ACS Shell-Autorisierungssätze für IOS- und ASA/PIX/FWSM-Konfigurationsbeispiel

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Autorisierungsgruppen
Einen Shell-Befehlsautorisierungssatz hinzufügen
Szenario 1: Berechtigung für Lese-/Schreibzugriff oder vollständigen Zugriff
Szenario 2: Berechtigung für schreibgeschützten Zugriff
Szenario 3: Berechtigung für eingeschränkten Zugriff
Ordnen Sie den Shell-Befehlsautorisierungssatz der Benutzergruppe zu.
Ordnen Sie den Shell-Befehlsautorisierungssatz (ReadWrite-Zugriff) der Benutzergruppe (Admin-Gruppe) zu.
Zuordnen des Shell-Befehlsautorisierungssatzes (schreibgeschützter Zugriff) zu einer Benutzergruppe (schreibgeschützte Gruppe)
Ordnen Sie den Shell-Befehlsautorisierungssatz (Restrict_access) dem Benutzer zu.
IOS-Router-Konfiguration
Konfiguration von ASA/PIX/FWSM
Fehlerbehebung
Fehler: Befehlsautorisierung fehlgeschlagen
Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie die Shell-Autorisierungssätze in Cisco Secure Access Control Server (ACS) für AAA-Clients wie Cisco IOS®-Router oder -Switches und Cisco Security Appliances (ASA/PIX/FWSM) mit TACACS+ als Autorisierungsprotokoll konfiguriert werden.

Hinweis: ACS Express unterstützt keine Befehlsautorisierung.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die grundlegenden Konfigurationen sowohl auf AAA-Clients als auch in ACS festgelegt sind.

Wählen Sie in ACS **Interface Configuration > Advanced Options aus**, und stellen Sie sicher, dass das Kontrollkästchen **Per-user TACACS+/RADIUS Attributes** aktiviert ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Secure Access Control Server (ACS), auf dem die Softwareversion 3.3 und höher ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Autorisierungsgruppen

Befehlsautorisierungssets stellen einen zentralen Mechanismus zur Verfügung, um die Autorisierung jedes Befehls zu steuern, der auf einem bestimmten Netzwerkgerät ausgegeben wird. Diese Funktion verbessert die Skalierbarkeit und Verwaltbarkeit, die zum Festlegen von Autorisierungsbeschränkungen erforderlich sind, erheblich.

Zu den Standardbefehlsautorisierungssätzen in ACS gehören Shell-Befehlsautorisierungssätze und PIX-Befehlsautorisierungssätze. Anwendungen für das Gerätemanagement von Cisco, z. B. CiscoWorks Management Center für Firewalls, können ACS anweisen, zusätzliche Typen von Befehls-Autorisierungssätzen zu unterstützen.

Hinweis: PIX-Befehlsautorisierungssätze erfordern, dass die TACACS+-Befehlsautorisierungsanforderung den Dienst als *pixshell* identifiziert. Stellen Sie sicher, dass dieser Service in der PIX-OS-Version implementiert wurde, die Ihre Firewalls verwenden. Verwenden Sie andernfalls Shell Command Authorization Sets, um die Befehlsautorisierung für PIX-Geräte durchzuführen. Weitere Informationen finden Sie unter Konfigurieren eines Shell-Befehlsautorisierungssatzes für eine Benutzergruppe.

Hinweis: Ab PIX OS 6.3 ist der pixshell-Service nicht mehr implementiert.

Hinweis: Bei den Cisco Security Appliances (ASA/PIX) kann der Benutzer derzeit nicht während der Anmeldung direkt in den Aktivierungsmodus versetzt werden. Der Benutzer muss manuell in den Aktivierungsmodus wechseln.

Um eine bessere Kontrolle über vom Gerät gehostete Telnet-Verwaltungssitzungen zu ermöglichen, kann ein Netzwerkgerät, das TACACS+ verwendet, die Autorisierung für jede Befehlszeile anfordern, bevor sie ausgeführt wird. Sie können eine Reihe von Befehlen definieren, die von einem bestimmten Benutzer auf einem bestimmten Gerät ausgeführt werden dürfen oder die nicht ausgeführt werden dürfen. ACS hat diese Funktion durch folgende Funktionen weiter verbessert:

- **Reusable Named Command Authorization Sets (Wiederverwendbare benannte**

Befehlsautorisierungssätze) - Sie können einen benannten Satz von Befehlsautorisierungen erstellen, ohne direkt einen Benutzer oder eine Benutzergruppe anzugeben. Sie können mehrere Autorisierungssätze für Befehle definieren, die unterschiedliche Zugriffsprofile definieren. Beispiele:Ein *Helpdesk*-Befehlsautorisierungssatz kann den Zugriff auf allgemeine Suchbefehle wie **show run** ermöglichen und Konfigurationsbefehle ablehnen.Ein Befehls-Autorisierungssatz *für alle Netzwerktechniker* könnte eine begrenzte Liste zulässiger Befehle für alle Netzwerktechniker im Unternehmen enthalten.Ein Befehls-Autorisierungssatz *für lokale Netzwerktechniker* kann alle Befehle zulassen (und Befehle zur Konfiguration von IP-Adressen enthalten).

- **Detaillierte Konfiguration** - Sie können Zuordnungen zwischen benannten Befehlsautorisierungssätzen und Netzwerk-Gerätegruppen (NDGs) erstellen. So können Sie je nach den Netzwerkgeräten, auf die zugegriffen wird, unterschiedliche Zugriffsprofile für Benutzer definieren. Sie können denselben benannten Befehlsautorisierungssatz mit mehreren NDGs verknüpfen und für mehrere Benutzergruppen verwenden. ACS sorgt für Datenintegrität. Benannte Befehlsautorisierungssätze werden in der internen ACS-Datenbank gespeichert. Sie können die ACS-Sicherungs- und Wiederherstellungsfunktionen verwenden, um diese zu sichern und wiederherzustellen. Sie können Befehls-Autorisierungssätze zusammen mit anderen Konfigurationsdaten auch auf sekundäre ACSs replizieren.

Für Autorisierungsgruppen, die Cisco Gerätemanagement-Anwendungen unterstützen, bieten sich ähnliche Vorteile, wenn Sie Autorisierungsgruppen verwenden. Sie können Autorisierungssätze für Befehle auf ACS-Gruppen anwenden, die Benutzer der Geräteverwaltungsanwendung enthalten, um die Autorisierung verschiedener Berechtigungen in einer Geräteverwaltungsanwendung durchzusetzen. Die ACS-Gruppen können verschiedenen Rollen innerhalb der Gerätemanagement-Anwendung entsprechen, und Sie können für jede Gruppe je nach Fall unterschiedliche Autorisierungssätze anwenden.

ACS umfasst drei aufeinander folgende Stufen der Autorisierungsfilterung. Jede Befehlsautorisierungsanfrage wird in der aufgeführten Reihenfolge ausgewertet:

1. **Command Match (Befehlsübereinstimmung**) - ACS bestimmt, ob der verarbeitete Befehl mit einem Befehl übereinstimmt, der im Befehlsautorisierungssatz aufgeführt ist. Wenn der Befehl nicht übereinstimmt, wird die Befehlsautorisierung durch die Einstellung für nicht übereinstimmende Befehle bestimmt: *zulassen* oder *verweigern*. Andernfalls wird die Auswertung fortgesetzt, wenn der Befehl zugeordnet wird.
2. **Argument Match** (Argumentübereinstimmung): ACS bestimmt, ob die angezeigten Befehlsargumente mit den im Befehlsautorisierungssatz aufgeführten Befehlsargumenten übereinstimmen.Wenn ein Argument nicht übereinstimmt, wird die Befehlsautorisierung davon bestimmt, ob die Option Nicht übereinstimmende Args zulassen aktiviert ist. Wenn nicht übereinstimmende Argumente zulässig sind, wird der Befehl autorisiert, und die Auswertung wird beendet. Andernfalls wird der Befehl nicht autorisiert, und die Evaluierung wird beendet.Wenn alle Argumente übereinstimmen, wird die Bewertung fortgesetzt.
3. **Argument Policy (Argumentrichtlinie**): Sobald ACS feststellt, dass die Argumente im Befehl mit den Argumenten im Autorisierungssatz übereinstimmen, bestimmt ACS, ob jedes Befehlsargument explizit zulässig ist. Wenn alle Argumente explizit zulässig sind, erteilt ACS die Befehlsautorisierung. Wenn Argumente nicht zulässig sind, verweigert ACS die Befehlsautorisierung.

Einen Shell-Befehlsautorisierungssatz hinzufügen

In diesem Abschnitt werden die folgenden Szenarien beschrieben, wie Sie einen Befehlsautorisierungssatz hinzufügen:

- Szenario 1: Berechtigung für Lese-/Schreibzugriff oder vollständigen Zugriff
- Szenario 2: Berechtigung für schreibgeschützten Zugriff
- Szenario 3: Berechtigung für eingeschränkten Zugriff

