ACS 5.x: Autenticación TACACS+ y autorización de comandos basada en el ejemplo de configuración de pertenencia al grupo AD

Contenido

Introducción

Este documento proporciona un ejemplo de configuración de autenticación TACACS+ y autorización de comandos basada en la pertenencia al grupo AD de un usuario con Cisco Secure Access Control System (ACS) 5.x y versiones posteriores. ACS utiliza Microsoft Active Directory (AD) como almacén de identidades externo para guardar recursos como usuarios, equipos, grupos y atributos.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ACS 5.x está totalmente integrado en el dominio AD deseado. Si ACS no está integrado con el dominio AD deseado, consulte ACS 5.x y posterior: Ejemplo de configuración de integración con Microsoft Active Directory para obtener más información para realizar la tarea de integración.

Componentes Utilizados

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

- Cisco Secure ACS 5.3
- Software Cisco IOS® versión 12.2(44)SE6.

  Nota: Esta configuración se puede realizar en todos los dispositivos Cisco IOS.
- Dominio de Microsoft Windows Server 2003

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Configuración

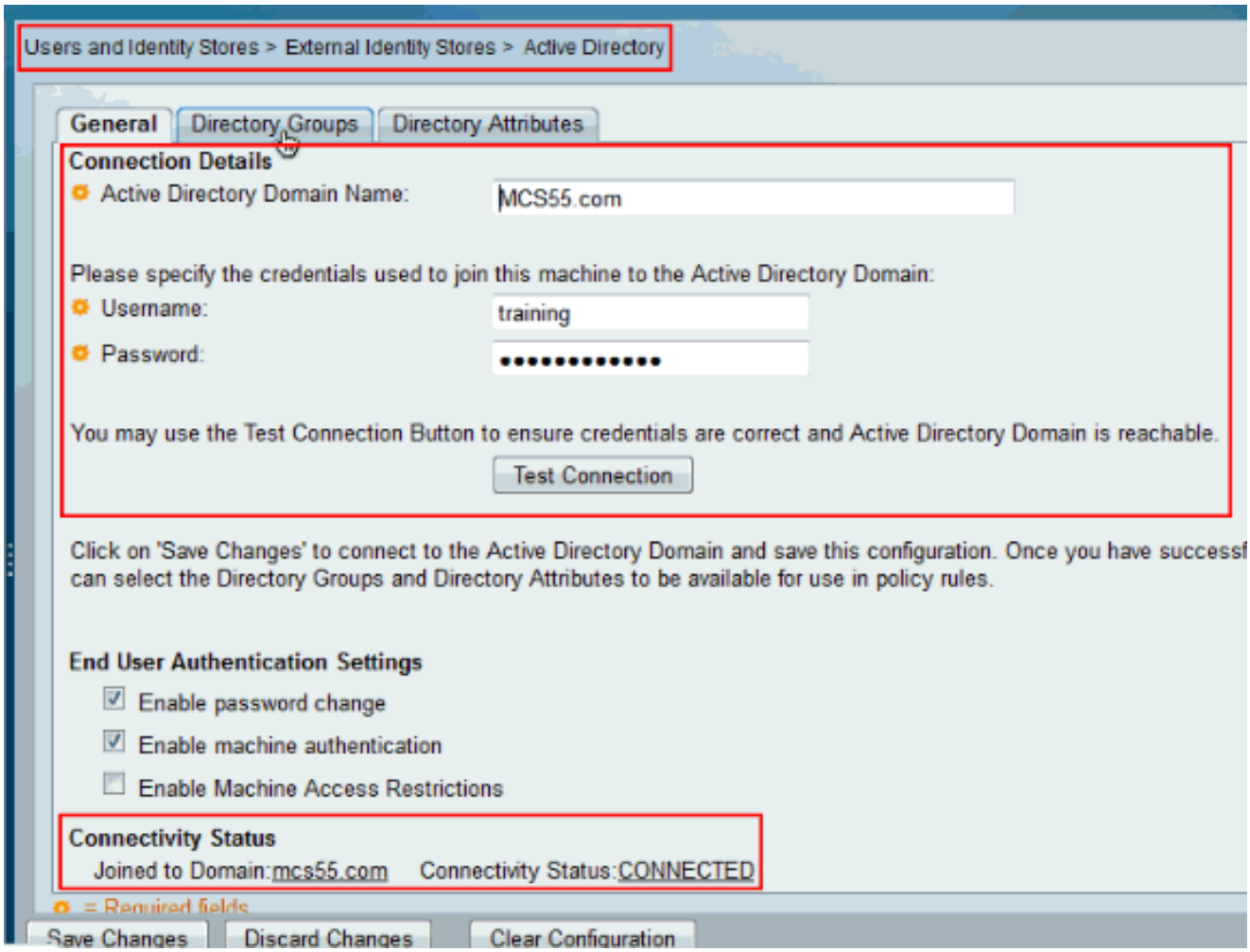
Configuración de ACS 5.x para autenticación y autorización

Antes de comenzar la configuración de ACS 5.x para autenticación y autorización, ACS debería haberse integrado correctamente con Microsoft AD. Si ACS no está integrado con el dominio AD deseado, consulte ACS 5.x y posterior: Ejemplo de configuración de integración con Microsoft Active Directory para obtener más información para realizar la tarea de integración.

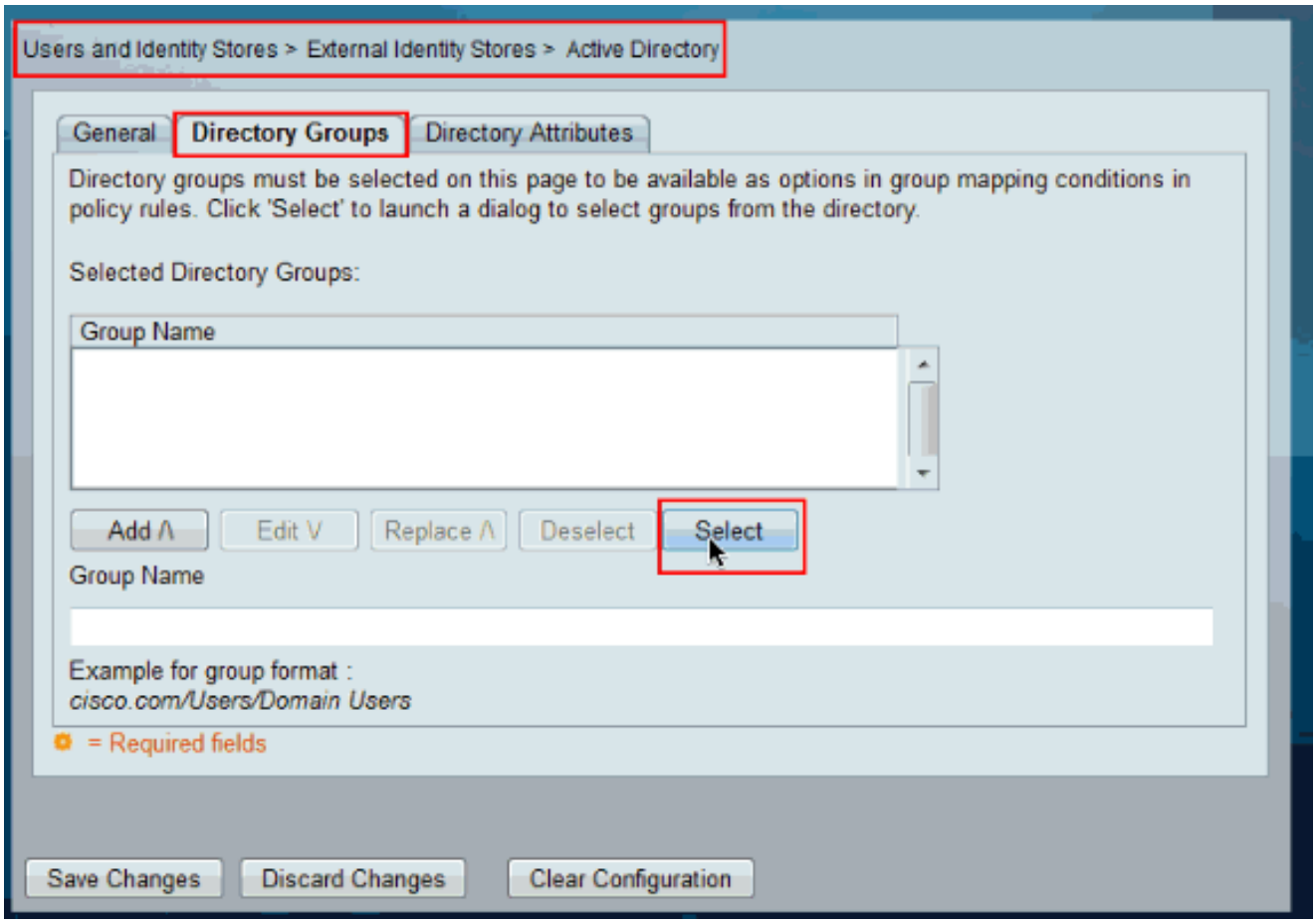
En esta sección, se asignan dos grupos de AD a dos conjuntos de comandos diferentes y dos perfiles de Shell, uno con acceso completo y el otro con acceso limitado en los dispositivos Cisco IOS.

1. Inicie sesión en la GUI de ACS con las credenciales de administrador.
2. Elija Users and Identity Stores > External Identity Stores > Active Directory y verifique que ACS se haya unido al dominio deseado y también que el estado de conectividad se muestre como conectado.

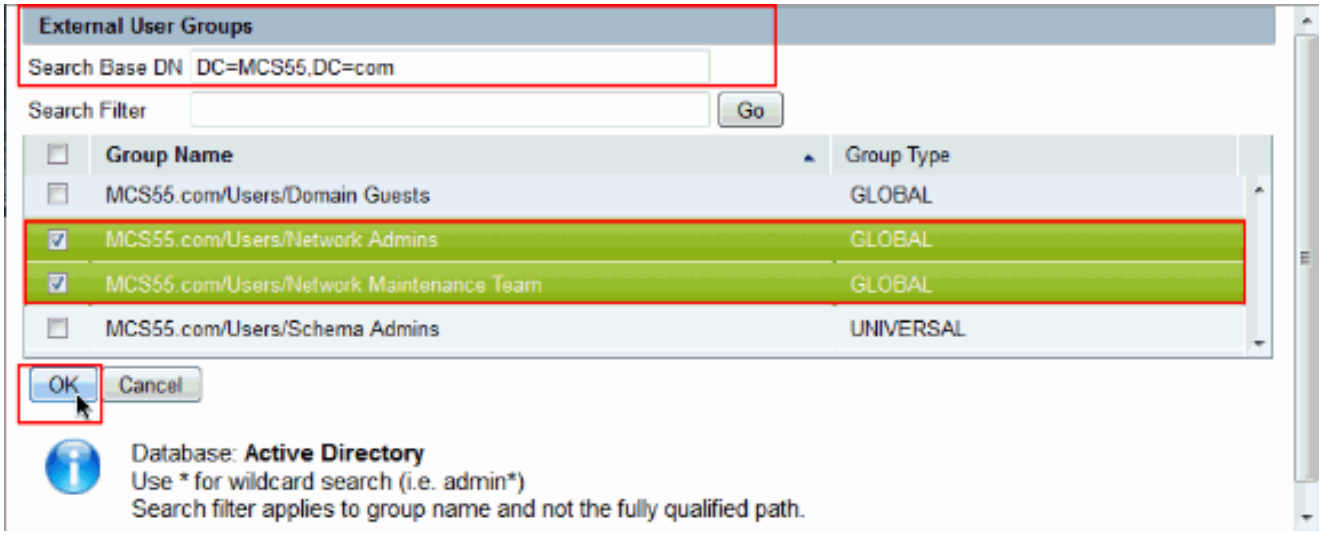
   Haga clic en la ficha Grupos de directorios.



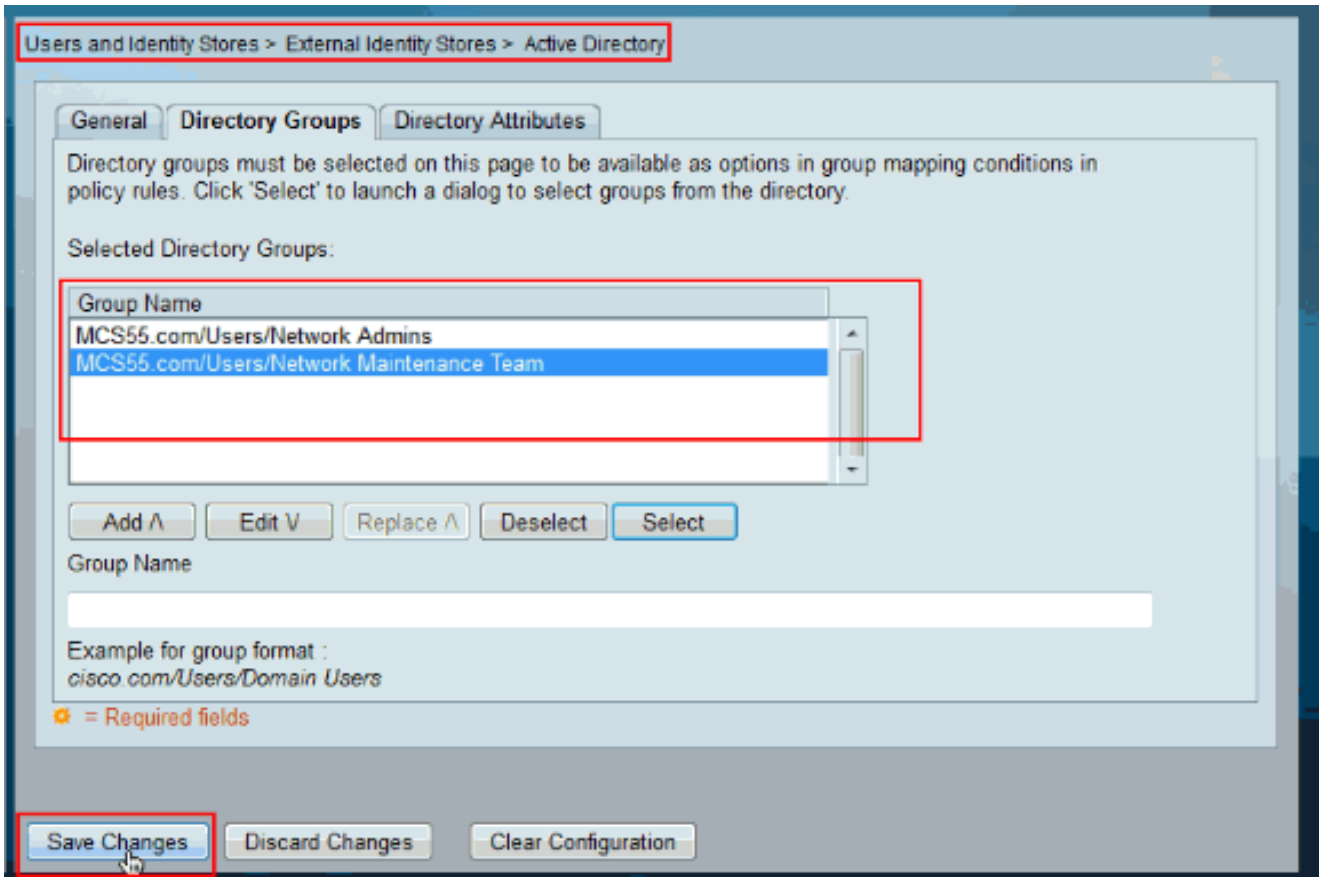
3. Haga clic en Seleccionar.



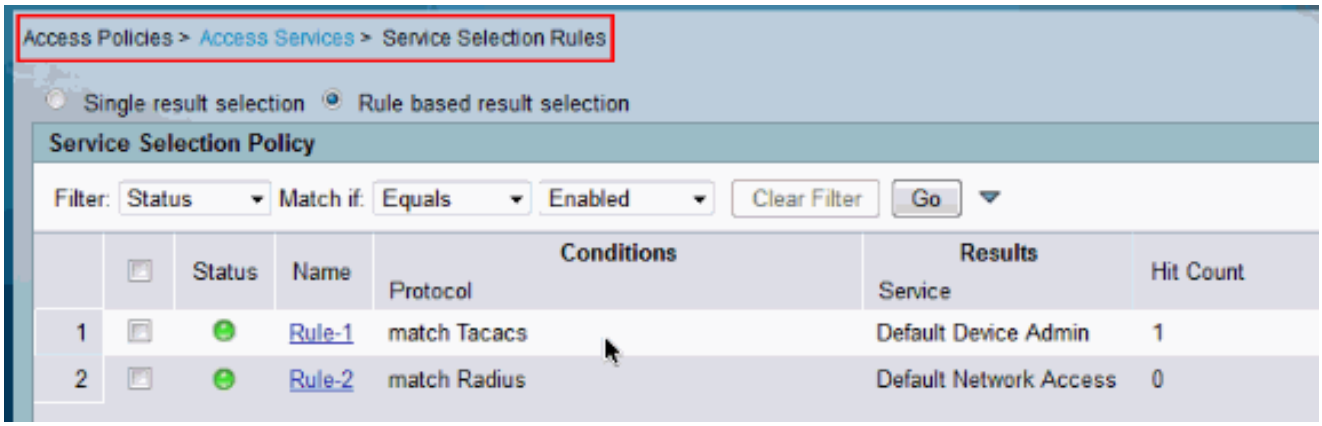
4. Elija los grupos que deben asignarse a los conjuntos de comandos y perfiles de shell en la parte posterior de la configuración. Click OK.



