ACS 5.x: Konfigurationsbeispiel für die AD-Gruppenmitgliedschaft: TACACS+-Authentifizierung und Befehlsautorisierung

Inhalt

Einführung

Dieses Dokument enthält ein Beispiel für die Konfiguration der TACACS+-Authentifizierung und -Befehlsautorisierung basierend auf der AD-Gruppenmitgliedschaft eines Benutzers mit dem Cisco Secure Access Control System (ACS) 5.x und höher. ACS verwendet Microsoft Active Directory (AD) als externen Identitätsspeicher, um Ressourcen wie Benutzer, Computer, Gruppen und Attribute zu speichern.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- ACS 5.x ist vollständig in die gewünschte AD-Domäne integriert. Wenn der ACS nicht in die gewünschte AD-Domäne integriert ist, lesen Sie ACS 5.x und höher: Integration in Microsoft Active Directory Konfigurationsbeispiel für weitere Informationen, um die Integrationsaufgabe durchzuführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS 5.3
- Cisco IOS® Softwareversion 12.2(44)SE6.**Hinweis:** Diese Konfiguration kann auf allen Cisco IOS-Geräten vorgenommen werden.
- Microsoft Windows Server 2003-Domäne

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

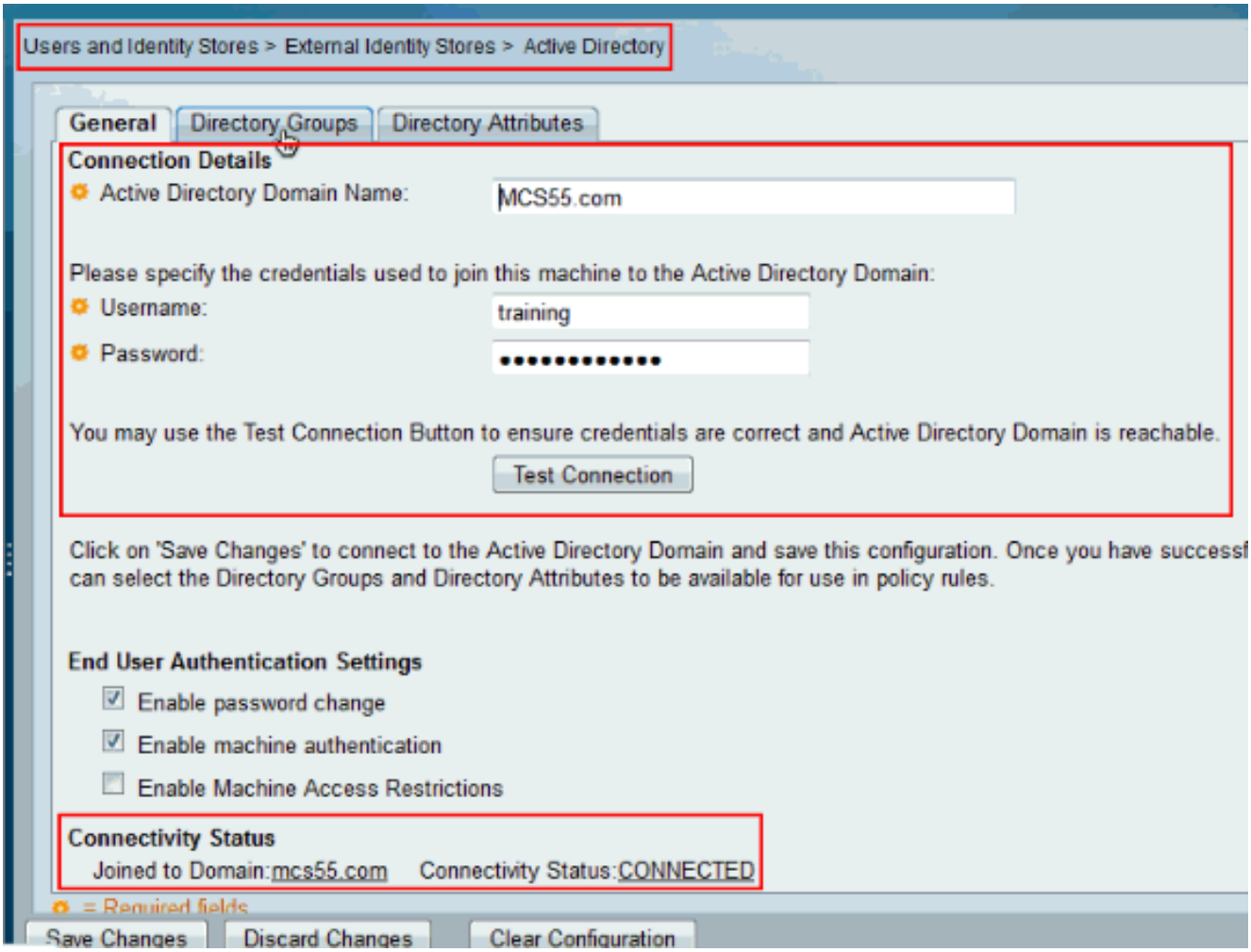
Konfiguration

Konfigurieren von ACS 5.x für Authentifizierung und Autorisierung

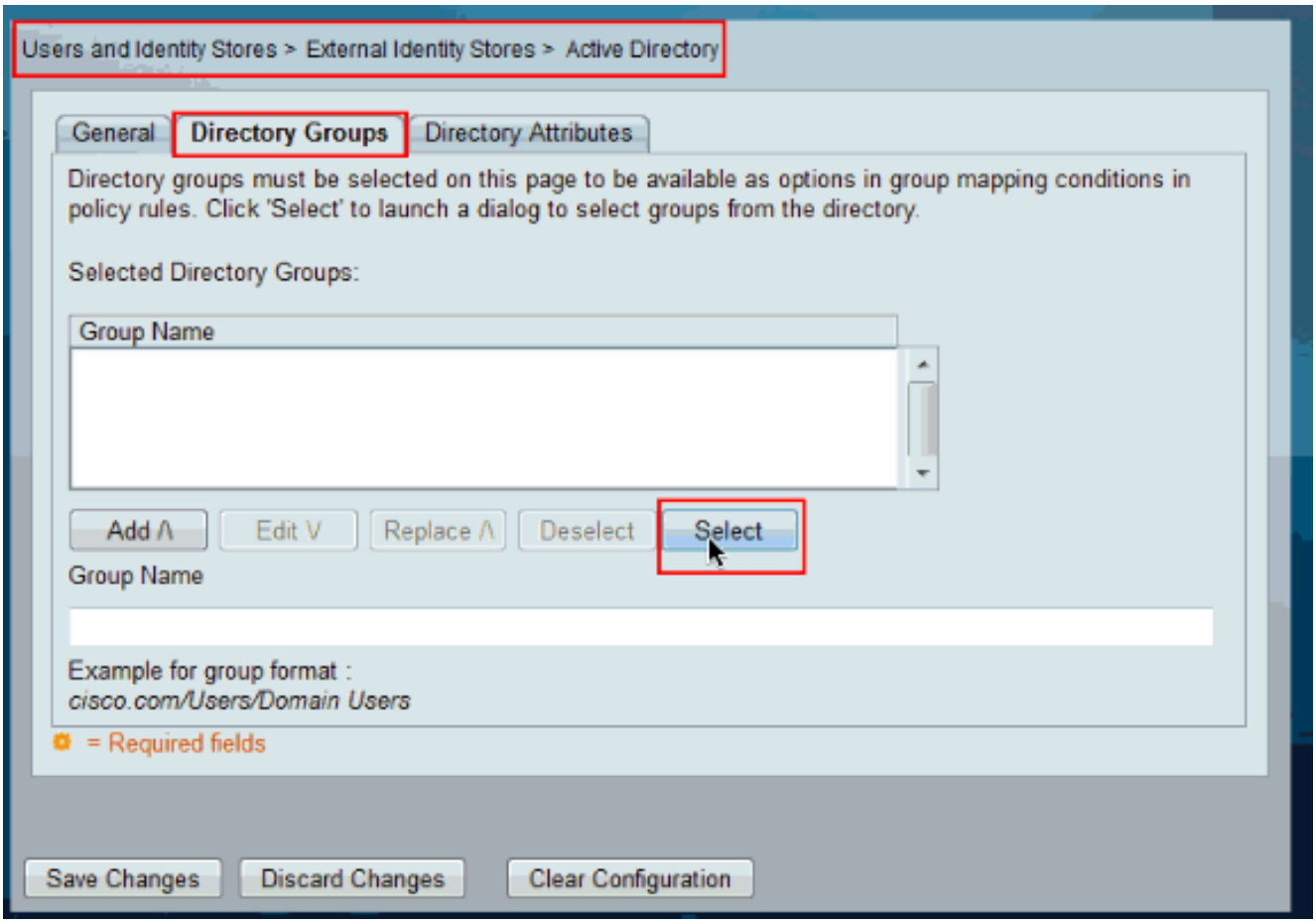
Bevor Sie mit der Konfiguration des ACS 5.x für Authentifizierung und Autorisierung beginnen, sollte der ACS erfolgreich in Microsoft AD integriert sein. Wenn der ACS nicht in die gewünschte AD-Domäne integriert ist, lesen Sie ACS 5.x und höher: Integration in Microsoft Active Directory Konfigurationsbeispiel für weitere Informationen, um die Integrationsaufgabe durchzuführen.

In diesem Abschnitt ordnen Sie zwei AD-Gruppen zwei verschiedenen Befehlssätzen und zwei Shell-Profilen zu, von denen eine vollständigen und die andere eingeschränkte Zugriffsmöglichkeiten auf Cisco IOS-Geräte bietet.

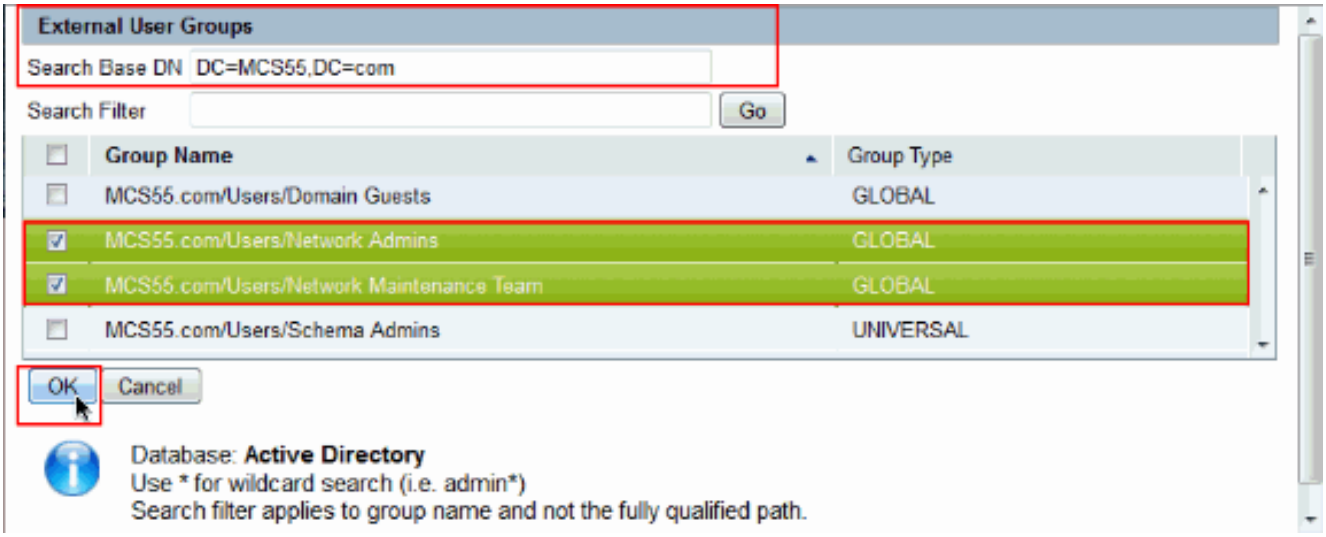
1. Melden Sie sich mit Administratorberechtigungen bei der ACS-GUI an.
2. Wählen Sie **Benutzer und Identitätsdaten > Externe Identitätsdaten > Active Directory aus**, und überprüfen Sie, ob der ACS der gewünschten Domäne beigetreten ist und ob der **Verbindungsstatus** als **verbunden** angezeigt wird.Klicken Sie auf die Registerkarte **Verzeichnisgruppen**.



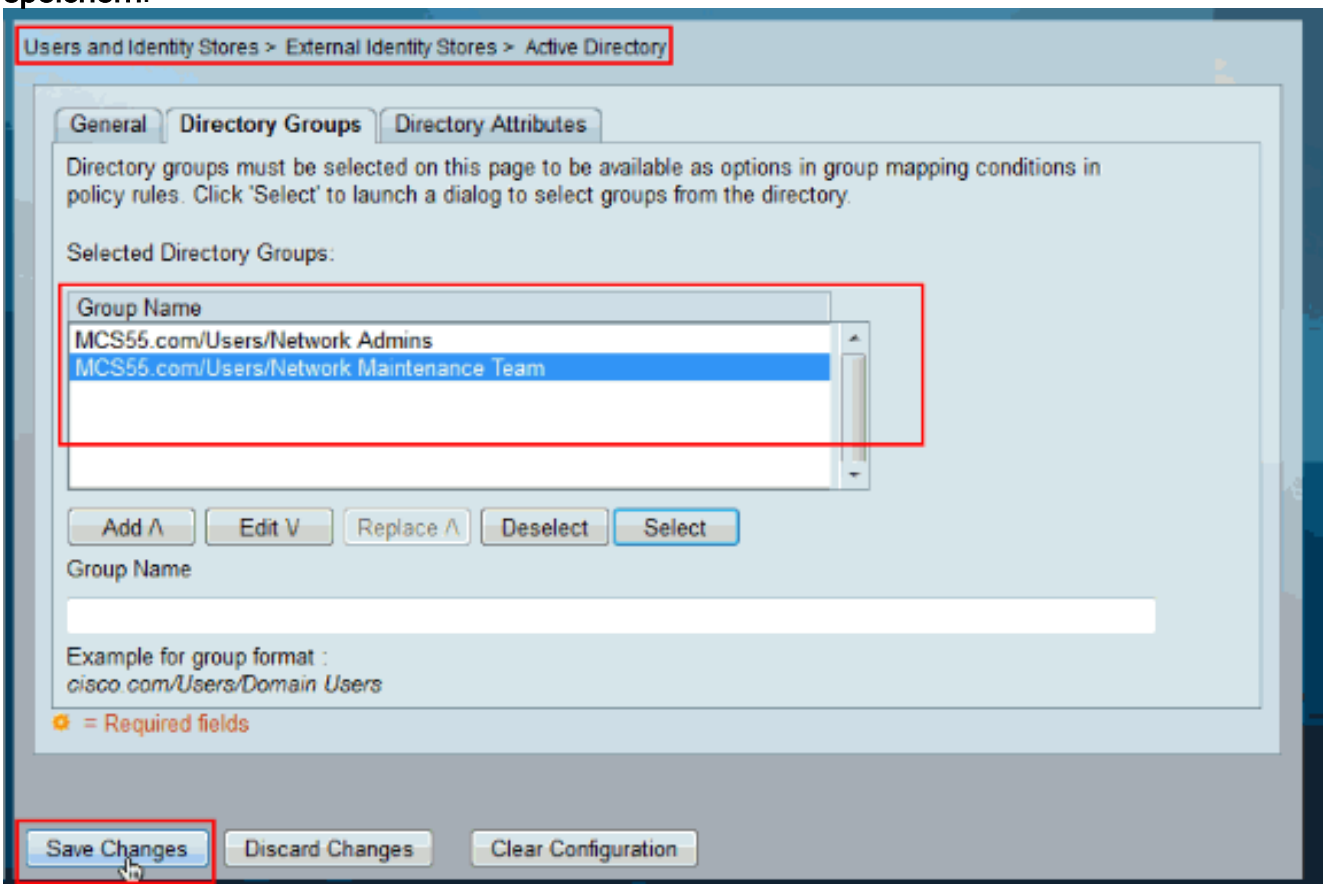
3. Klicken Sie auf **Auswählen**.



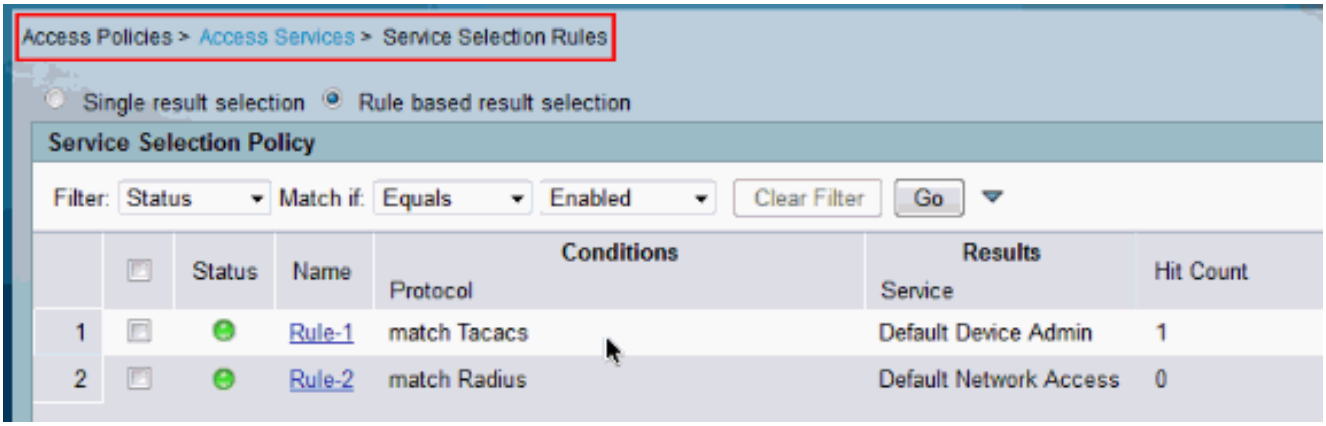
4. Wählen Sie die Gruppen aus, die den Shell-Profilen und Befehlssätzen im späteren Teil der Konfiguration zugeordnet werden müssen. Klicken Sie auf **OK**.