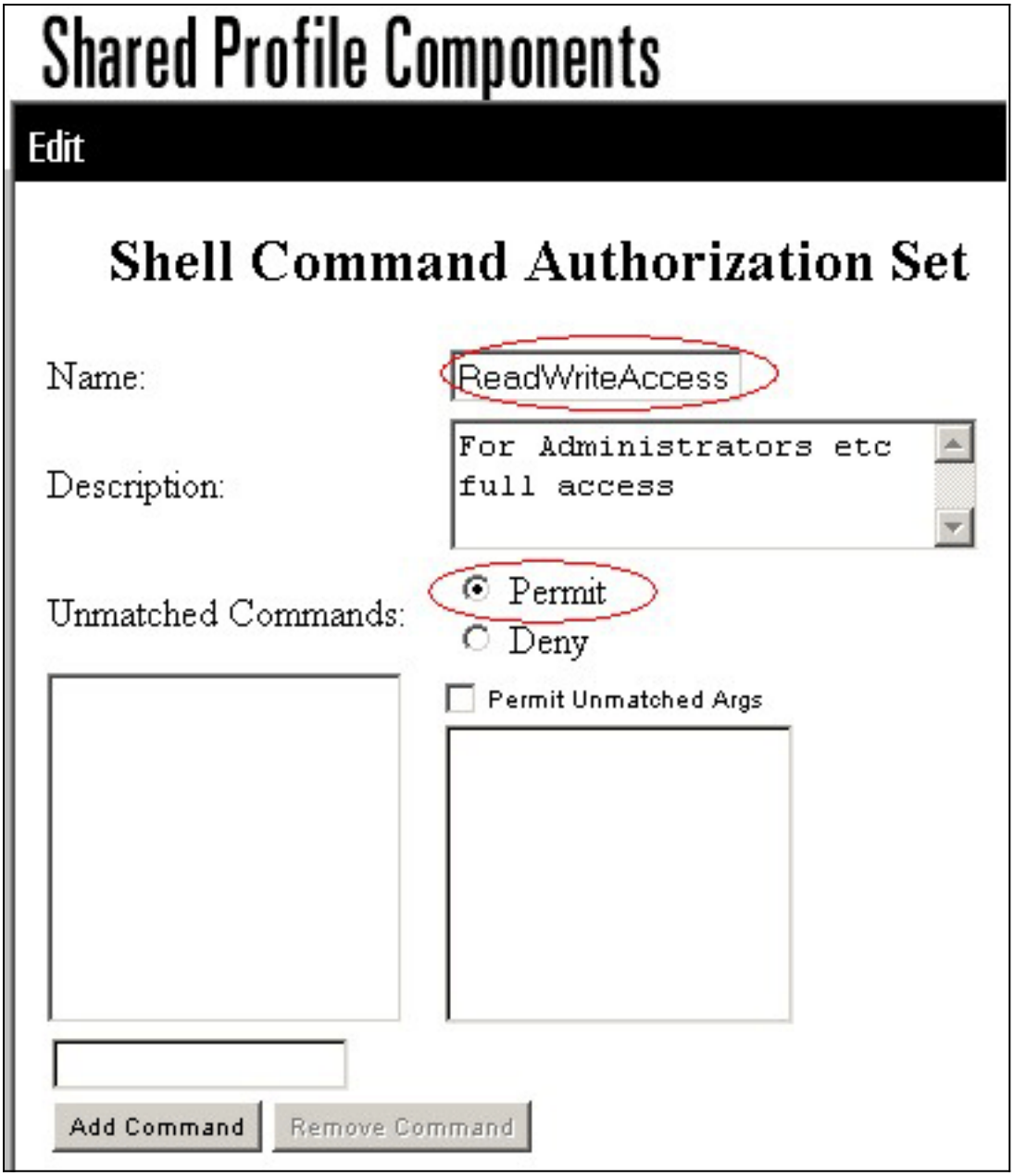
Hinweis: Im Abschnitt Hinzufügen eines Befehls-Autorisierungssatzes des Benutzerhandbuchs für Cisco Secure Access Control Server 4.1 finden Sie weitere Informationen zum Erstellen von Befehls-Autorisierungssätzen. Weitere Informationen zum Bearbeiten und Löschen von Befehlsautorisierungssätzen finden Sie unter Bearbeiten eines Befehlsautorisierungssatzes und Löschen eines Befehlsautorisierungssatzes.

Szenario 1: Berechtigung für Lese-/Schreibzugriff oder vollständigen Zugriff

In diesem Szenario erhalten Benutzer Lese- und Schreibzugriff (oder vollständigen Zugriff).

Konfigurieren Sie im Bereich Shell Command Authorization Set des Fensters Shared Profile Components die folgenden Einstellungen:

1. Geben Sie im Feld Name den Namen **ReadWriteAccess** als Autorisierungsset für den Befehl ein.
2. Geben Sie im Feld Description (Beschreibung) eine Beschreibung für den Autorisierungssatz des Befehls ein.
3. Klicken Sie auf das Optionsfeld **Zulassen** und dann auf **Senden**.

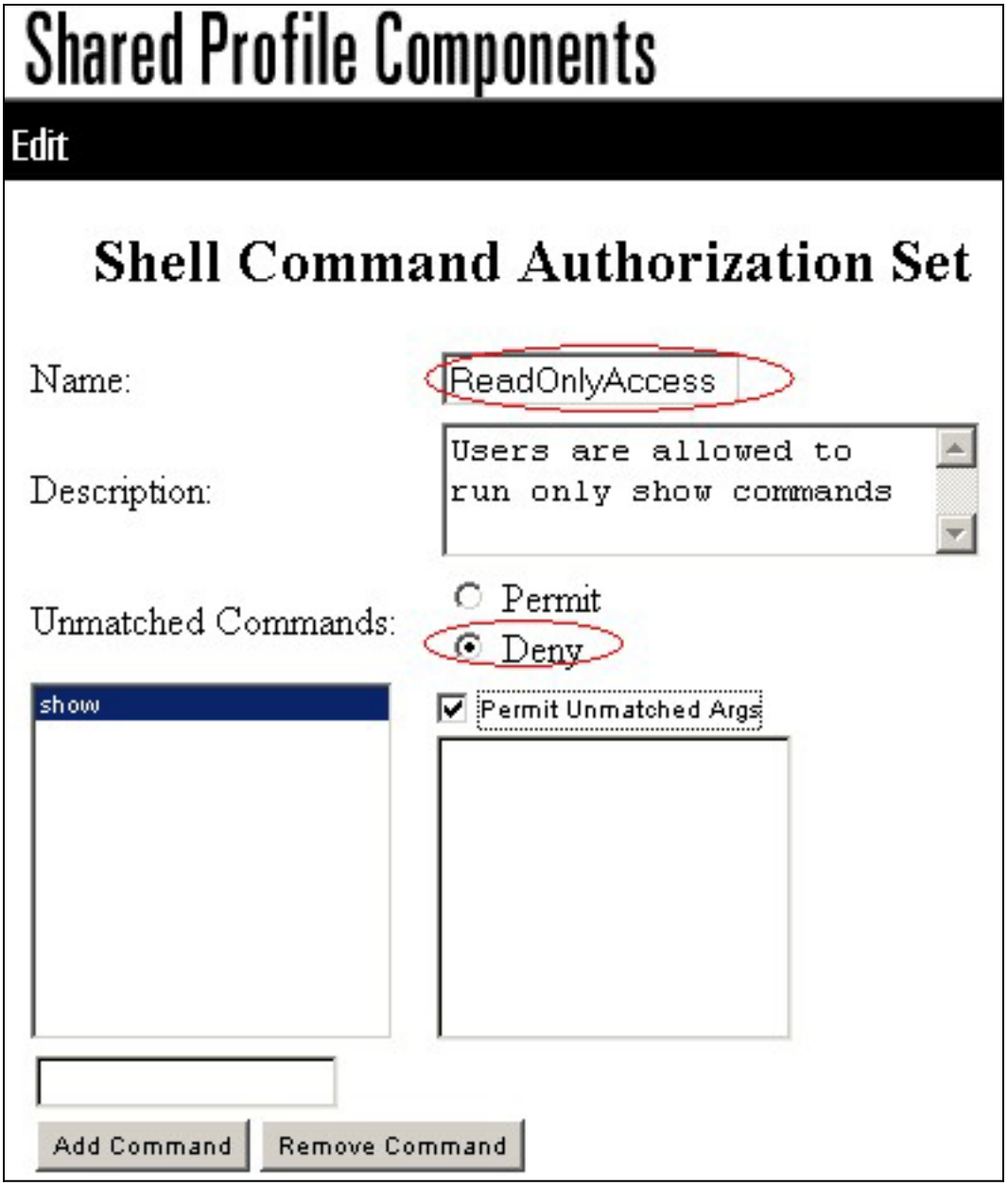


Szenario 2: Berechtigung für schreibgeschützten Zugriff

In diesem Szenario können Benutzer nur **show**-Befehle verwenden.

Konfigurieren Sie im Bereich Shell Command Authorization Set des Fensters Shared Profile Components die folgenden Einstellungen:

1. Geben Sie im Feld Name **ReadOnlyAccess** als Namen des Befehlsautorisierungssatzes ein.
2. Geben Sie im Feld Description (Beschreibung) eine Beschreibung für den Autorisierungssatz des Befehls ein.
3. Klicken Sie auf das Optionsfeld **Verweigern**.
4. Geben Sie den Befehl **show** in das Feld über der Schaltfläche "Befehl hinzufügen" ein, und klicken Sie dann auf **Befehl hinzufügen**.
5. Aktivieren Sie das Kontrollkästchen **"Nicht übereinstimmende Argumente zulassen"**, und klicken Sie auf **Senden**