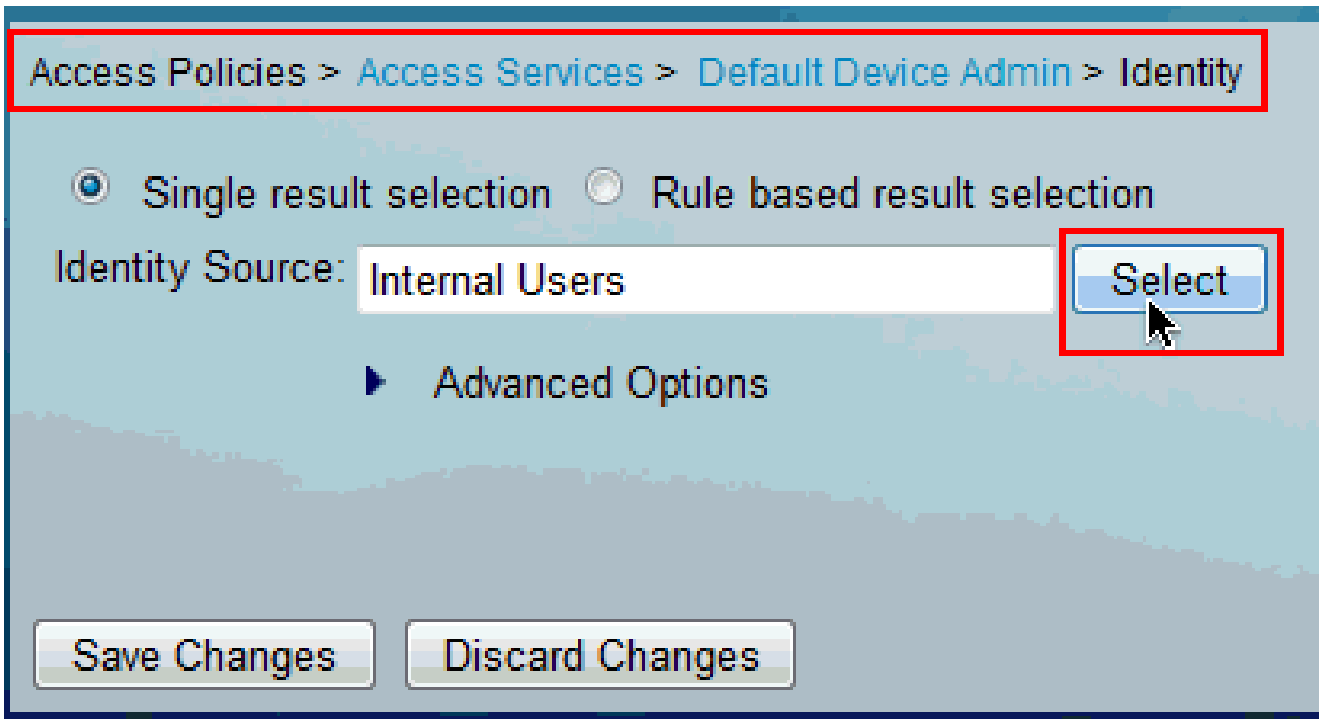
5. Haga clic en Guardar cambios.



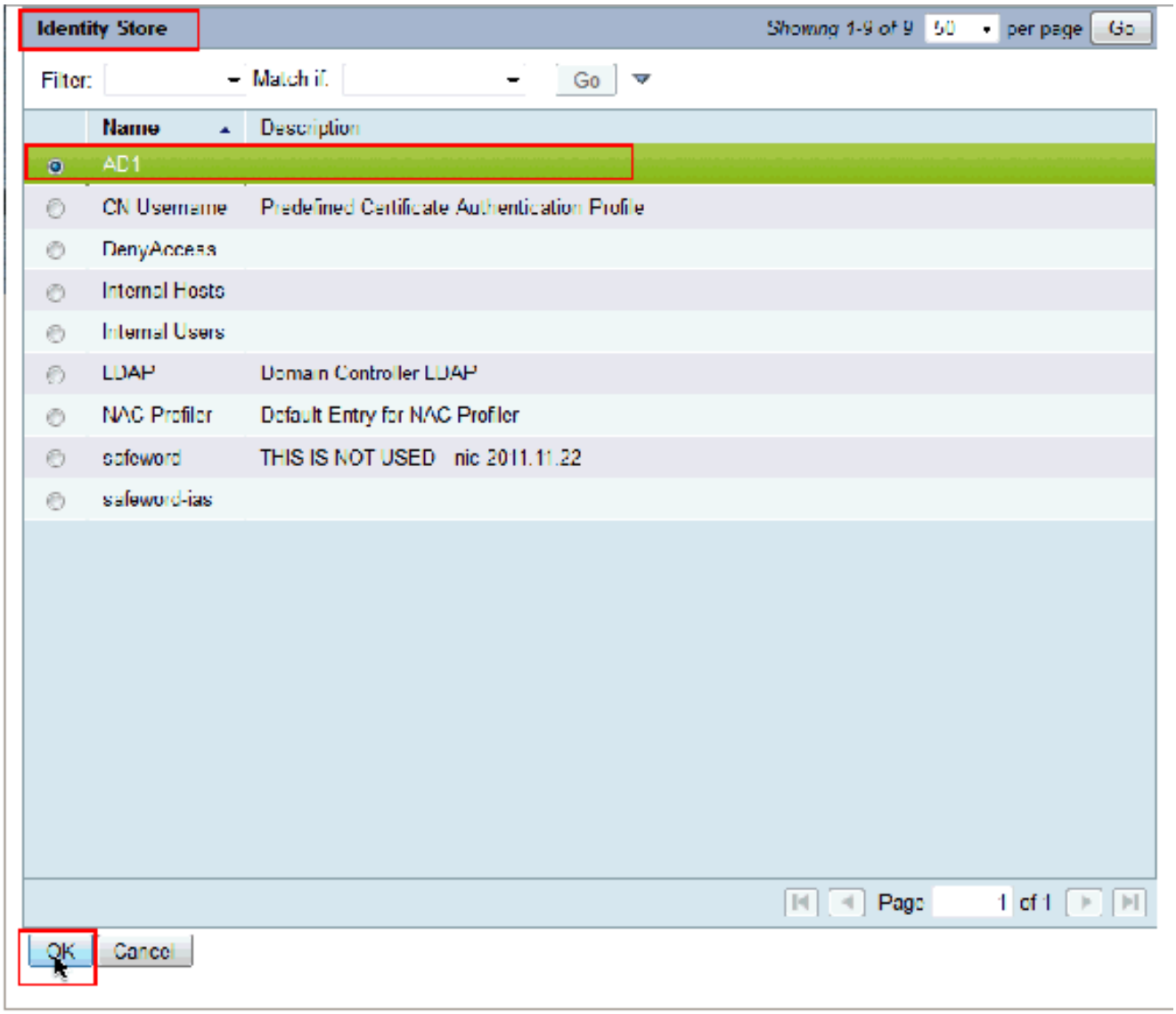
6. Elija Access Policies > Access Services > Service Selection Rules e identifique el servicio de acceso, que procesa la autenticación TACACS+. En este ejemplo, es Default Device Admin.



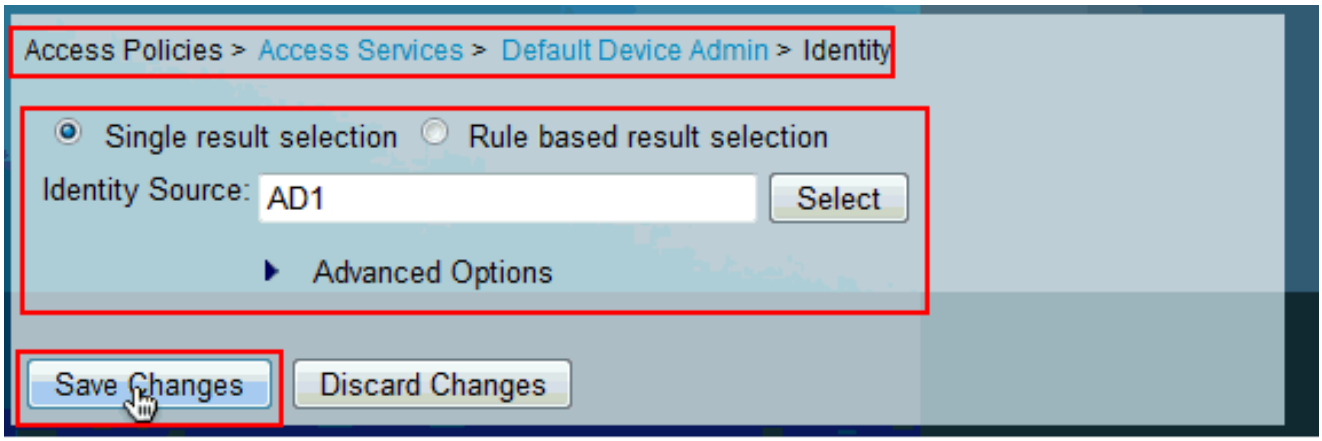
7. Elija Access Policies > Access Services > Default Device Admin > Identity y haga clic en Select junto a Identity Source.



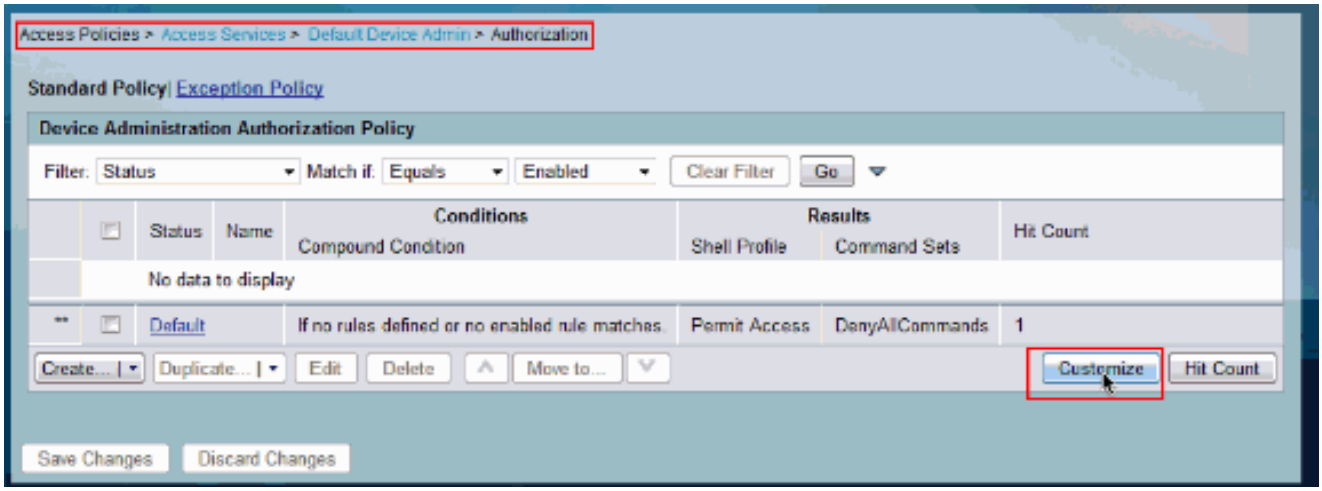
8. Elija AD1 y haga clic en Aceptar.



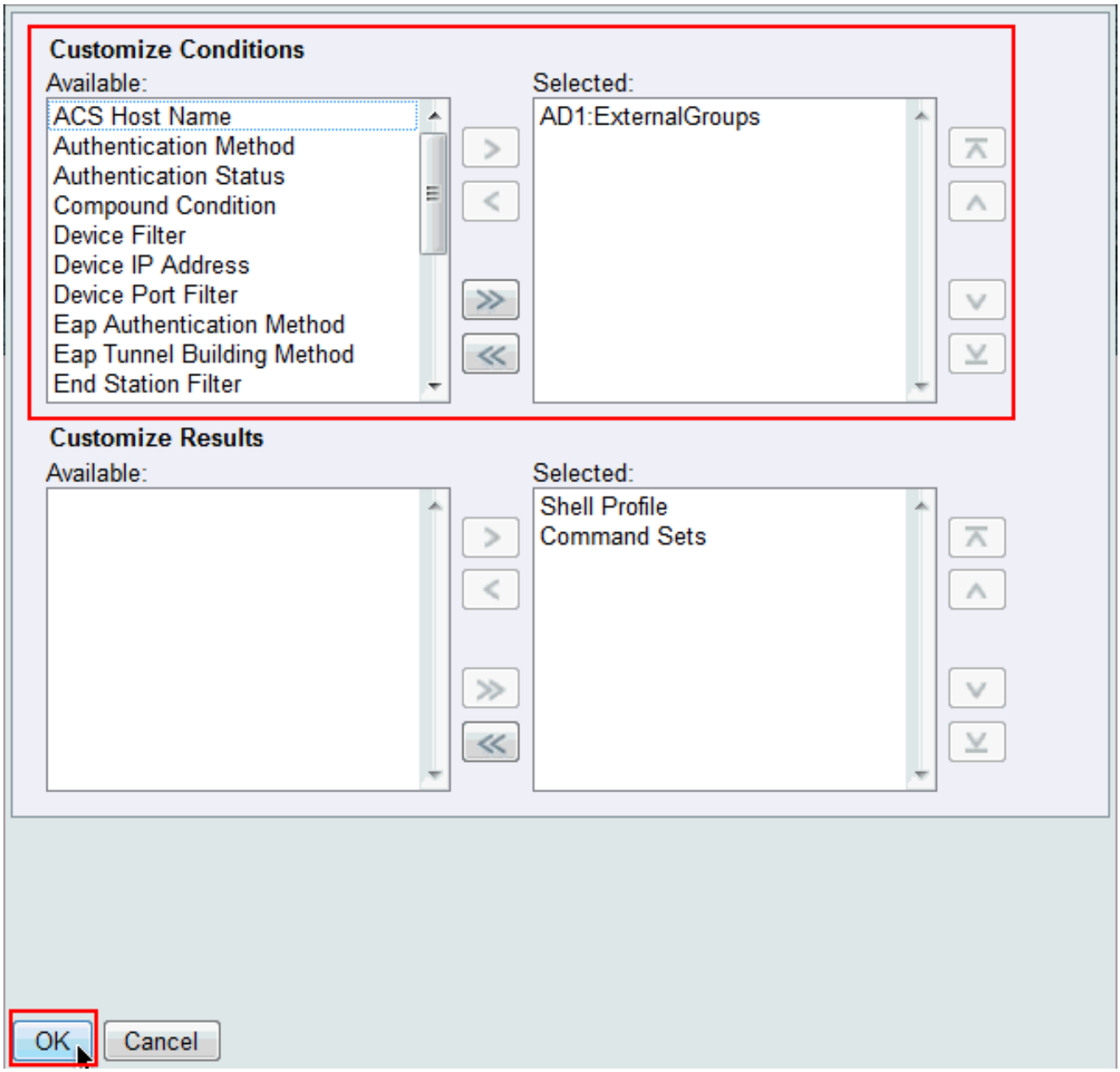
9. Haga clic en Guardar cambios.



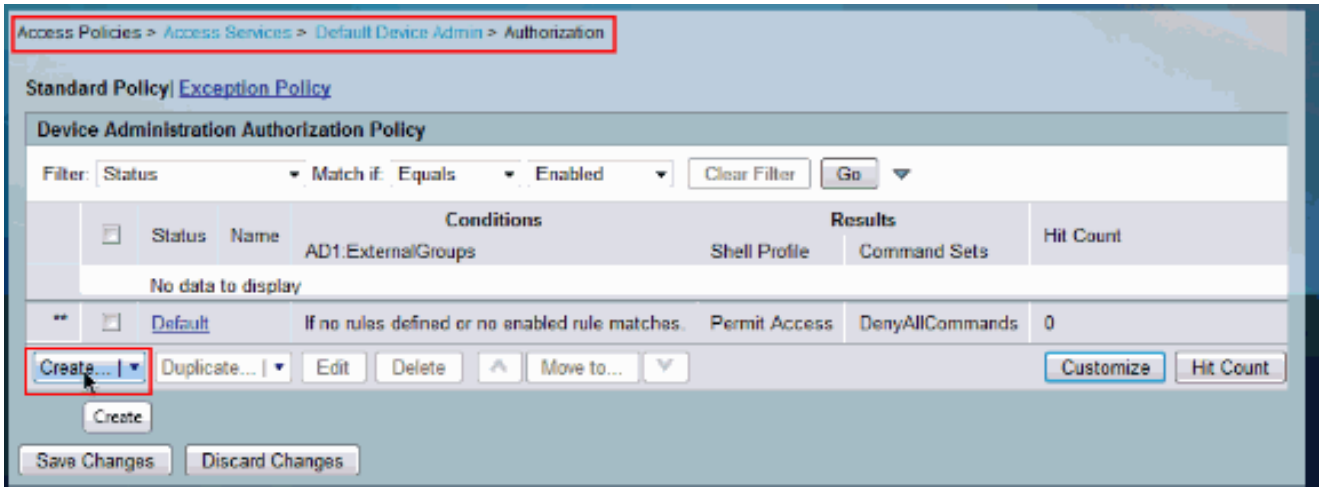
10. Elija Access Policies > Access Services > Default Device Admin > Authorization y haga clic en Customize.



