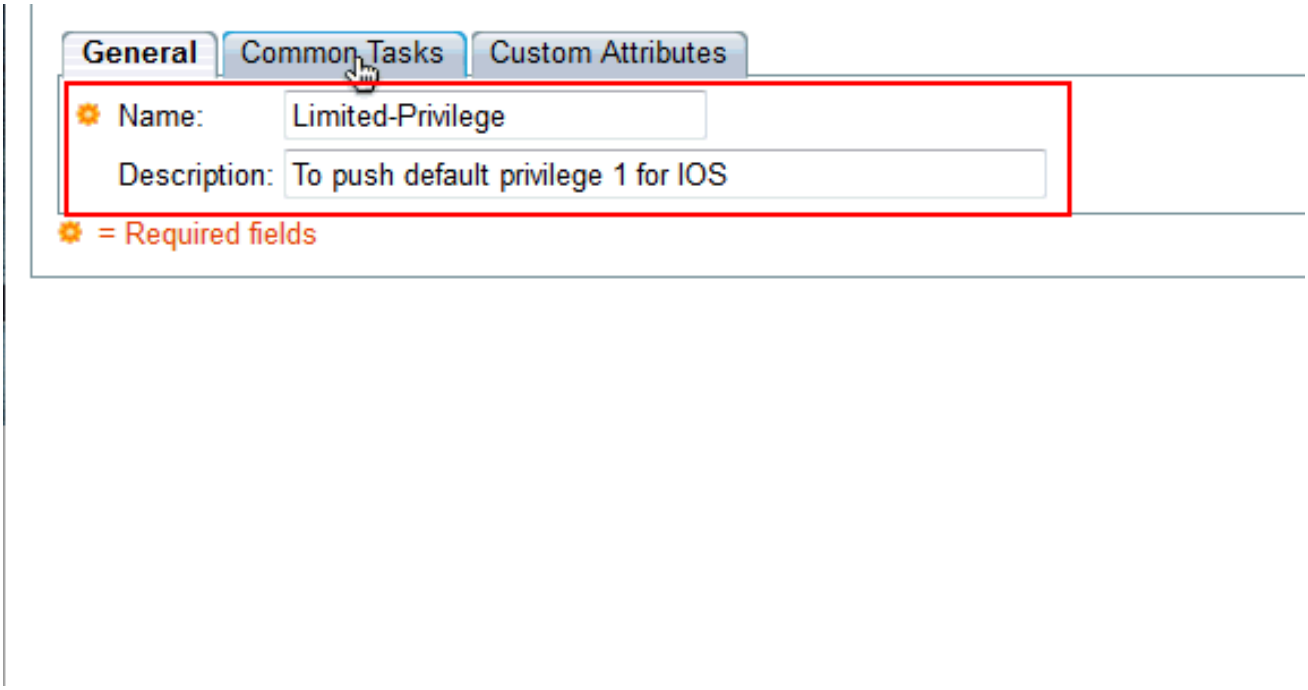
28. Haga clic **selecto** en el campo del perfil del shell.



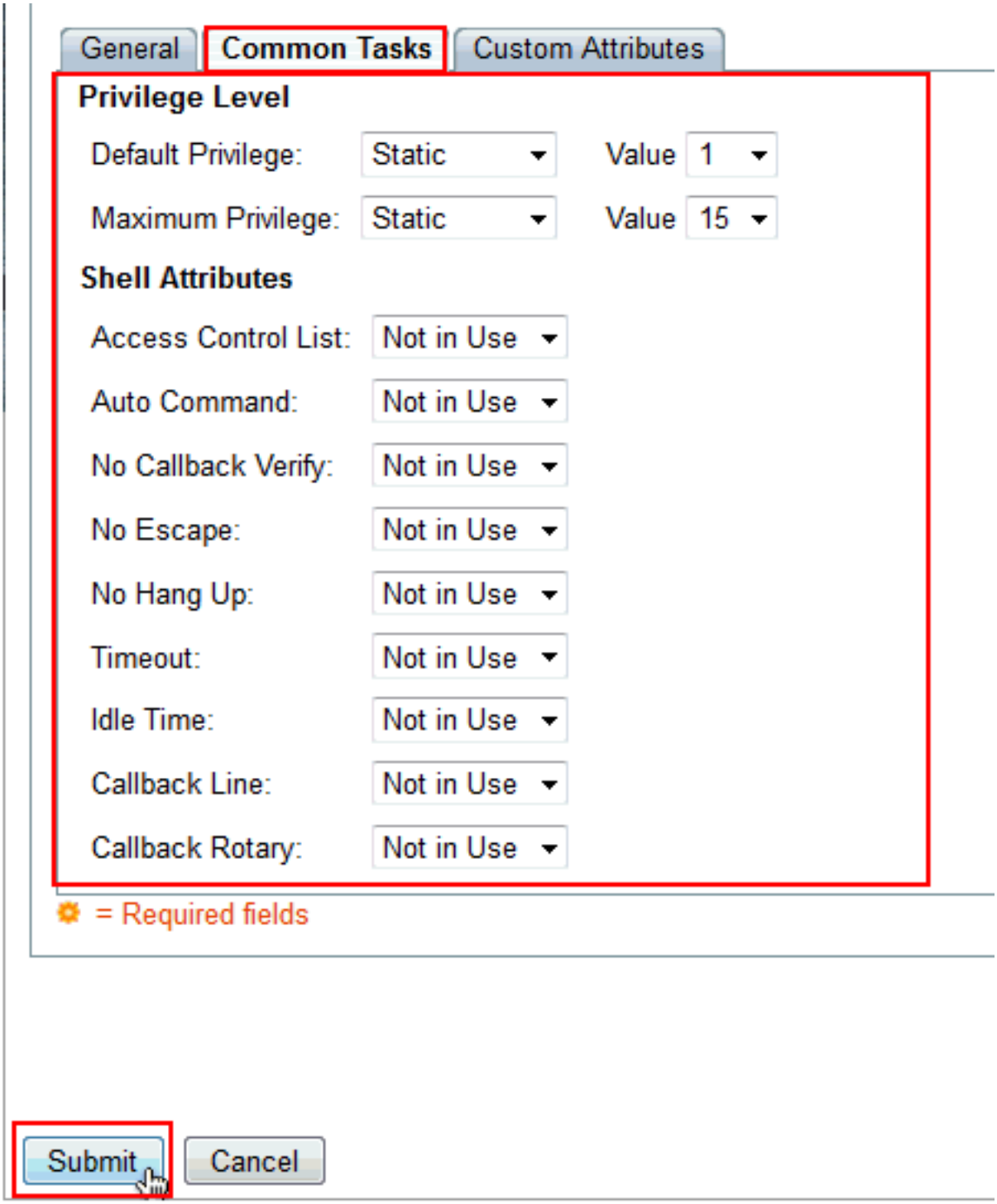
29. El tecleo **crea** para crear un nuevo **perfil del shell** para el acceso limitado.