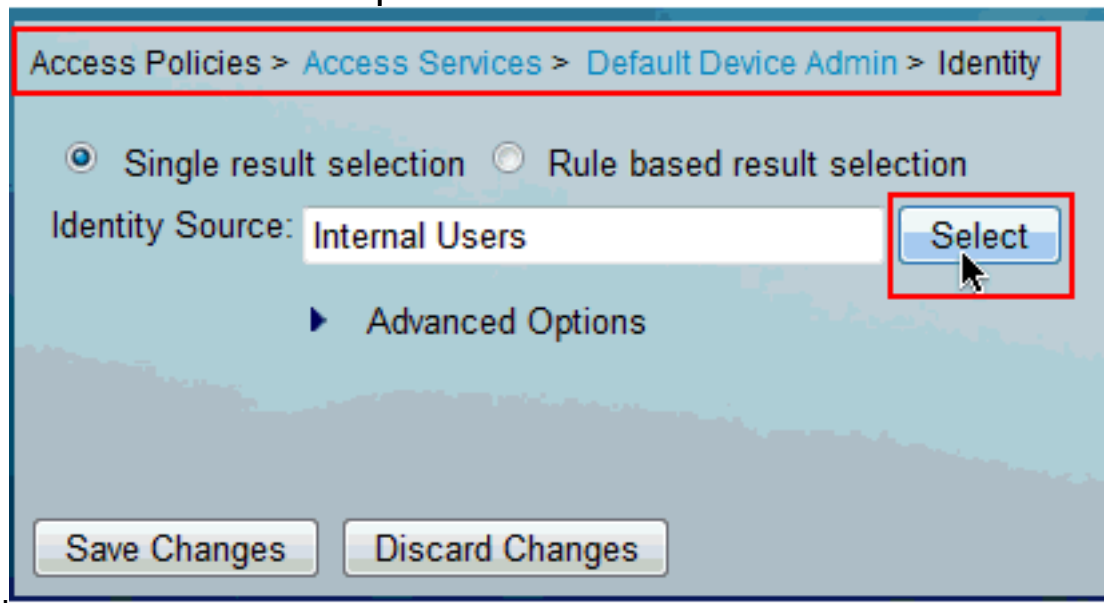
5. Klicken Sie auf **Änderungen speichern**.



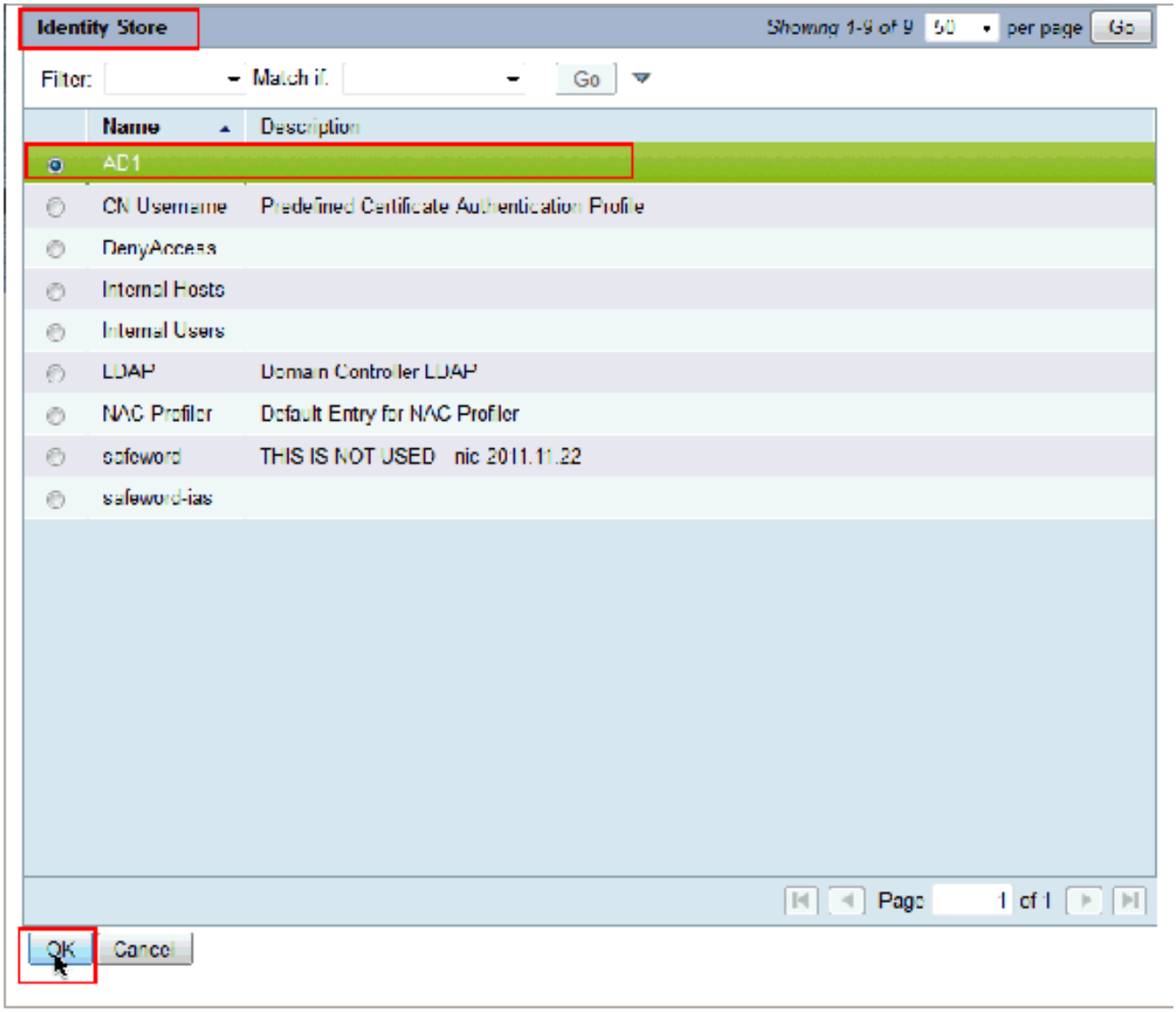
6. Wählen Sie **Access Policies > Access Services > Service Selection Rules** (Zugriffsrichtlinien > Zugriffsdienste > Serviceauswahlregeln), und bestimmen Sie den Zugriffsdienst, der die TACACS+-Authentifizierung verarbeitet. In diesem Beispiel ist es **Standardgeräteadministrator**.



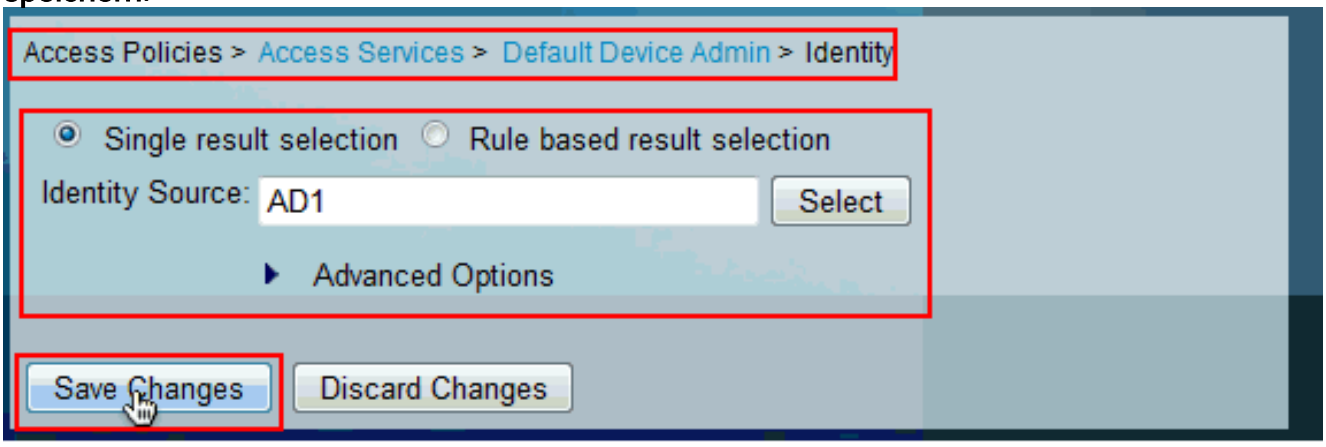
7. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardgeräteadministrator > Identität aus,** und klicken Sie neben **Identitätsquelle** auf **Auswählen**.



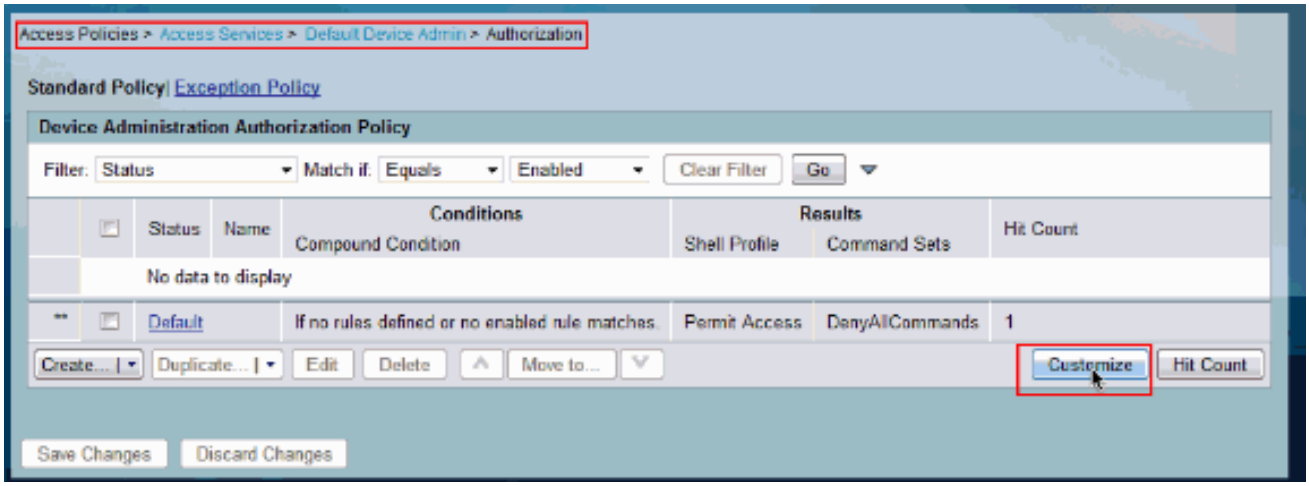
8. Wählen Sie **AD1 aus**, und klicken Sie auf **OK**.



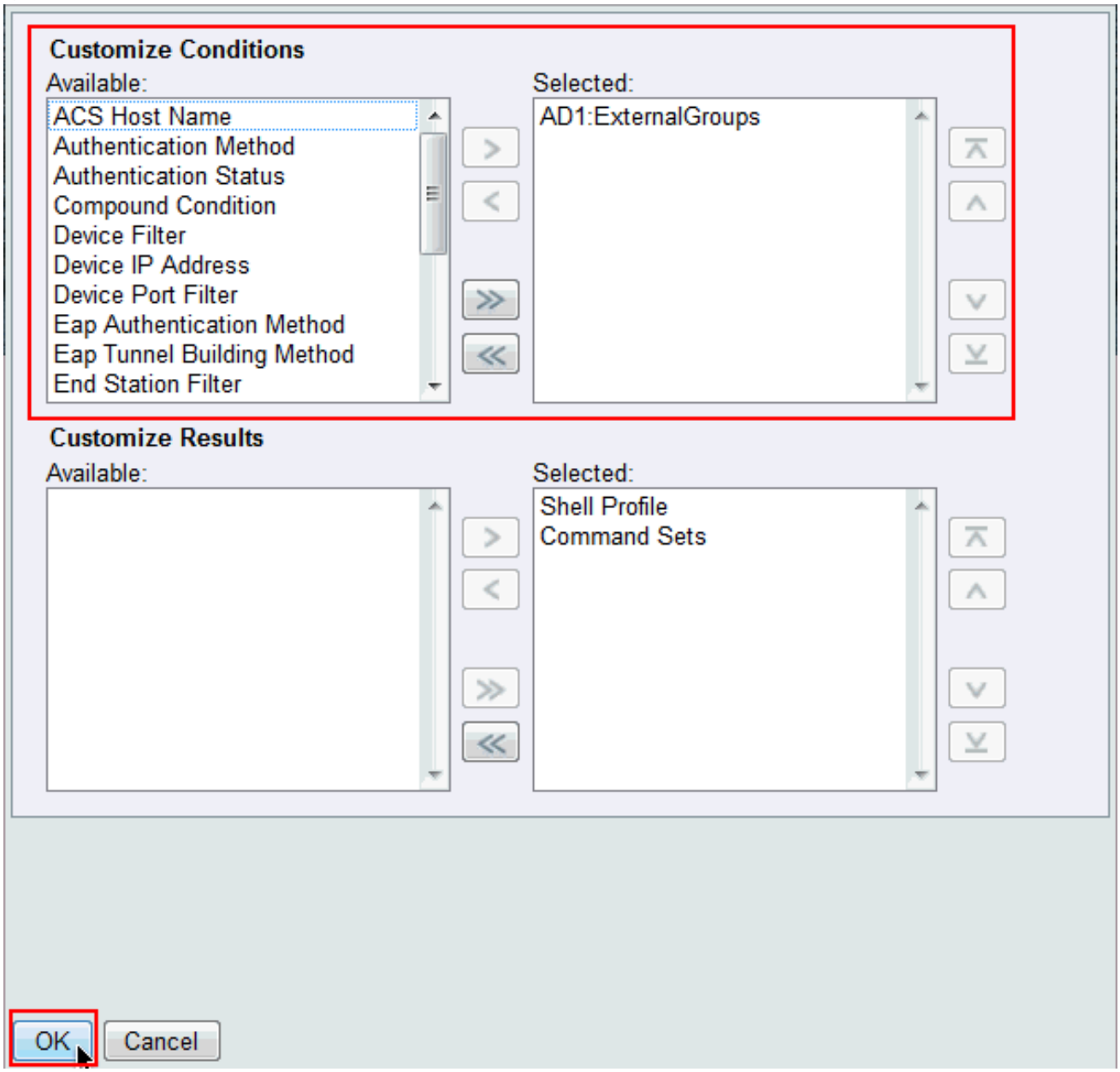
9. Klicken Sie auf **Änderungen speichern**.



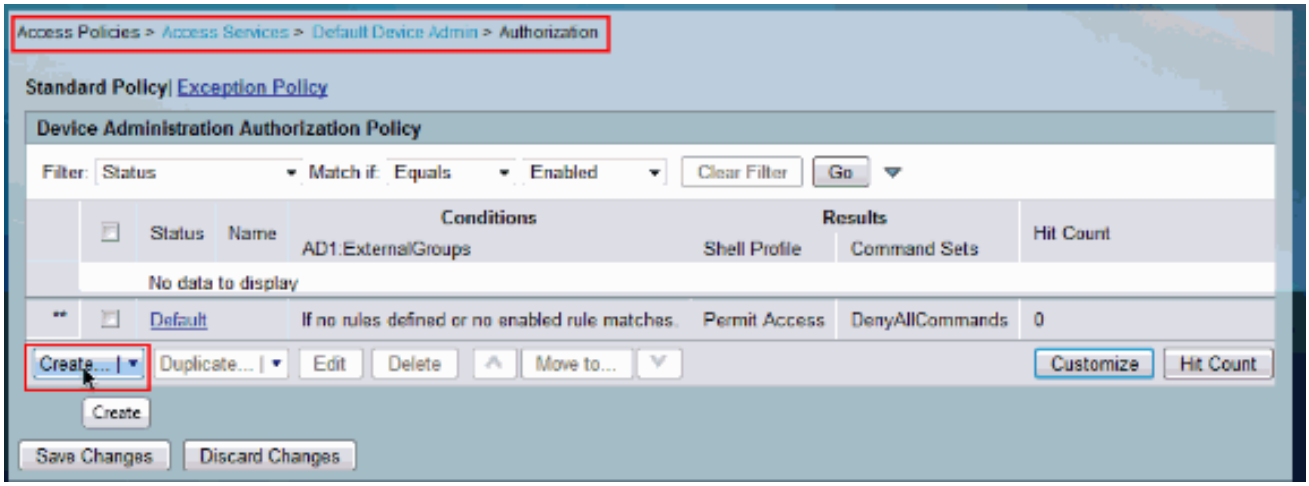
10. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardgeräteadministrator > Autorisierung aus,** und klicken Sie auf **Anpassen**.