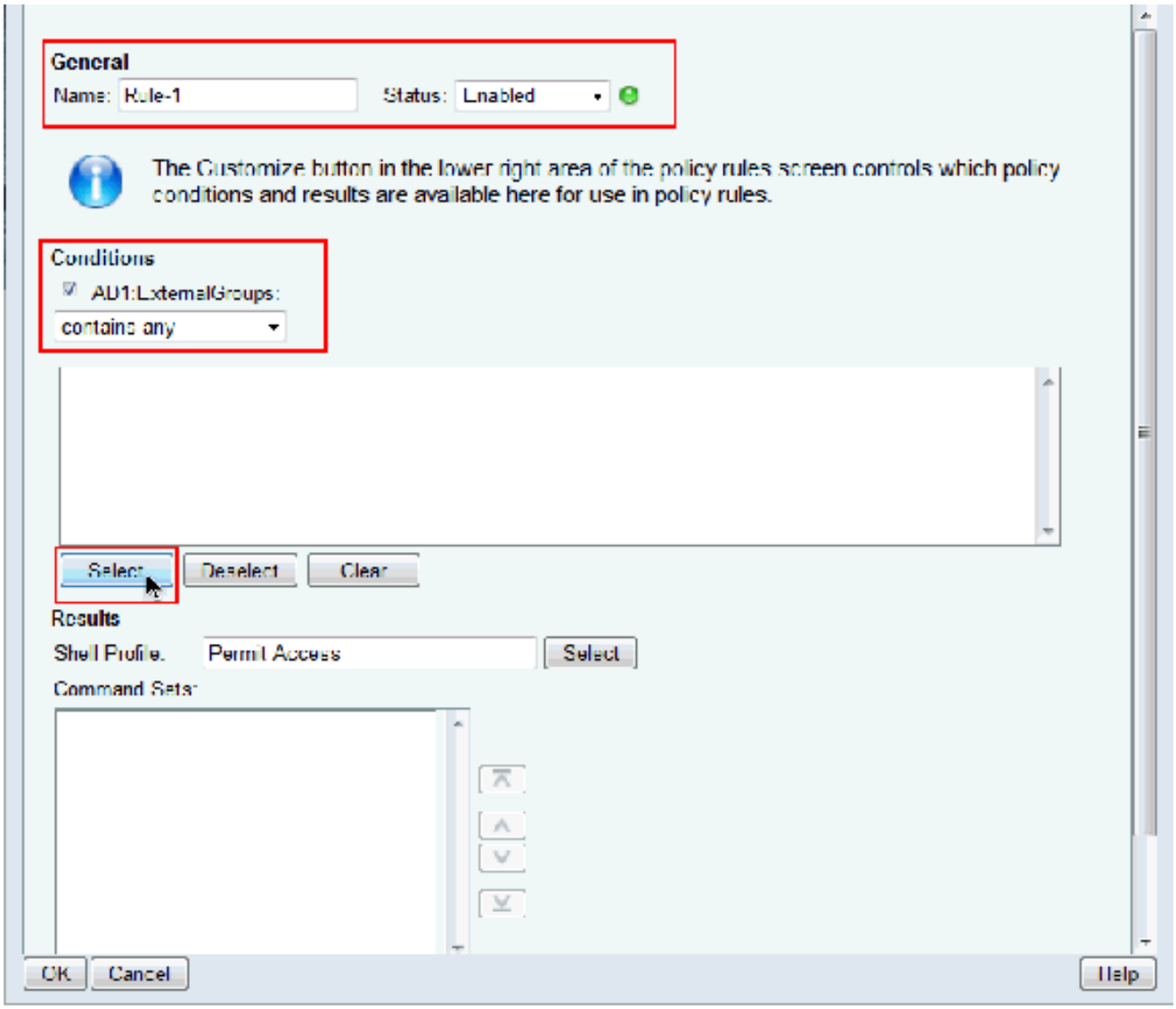
11. Copie AD1:ExternalGroups de la sección Available a Selected de Customize Conditions y luego mueva el perfil de shell y los conjuntos de comandos de la sección Available a Selected de Customize Results. Ahora haga clic en Aceptar.



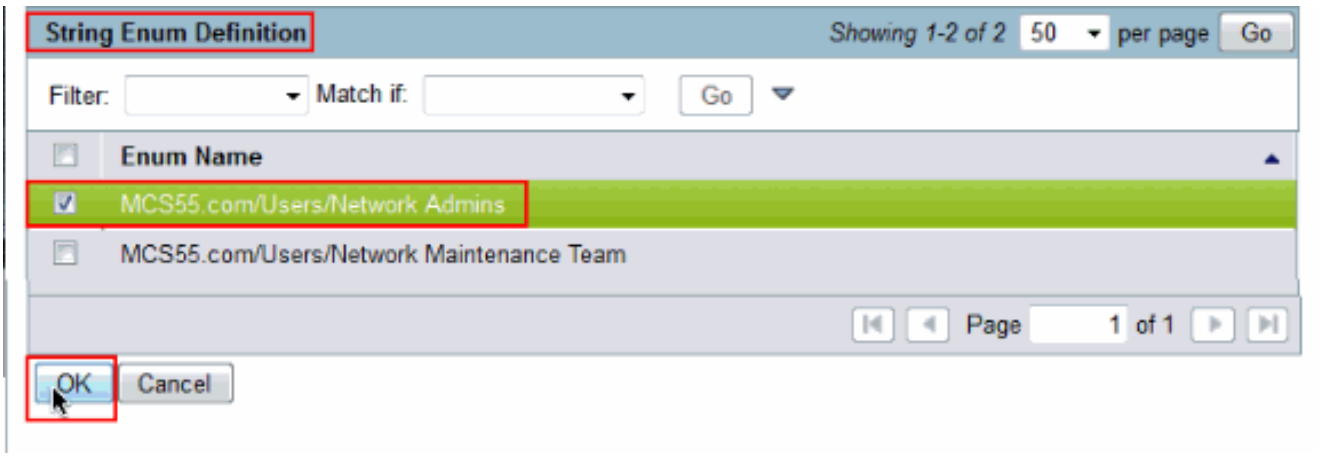
12. Haga clic en Create para crear una nueva regla.



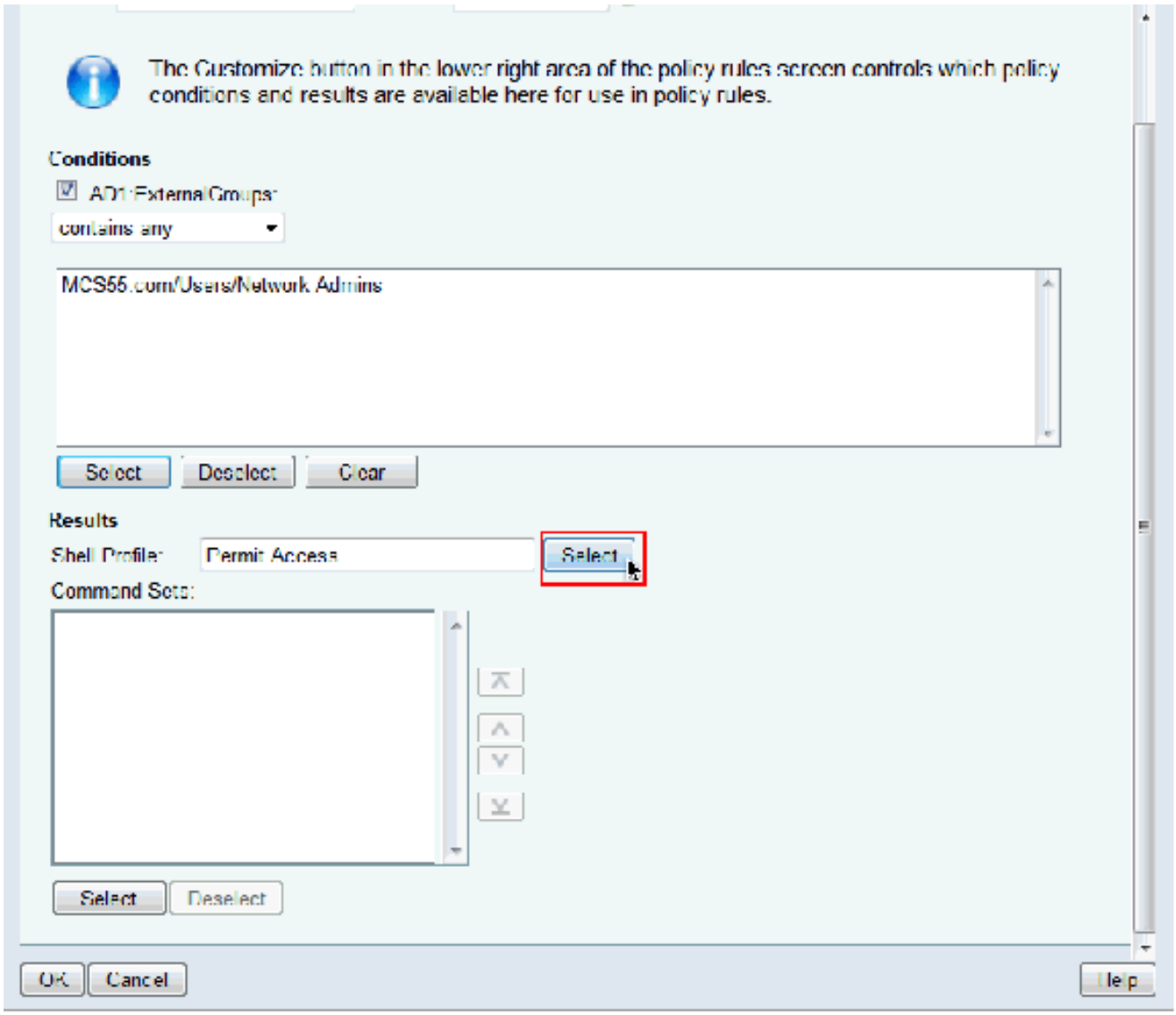
13. Haga clic en Select en la condición AD1:ExternalGroups.



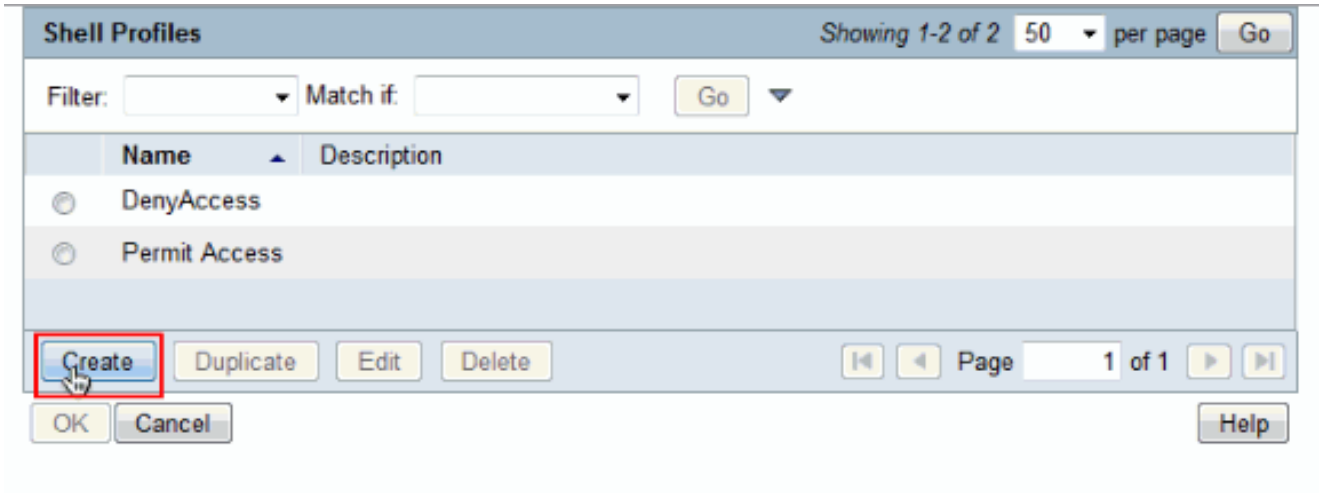
14. Elija el grupo al que desea proporcionar acceso completo en el dispositivo Cisco IOS. Click OK.



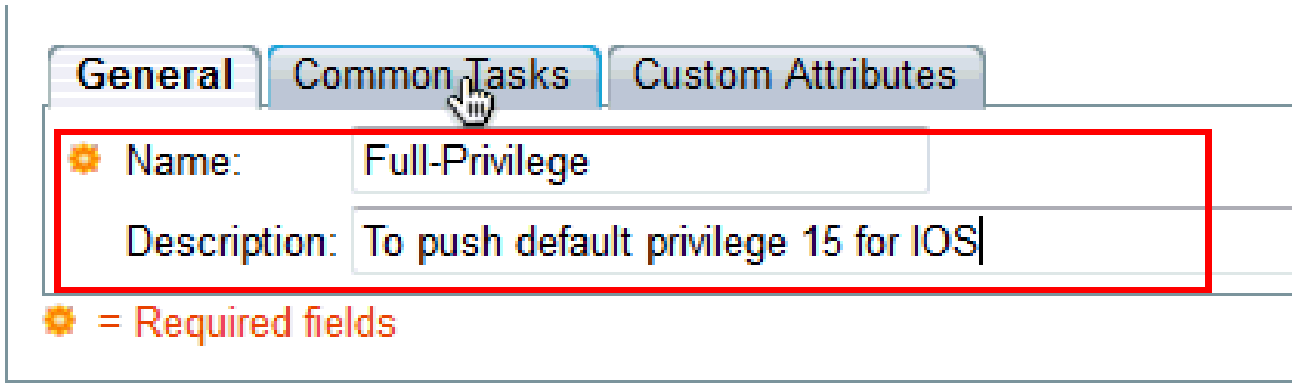
15. Haga clic en Select en el campo Shell Profile.



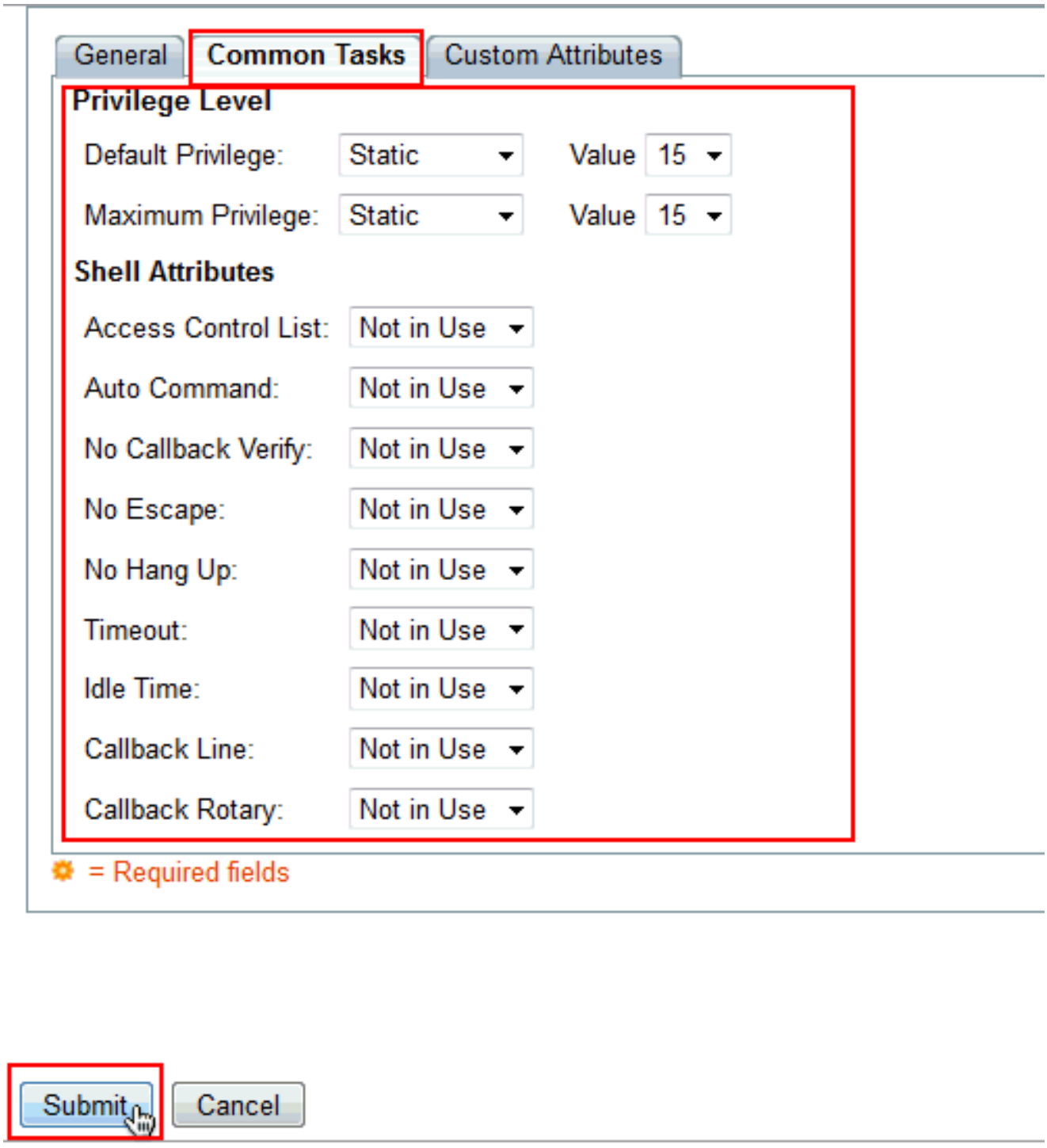
16. Haga clic en Create para crear un nuevo perfil de shell para los usuarios de acceso completo.