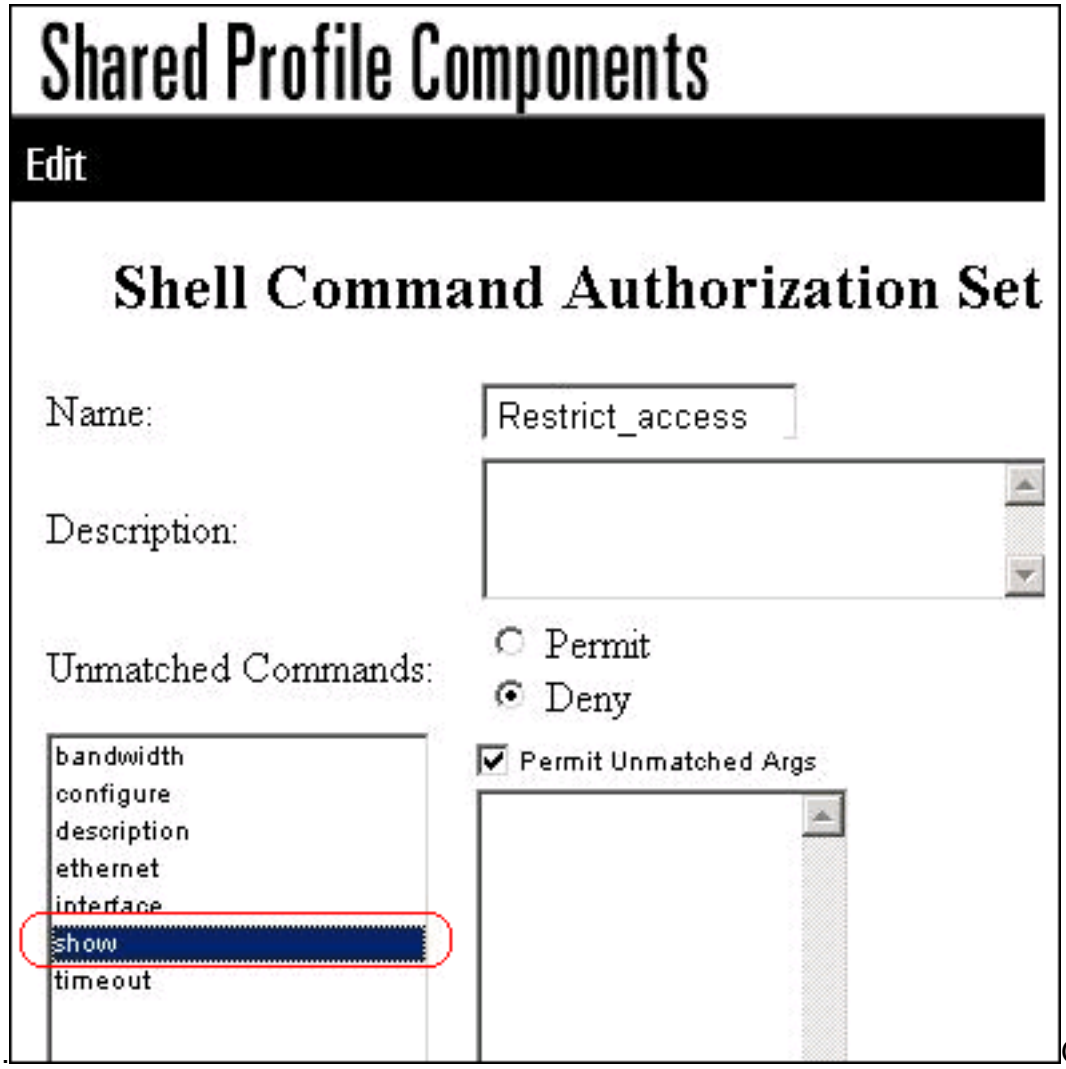


Szenario 3: Berechtigung für eingeschränkten Zugriff

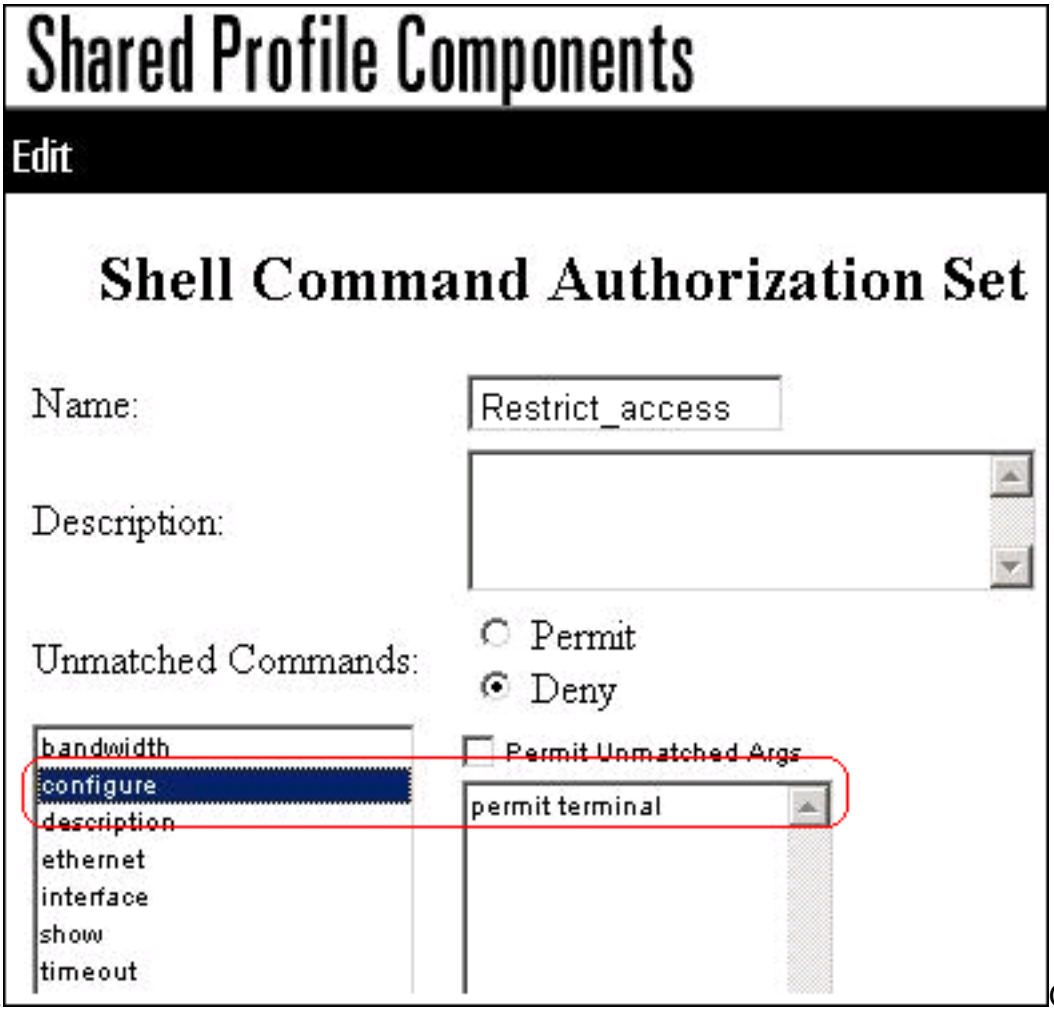
In diesem Szenario können Benutzer selektive Befehle verwenden.

Konfigurieren Sie im Bereich Shell Command Authorization Set des Fensters Shared Profile Components die folgenden Einstellungen:

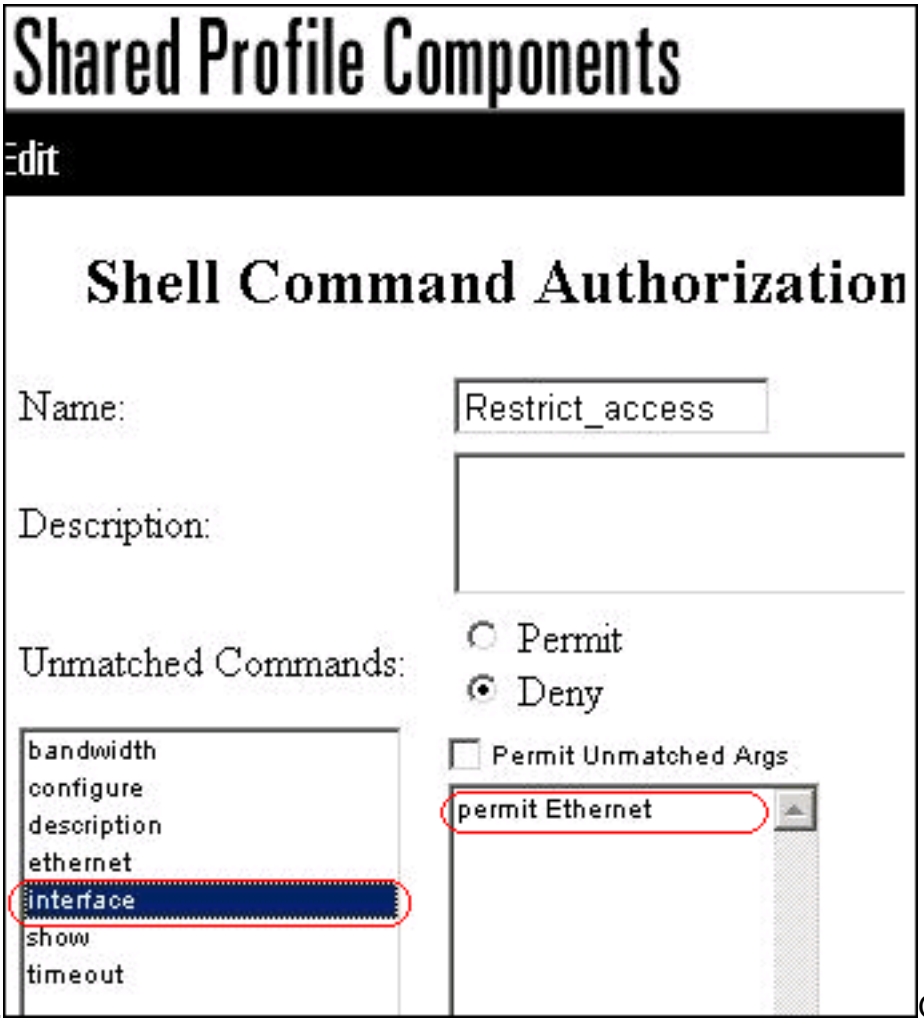
1. Geben Sie im Namensfeld **Restrict_access** als Namen des Befehlsautorisierungssatzes ein.
2. Klicken Sie auf das Optionsfeld **Verweigern**.
3. Geben Sie die Befehle ein, die Sie auf den AAA-Clients zulassen möchten.Geben Sie in das Feld über der Schaltfläche "Befehl hinzufügen" den Befehl **show ein**, und klicken Sie auf **Befehl**