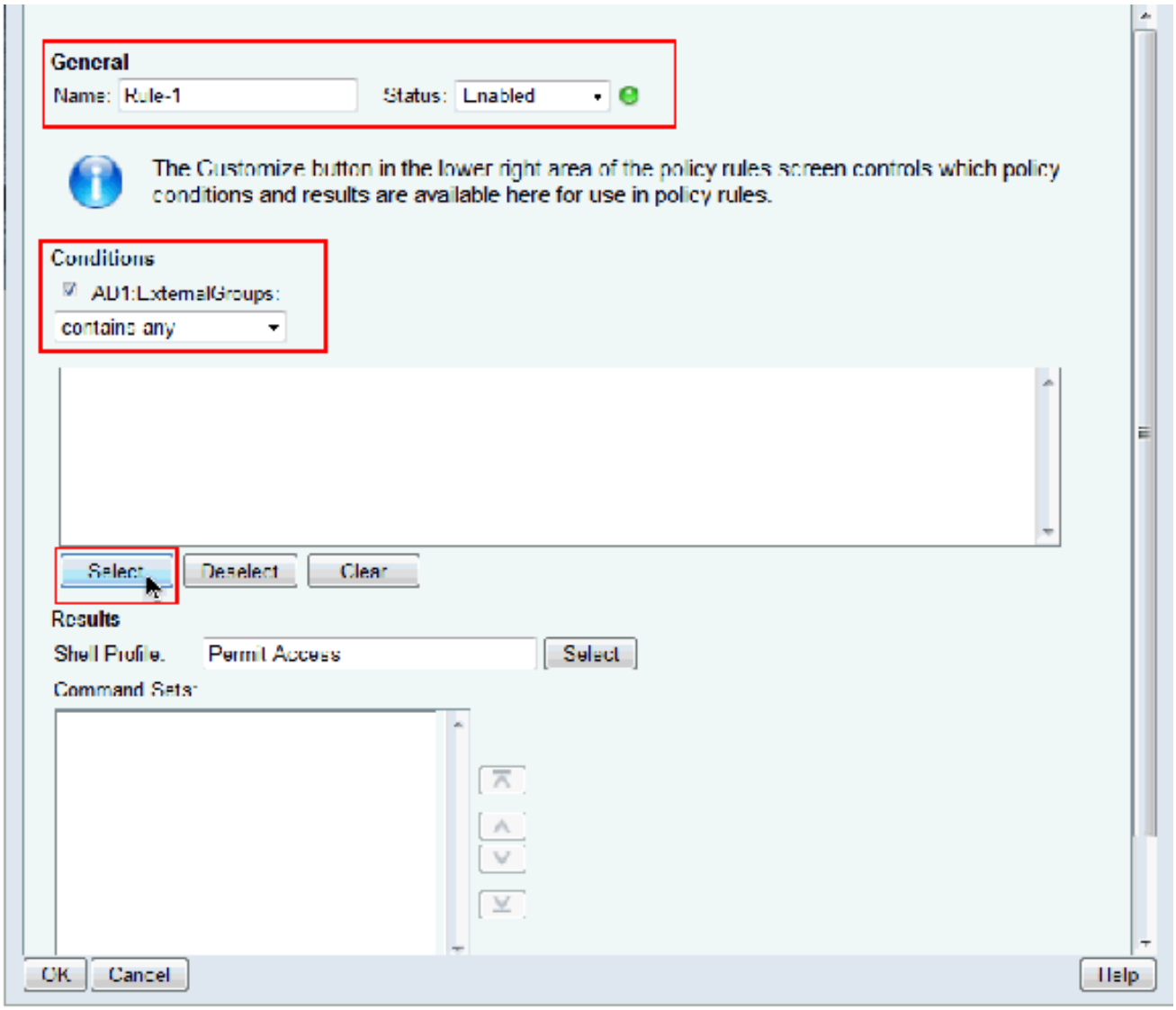
11. Kopieren Sie AD1:ExternalGroups aus Available in den ausgewählten Abschnitt unter Customize Conditions und verschieben Sie dann Shell-Profile und Befehlssätze aus Available in den **ausgewählten** Abschnitt Customize Results (Ergebnisse anpassen). Klicken Sie jetzt auf **OK**.



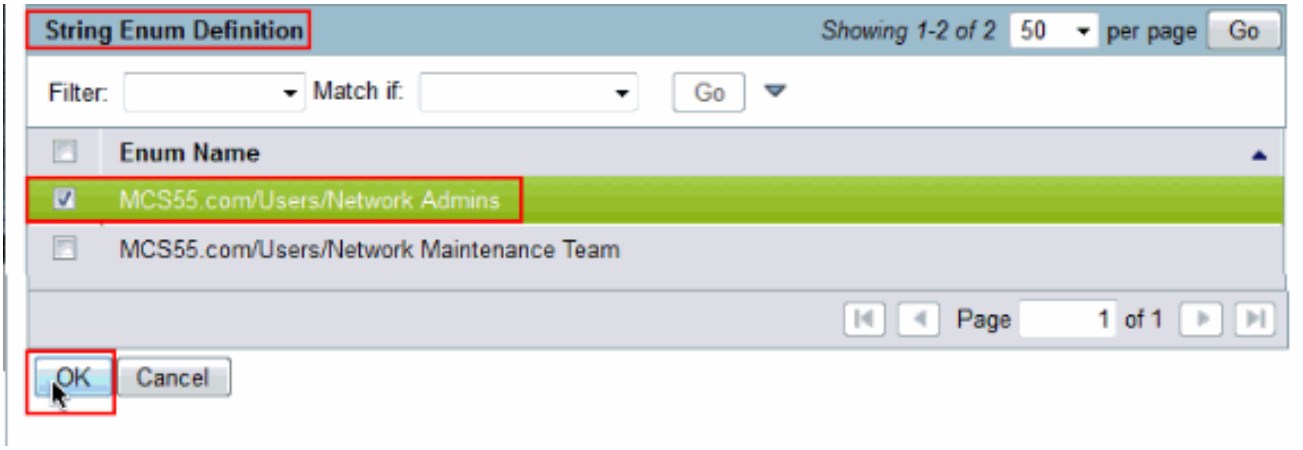
12. Klicken Sie auf **Erstellen**, um eine neue Regel zu erstellen.



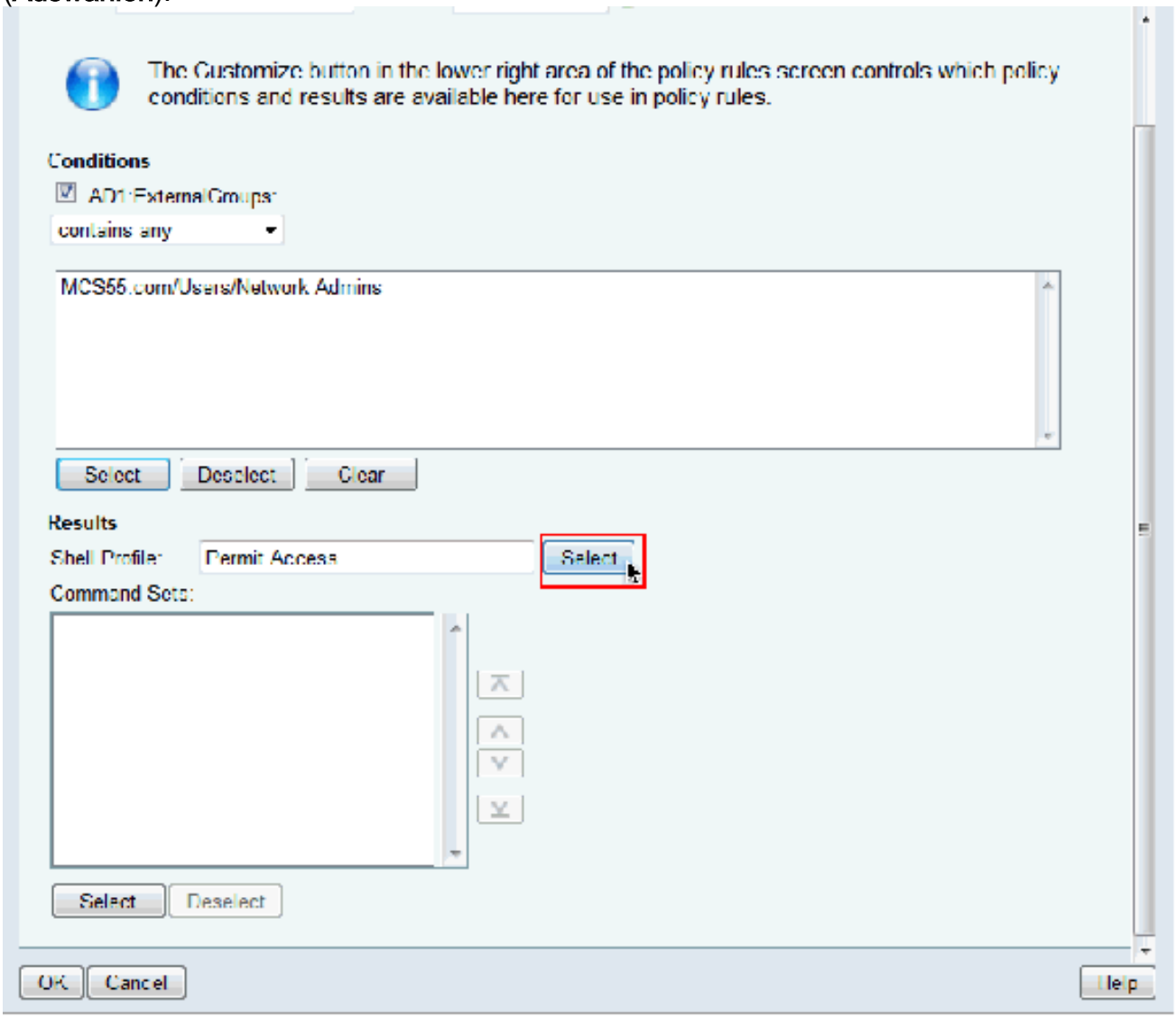
13. Klicken Sie im **AD1:ExternalGroups** Condition auf **Auswählen**.



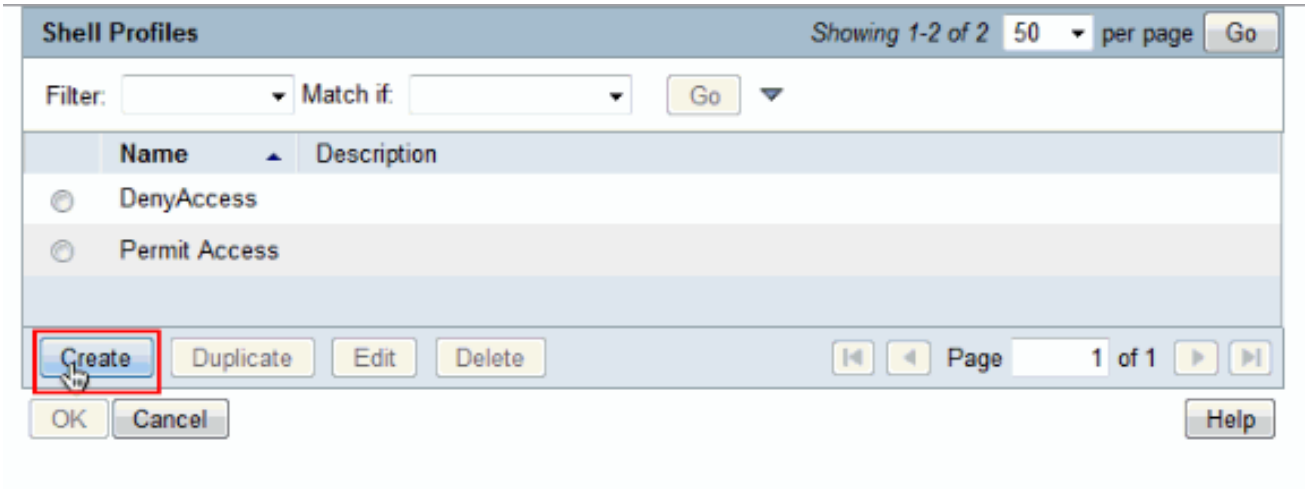
14. Wählen Sie die Gruppe aus, für die Sie vollständigen Zugriff auf das Cisco IOS-Gerät bereitstellen möchten. Klicken Sie auf **OK**.



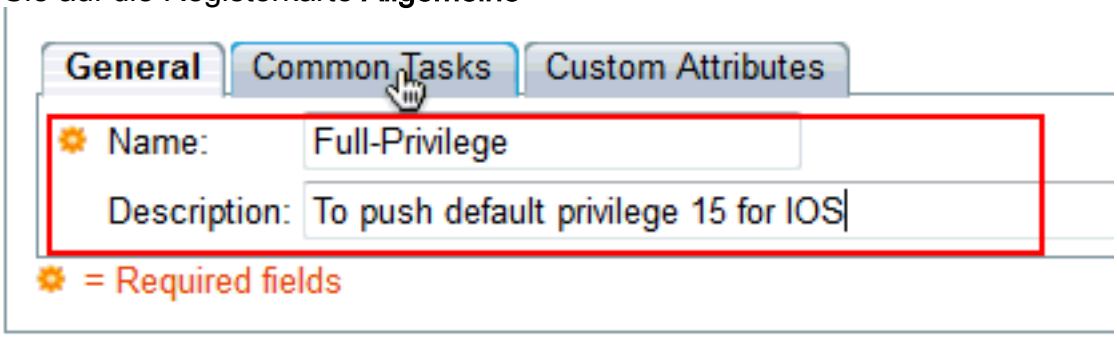
15. Klicken Sie im Feld Shell Profile (Shell-Profil) auf **Select** (**Auswählen**).



16. Klicken Sie auf **Erstellen**, um ein neues **Shell-Profil** für Benutzer mit vollem Zugriff zu erstellen.

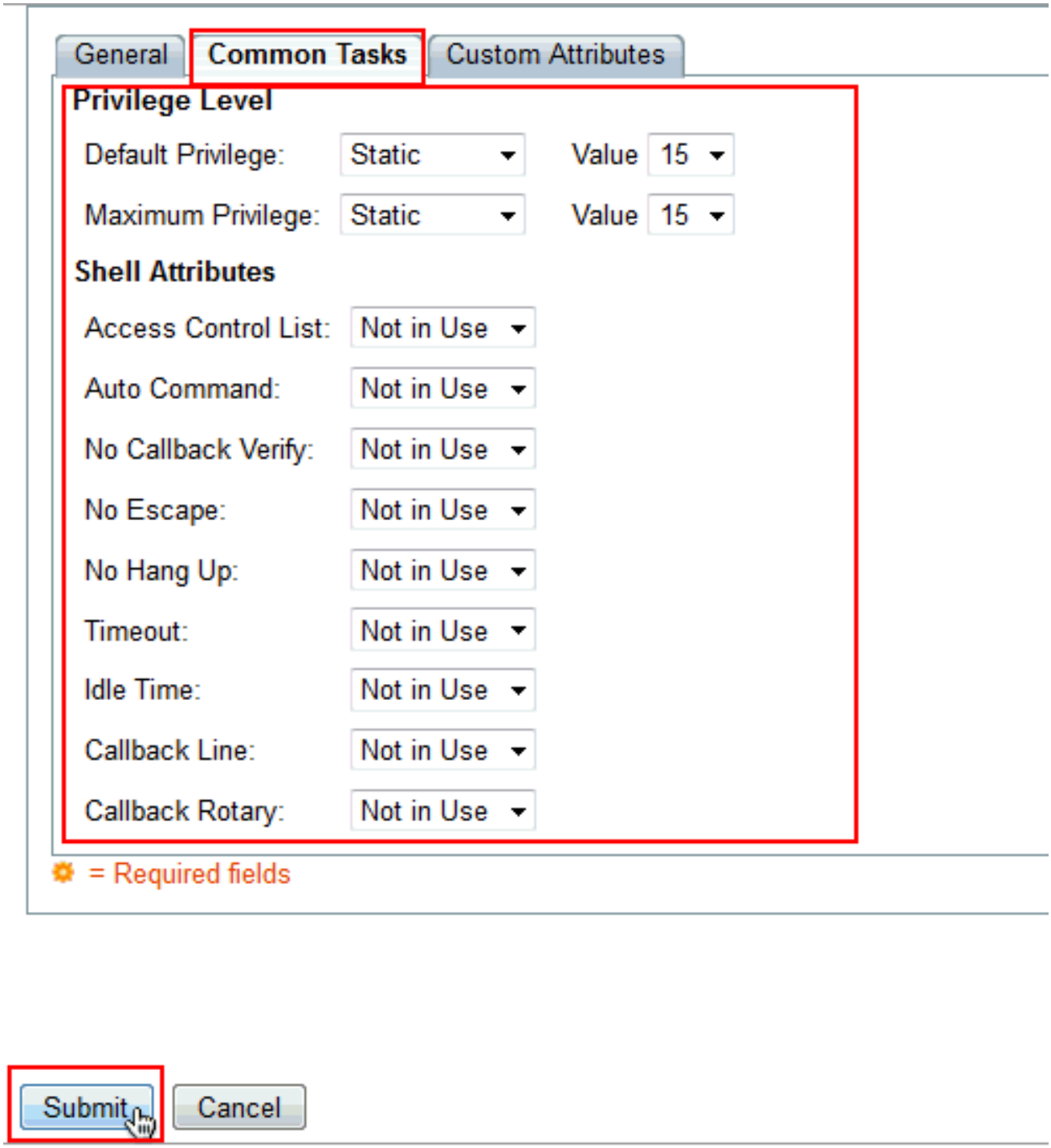


17. Geben Sie **Namen** und **Beschreibung** (optional) auf der **Registerkarte Allgemein ein ein,** und klicken Sie auf die Registerkarte **Allgemeine**

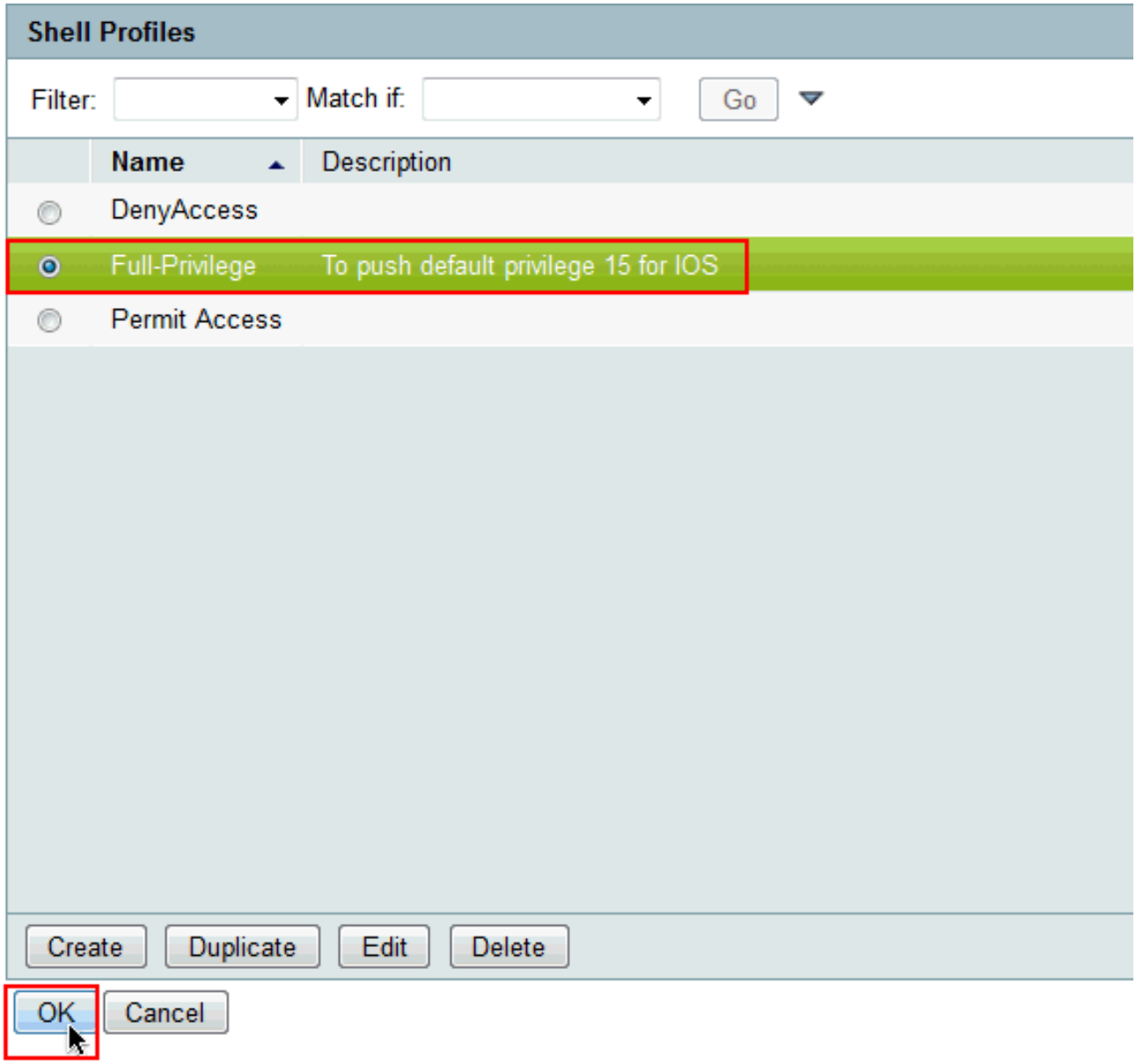


Aufgaben.