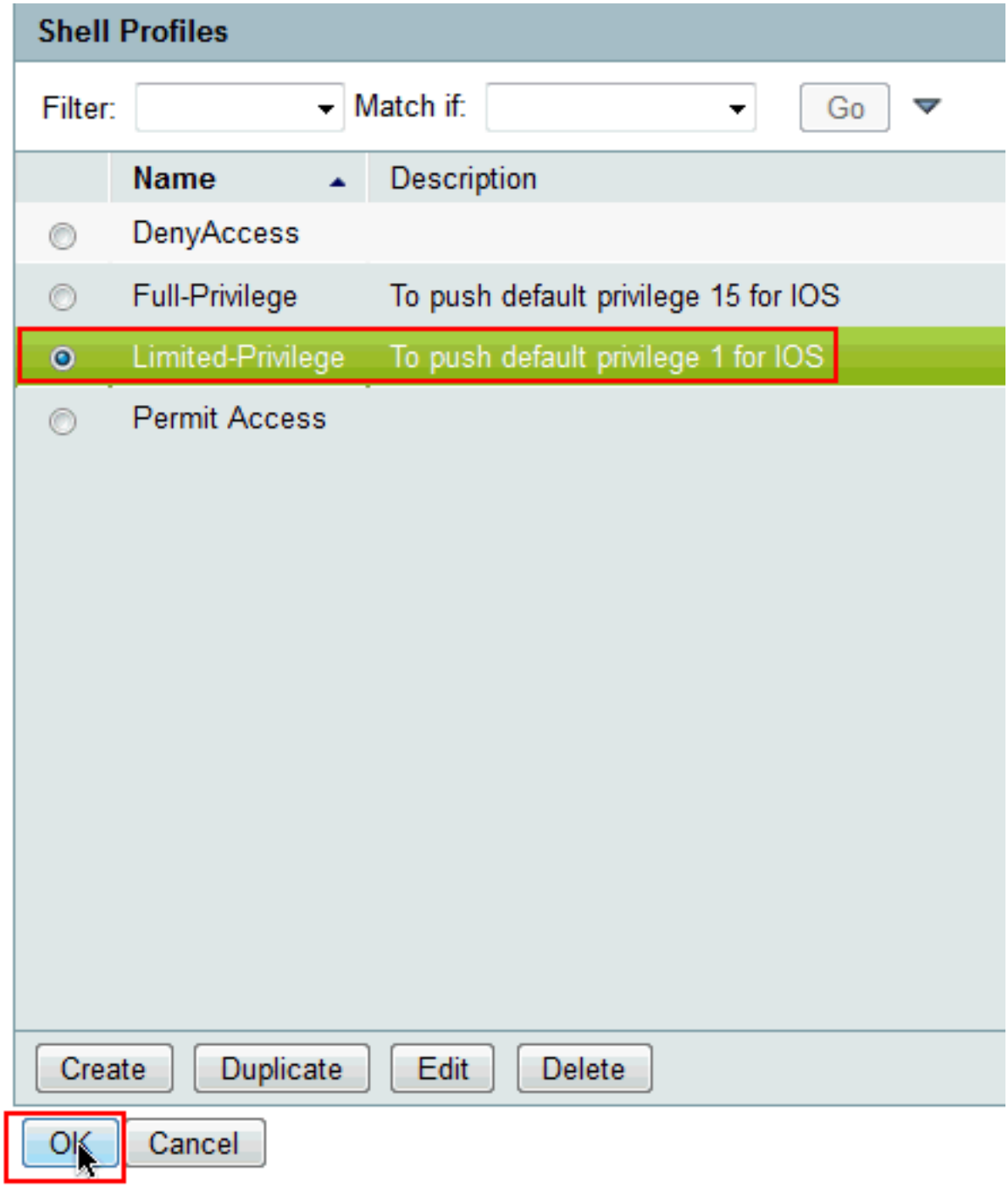
30. Proporcione un **nombre** y un **Description(optional)** en la **ficha general** y haga clic en la lengueta **común de las tareas**.



31. Cambie el **privilegio predeterminado** y el **privilegio del máximo a los parásitos atmosféricos** con los valores **1** y **15** respectivamente. Haga clic en Submit (Enviar).