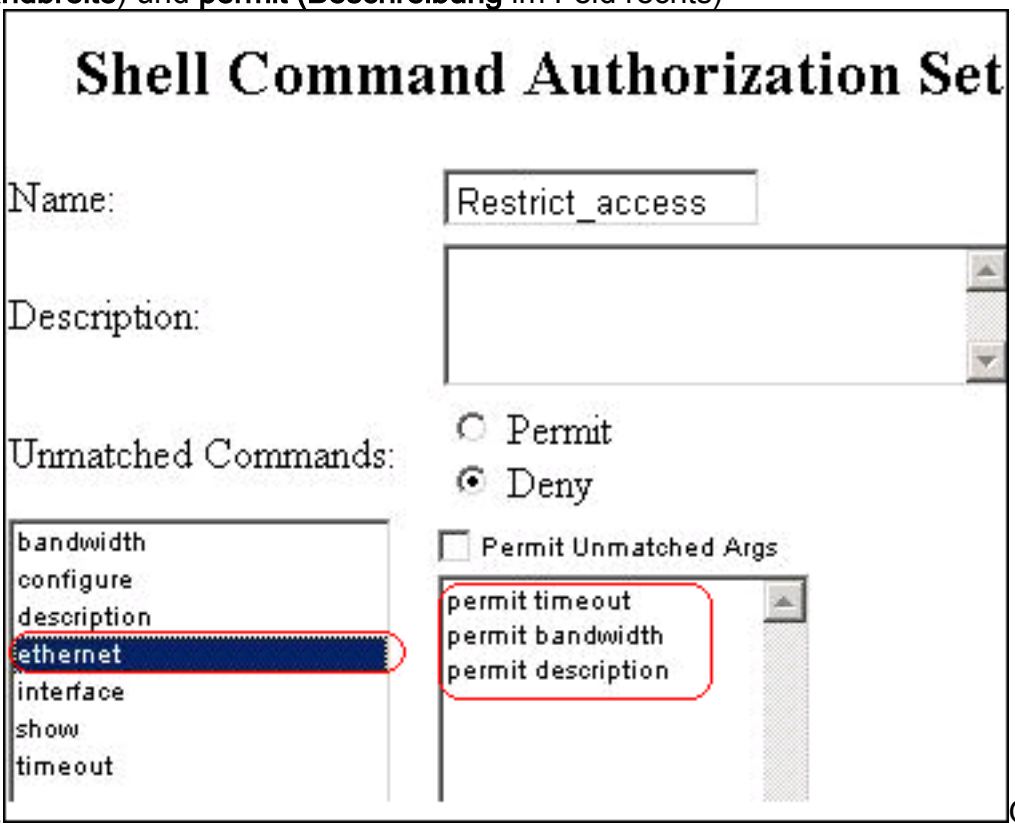
hinzufügen.Geben Sie den Befehl **configure** ein, und klicken Sie auf **Add Command**.Wählen Sie den Befehl **configure** aus, und geben Sie **permit terminal** in das Feld rechts



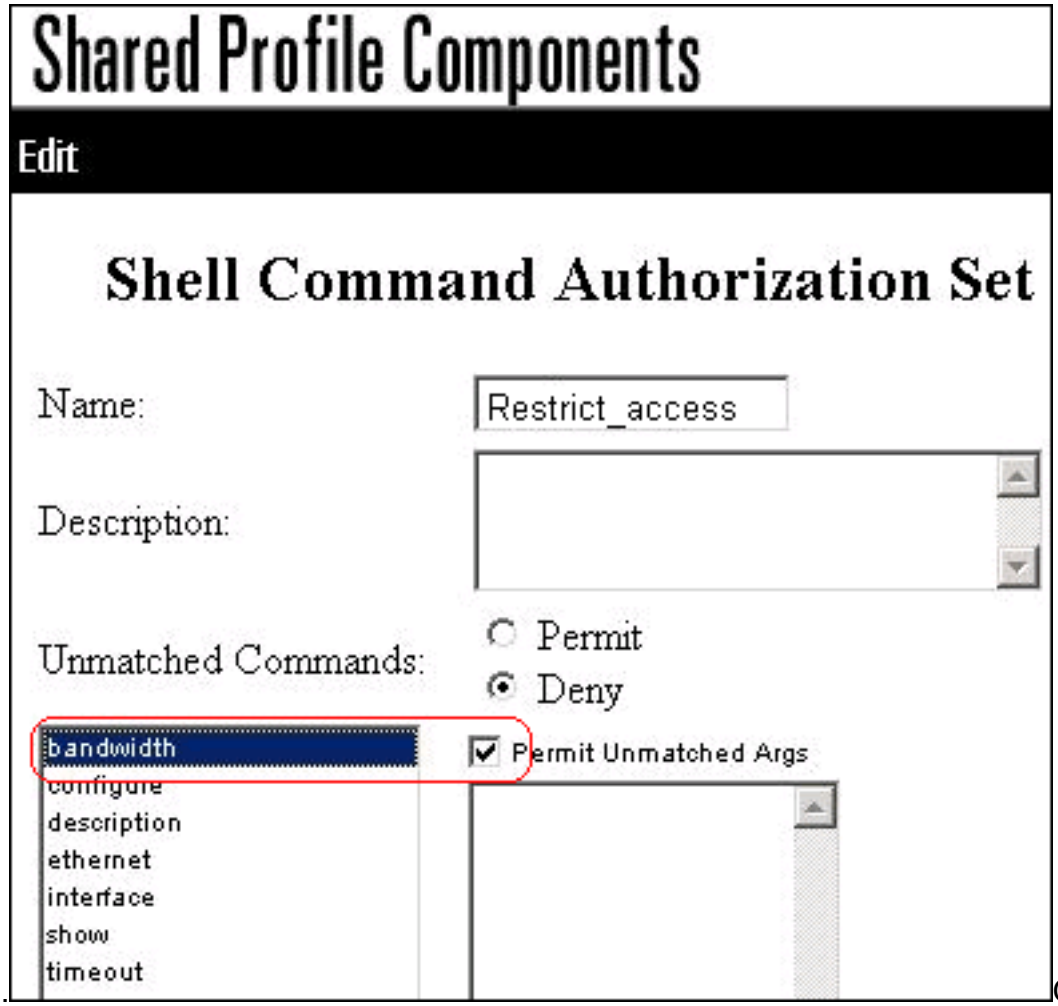
ein.Geben Sie den Befehl **interface** ein, und klicken Sie auf **Add Command**.Wählen Sie den Befehl **interface** aus, und geben Sie in das Feld rechts **permit Ethernet**



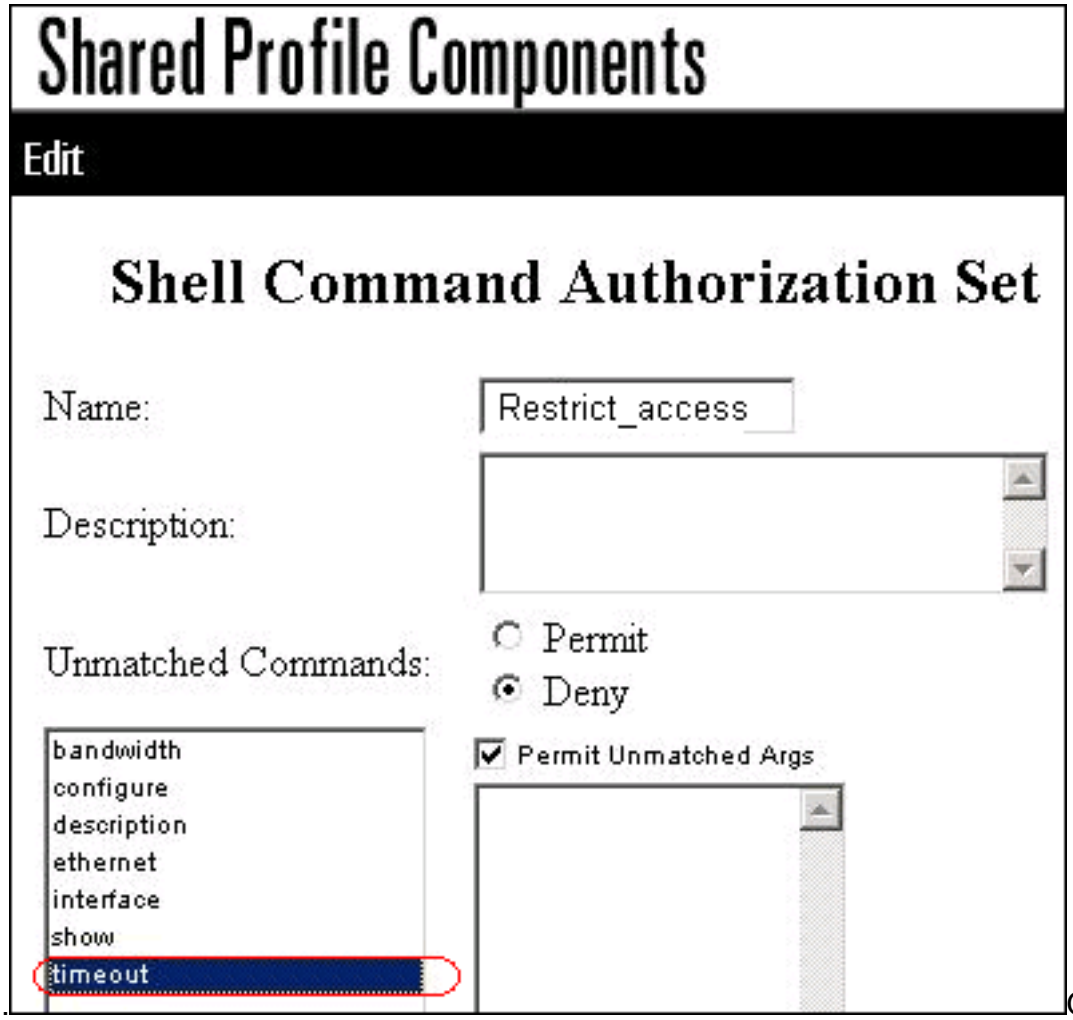
ein. Geben Sie den Befehl **ethernet** ein, und klicken Sie auf **Befehl hinzufügen**.Wählen Sie den Befehl **interface (Schnittstelle)** aus, und geben Sie **permit timeout (**Zeitüberschreitung), **permit bandwidth (Bandbreite)** und **permit (Beschreibung** im Feld rechts)