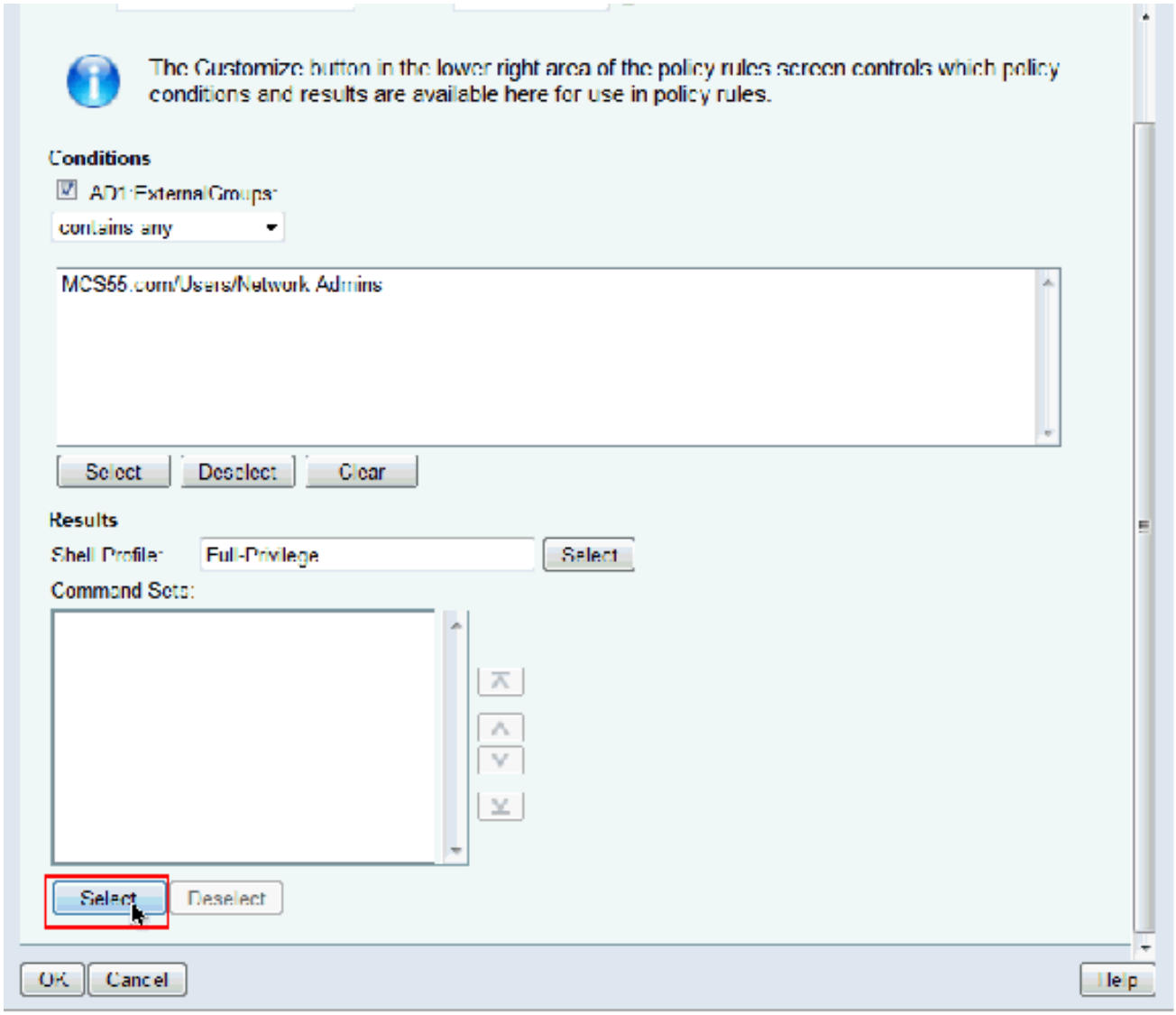
18. Ändern Sie die **Standardberechtigung** und die **maximale Berechtigung** in **Statisch** mit dem **Wert 15**. Klicken Sie auf **Senden**.



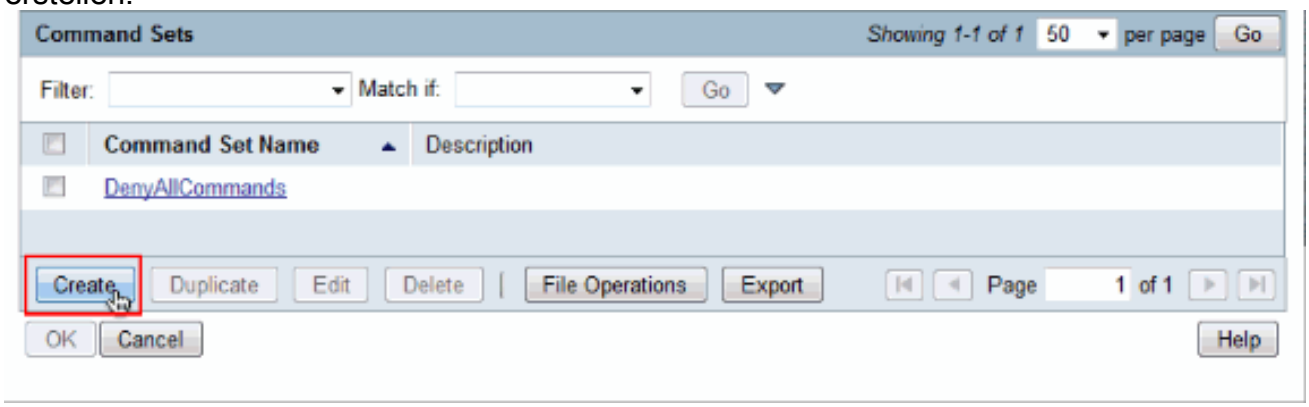
19. Wählen Sie jetzt das neu erstellte **Shell-Profil für** vollständigen Zugriff (in diesem Beispiel Vollberechtigungen) aus, und klicken Sie auf **OK**.



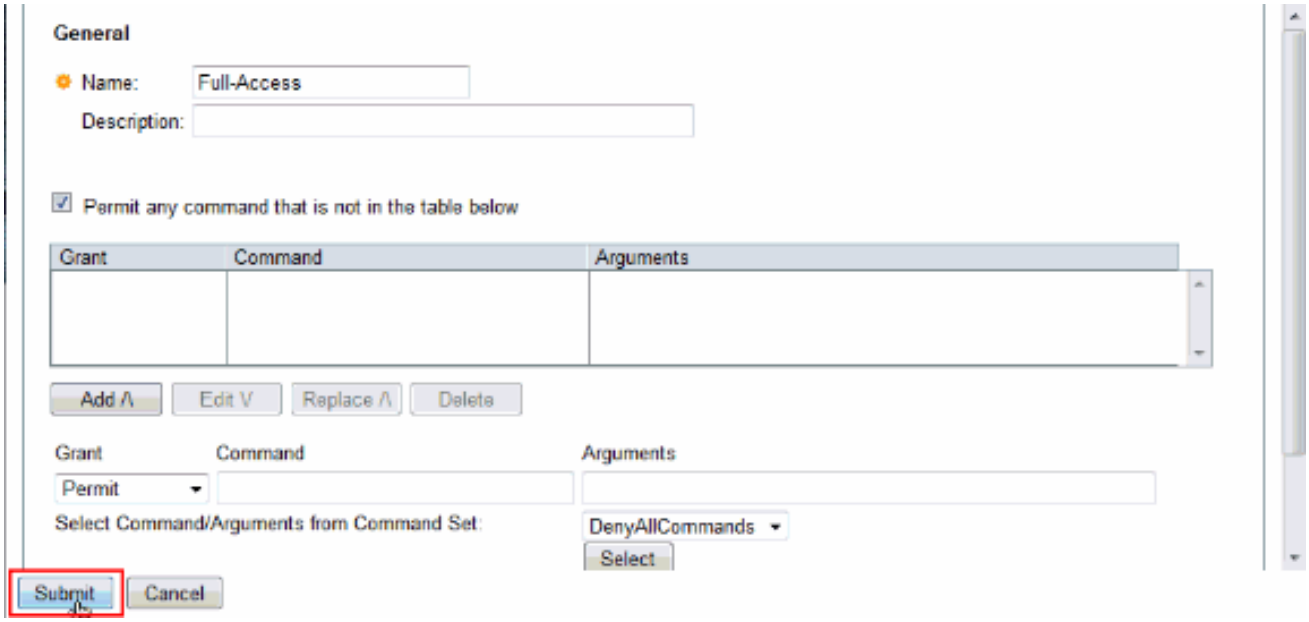
20. Klicken Sie im Feld Befehlssätze auf **Auswählen**.



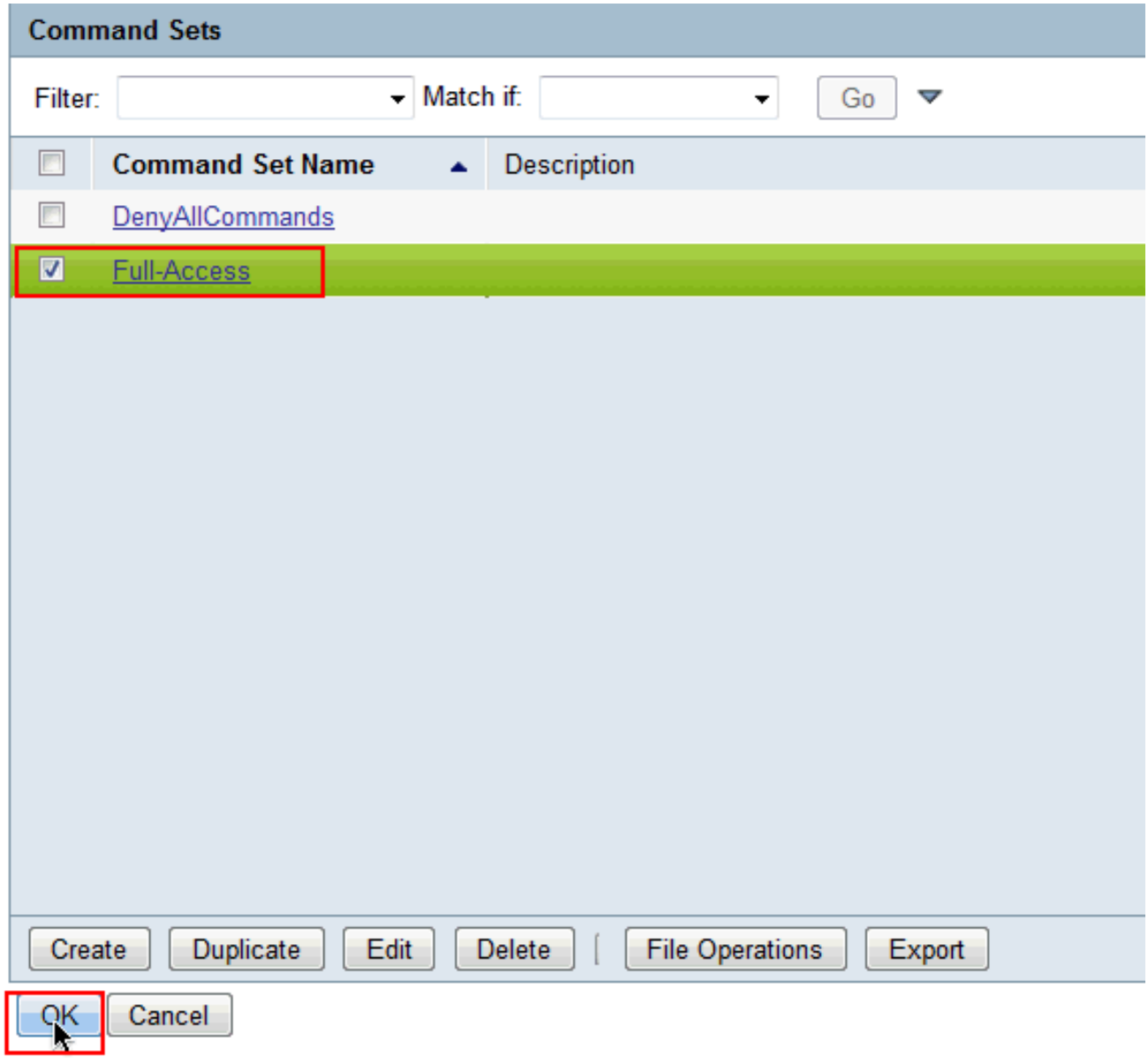
21. Klicken Sie auf **Erstellen**, um einen neuen **Befehlssatz** für **Vollzugriff-**Benutzer zu erstellen.



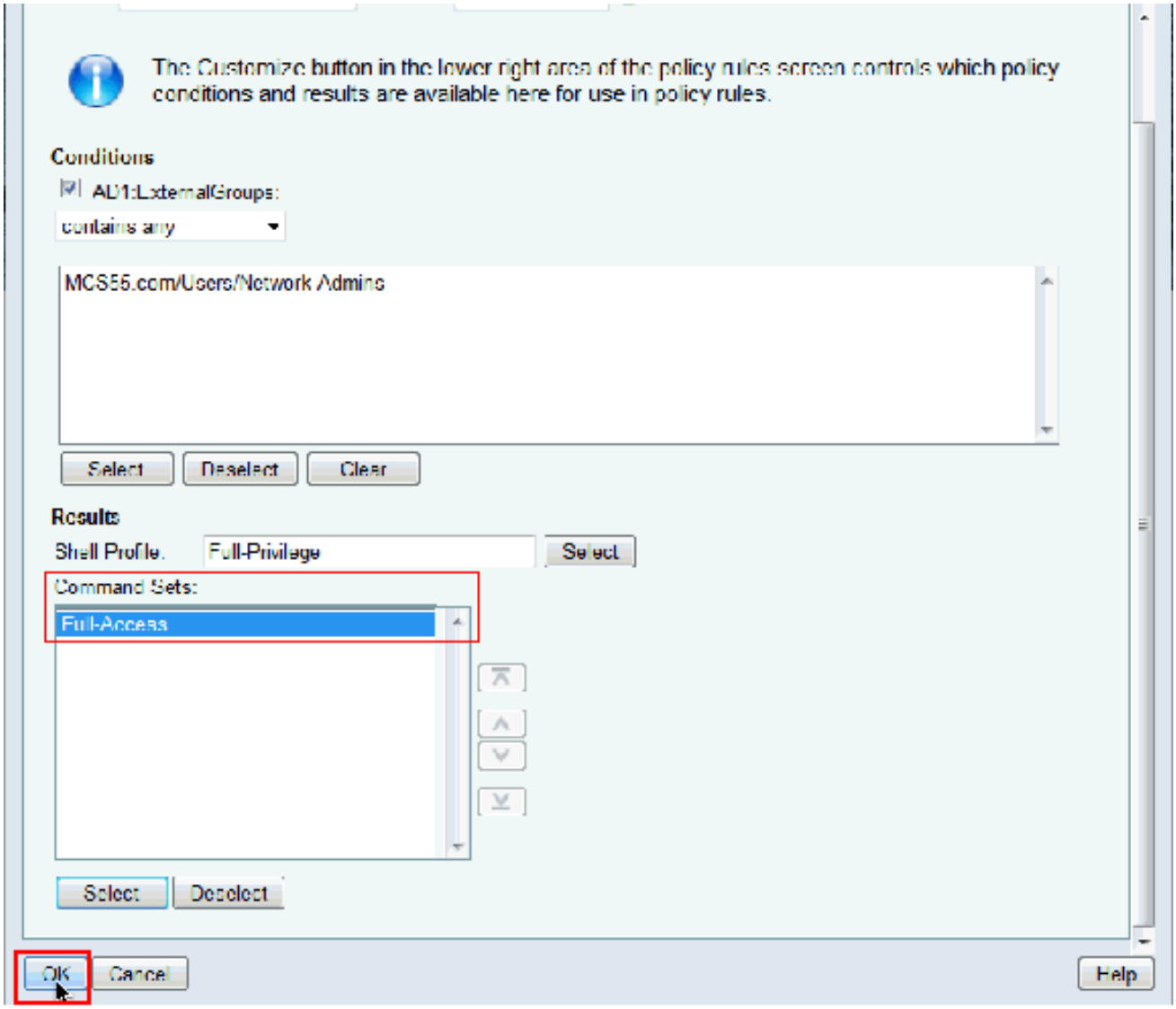
22. Geben Sie einen **Namen ein**, und vergewissern Sie sich, dass das Kontrollkästchen neben **Zulassen von Befehlen, die nicht in der Tabelle unten aufgeführt sind,** aktiviert ist. Klicken Sie auf **Senden**.**Hinweis:** Weitere Informationen zu Befehlssätzen finden Sie unter Erstellen, Duplizieren und Bearbeiten von Befehlssätzen für die Geräteverwaltung.