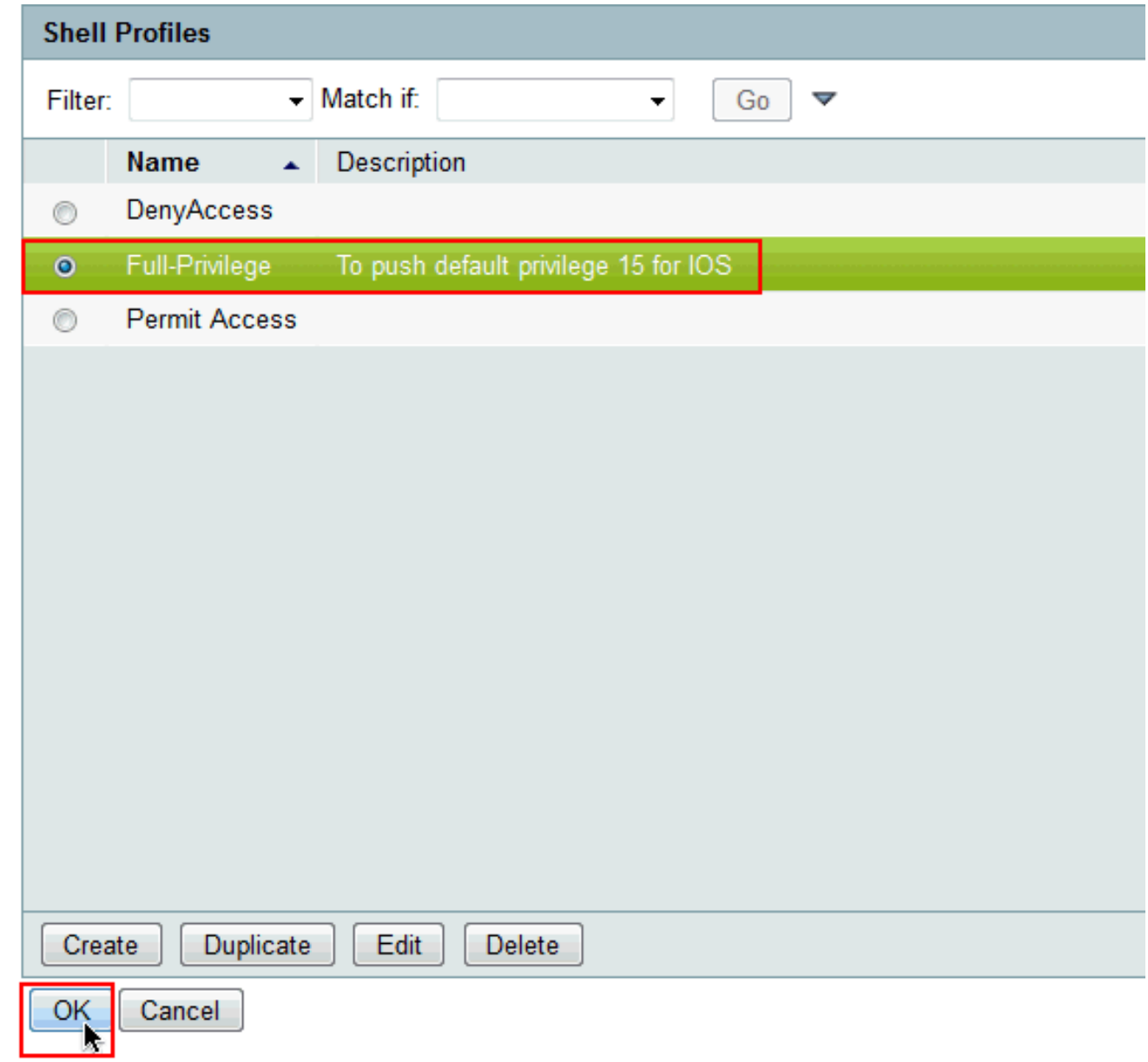
17. Proporcione un nombre y una descripción (opcional) en la ficha General y haga clic en la pestaña Tareas comunes.



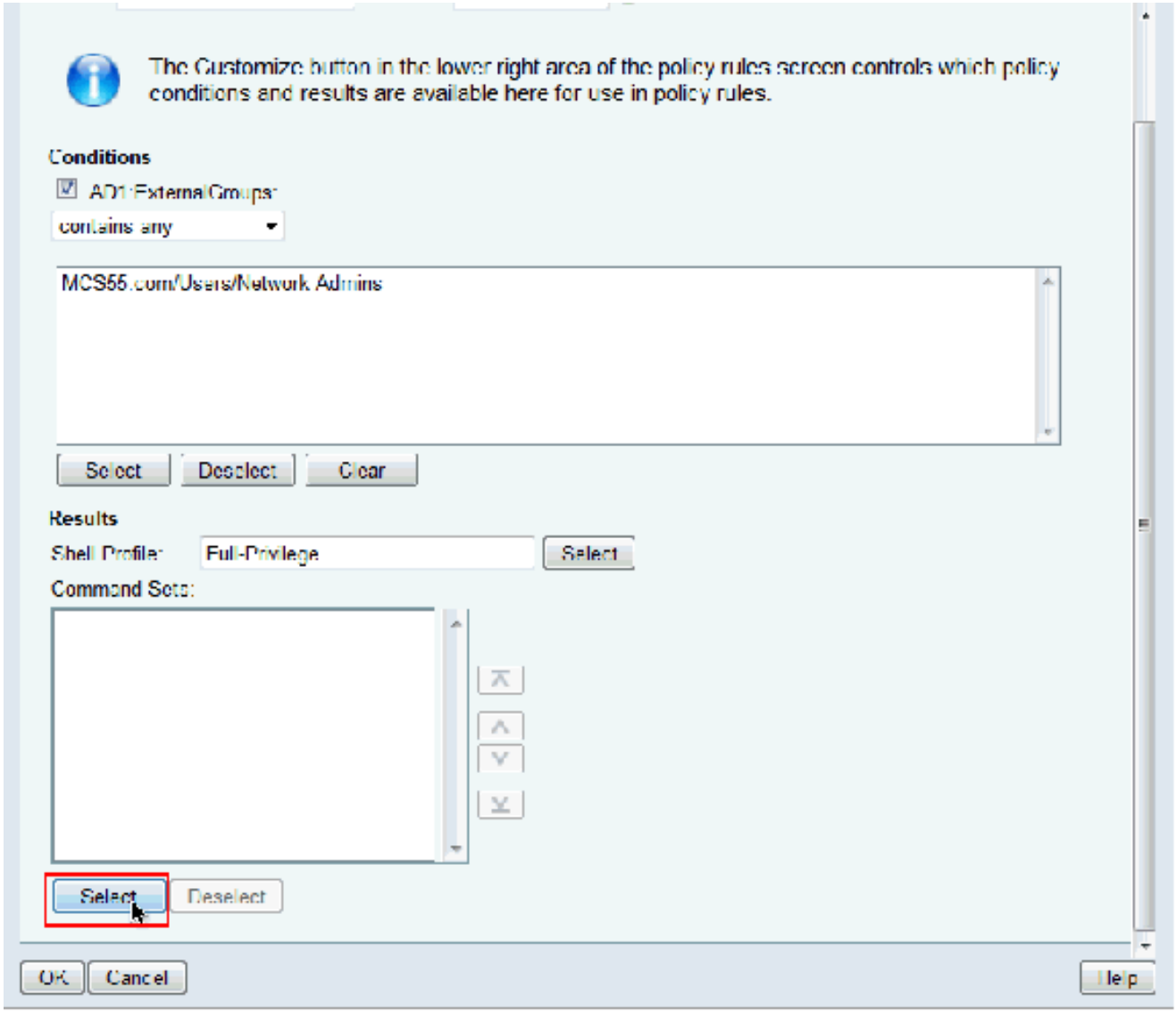
18. Cambie el Privilegio Predeterminado y el Privilegio Máximo a Estático con Valor 15. Haga clic en Submit (Enviar).



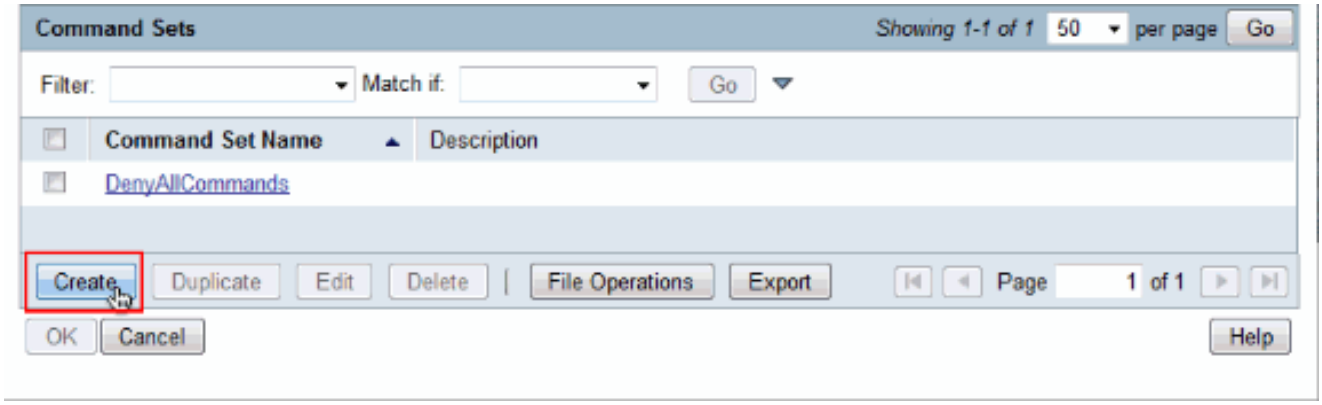
19. Ahora elija el perfil de shell de acceso completo recién creado (Full-Privilege en este ejemplo) y haga clic en OK.



20. Haga clic en Seleccionar en el campo Conjuntos de comandos.

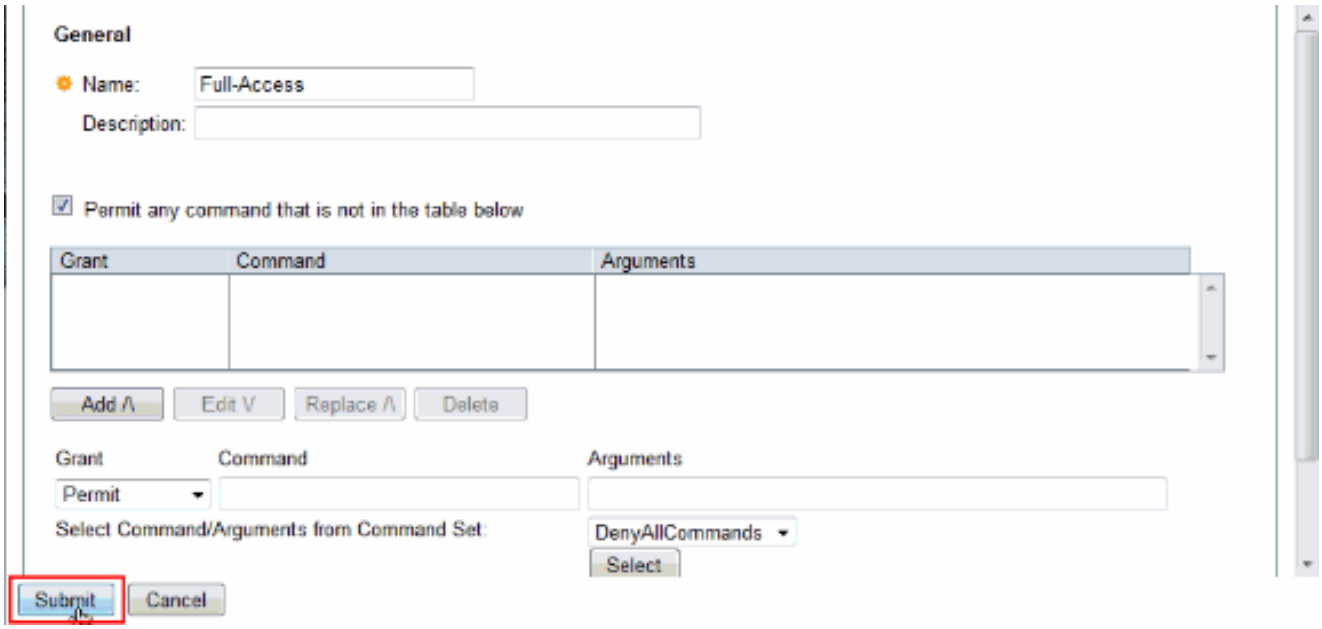


21. Haga clic en Create para crear un nuevo Command Set para los usuarios Full-Access.

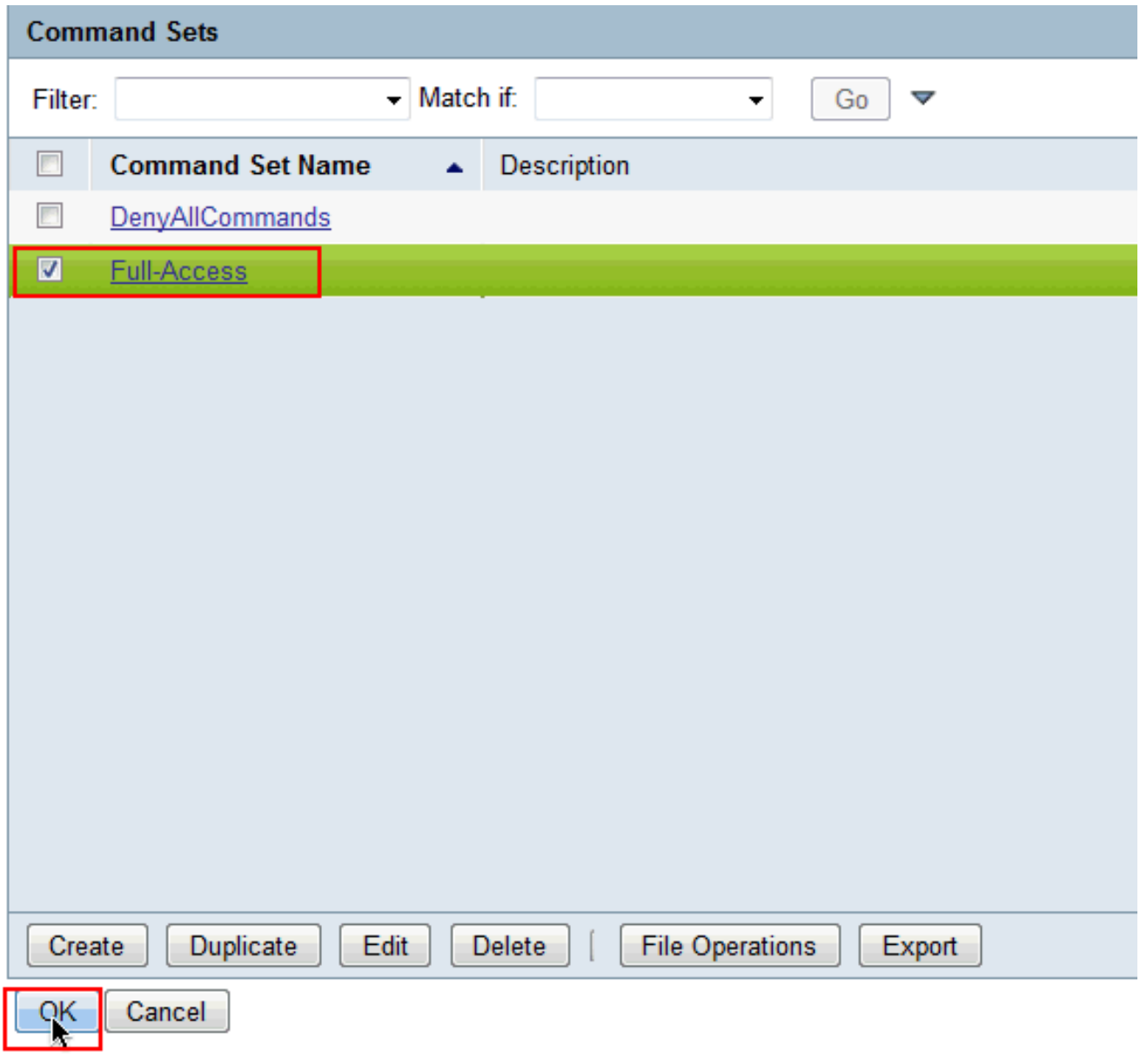


22. Proporcione un Nombre y asegúrese de que la casilla de verificación junto a Permitir cualquier comando que no esté en la tabla siguiente esté marcada. Haga clic en Submit (Enviar).