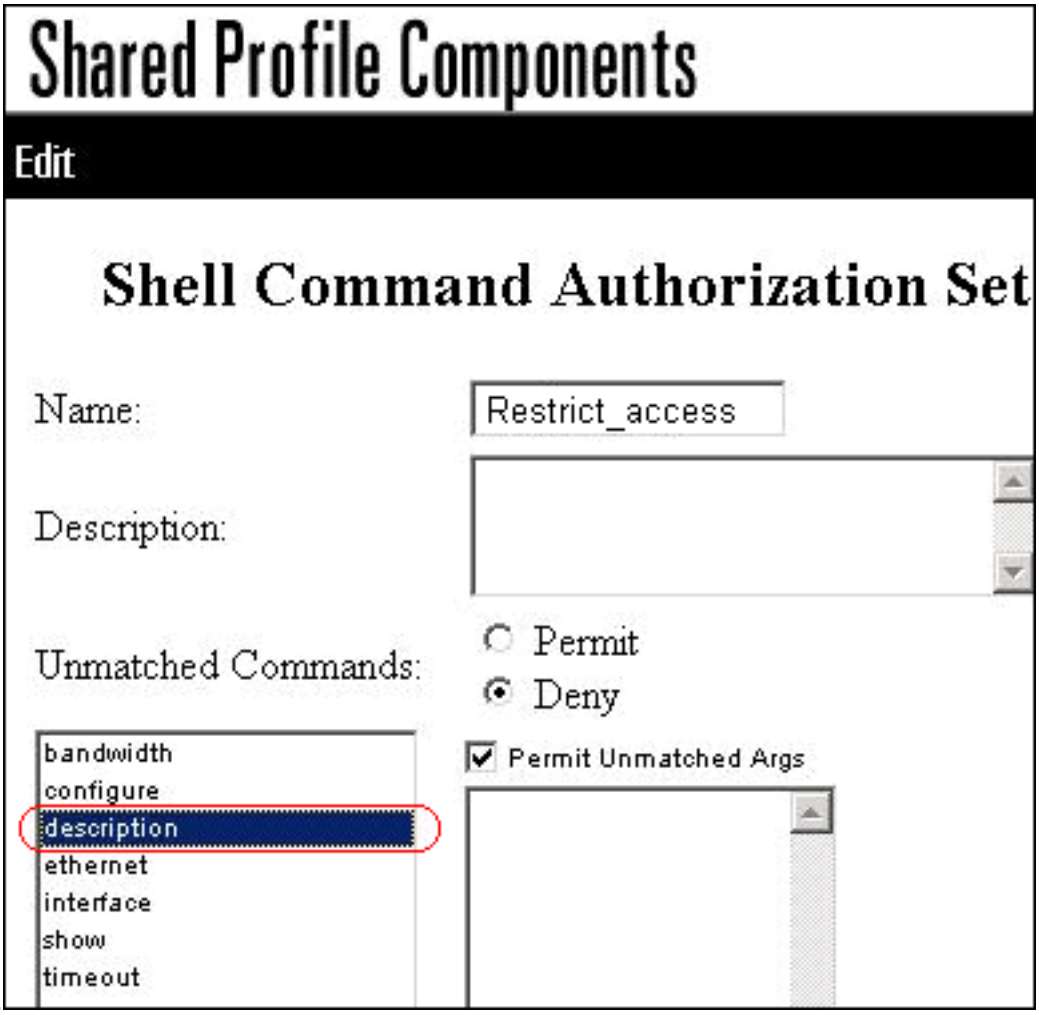
ein. Geben Sie den Befehl **bandwidth** ein, und klicken Sie auf **Add Command (Befehl**



hinzufügen). Geben Sie den Befehl **timeout** ein, und klicken Sie auf **Befehl**



hinzufügen. Geben Sie den Befehl **description** ein, und klicken Sie auf **Add**



Command.

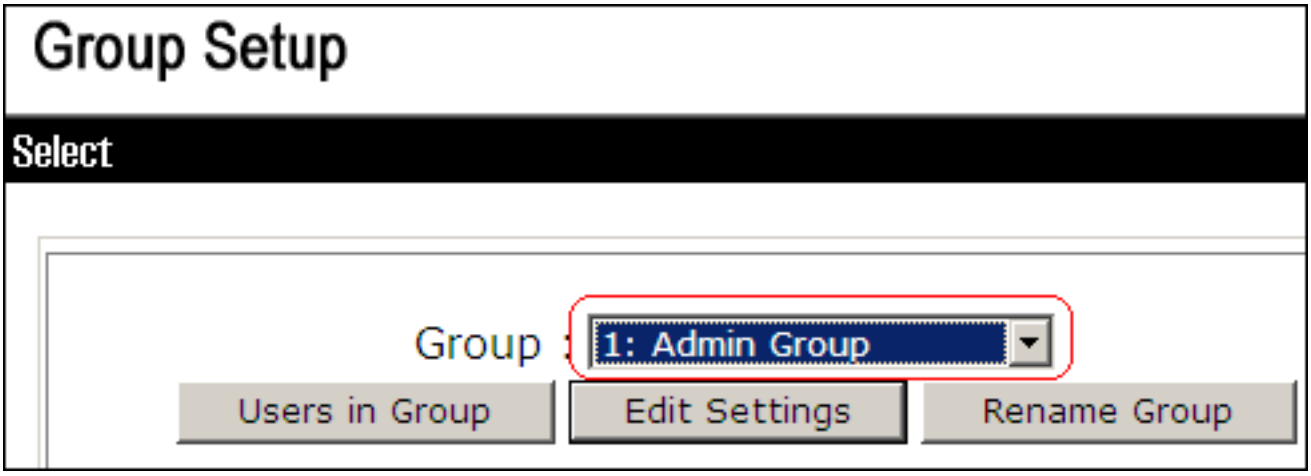
4. Klicken Sie auf **Senden**.

Ordnen Sie den Shell-Befehlsautorisierungssatz der Benutzergruppe zu.

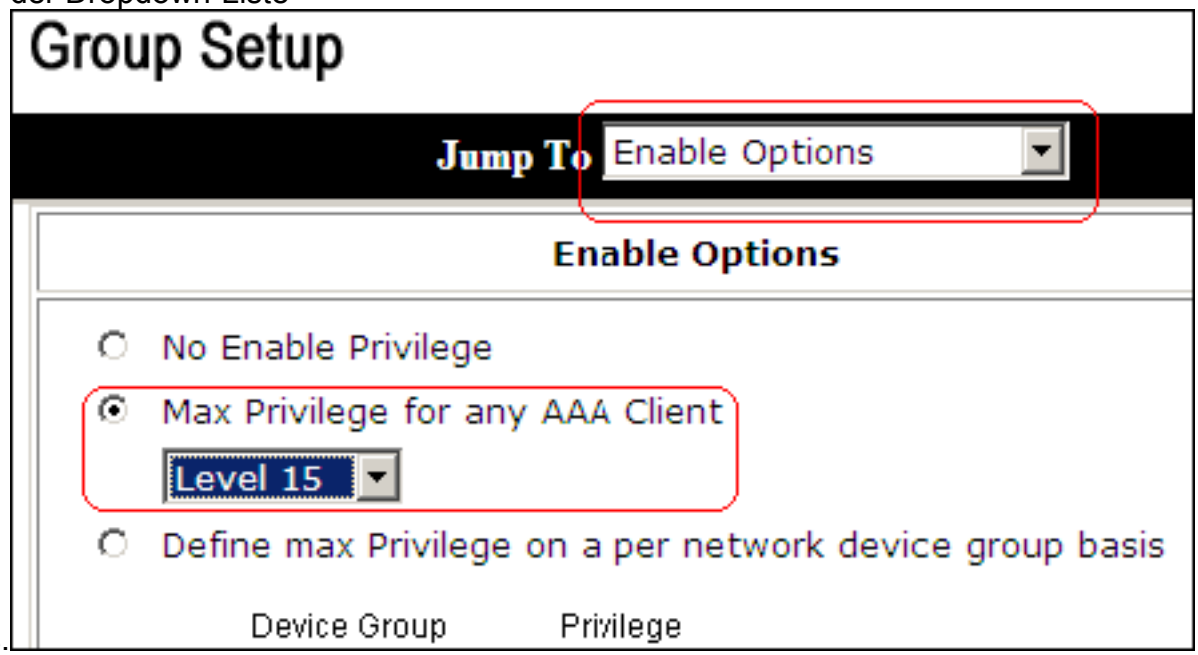
Weitere Informationen zur Konfiguration des Shell-Befehls-Autorisierungssatzes für Benutzergruppen finden Sie im Abschnitt Configuring a Shell Command Authorization Set for a User Group (Konfigurieren eines Shell-Befehls-Autorisierungssatzes für eine Benutzergruppe) des Benutzerhandbuchs für Cisco Secure Access Control Server 4.1.

Ordnen Sie den Shell-Befehlsautorisierungssatz (ReadWrite-Zugriff) der Benutzergruppe (Admin-Gruppe) zu.

1. Klicken Sie im ACS-Fenster auf **Group Setup (Gruppeneinrichtung)**, und wählen Sie **Admin Group (Admin-Gruppe)** aus der Dropdown-Liste Group (Gruppe) aus.