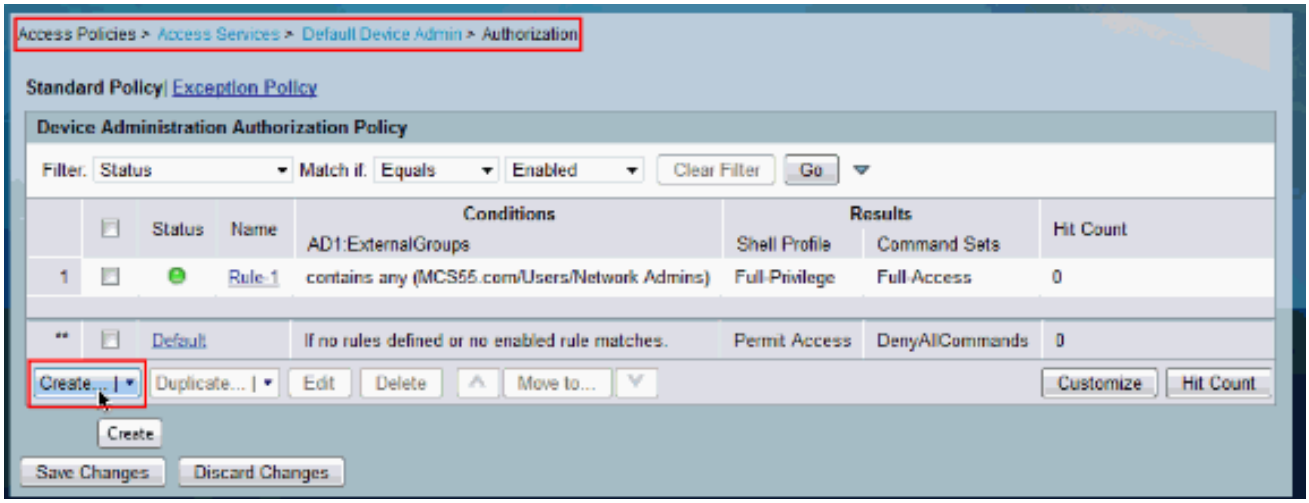
23. Klicken Sie auf **OK**.



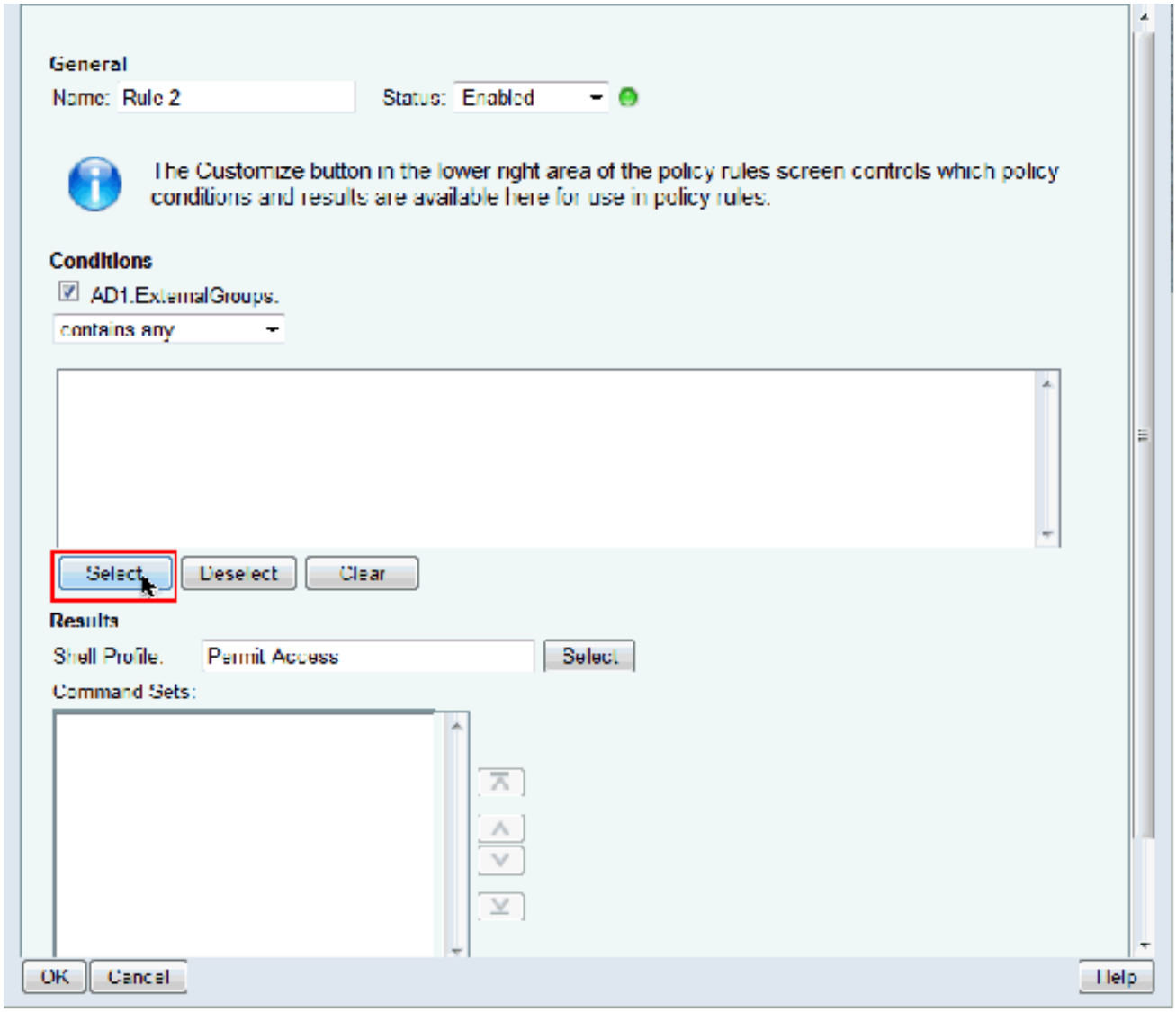
24. Klicken Sie auf **OK**. Damit ist die Konfiguration von **Regel 1 abgeschlossen**.



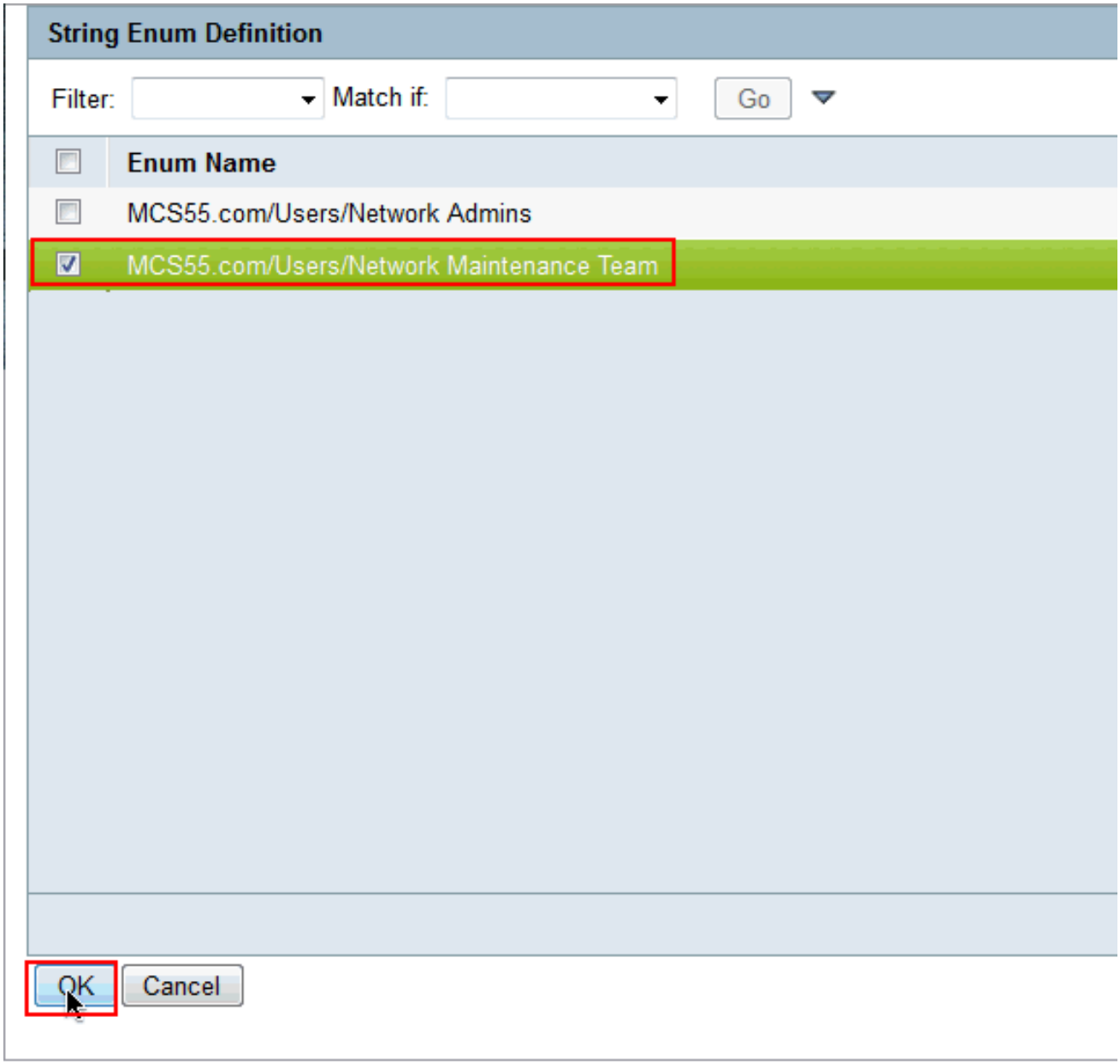
25. Klicken Sie auf **Erstellen**, um eine neue Regel für Benutzer mit **beschränktem Zugriff** zu erstellen.



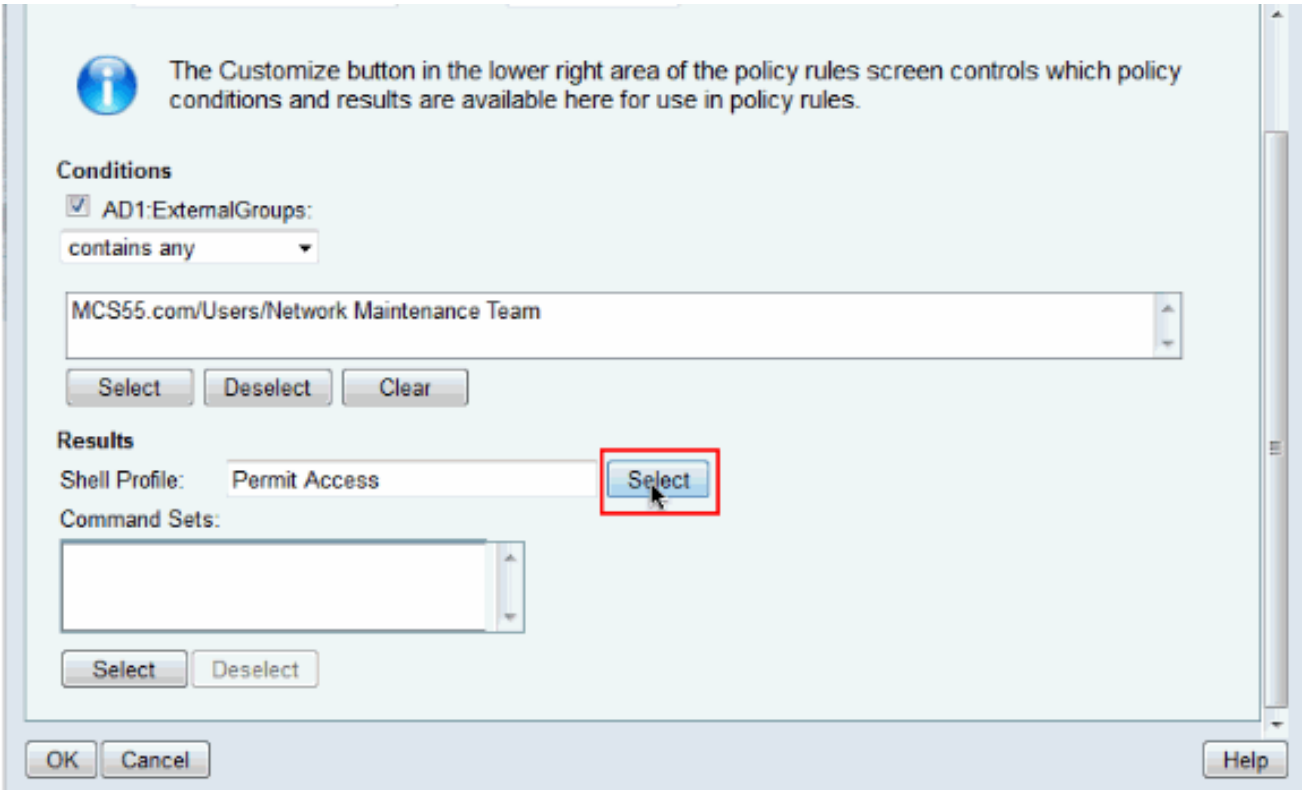
26. Wählen Sie **AD1:ExternalGroups** aus, und klicken Sie auf **Auswählen**.



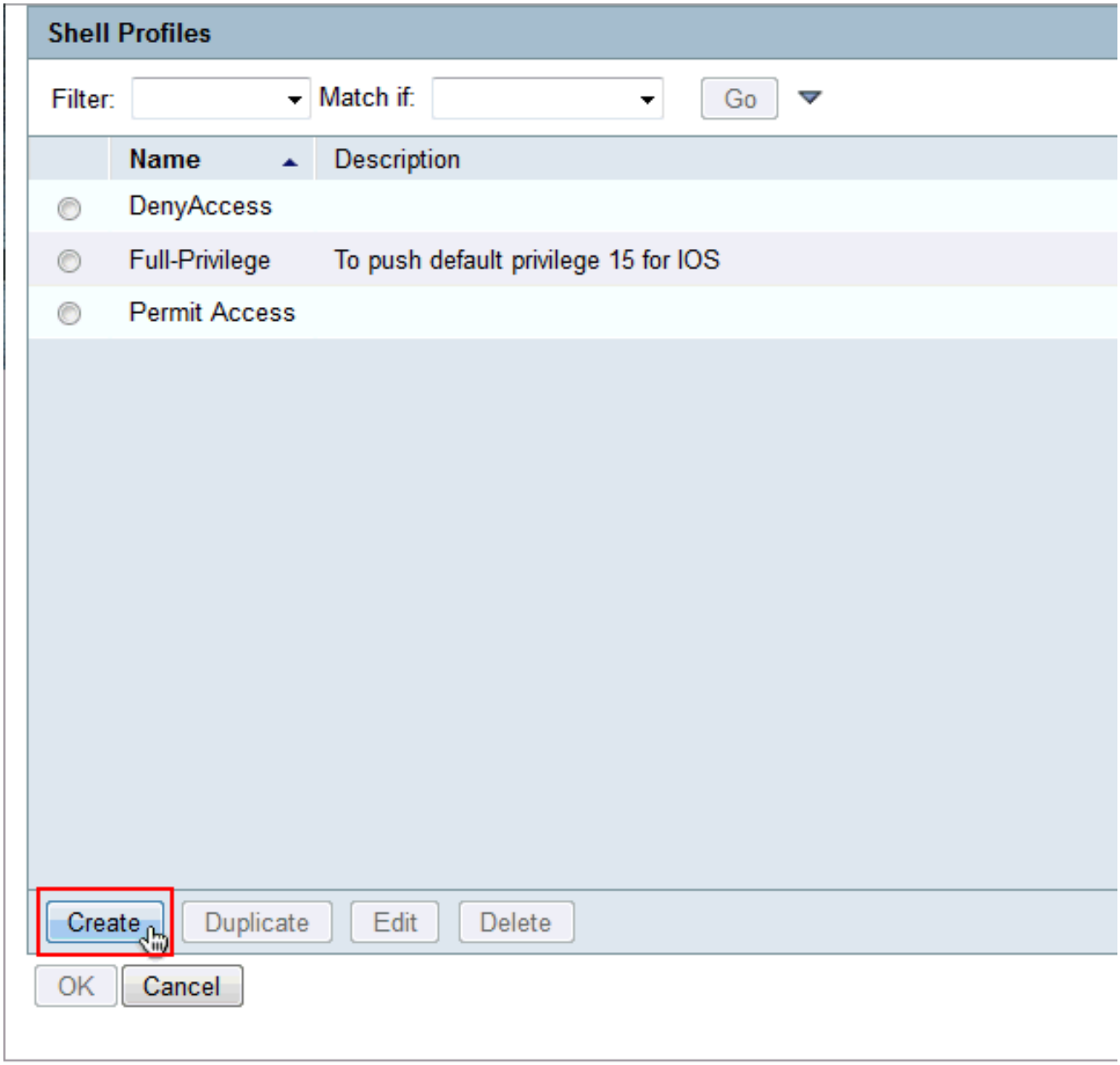
27. Wählen Sie die Gruppen aus, für die Sie eingeschränkten Zugriff bereitstellen möchten, und klicken Sie auf
OK.