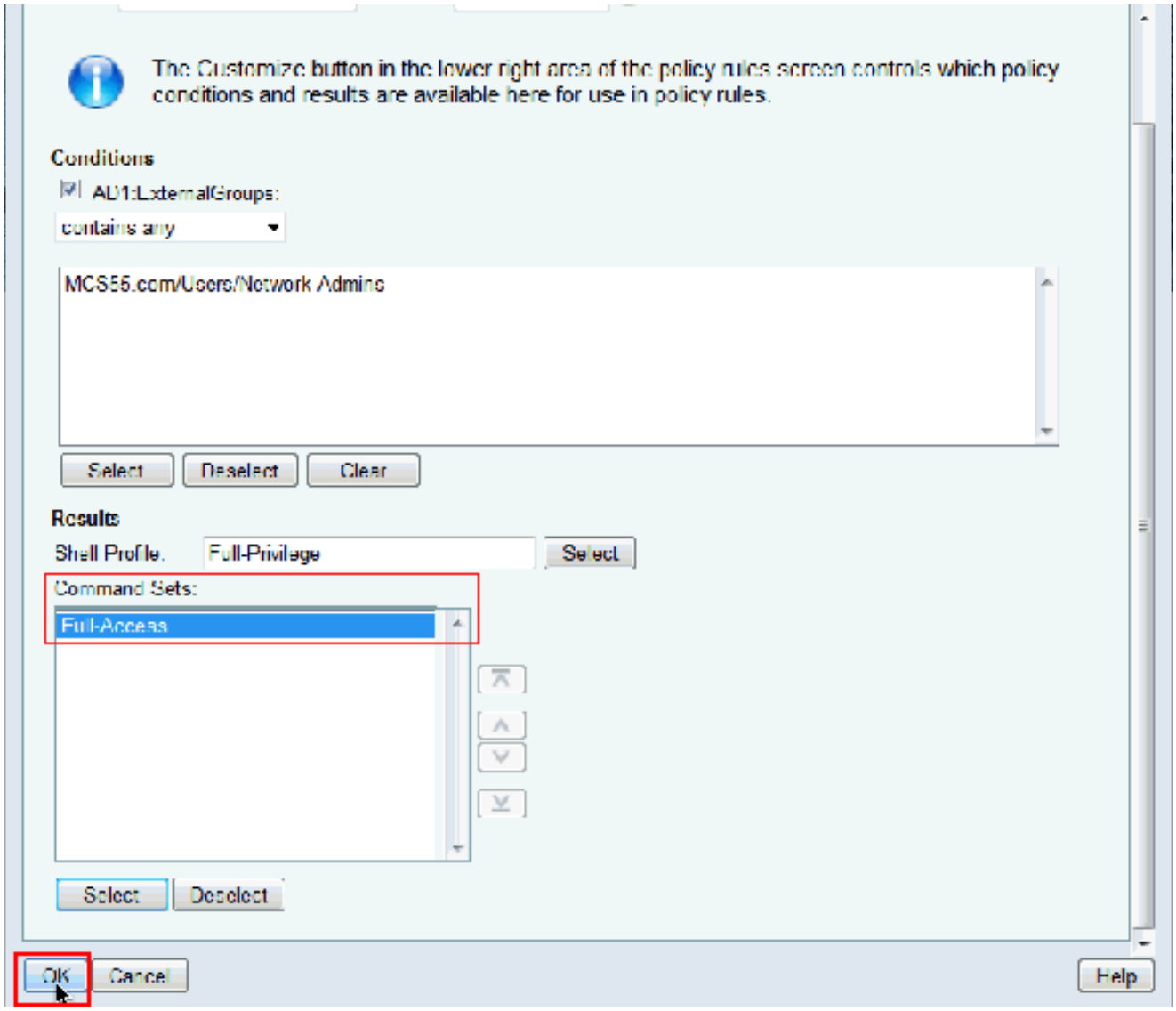
    Nota: Consulte Creación, Duplicación y Edición de Conjuntos de Comandos para la Administración de Dispositivos para obtener más información sobre los Juegos de Comandos.


General
Name:
Full-Access
Description:
Permit any command that is not in the table below
Grant
Command
Arguments
Add /\
Edit V
Replace /\
Delete
Grant
Command
Arguments
Permit
Select Command/Arguments from Command Set:
DenyAllCommands
Select
Submit
Cancel

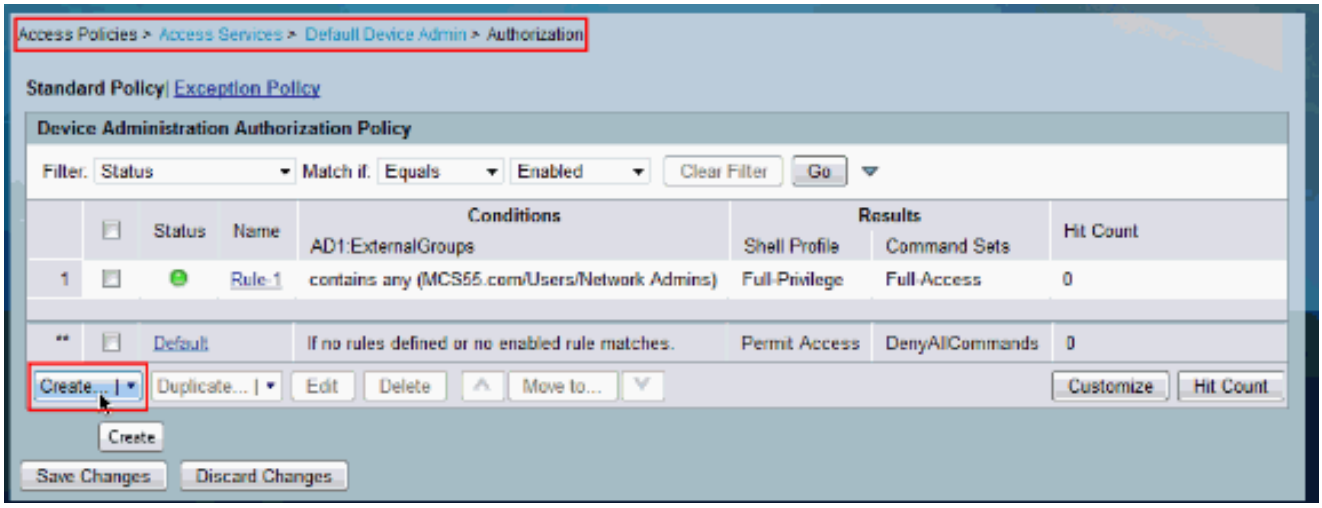
23. Click OK.


Command Sets
Filter:
Match if:
Go
Command Set Name
Description
DenyAllCommands
Full-Access
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel

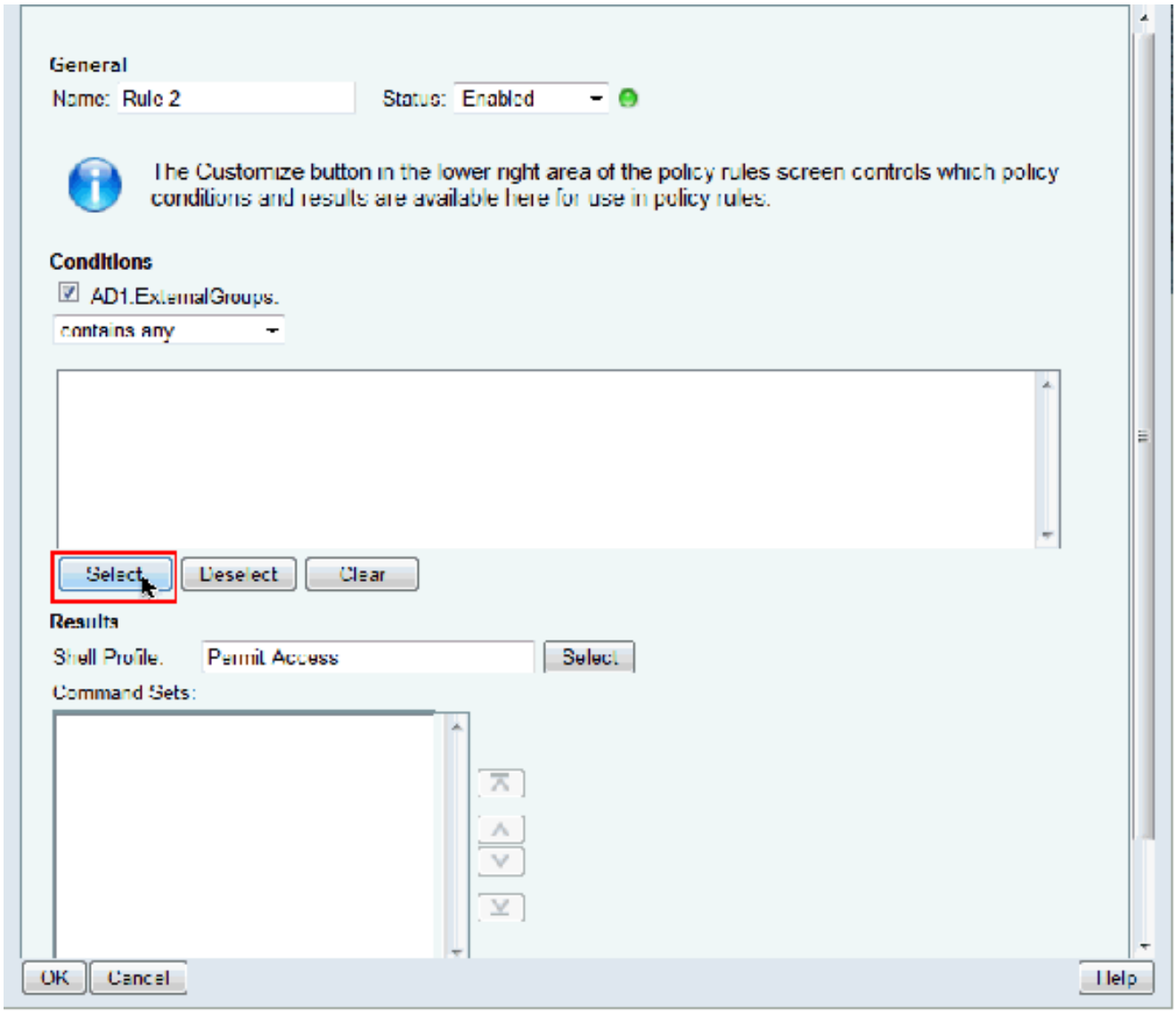
24. Click OK. Esto completa la configuración de la Regla-1.



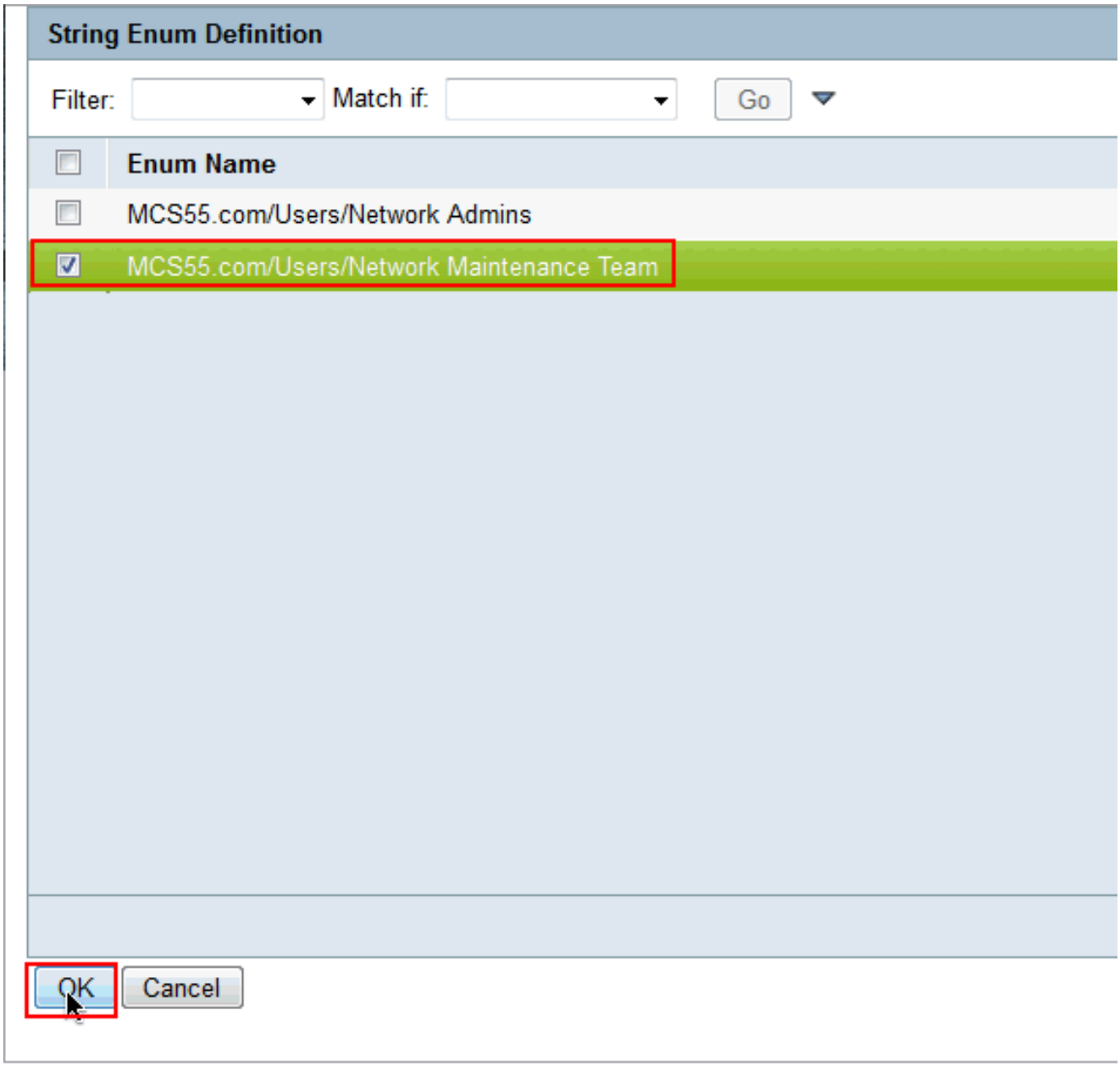
25. Haga clic en Create para crear una nueva regla para los usuarios de acceso limitado.



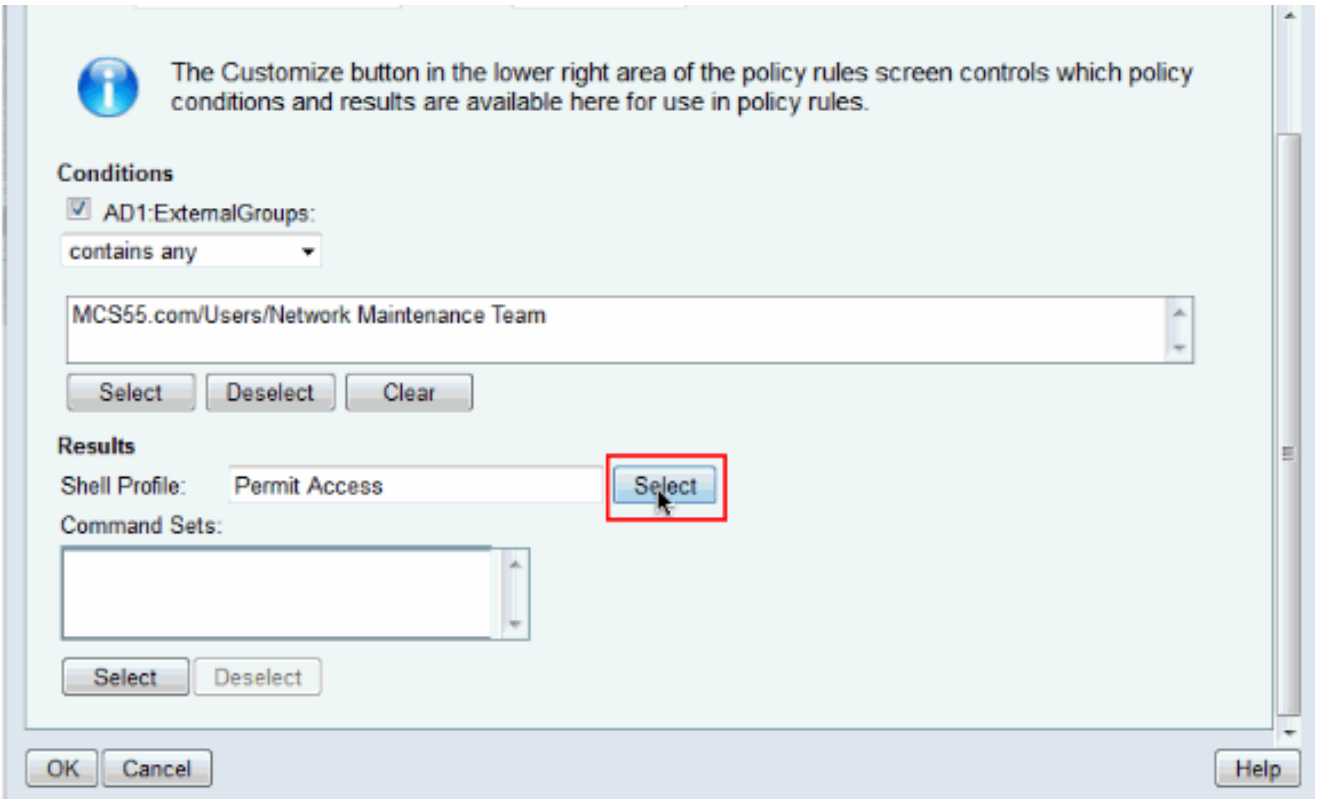
26. Elija AD1:ExternalGroups y haga clic en Select.