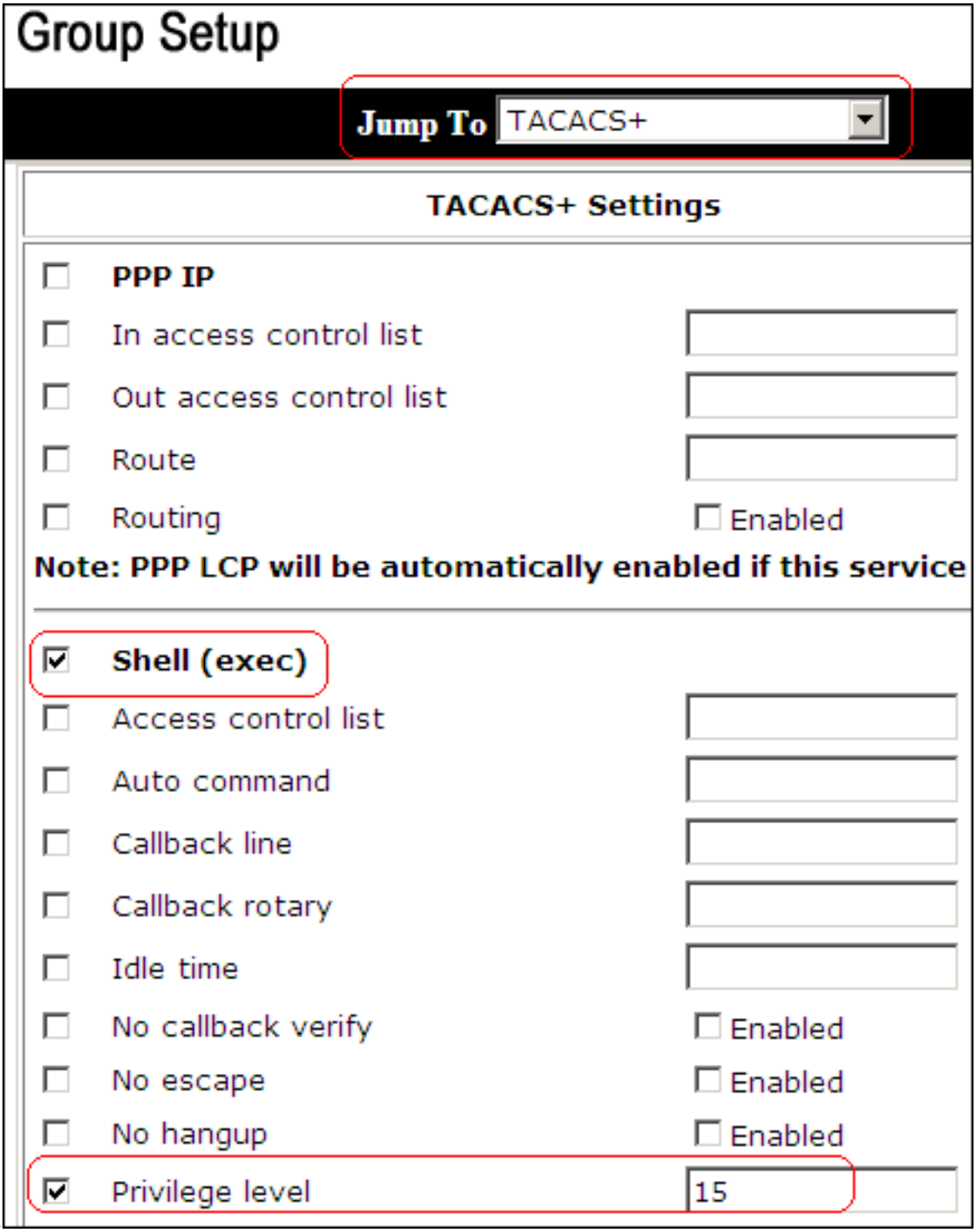


2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie in der Dropdown-Liste Sprung zu die Option **Optionen aktivieren aus**.
4. Klicken Sie im Bereich "Enable Options" (Optionen aktivieren) auf das Optionsfeld **Max Privilege (Maximale Berechtigung) für einen beliebigen AAA-Client,** und wählen Sie **Level 15** aus der Dropdown-Liste



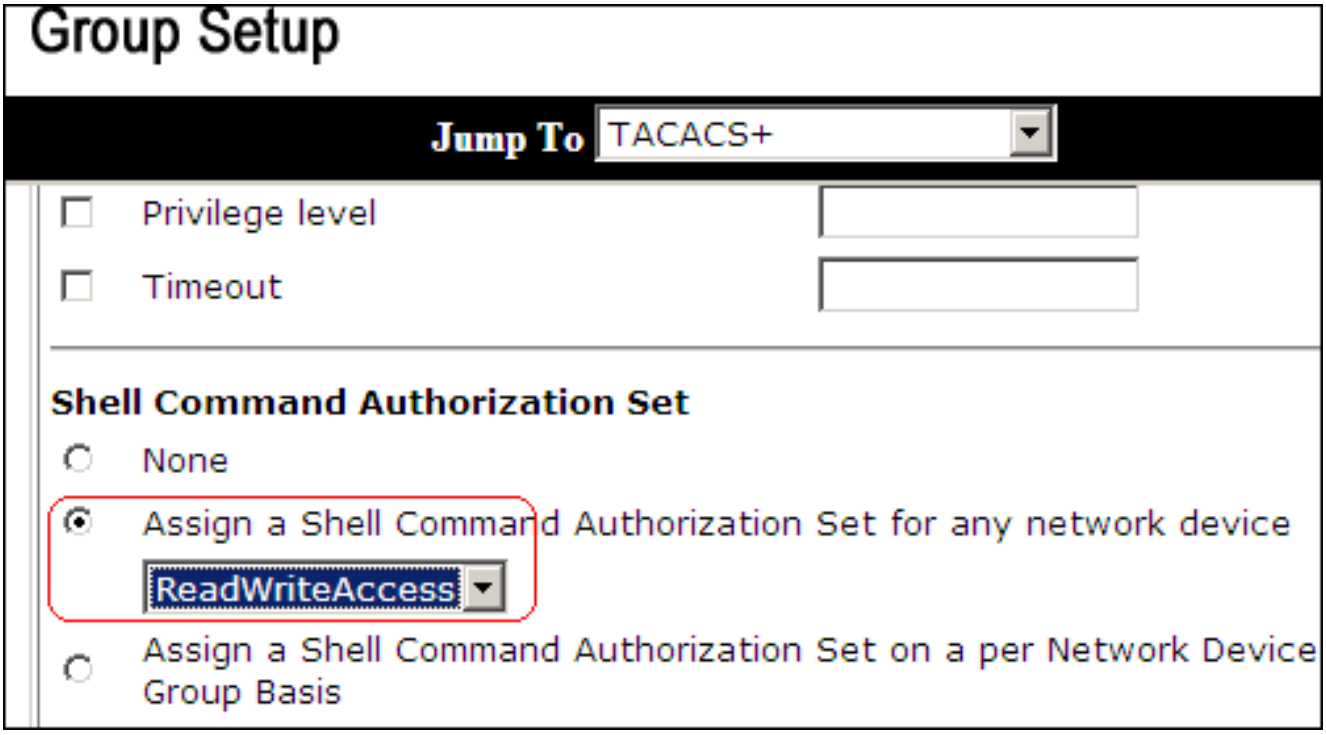
aus.

5. Wählen Sie in der Dropdown-Liste Wechseln zu die Option **TACACS+ aus**.
6. Aktivieren Sie im Bereich TACACS+ Settings (TACACS+-Einstellungen) das Kontrollkästchen **Shell (exec)**, aktivieren Sie das Kontrollkästchen **Privilege level (Berechtigungsstufe)**, und geben Sie **15** in das Feld Privilege level (Berechtigungsstufe)



ein.

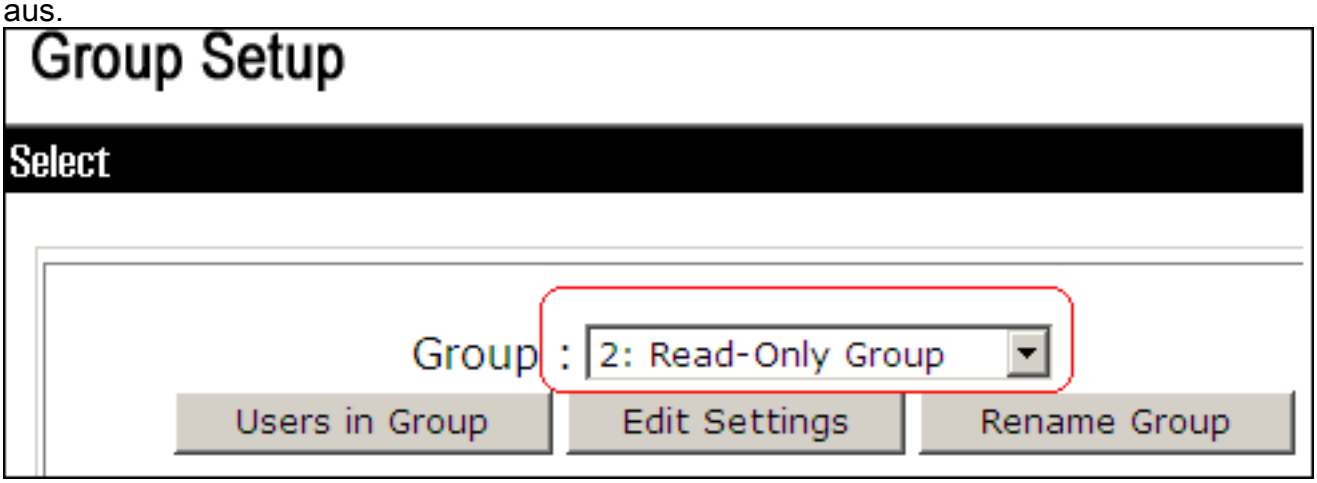
7. Klicken Sie im Bereich Shell Command Authorization Set auf das Optionsfeld **Shell Command Authorization Set für ein Netzwerkgerät zuweisen,** und wählen Sie **ReadWriteAccess** aus der Dropdown-Liste aus.



8. Klicken Sie auf **Senden**

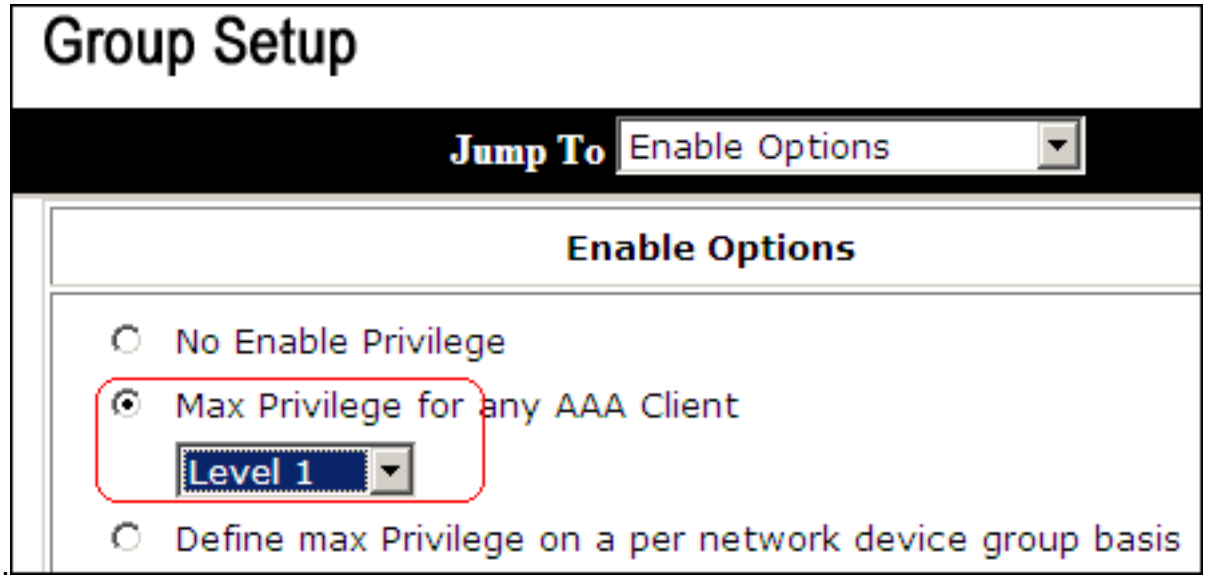
Zuordnen des Shell-Befehlsautorisierungssatzes (schreibgeschützter Zugriff) zu einer Benutzergruppe (schreibgeschützte Gruppe)

1. Klicken Sie im ACS-Fenster auf **Group Setup (Gruppeneinrichtung)**, und wählen Sie **Read-Only Group (Schreibgeschützte Gruppe)** aus der Dropdown-Liste Group (Gruppe) aus.