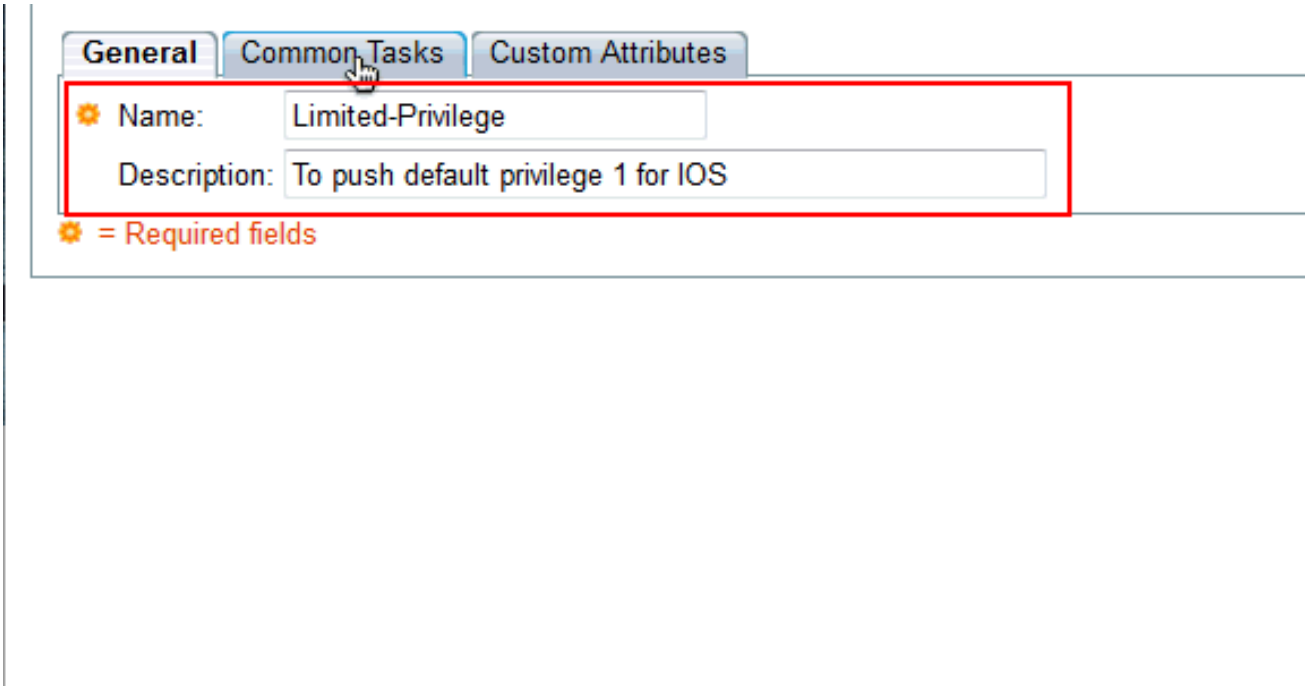
28. Klicken Sie im Feld Shell Profile (Shell-Profil) auf **Select** (**Auswählen**).



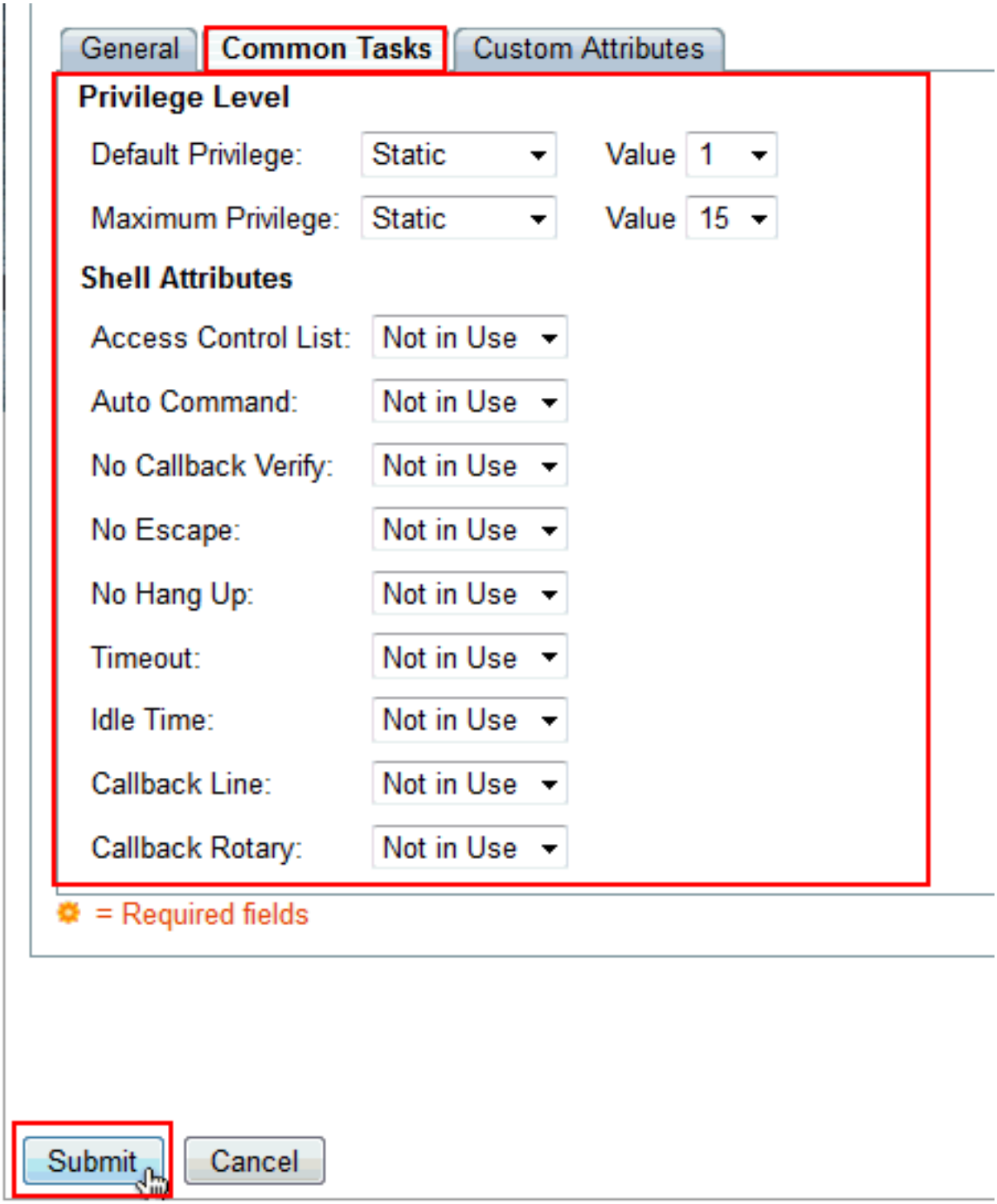
29. Klicken Sie auf **Erstellen**, um ein neues **Shell-Profil** für eingeschränkten Zugriff zu erstellen.



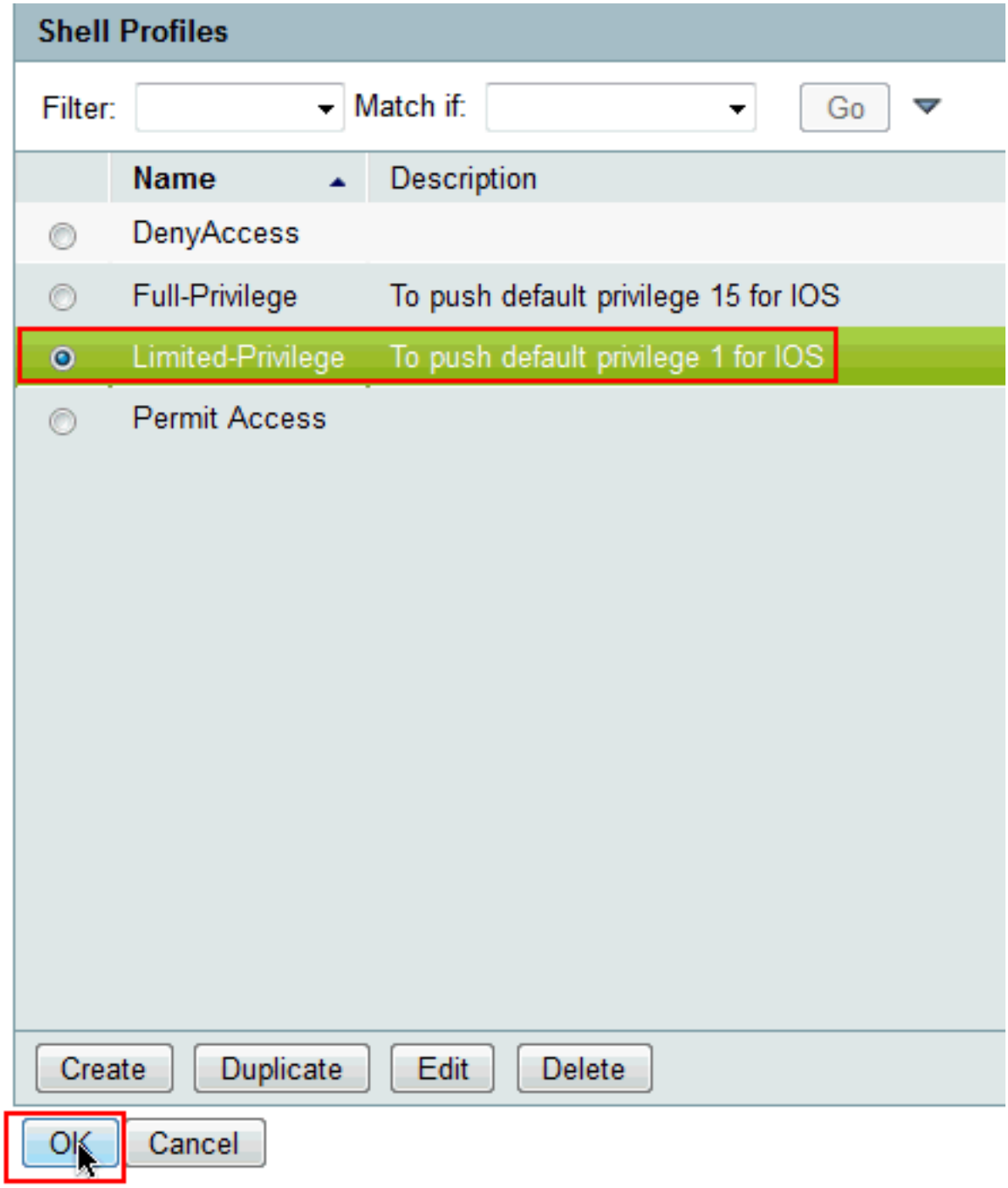
30. Geben Sie **Namen** und **Beschreibung** (optional) auf der Registerkarte **Allgemein ein ein,** und klicken Sie auf die Registerkarte **Allgemeine Aufgaben**.



31. Ändern Sie die **Standardberechtigung** und die **maximale Berechtigung** in **Statisch** mit den Werten **1** und **15.** Klicken Sie auf **Senden**.

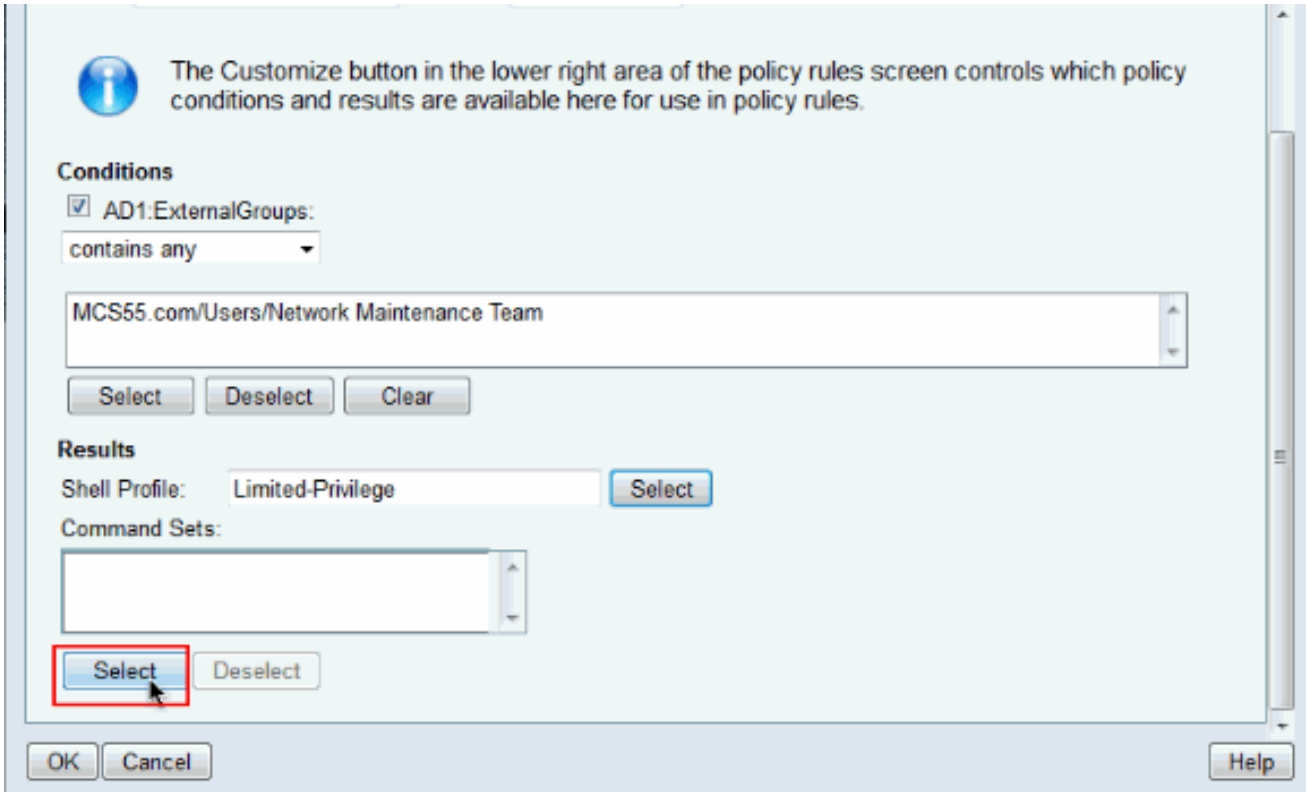


32. Klicken Sie auf

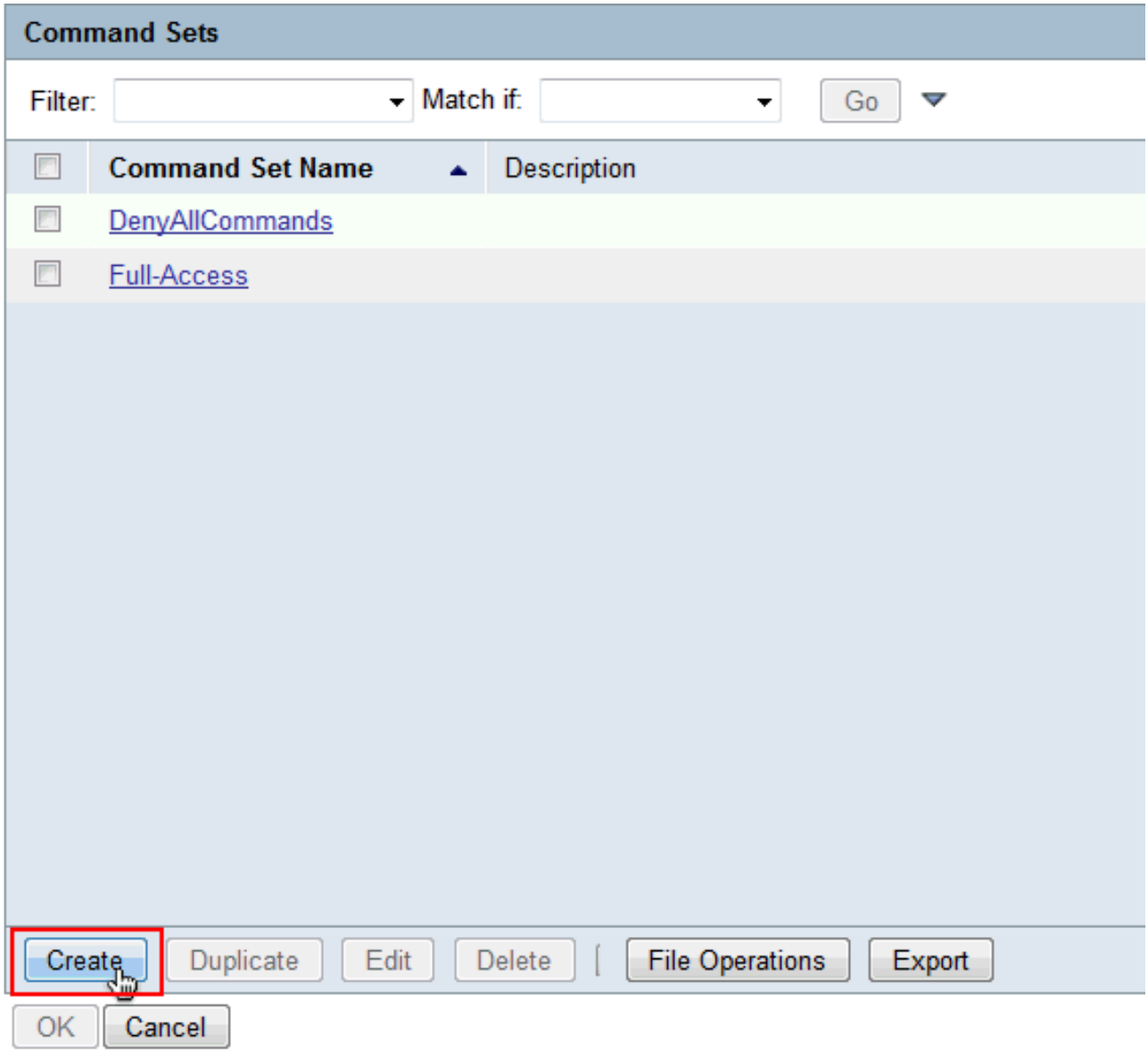


OK.