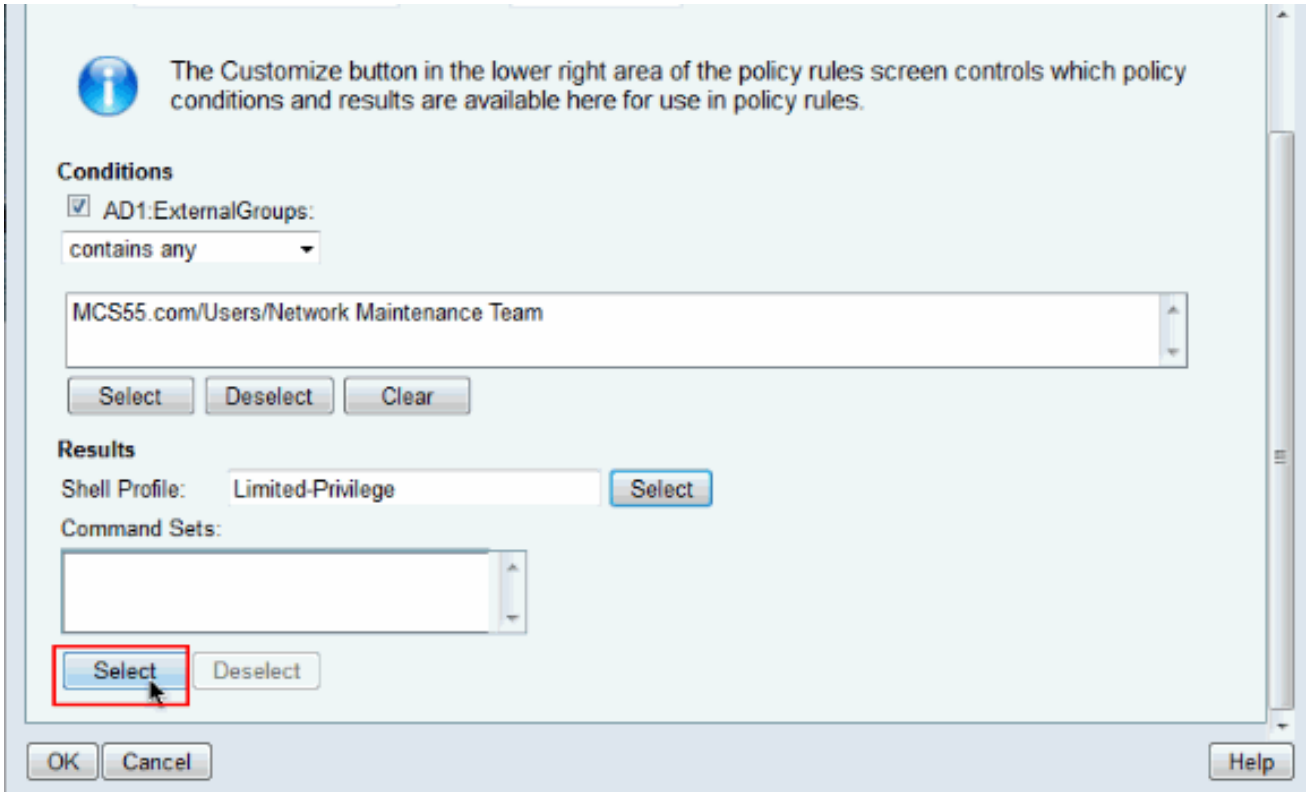


32. Haga clic en

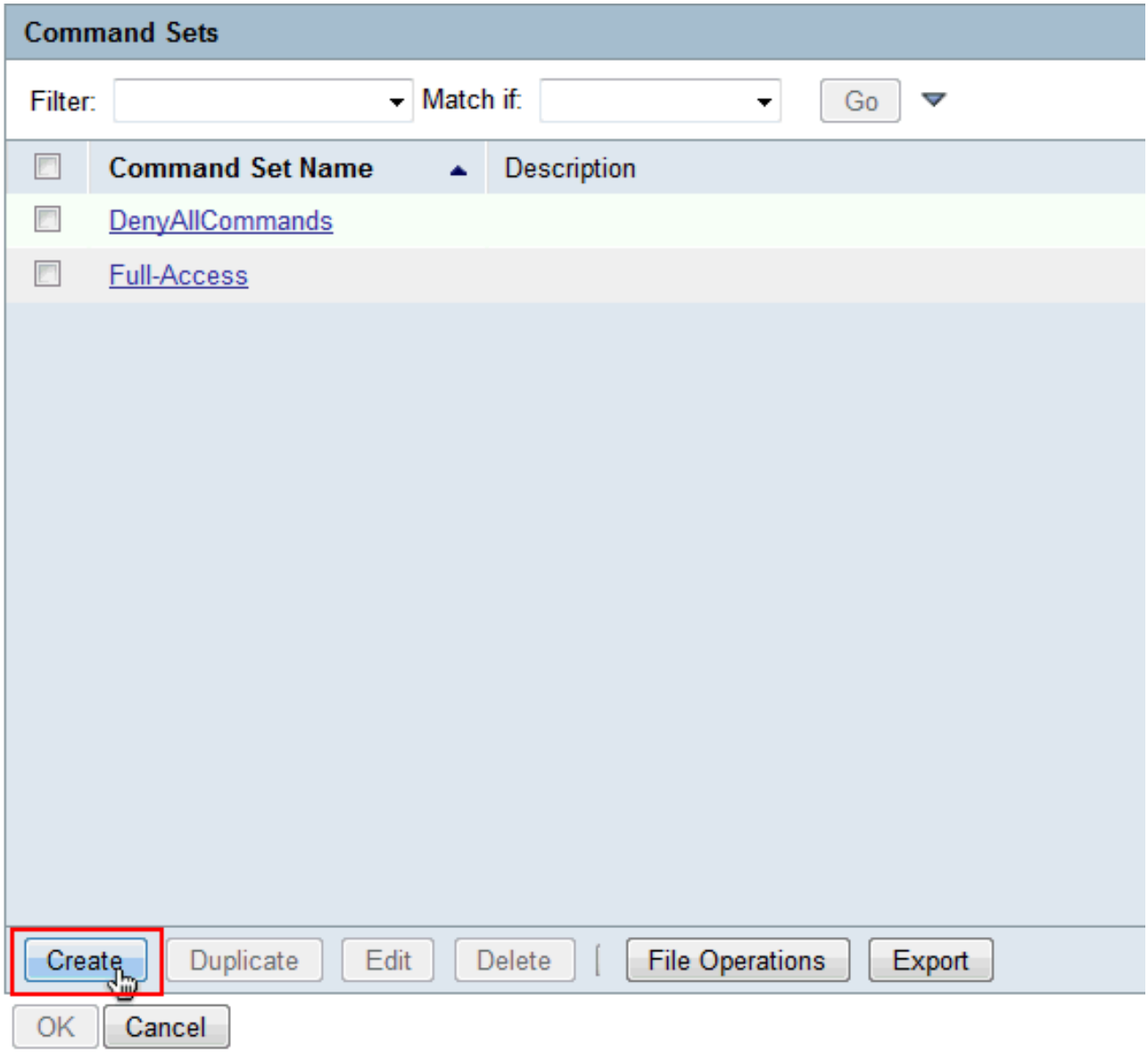


OK.