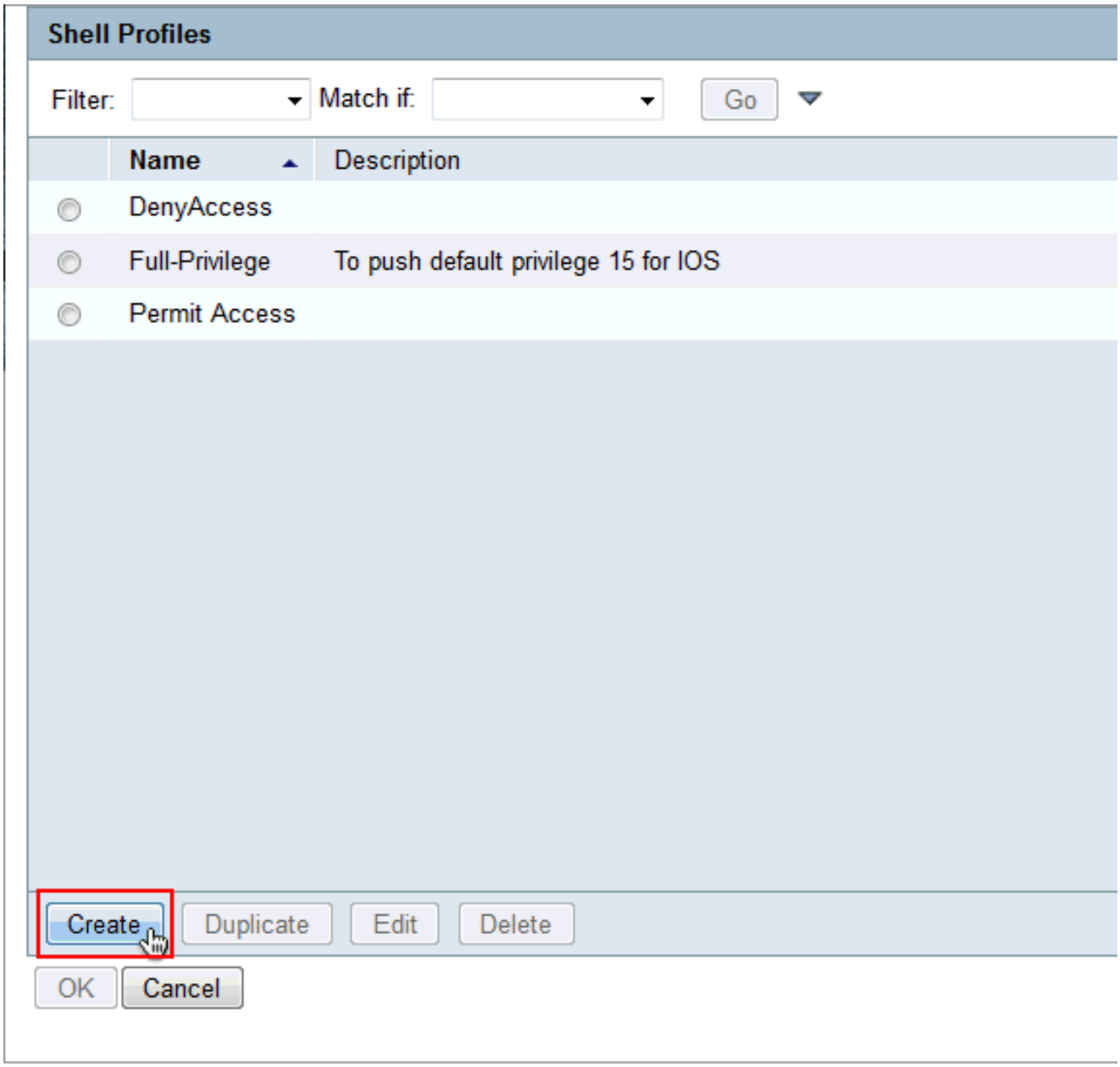
27. Elija el grupo (o grupos) al que desea proporcionar acceso limitado y haga clic en Aceptar.



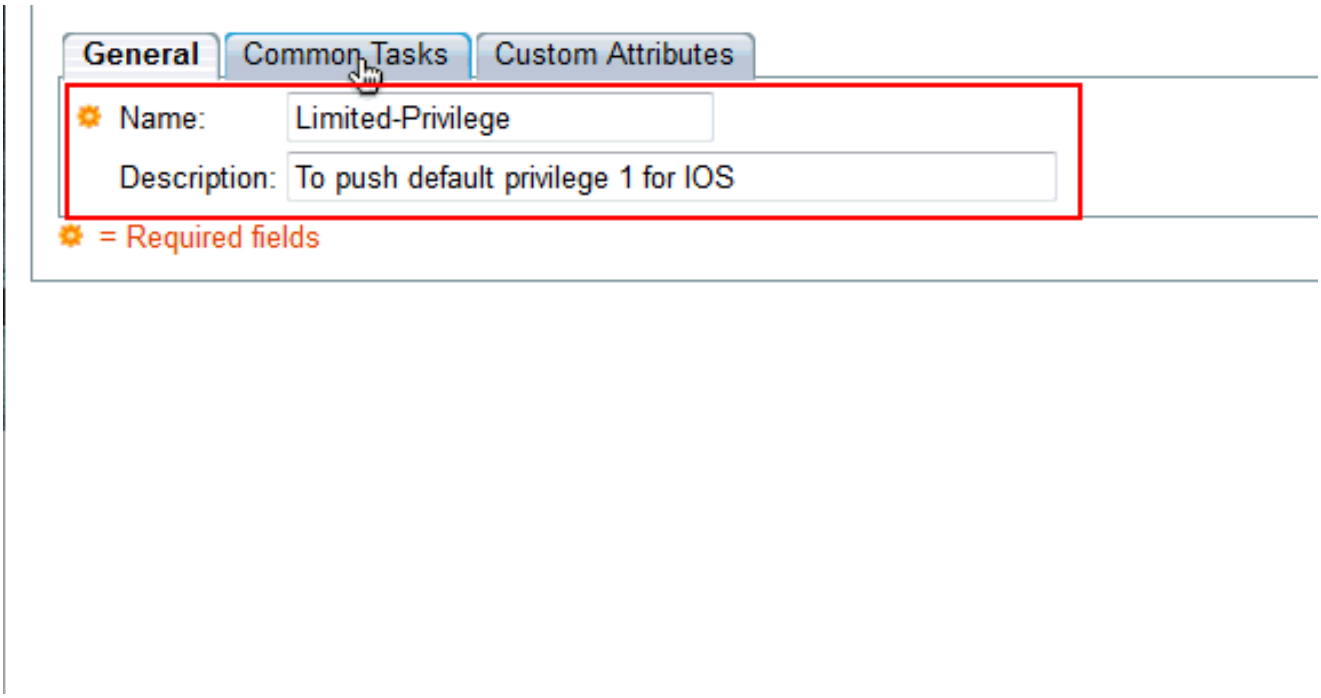
28. Haga clic en Select en el campo Shell Profile.



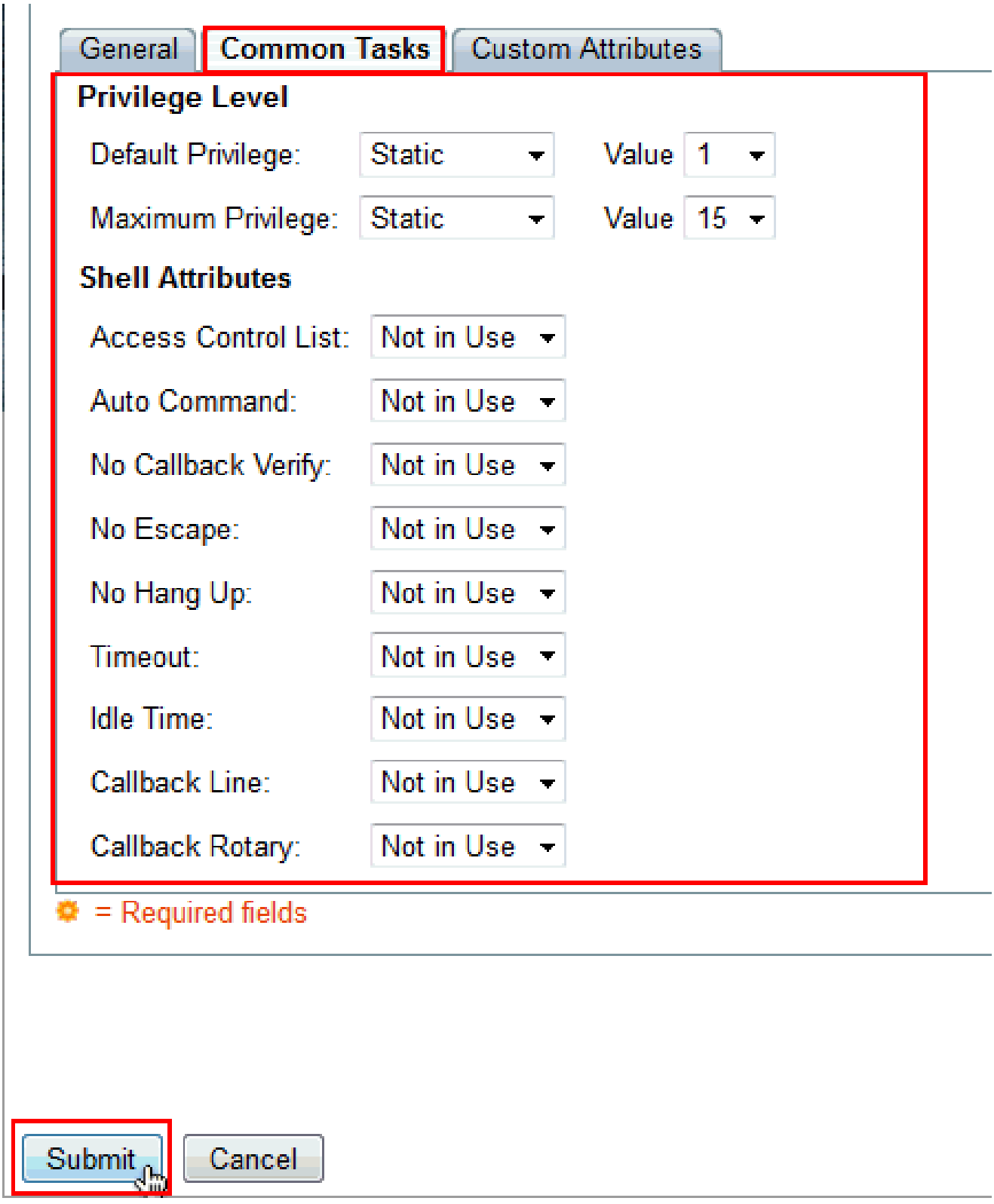
29. Haga clic en Create para crear un nuevo perfil de shell para acceso limitado.



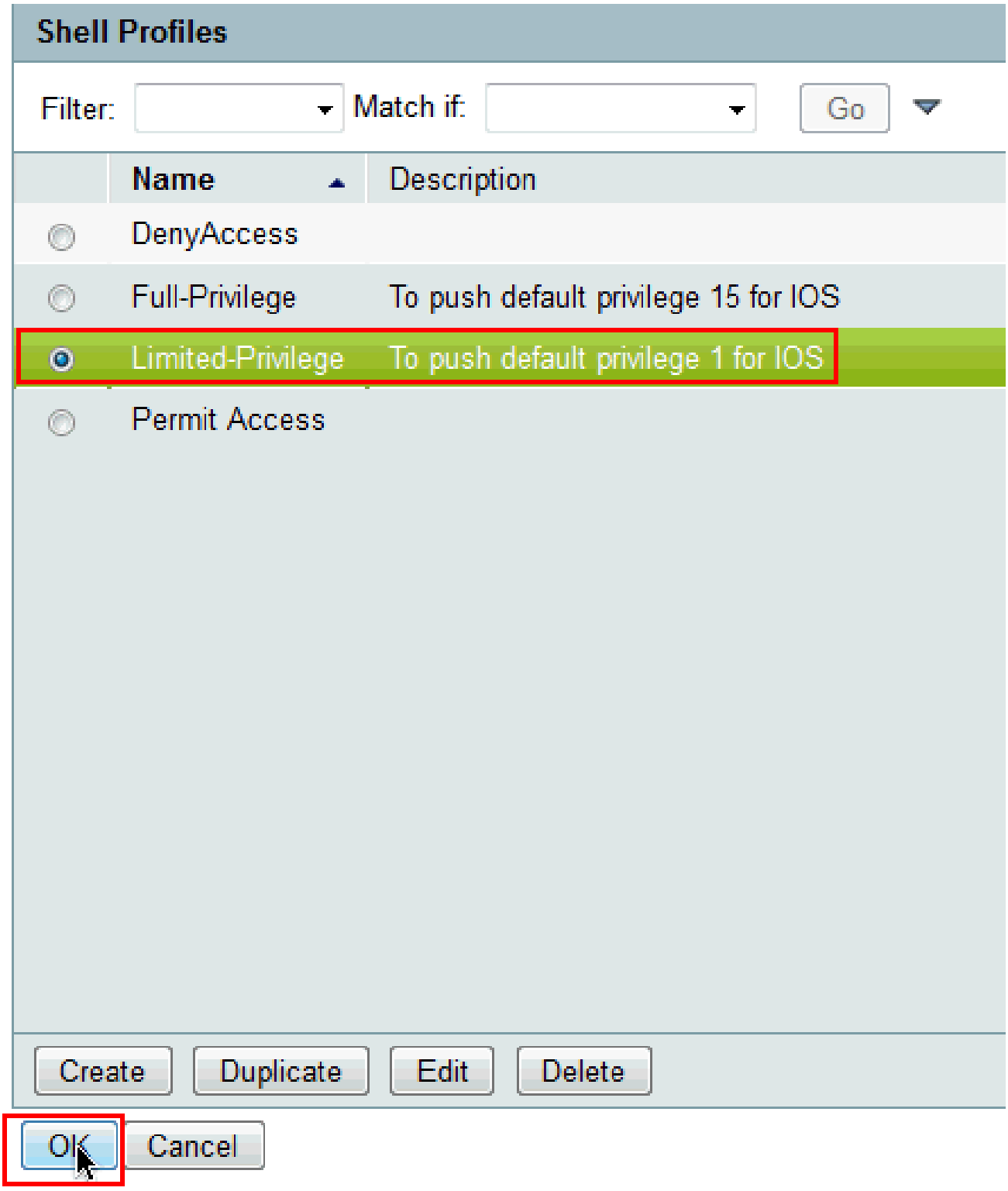
30. Proporcione un Nombre y una Descripción (opcional) en la pestaña General y haga clic en la pestaña Tareas comunes.



31. Cambie el privilegio predeterminado y el privilegio máximo a estático con valores 1 y 15respectivamente. Haga clic en Submit (Enviar).

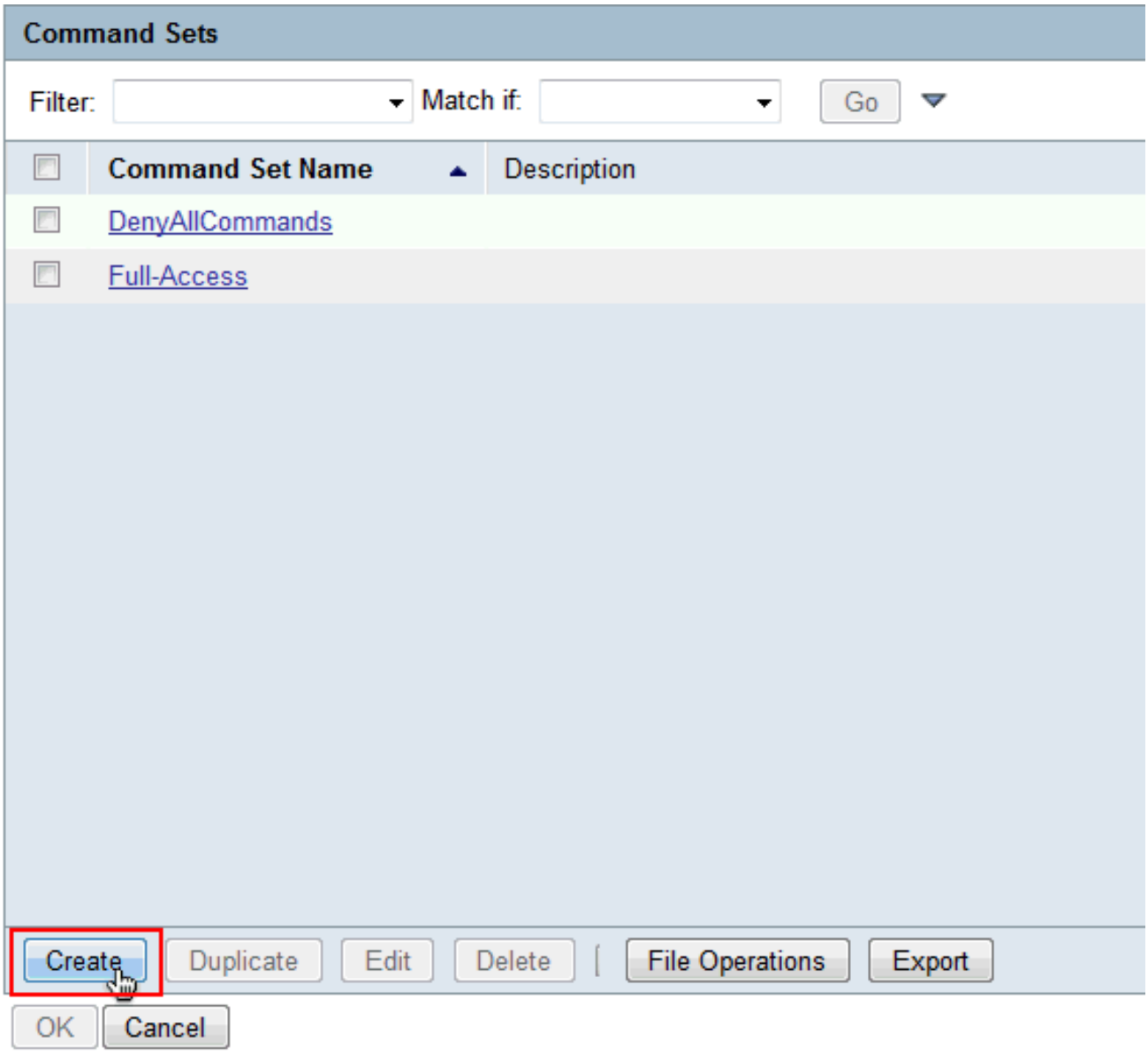

General
Common Tasks
Custom Attributes
Privilege Level
Default Privilege:
Static
Value
1
Maximum Privilege:
Static
Value
15
Shell Attributes
Access Control List:
Not in Use
Auto Command:
Not in Use
No Callback Verify:
Not in Use
No Escape:
Not in Use
No Hang Up:
Not in Use
Timeout:
Not in Use
Idle Time:
Not in Use
Callback Line:
Not in Use
Callback Rotary:
Not in Use
= Required fields
Submit
Cancel