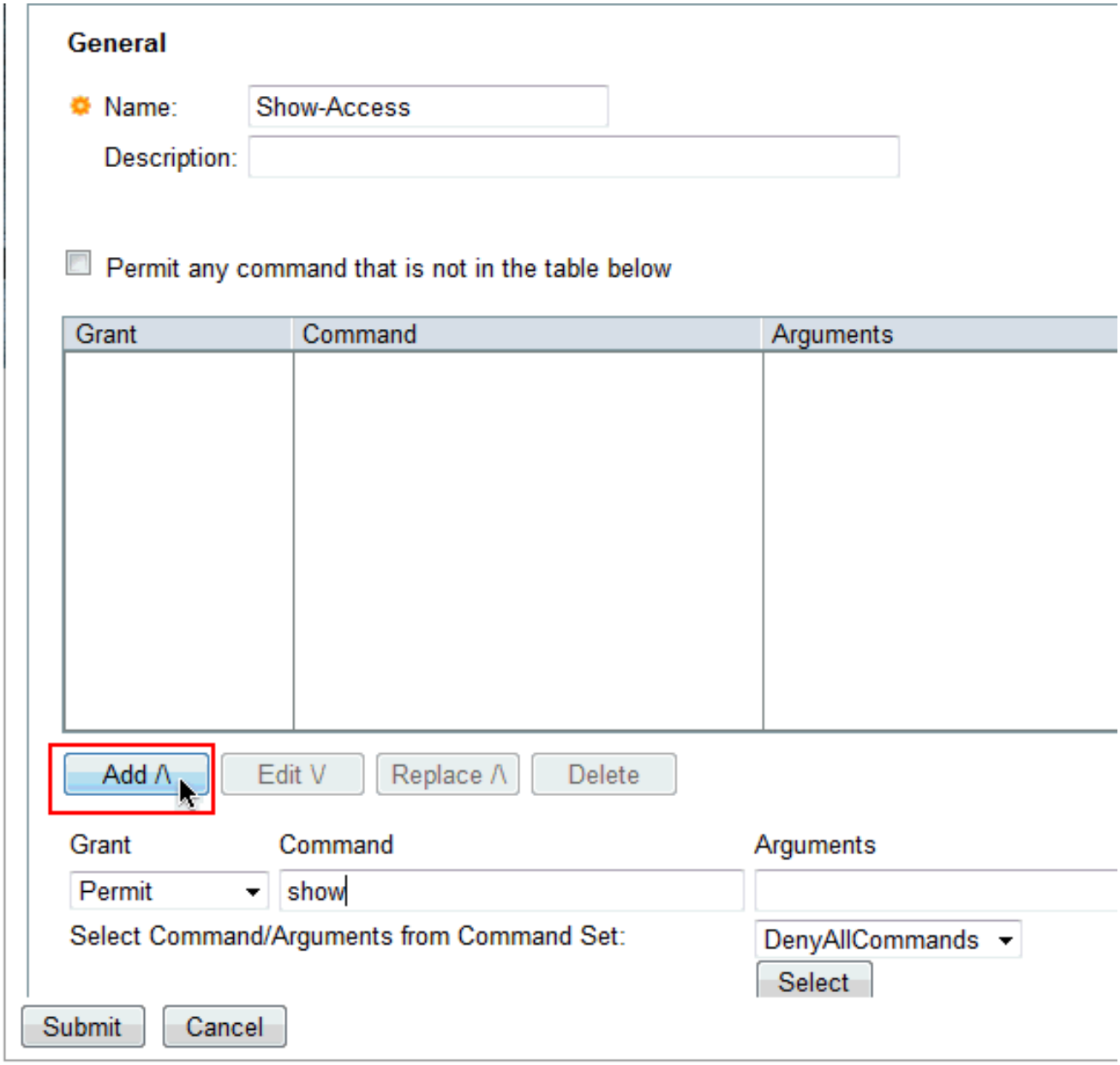
33. Klicken Sie im Feld Befehlssätze auf **Auswählen**.



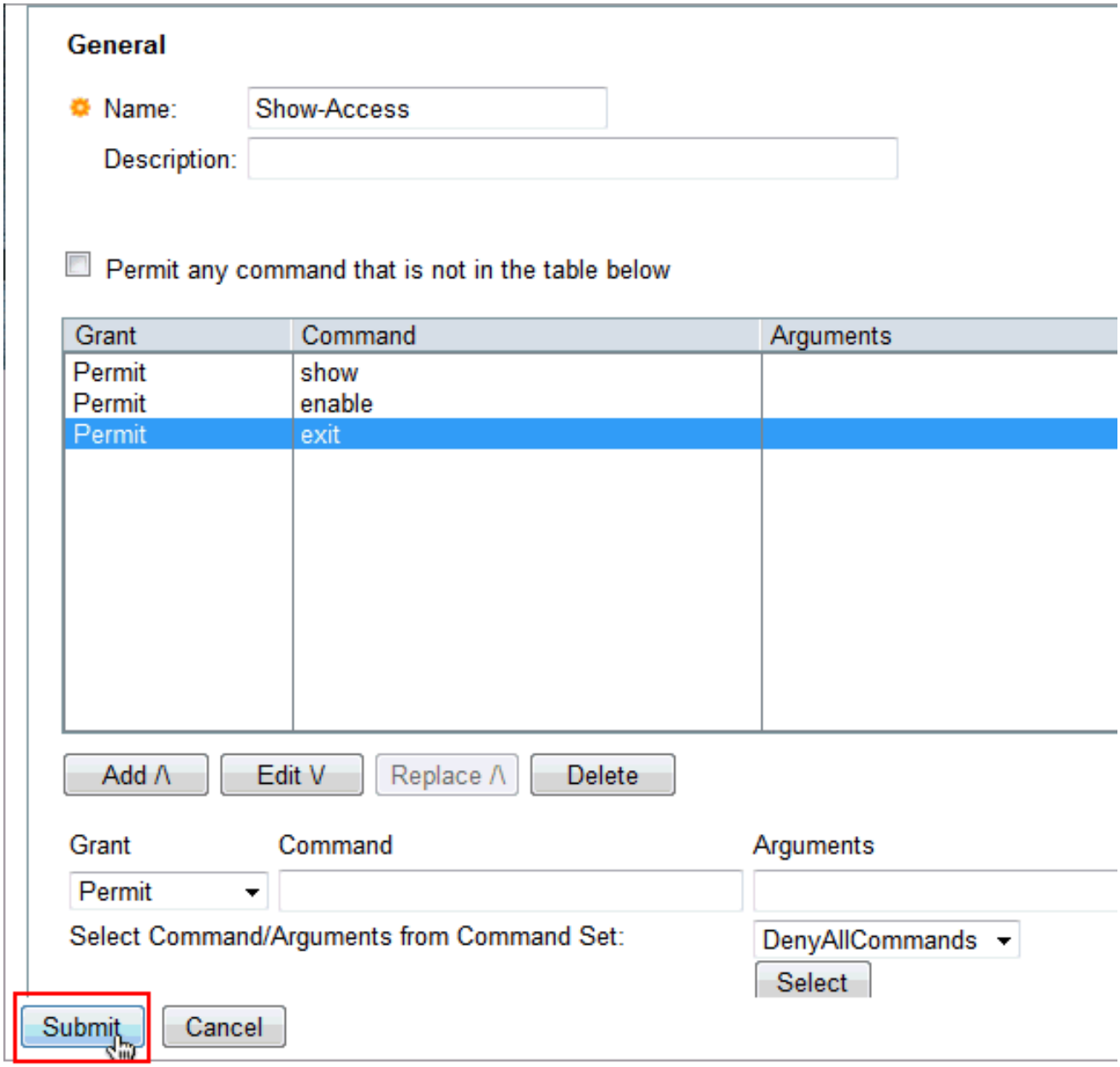
34. Klicken Sie auf **Erstellen**, um einen neuen **Befehlssatz** für die Gruppe mit beschränktem Zugriff zu
erstellen.



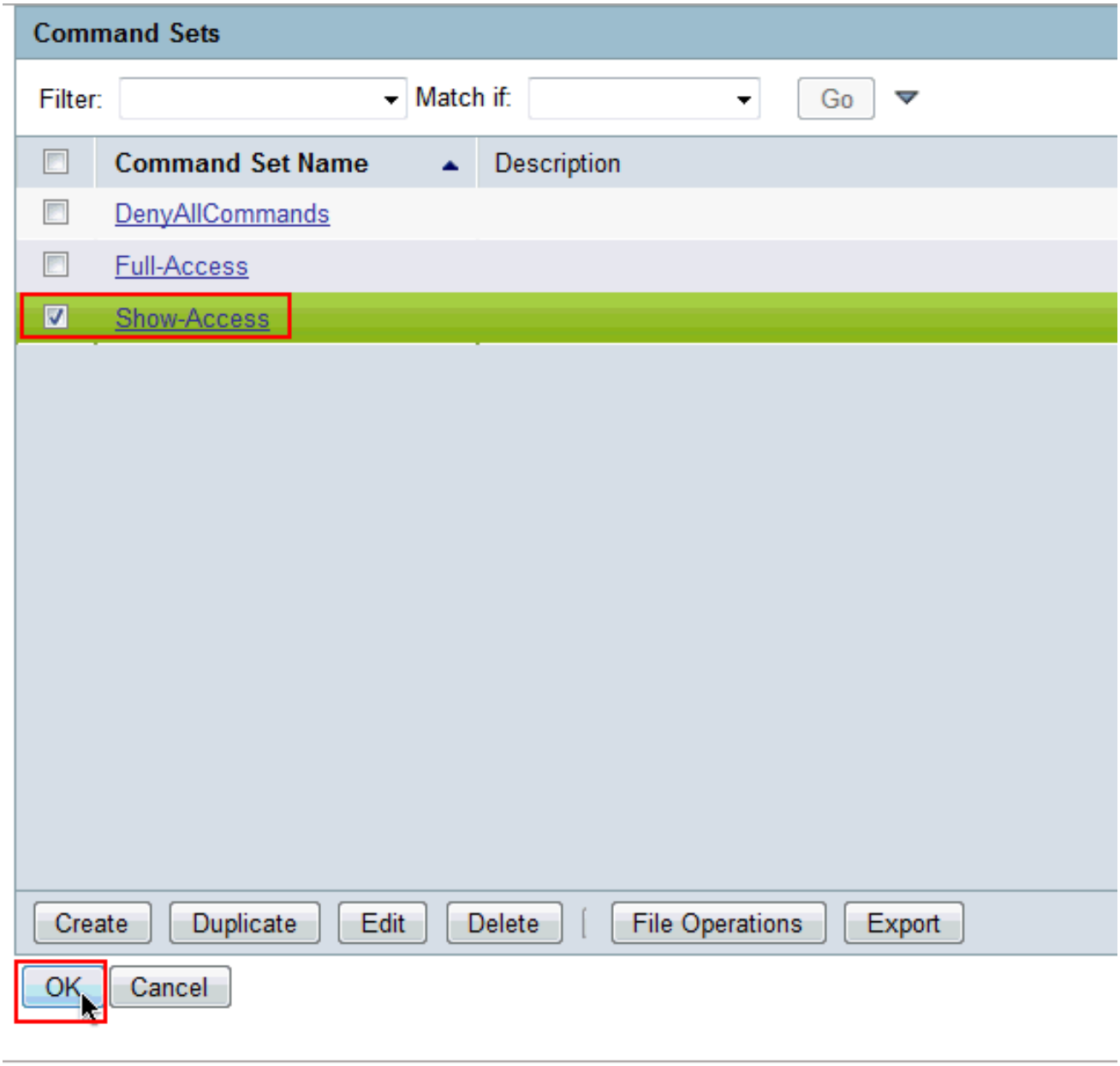
35. Geben Sie einen **Namen ein**, und vergewissern Sie sich, dass das Kontrollkästchen neben **Zulassen von Befehlen, die nicht in der Tabelle unten aufgeführt sind,** nicht aktiviert ist. Klicken Sie nach der Eingabe von **show** im **Befehlsbereich** auf **Add** und wählen Sie **Permit** im **Abschnitt Grant aus, sodass nur die Befehle zum Anzeigen für die Benutzer in der Gruppe mit beschränktem Zugriff zulässig sind.**



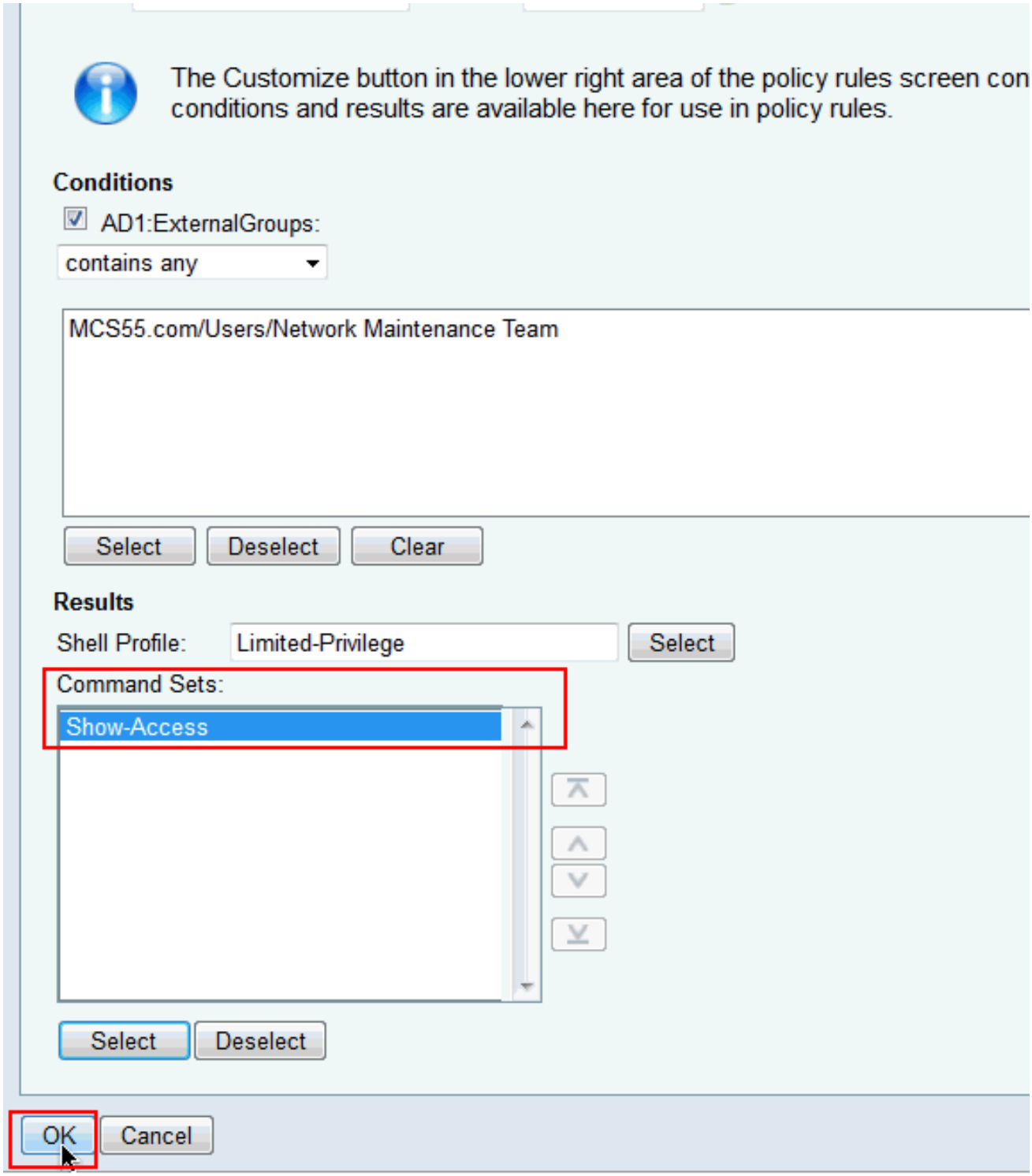
36. Fügen Sie in ähnlicher Weise alle anderen Befehle hinzu, die Benutzern in einer Gruppe mit eingeschränktem Zugriff unter Verwendung von **Add** erlaubt werden sollen. Klicken Sie auf **Senden**.**Hinweis:** Weitere Informationen zu Befehlssätzen finden Sie unter Erstellen, Duplizieren und Bearbeiten von Befehlssätzen für die Geräteverwaltung.