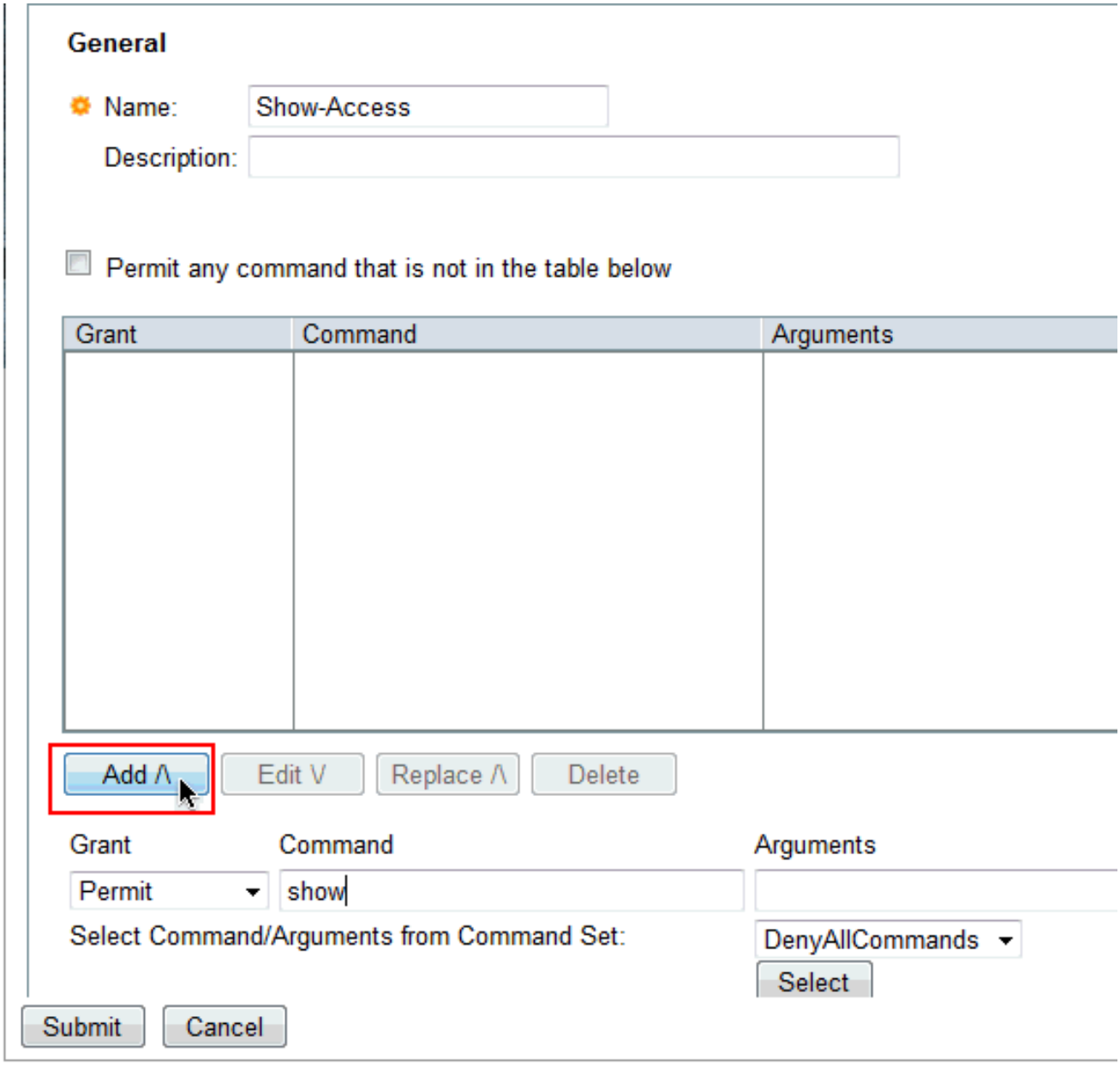
33. Tecleo **selecto** en el campo de los comandos estableces.



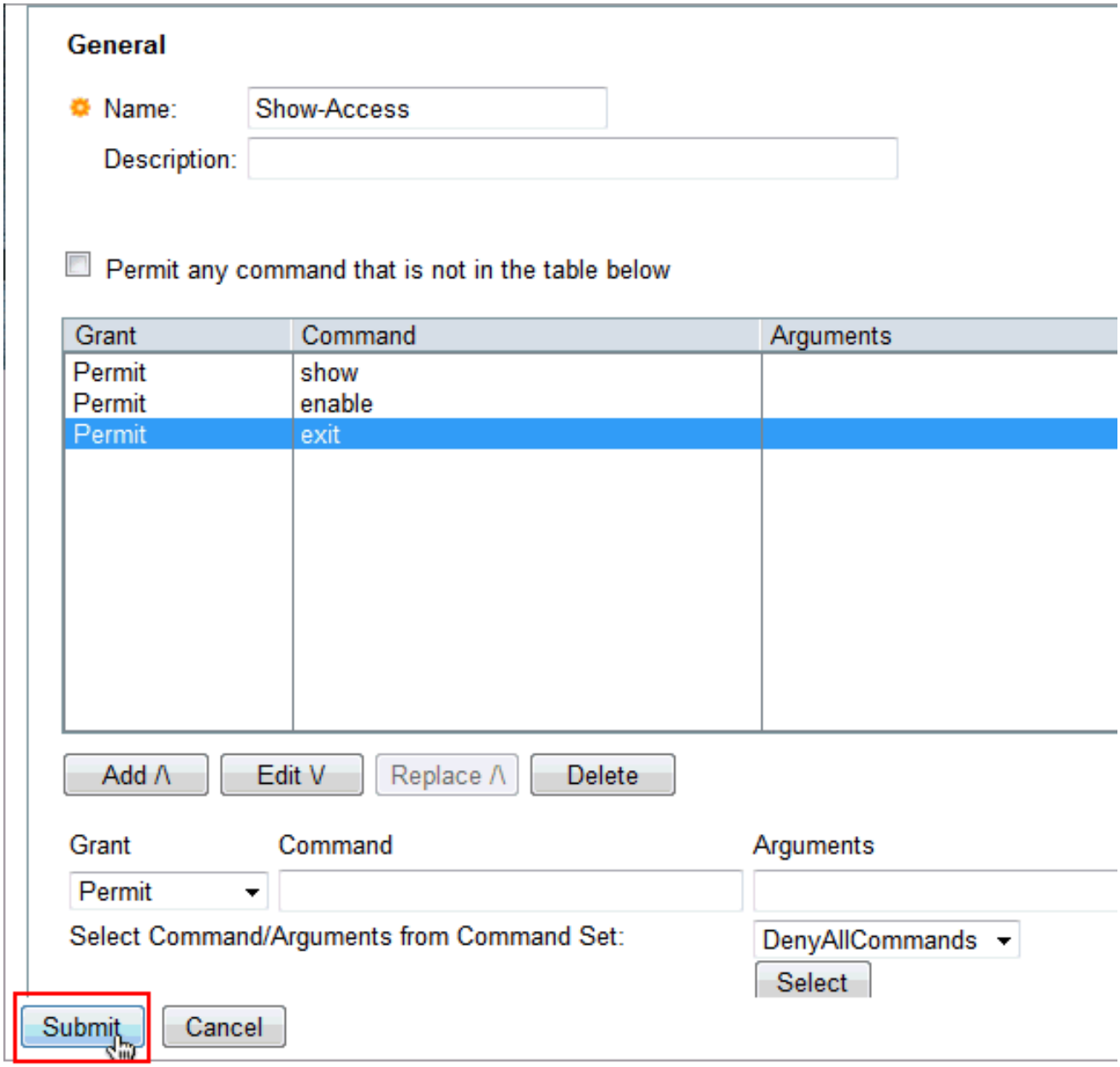
34. El tecleo **crea** para crear un comando new **fijado** para el grupo de acceso limitado.