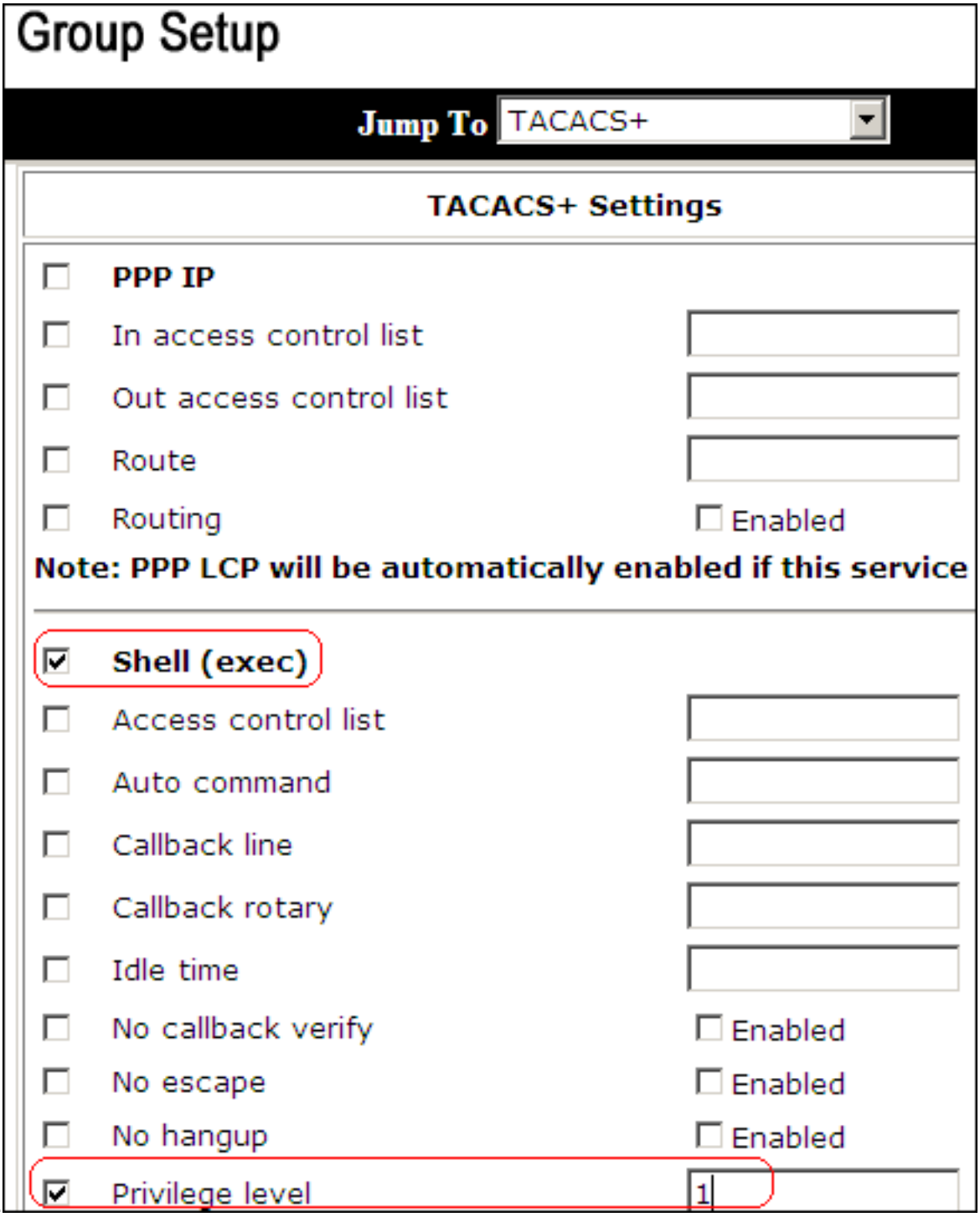
2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie in der Dropdown-Liste Sprung zu die Option **Optionen aktivieren aus**.
4. Klicken Sie im Bereich "Enable Options" (Optionen aktivieren) auf das Optionsfeld **Max Privilege (Maximale Berechtigung für einen beliebigen AAA-Client)**, und wählen Sie **Level 1** aus der Dropdown-Liste

aus.



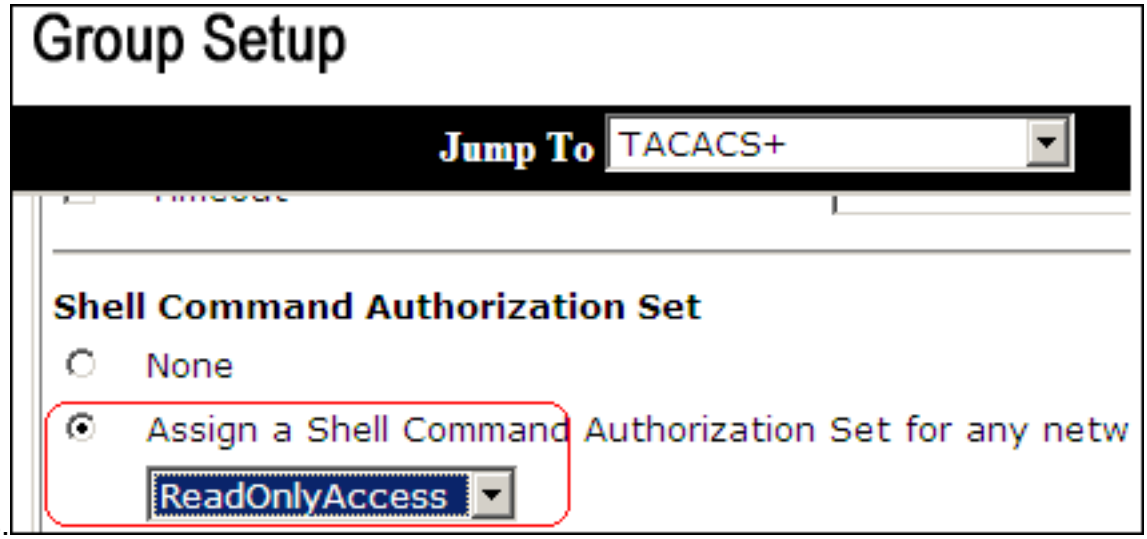
5. Aktivieren Sie im Bereich TACACS+ Settings (TACACS+-Einstellungen) das Kontrollkästchen **Shell (exec)**, aktivieren Sie das Kontrollkästchen **Privilege level (Berechtigungsstufe)**, und geben Sie **1** in das Feld Privilege level (Berechtigungsstufe)

ein.



6. Klicken Sie im Bereich Shell Command Authorization Set auf das Optionsfeld **Shell Command Authorization Set für ein Netzwerkgerät zuweisen,** und wählen Sie **ReadOnlyAccess** aus der Dropdown-Liste

aus.



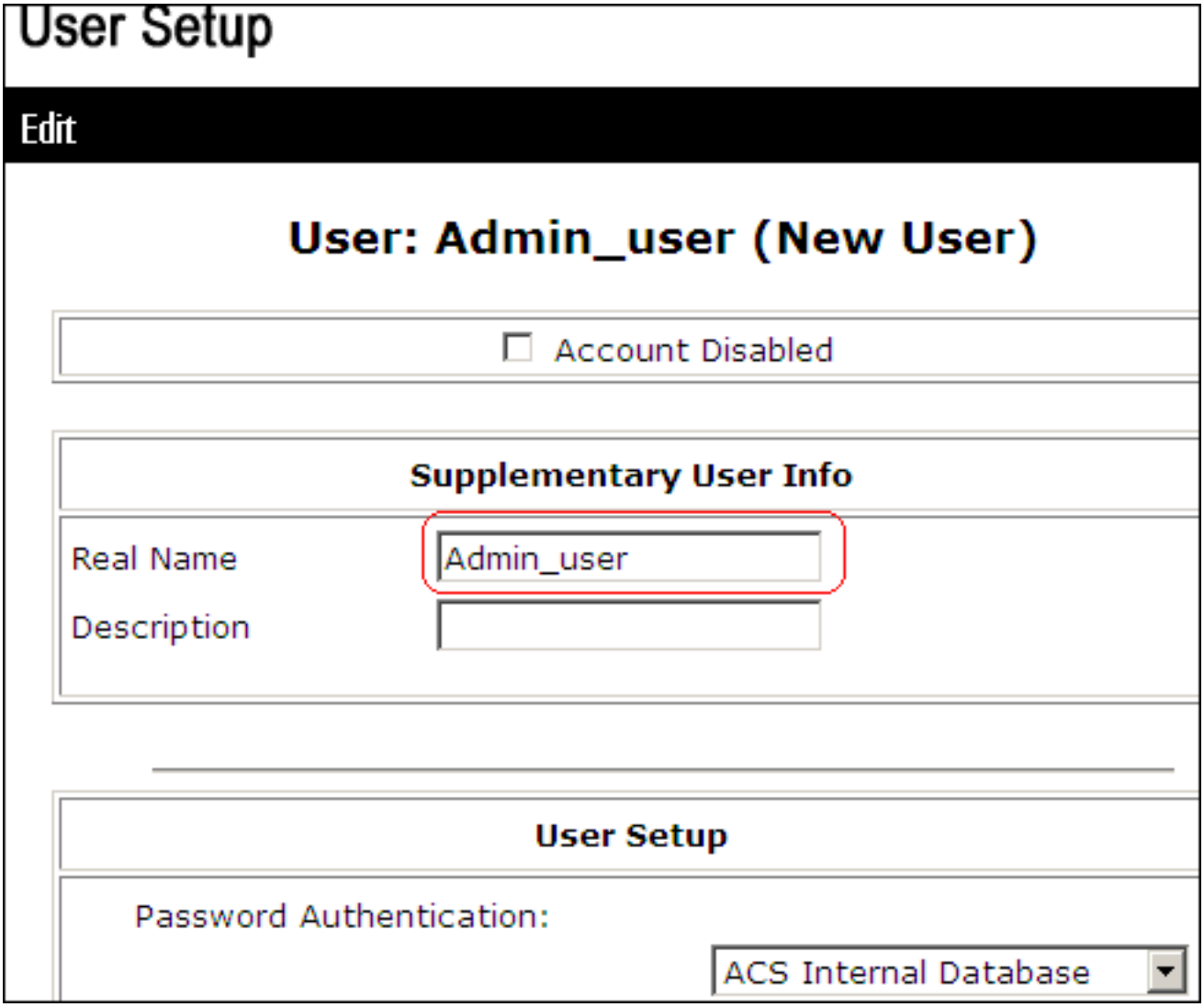
7. Klicken Sie auf **Senden**

Ordnen Sie den Shell-Befehlsautorisierungssatz (Restrict_access) dem Benutzer zu.