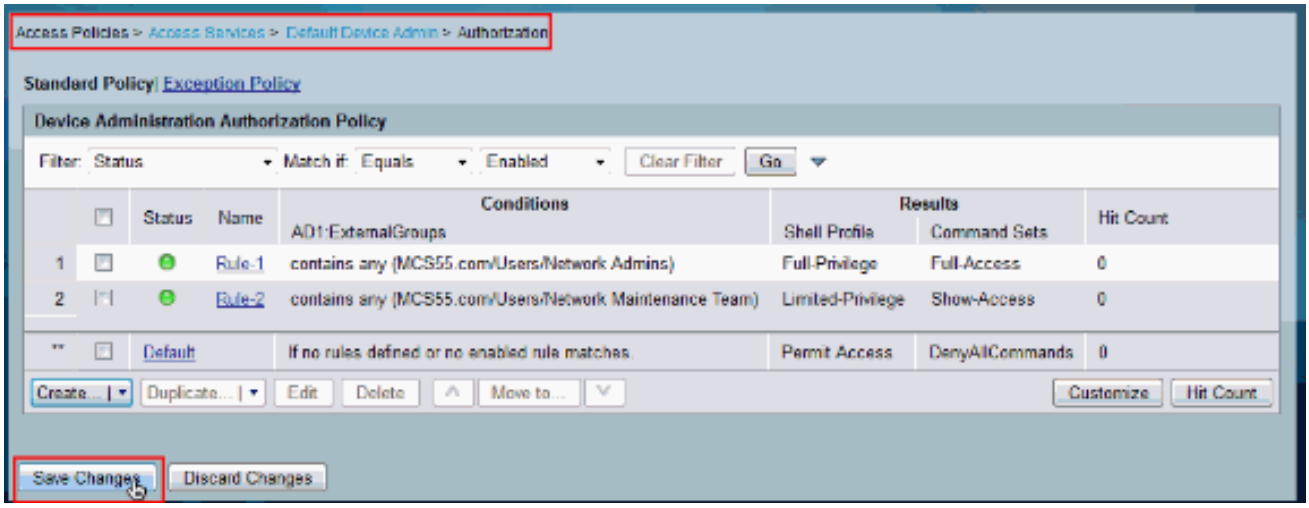
37. Klicken Sie auf **OK**.



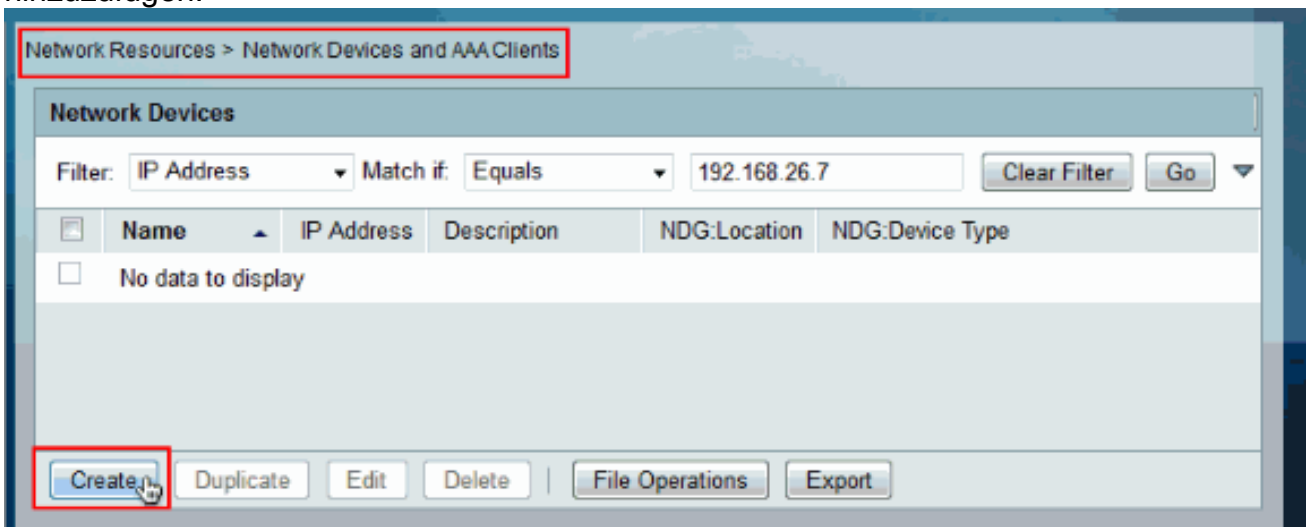
38. Klicken Sie auf **OK**.



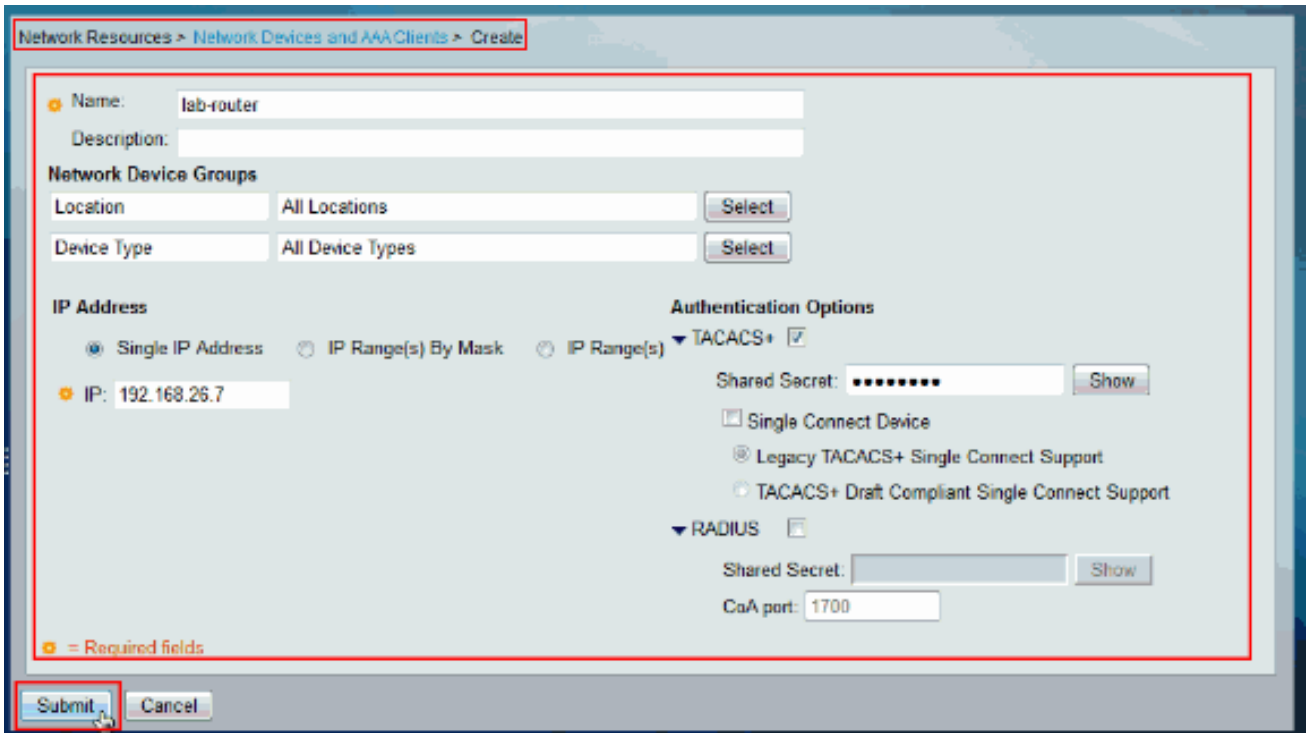
39. Klicken Sie auf **Änderungen speichern**.



40. Klicken Sie auf **Erstellen**, um das **Cisco IOS**-Gerät als **AAA-Client** im ACS hinzuzufügen.



41. Geben Sie einen **Namen, eine IP-Adresse, einen gemeinsamen geheimen Schlüssel** für **TACACS+** an, und klicken Sie auf **Senden**.



[Konfigurieren des Cisco IOS-Geräts für Authentifizierung und Autorisierung]

Führen Sie diese Schritte aus, um das Cisco IOS-Gerät und den ACS für die Authentifizierung und Autorisierung zu konfigurieren.

1. Erstellen Sie einen lokalen Benutzer mit voller Berechtigung für Fallback mit dem Befehl **username**, wie hier gezeigt:
   ```
   username admin privilege 15 password 0 cisco123!
   ```
2. Geben Sie die IP-Adresse des ACS an, um AAA zu aktivieren und ACS 5.x als TACACS-Server hinzuzufügen.
   ```
   aaa new-model
   tacacs-server host 192.168.26.51 key cisco123
   ```
   Hinweis: Der Schlüssel muss mit dem auf dem ACS für dieses Cisco IOS-Gerät bereitgestellten Shared-Secret übereinstimmen.
3. Testen Sie die Erreichbarkeit des TACACS-Servers mit dem **Befehl** test aaa **(Test aa**) wie gezeigt.
   ```
   test aaa group tacacs+ user1 xxxxx legacy
   Attempting authentication test to server-group tacacs+ using tacacs+
   User was successfully authenticated.
   ```
   Die Ausgabe des vorherigen Befehls zeigt, dass der TACACS-Server erreichbar ist und der Benutzer erfolgreich authentifiziert wurde.**Hinweis:** Benutzer1 und Kennwort xxx gehören zu AD. Wenn der Test fehlschlägt, stellen Sie sicher, dass der im vorherigen Schritt angegebene Shared-Secret korrekt ist.
4. Konfigurieren Sie die Anmeldung, aktivieren Sie die Authentifizierung, und verwenden Sie dann die Exec- und Befehlsautorisierungen, wie hier gezeigt:
   ```
   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
   ```
   Hinweis: Die Schlüsselwörter "Lokal" und "Aktivieren" werden für Fallback zum lokalen Cisco IOS-Benutzer verwendet und aktivieren "geheim", wenn der TACACS-Server nicht erreichbar ist.

Überprüfen

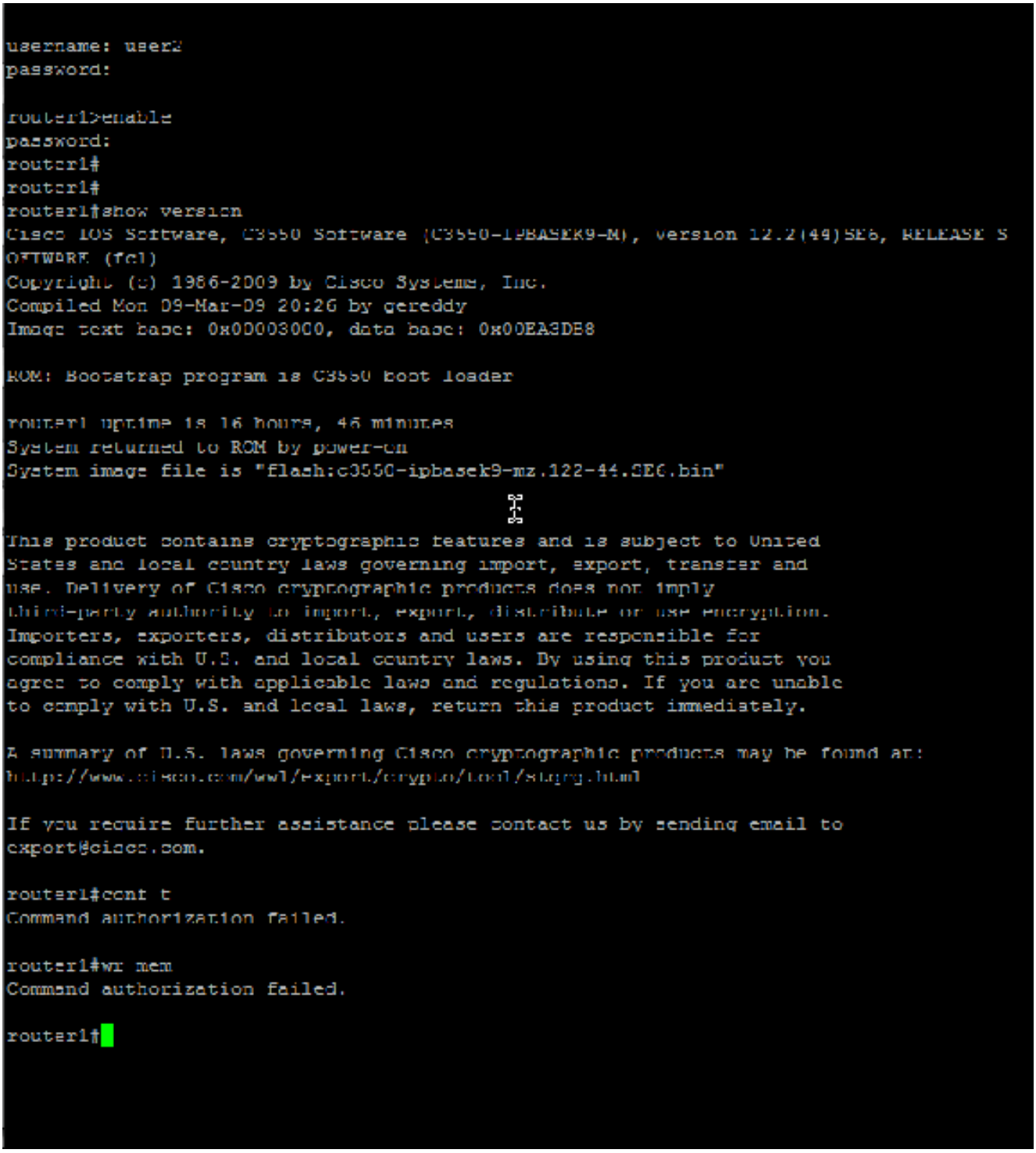
Zur Verifizierung der Authentifizierung und Autorisierung melden Sie sich über Telnet beim Cisco IOS-Gerät an.

1. Telnet zum Cisco IOS-Gerät als Benutzer1, der zur Gruppe mit vollem Zugriff in AD gehört Die Gruppe "Netzwerkadministratoren" ist die Gruppe in AD, die dem vollständigen Privileg-Shell-Profil und dem Vollzugriff-Befehlssatz im ACS zugeordnet ist. Versuchen Sie, einen beliebigen Befehl auszuführen, um sicherzustellen, dass Sie vollständigen Zugriff haben.

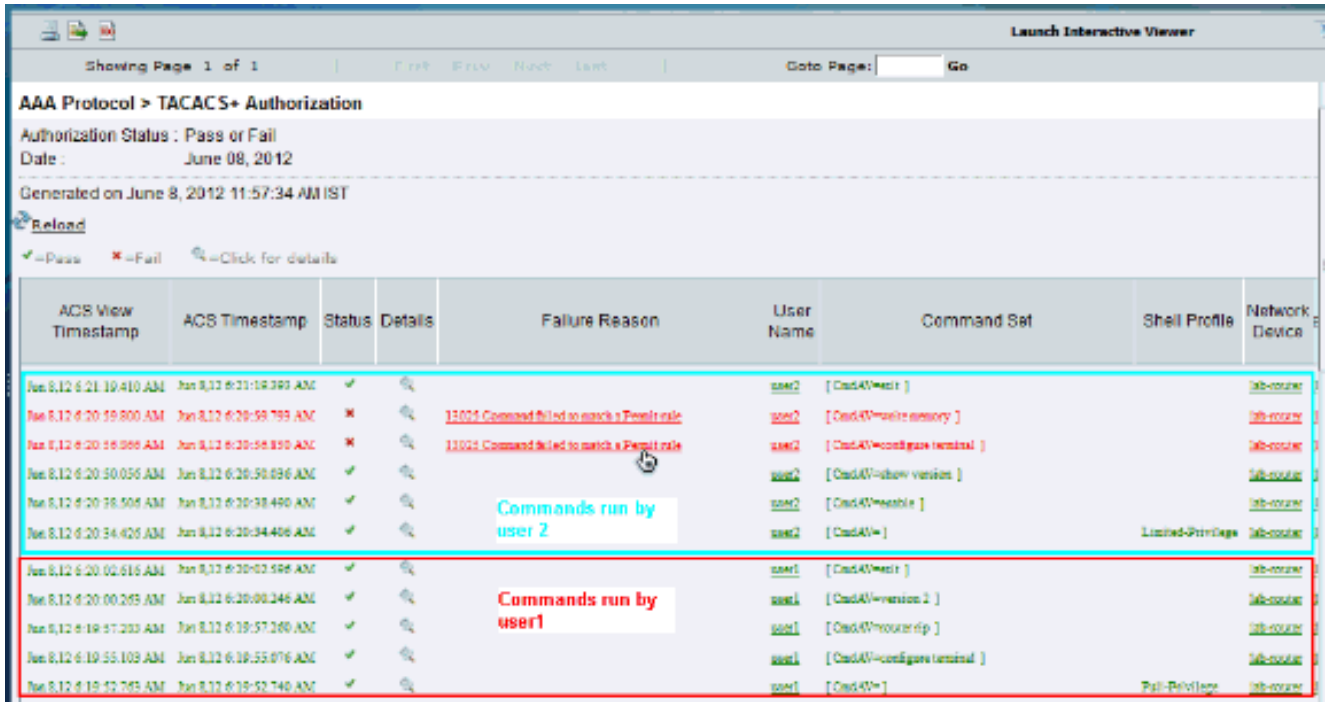
```
username: user1
password:

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 zum Cisco IOS-Gerät als Benutzer2, der zur Gruppe mit beschränktem Zugriff in AD gehört (Die Gruppe des **Netzwerkwartungsteams** ist die Gruppe in AD, die dem **Shell-Profil mit begrenzter Berechtigung** und dem **Befehlssatz Show-Access** auf dem ACS zugeordnet ist.) Wenn Sie versuchen, einen anderen als den im Befehlssatz Show-Access erwähnten Befehl auszuführen, sollten Sie einen Fehler `Command Authorization Failed (Befehlsautorisierung fehlgeschlagen)` erhalten, der anzeigt, dass der Benutzer2 eingeschränkten Zugriff
hat.



3. Melden Sie sich bei der ACS-GUI an, und starten Sie die **Überwachungs- und Berichtsanzeige**. Wählen Sie **AAA Protocol > TACACS+Authorization**, um die von user1 und user2 ausgeführten Aktivitäten zu überprüfen.



Zugehörige Informationen

- Cisco Secure Access Control System
- Technischer Support und Dokumentation - Cisco Systems