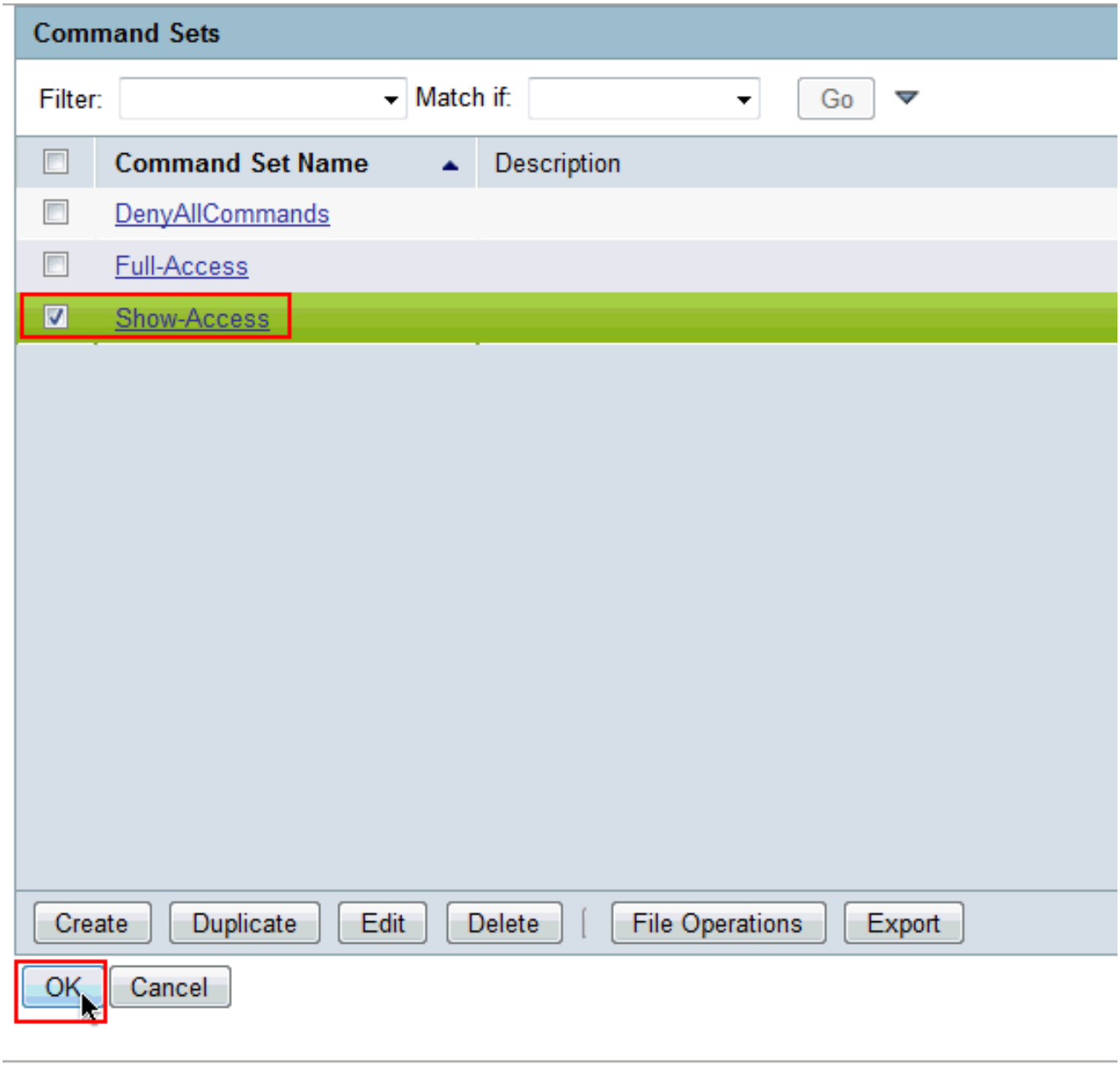
35. Proporcione un **nombre** y asegúrese de que el checkbox al lado del **comando permit any que no está en la tabla abajo** no está seleccionado. El tecleo **agrega** después de teclear la **demostración** en el espacio proporcionado en el **comando section** y elige el **permiso** en la sección de **Grant** para solamente permitir los comandos show para los usuarios en el grupo de acceso
limitado.