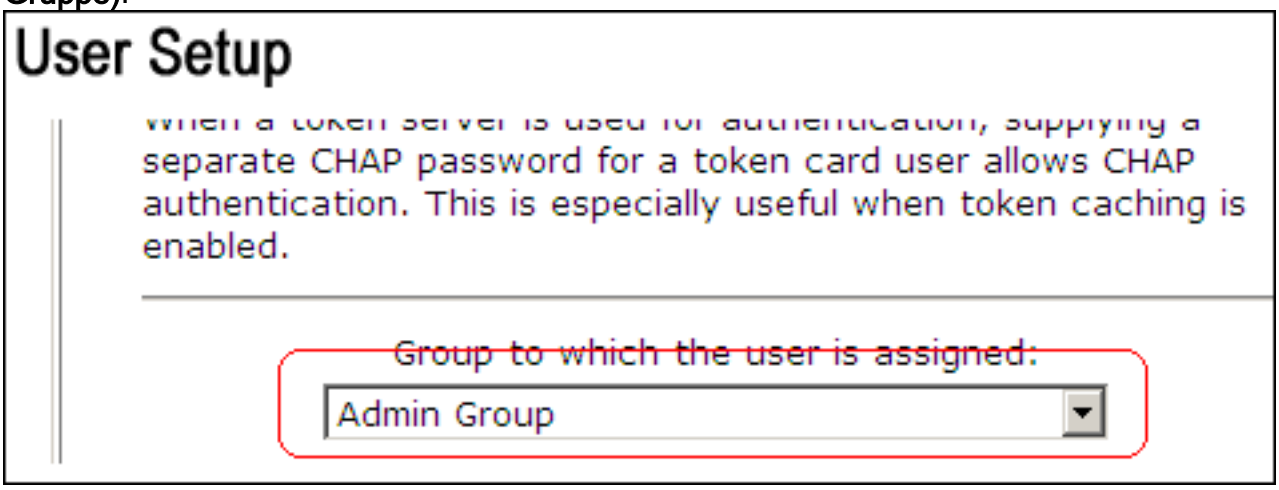
Weitere Informationen zur Konfiguration des Shell-Befehls-Autorisierungssatzes für Benutzer finden Sie im Abschnitt Configuring a Shell Command Authorization Set for a User im Benutzerhandbuch für Cisco Secure Access Control Server 4.1.

Hinweis: Einstellungen auf Benutzerebene setzen die Einstellungen auf Gruppenebene in ACS außer Kraft. Wenn der Benutzer also in den Einstellungen auf Benutzerebene über eine Shell-Befehlsautorisierung verfügt, werden die Einstellungen auf Gruppenebene außer Kraft gesetzt.

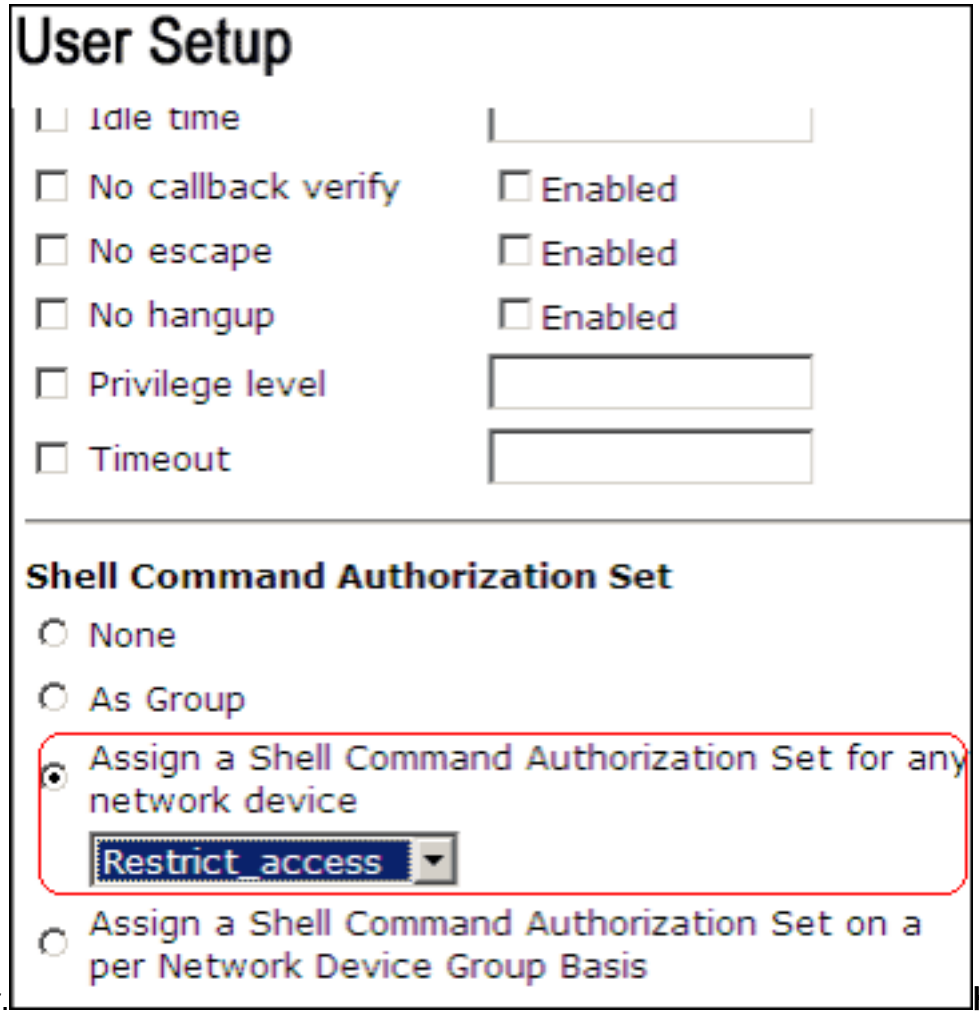
1. Klicken Sie auf **User Setup > Add/Edit**, um einen neuen Benutzer mit dem Namen *Admin_user* zu erstellen, der Teil der Admin-Gruppe sein soll.



2. Wählen Sie in der Dropdown-Liste, der der Benutzer zugewiesen ist, die Option **Admin Group (Admin-Gruppe)**.



3. Klicken Sie im Bereich Shell Command Authorization Set auf das Optionsfeld **Shell Command Authorization Set für ein Netzwerkgerät zuweisen,** und wählen Sie **Restrict_access** aus der Dropdown-Liste aus.**Hinweis:** In diesem Szenario ist dieser Benutzer Teil der Admin-Gruppe. Der Shell-Autorisierungssatz *Restrict_Access* ist anwendbar. der Autorisierungssatz der *ReadWrite Access*-Shell ist nicht



anwendbar. **Hinweis:** Vergewissern Sie sich im Abschnitt TACACS+ (Cisco) des Bereichs "Interface Configuration", dass die Option **Shell (exec)** in der Spalte User ausgewählt ist.

IOS-Router-Konfiguration

Zusätzlich zu Ihrer voreingestellten Konfiguration sind diese Befehle auf einem IOS-Router oder -Switch erforderlich, um die Befehlsautorisierung über einen ACS-Server zu implementieren:

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

Konfiguration von ASA/PIX/FWSM

Zusätzlich zu Ihrer voreingestellten Konfiguration sind diese Befehle auf ASA/PIX/FWSM erforderlich, um die Befehlsautorisierung über einen ACS-Server zu implementieren:

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

Hinweis: Es ist nicht möglich, das RADIUS-Protokoll zu verwenden, um den Benutzerzugriff auf

ASDM zu schreibgeschützten Zwecken zu beschränken. Da die RADIUS-Pakete gleichzeitig Authentifizierung und Autorisierung enthalten, haben alle Benutzer, die im RADIUS-Server authentifiziert werden, die Privilegstufe 15. Dies kann durch TACACS mit der Implementierung von Befehlsautorisierungssätzen erreicht werden.

Hinweis: Die Ausführung jedes typisierten Befehls durch ASA/PIX/FWSM dauert lange, auch wenn ACS für die Befehlsautorisierung nicht verfügbar ist. Wenn ACS nicht verfügbar ist und ASA über eine Befehlsautorisierung verfügt, fordert ASA die Befehlsautorisierung für jeden Befehl an.

Fehlerbehebung

Fehler: Befehlsautorisierung fehlgeschlagen

Problem

Nachdem Sie sich über die TACACS-Protokollierung bei der Firewall angemeldet haben, funktionieren die Befehle nicht mehr. Wenn Sie einen Befehl eingeben, wird dieser Fehler angezeigt: `Befehlsautorisierung fehlgeschlagen.`

Lösung

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Stellen Sie sicher, dass der richtige Benutzername verwendet wird und dem Benutzer alle erforderlichen Berechtigungen zugewiesen sind.
2. Wenn Benutzername und Berechtigungen korrekt sind, stellen Sie sicher, dass die ASA über eine Verbindung mit dem ACS verfügt und dass der ACS aktiv ist.

Hinweis: Dieser Fehler kann auch auftreten, wenn der Administrator versehentlich die Befehlsautorisierung für lokale Benutzer sowie für TACACS-Benutzer konfiguriert hat. Führen Sie in diesem Fall eine Kennwortwiederherstellung durch, um das Problem zu beheben.

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Sicherheitsprodukt - Problemhinweise (einschließlich PIX)
- Request For Comments (RFCs)
- Support-Seite für Cisco Secure Control Access Control Server
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.