32. Click OK.

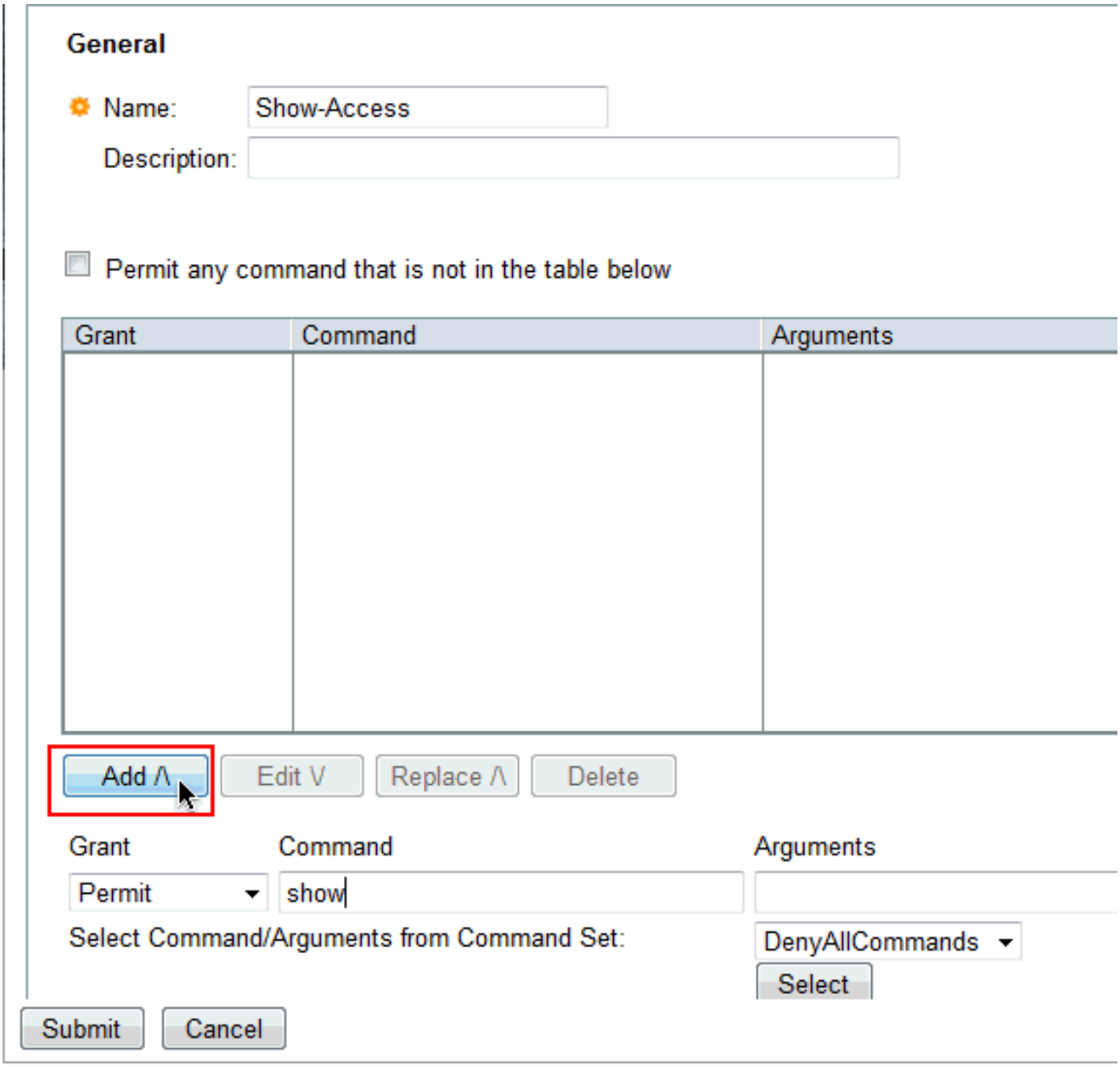


33. Haga clic en Seleccionar en el campo Conjuntos de comandos.

34. Haga clic en Create para crear un nuevo Command Set para el grupo de acceso limitado.

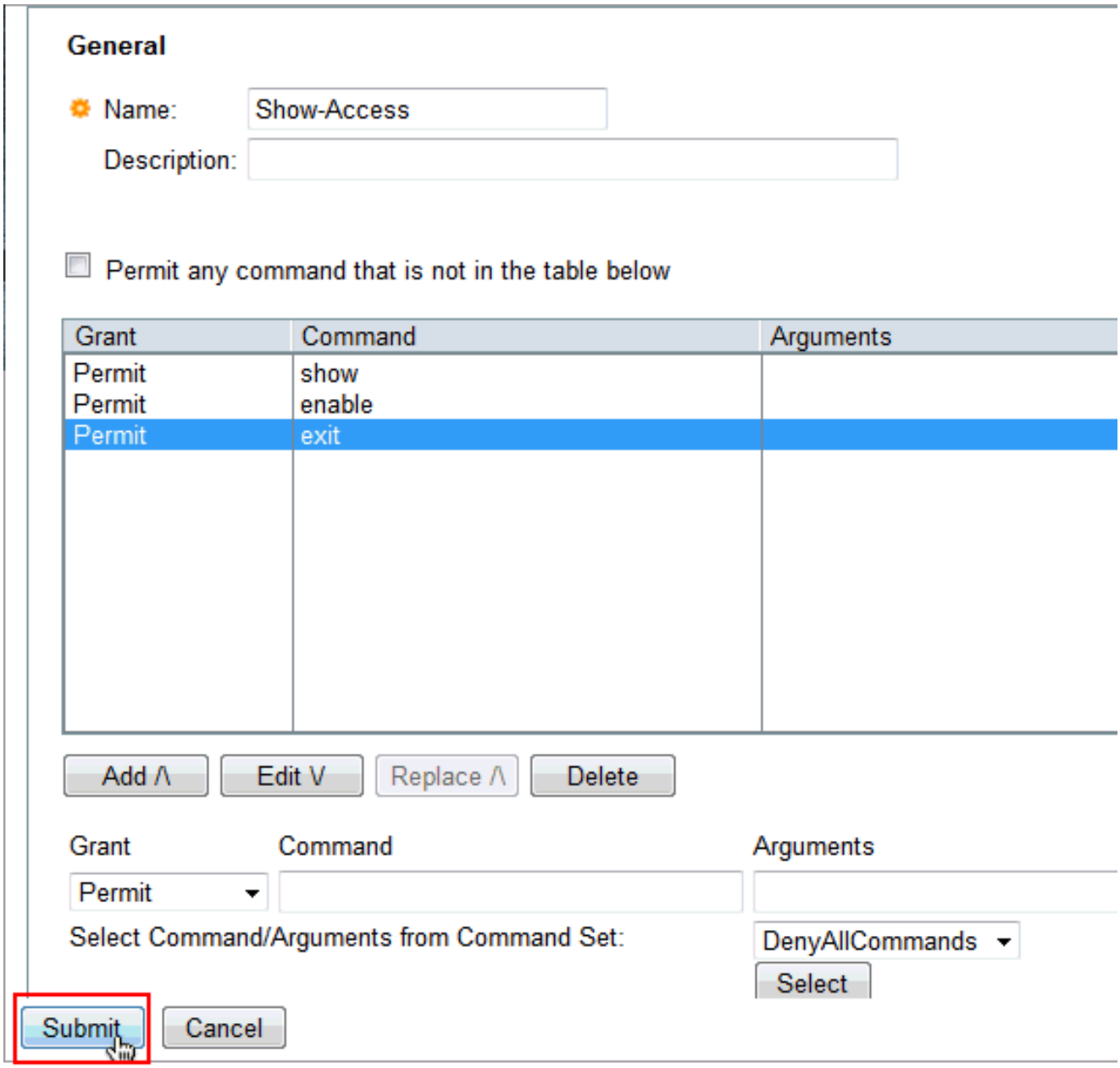


35. Proporcione un Nombre y asegúrese de que la casilla de verificación junto a Permitir cualquier comando que no esté en la tabla siguiente no esté seleccionada. Haga clic en Agregar después de escribir show en el espacio proporcionado en la sección comando y elija Permitir en la sección Conceder para que sólo se permitan los comandos show para los usuarios del grupo de acceso limitado.

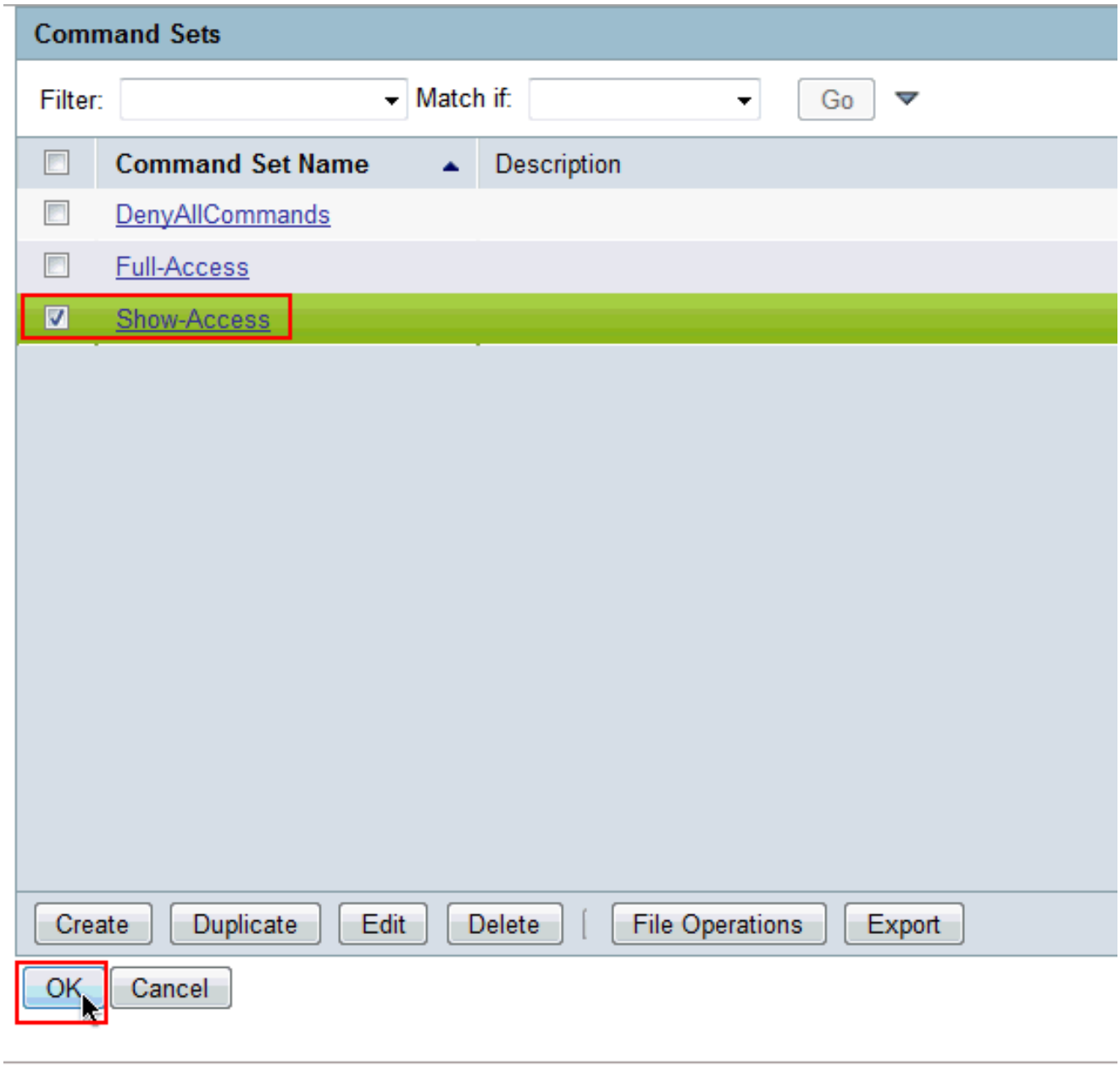


36. De manera similar, agregue cualquier otro comando que se permita para los usuarios en el grupo de acceso limitado con el uso de Add. Haga clic en Submit (Enviar).

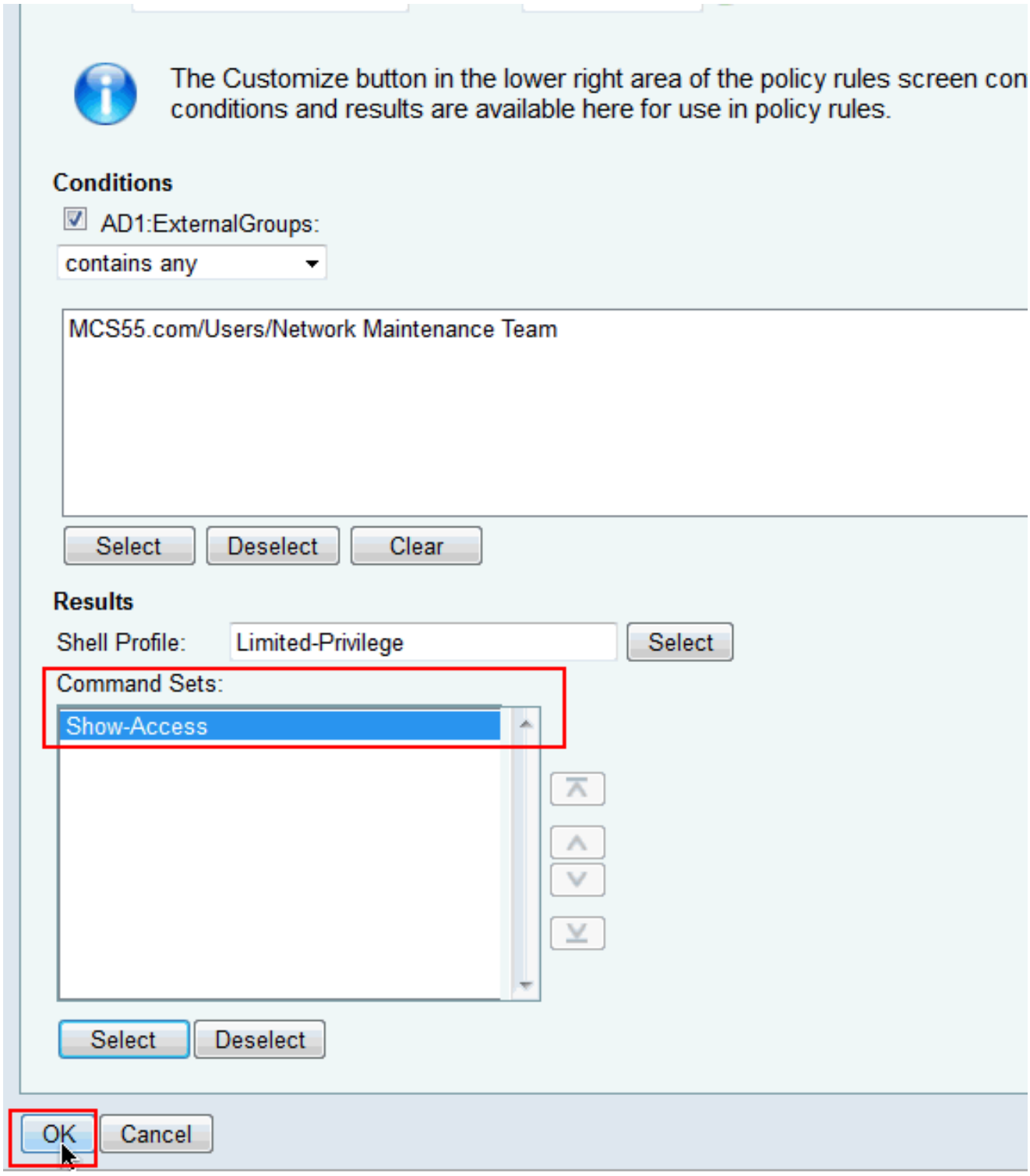
    Nota: Consulte Creación, Duplicación y Edición de Conjuntos de Comandos para la Administración de Dispositivos para obtener más información sobre los Juegos de Comandos.


General
Name:
Show-Access
Description:
Permit any command that is not in the table below
Grant
Command
Arguments
Permit
show
Permit
enable
Permit
exit
Add /\
Edit V
Replace /\
Delete
Grant
Command
Arguments
Permit
Select Command/Arguments from Command Set:
DenyAllCommands
Select
Submit
Cancel

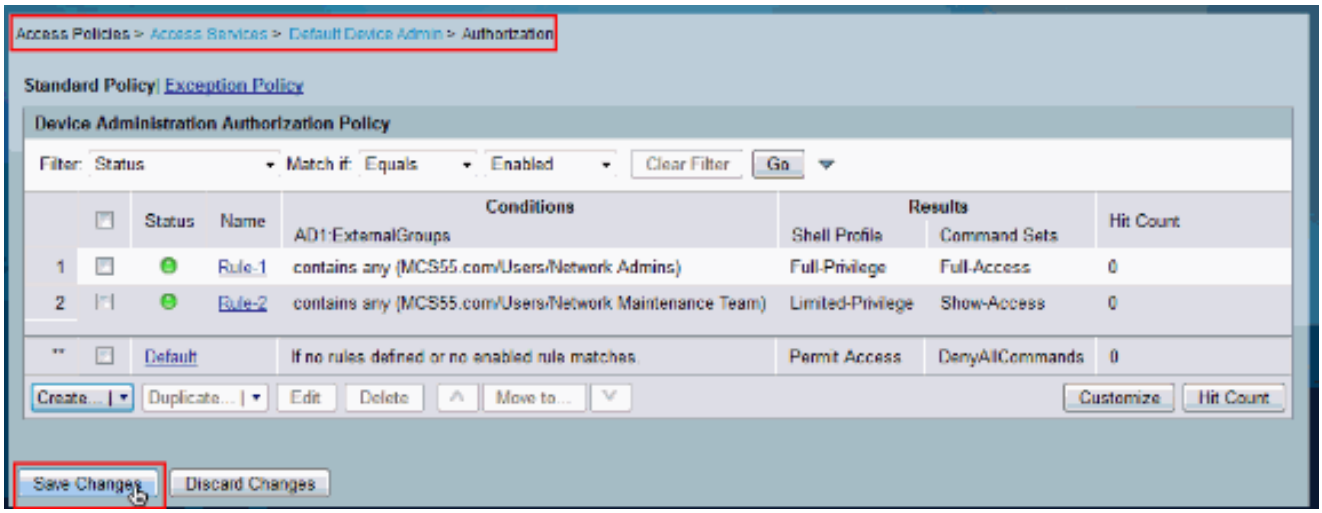
37. Click OK.