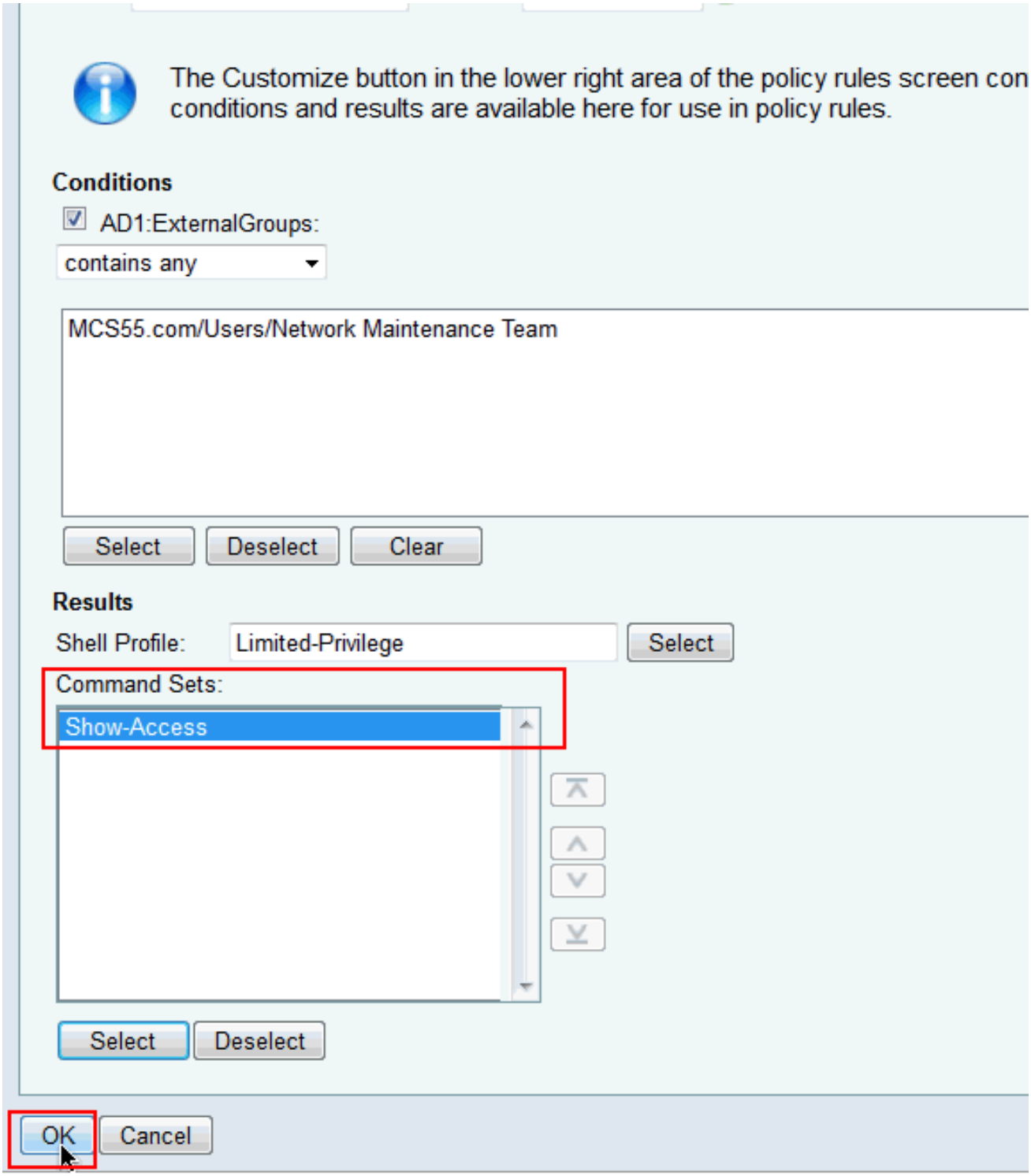
36. Agregue semejantemente cualquier otro comando de ser permitido para los usuarios en el grupo de acceso limitado con el uso **Add**. Haga clic en Submit (Enviar).**Nota:** Refiera a crear, a duplicación, y a los conjuntos del comando editing para Device Administration (Administración del dispositivo) para más información sobre los comandos estableces.



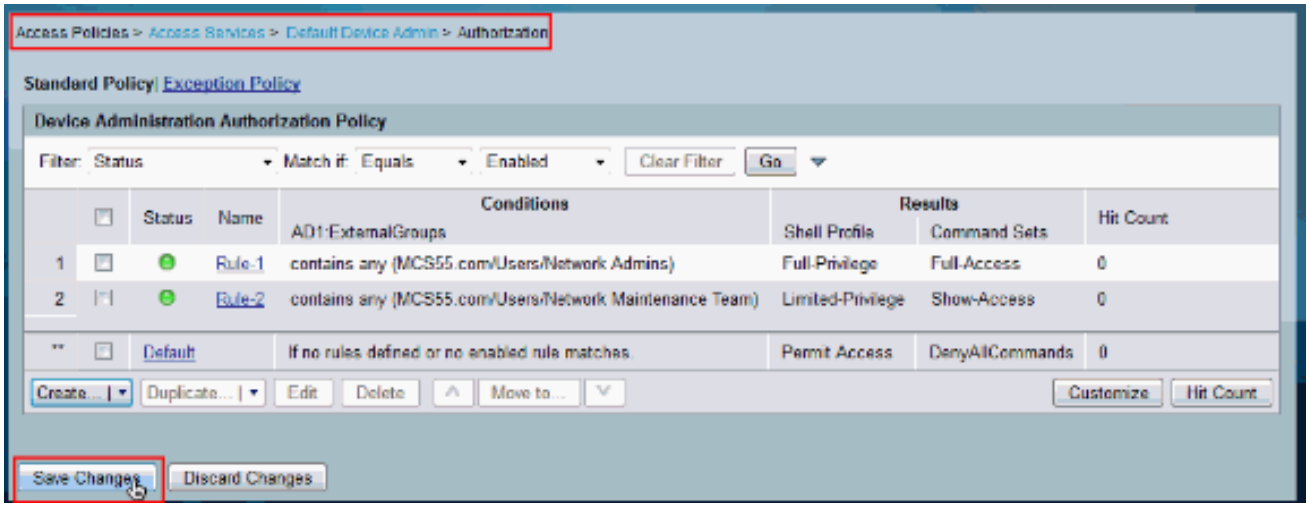
37. Haga clic en OK.



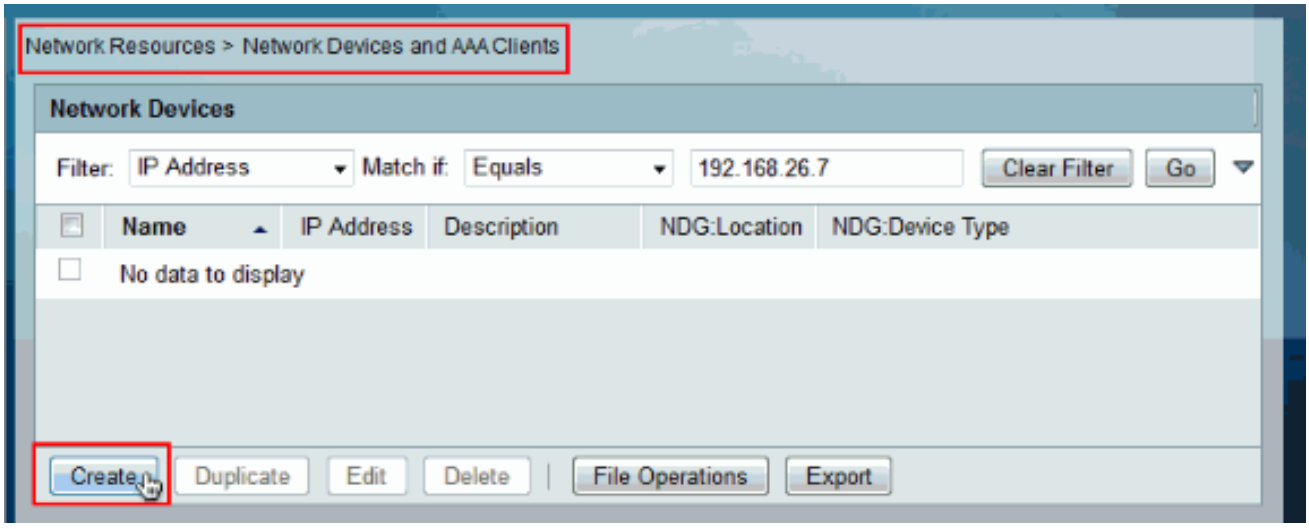
38. Haga clic en OK.



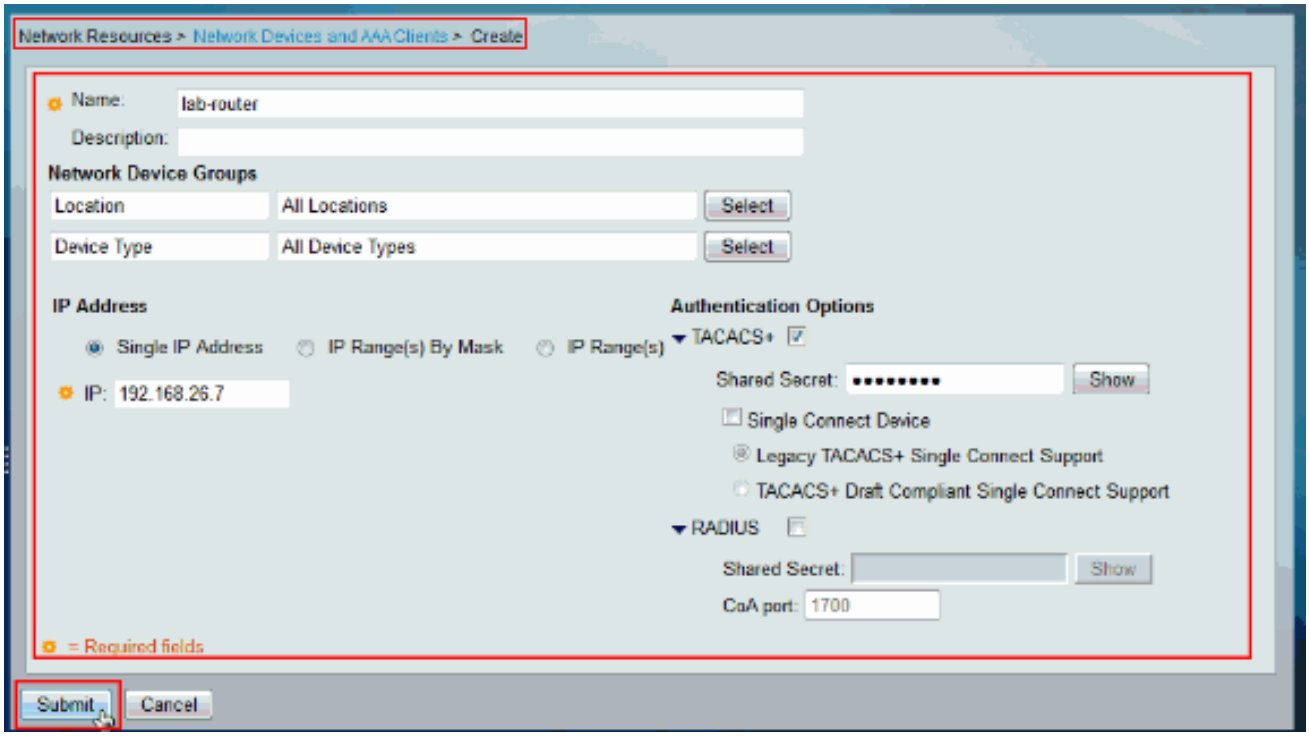
39. **Cambios de la salvaguardia del** tecleo.