Command Sets
Filter:
Match if:
Go
Command Set Name
Description
DenyAllCommands
Full-Access
Show-Access
Create
Duplicate
Edit
Delete
File Operations
Export
OK
Cancel

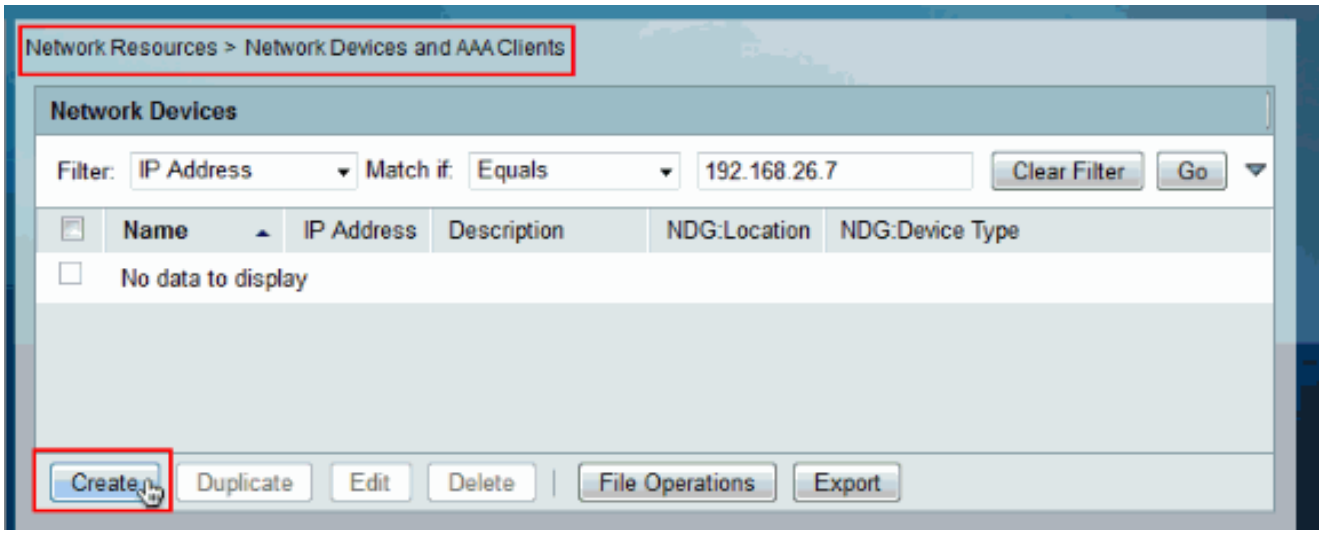
38. Click OK.



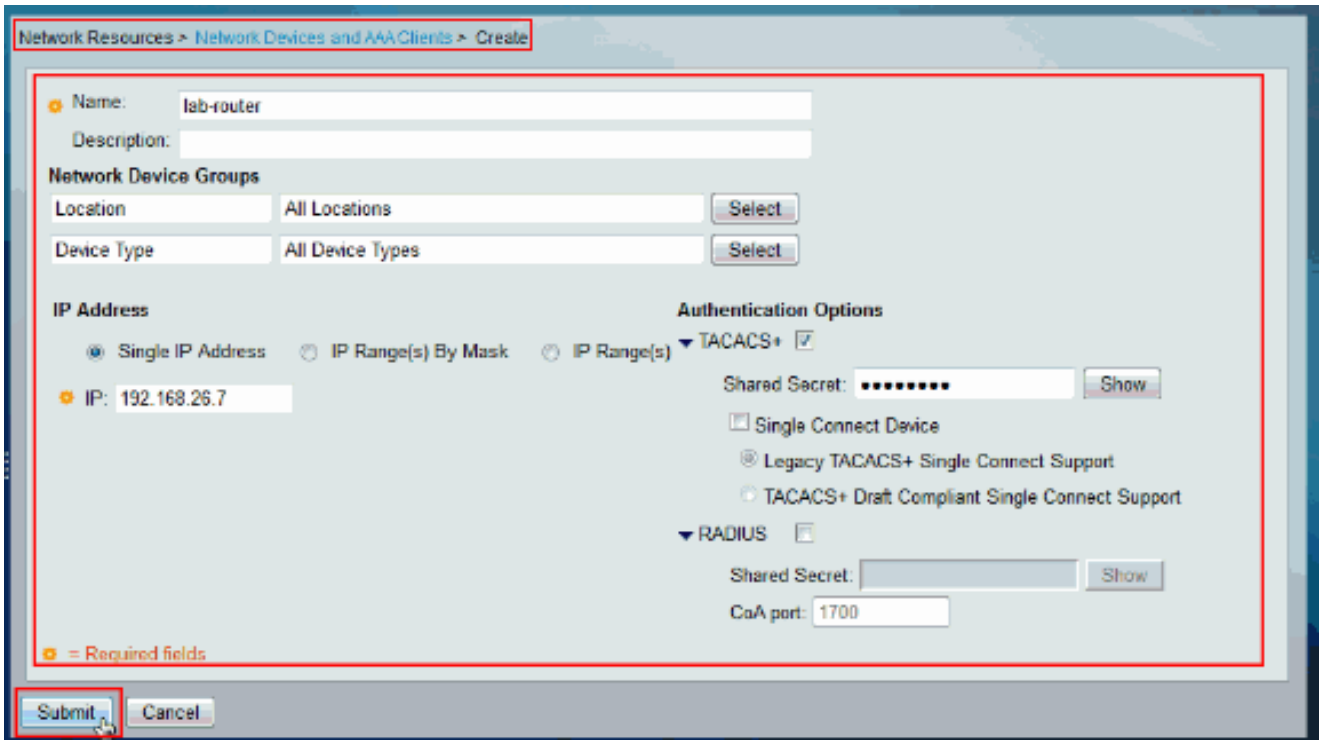
39. Haga clic en Guardar cambios.



40. Haga clic en Create para agregar el dispositivo Cisco IOS como un cliente AAA en el ACS.



41. Proporcione un Nombre, Dirección IP, Secreto compartido para TACACS+ y haga clic en Enviar.



Configuración del dispositivo Cisco IOS para autenticación y autorización

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

1. Cree un usuario local con privilegios completos para el repliegue con el comando username como se muestra aquí:

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

2. Proporcione la dirección IP del ACS para habilitar 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 coincidir con la clave secreta compartida proporcionada en el ACS para este dispositivo Cisco IOS.

3. Pruebe la disponibilidad del servidor TACACS con el comando test aaa como se muestra.

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

```
User was successfully authenticated.
```

El resultado del comando anterior muestra que el servidor TACACS es accesible y que el usuario se ha autenticado correctamente.

Nota: Usuario1 y contraseña xxx pertenecen a AD. Si la prueba falla, asegúrese de que Shared-Secret proporcionado en el paso anterior sea correcto.

4. Configure el login y habilite las autenticaciones y luego utilice las autorizaciones Exec y de comando como se muestra aquí:

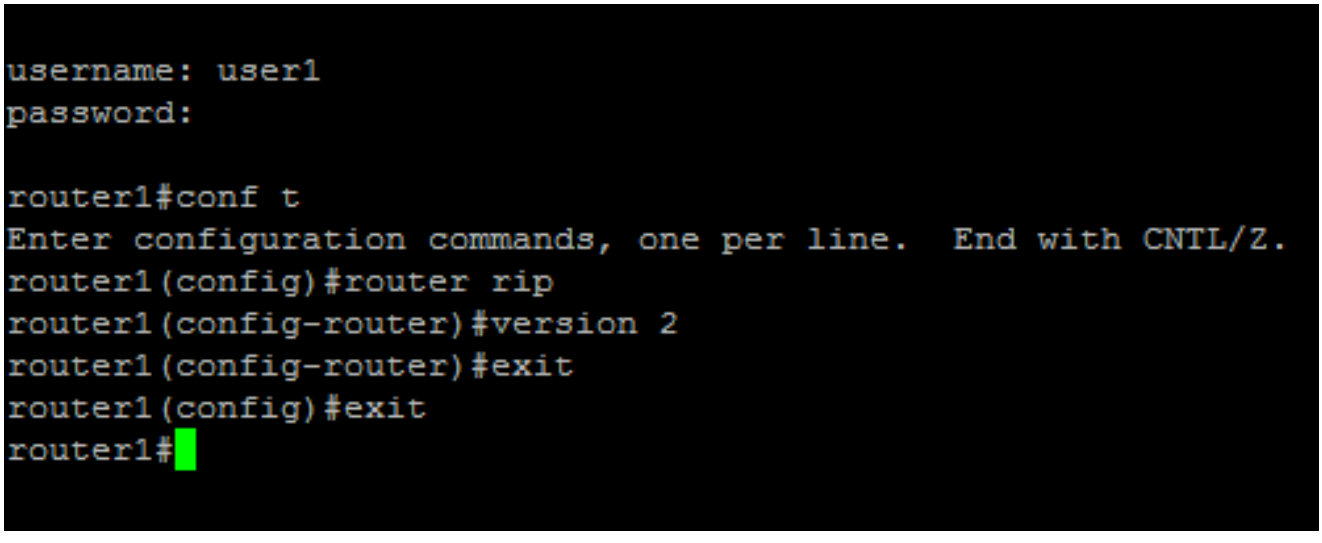
```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization config-commands
```

Nota: Las palabras clave Local y Enable se utilizan para el respaldo al usuario local de Cisco IOS y enable secret respectivamente si el servidor TACACS no está accesible.

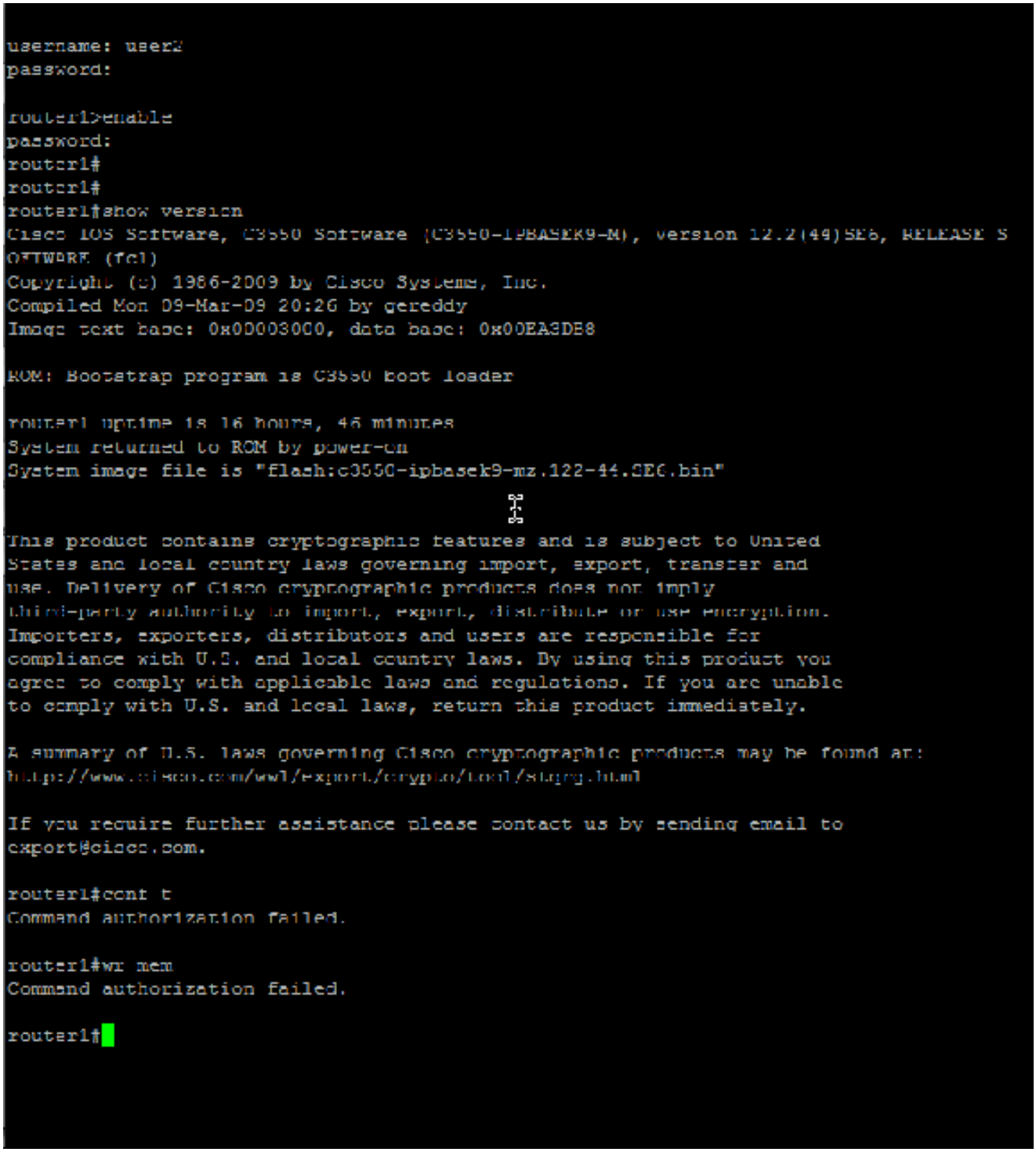
Verificación

Para verificar la autenticación y la autorización de inicio de sesión en el dispositivo Cisco IOS a través de Telnet.

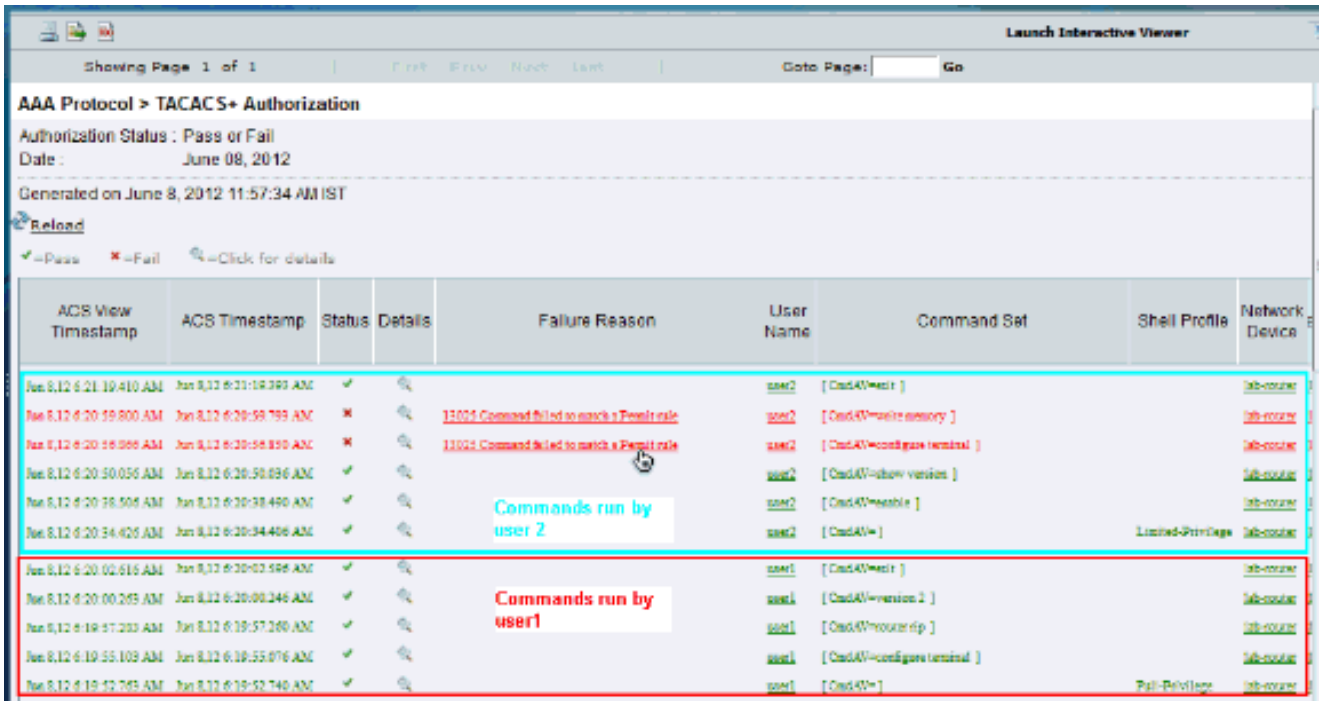
1. Telnet al dispositivo Cisco IOS como usuario1 que pertenece al grupo de acceso completo en AD. El grupo Network Admins es el grupo en AD que está mapeado con el perfil de shell de privilegio completo y el comando de acceso completo establecidos en ACS. Intente ejecutar cualquier comando para asegurarse de que tiene acceso completo.



2. Telnet al dispositivo Cisco IOS como usuario2 que pertenece al grupo de acceso limitado en AD. (El grupo Equipo de mantenimiento de red es el grupo en AD que está asignado al perfil de shell de privilegio limitado y al conjunto de comandos Show-Access en ACS). Si intenta ejecutar cualquier comando que no sea los mencionados en el conjunto de comandos Show-Access, debería recibir el error `Command Authorization Failed`, que muestra que el usuario user2 tiene acceso limitado.



3. Inicie sesión en la GUI de ACS e inicie el visor de Monitoreo e Informes. Elija AAA Protocol > TACACS+Authorization para verificar las actividades realizadas por user1 y user2.



Información Relacionada

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).