40. El tecleo **crea** para agregar el **dispositivo Cisco IOS** como **cliente AAA** en el ACS.



41. Proporcione un **nombre, la dirección IP, el secreto compartido** para el **TACACS+** y el tecleo **someten**.



Configure el dispositivo Cisco IOS para la autenticación y autorización

Complete estos pasos para configurar el dispositivo Cisco IOS y el ACS para la autenticación y autorización.

1. Cree a un usuario local con el privilegio completo para el retraso con el **comando username** como se muestra aquí:`username admin privilege 15 password 0 cisco123!`
2. Proporcione la dirección IP del ACS para habilitar el AAA y agregar ACS 5.x como servidor TACACS.`aaa new-model`
   `tacacs-server host 192.168.26.51 key cisco123`**Nota:** La clave debe hacer juego con el secreto compartido proporcionado en el ACS para este dispositivo Cisco IOS.
3. Pruebe el accesibilidad del servidor TACACS con el [comando aaa de la prueba](#) como se muestra.`test aaa group tacacs+ user1 xxxxx legacy`
   `Attempting authentication test to server-group tacacs+ using tacacs+`
   `User was successfully authenticated.`La salida del comando anterior muestra que el servidor TACACS es accesible y han autenticado al usuario con éxito.**Nota:** El user1 y el xxx de la contraseña pertenecen al AD. Si la prueba falla por favor asegúrese de que el secreto compartido proporcionado en el paso anterior esté correcto.
4. Configure el login y habilite las autenticaciones y después utilice el ejecutivo y las autorizaciones de comando como se muestra aquí:`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`**Nota:** Las palabras claves del Local y del permiso se utilizan para el retraso al usuario local del Cisco IOS y habilitan el secreto respectivamente si el servidor TACACS es inalcanzable.

Verificación

Para verificar la autenticación y autorización inicie sesión al dispositivo Cisco IOS con Telnet.

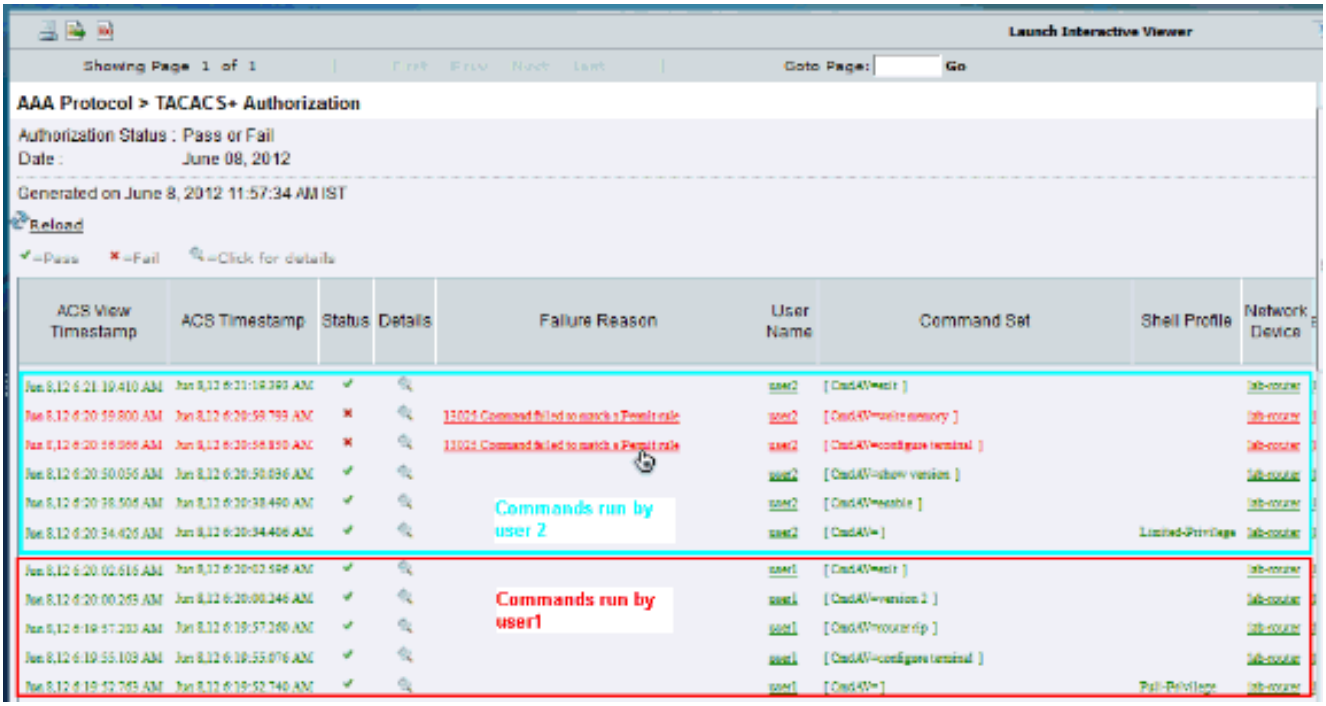
1. Telnet al dispositivo Cisco IOS como user1 que pertenece al grupo de total acceso en el AD. El grupo de Admins de la red es el grupo en el AD que es perfil asociado del shell del FULL-privilegio y comando set de total acceso en el ACS. Intente funcionar con el comando any de asegurarse de que usted tiene acceso
   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. Telnet al dispositivo Cisco IOS como user2 que pertenece al grupo del limitado-acceso en el AD. (El grupo del **equipo del mantenimiento de red** es el grupo en el AD que es **comando set** asociado del **perfil** y del Demostración-**acceso del shell del Limitado-privilegio** en el ACS). Si usted intenta funcionar con el comando any con excepción de los que está mencionados en el comando set del Demostración-acceso, usted debe conseguir un error `fallado comando authorization`, que muestra que el user2 ha limitado el
acceso.

```
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"

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/wwl/export/crypto/tool/stqrg.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. Inicie sesión al ACS GUI y ponga en marcha la **supervisión y señala el Visualizador**. Elija el **protocolo AAA > TACACS+Authorization** para verificar las actividades realizadas por el user1 y
user2.



Información Relacionada

- Cisco Secure Access Control System
- Soporte Técnico y Documentación - Cisco Systems