Esempi di set di autorizzazioni dei comandi della shell ACS su IOS e ASA/PIX/FWSM

Sommario

Introduzione

In questo documento viene descritto come configurare i set di autorizzazioni della shell in Cisco Secure Access Control Server (ACS) per i client AAA, come router o switch Cisco IOS® e le appliance di sicurezza Cisco (ASA/PIX/FWSM) con TACACS+ come protocollo di autorizzazione.

Nota: ACS Express non supporta l'autorizzazione dei comandi.

Prerequisiti

Requisiti

In questo documento si presume che le configurazioni di base siano impostate sia nei client AAA che negli ACS.

In ACS, selezionare **Configurazione interfaccia > Opzioni avanzate** e verificare che la casella di controllo **Attributi TACACS+/RADIUS per utente** sia selezionata.

Componenti usati

Per questo documento, è stato usato un Cisco Secure Access Control Server (ACS) con software versione 3.3 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Set di autorizzazioni dei comandi

I set di autorizzazioni dei comandi forniscono un meccanismo centrale per controllare l'autorizzazione di ciascun comando emesso su un determinato dispositivo di rete. Questa funzionalità migliora notevolmente la scalabilità e la gestibilità richieste per impostare le restrizioni alle autorizzazioni.

In ACS, i set di autorizzazioni dei comandi predefiniti includono i Set di autorizzazioni dei comandi Shell e i Set di autorizzazioni dei comandi PIX. Le applicazioni di gestione dei dispositivi Cisco, ad esempio CiscoWorks Management Center for Firewall, possono indicare ad ACS di supportare tipi di set di autorizzazioni dei comandi aggiuntivi.

Nota: i set di autorizzazioni dei comandi PIX richiedono che la richiesta di autorizzazione dei comandi TACACS+ identifichi il servizio come *pixshell*. Verificare che il servizio sia stato implementato nella versione di PIX OS utilizzata dai firewall; in caso contrario, utilizzare i set di autorizzazione dei comandi Shell per eseguire l'autorizzazione dei comandi per i dispositivi PIX. per ulteriori informazioni, fare riferimento a Configurazione di un set di autorizzazioni dei comandi della shell per un gruppo di utenti.

Nota: a partire dalla versione 6.3 di PIX OS, il servizio pixshell non è stato implementato.

Nota: le appliance di sicurezza Cisco (ASA/PIX) non consentono al momento di attivare la modalità di abilitazione direttamente dall'utente durante il login. L'utente deve accedere manualmente alla modalità di abilitazione.

Per offrire un maggiore controllo delle sessioni Telnet amministrative ospitate dai dispositivi, un dispositivo di rete che utilizza TACACS+ può richiedere l'autorizzazione per ciascuna riga di comando prima dell'esecuzione. È possibile definire una serie di comandi che possono essere o meno eseguiti da un utente specifico su un determinato dispositivo. ACS ha ulteriormente migliorato questa funzionalità con queste caratteristiche:

- **Set di autorizzazioni dei comandi denominati riutilizzabili**: senza la citazione diretta di alcun utente o gruppo di utenti, è possibile creare un set denominato di autorizzazioni dei comandi.

È possibile definire diversi set di autorizzazioni dei comandi che delineano diversi profili di accesso. Ad esempio:Un set di autorizzazioni dei comandi dell'*help desk* potrebbe consentire l'accesso a comandi di esplorazione di alto livello, ad esempio **show run**, e negare qualsiasi comando di configurazione.Un set di autorizzazioni dei comandi *Tutti i tecnici di rete* può contenere un elenco limitato di comandi consentiti per qualsiasi tecnico di rete dell'organizzazione.Un set di autorizzazioni dei comandi dei *tecnici di rete locali* potrebbe consentire tutti i comandi e includere i comandi di configurazione degli indirizzi IP.

- **Granularità di configurazione fine**: è possibile creare associazioni tra set di autorizzazioni dei comandi denominati e gruppi di dispositivi di rete (NDG). Pertanto, è possibile definire profili di accesso diversi per gli utenti a seconda dei dispositivi di rete a cui accedono. È possibile associare lo stesso set di autorizzazioni dei comandi con nome a più di un gruppo di nomi e utilizzarlo per più gruppi di utenti. ACS applica l'integrità dei dati. I set di autorizzazioni dei comandi denominati vengono conservati nel database interno di ACS. È possibile utilizzare le funzionalità di backup e ripristino di ACS per eseguirne il backup e il ripristino. È inoltre possibile replicare i set di autorizzazioni dei comandi negli ACS secondari insieme ad altri dati di configurazione.

Per i tipi di set di autorizzazione dei comandi che supportano le applicazioni di gestione dei dispositivi Cisco, i vantaggi sono simili quando si utilizzano i set di autorizzazione dei comandi. È possibile applicare i set di autorizzazioni dei comandi ai gruppi ACS che contengono gli utenti dell'applicazione di gestione dei dispositivi per applicare l'autorizzazione di vari privilegi in un'applicazione di gestione dei dispositivi. I gruppi ACS possono corrispondere a ruoli diversi all'interno dell'applicazione di gestione dei dispositivi ed è possibile applicare set di autorizzazioni dei comandi diversi a ciascun gruppo, a seconda dei casi.

ACS prevede tre fasi sequenziali di filtraggio delle autorizzazioni dei comandi. Ogni richiesta di autorizzazione del comando viene valutata nell'ordine elencato:

1. **Corrispondenza comandi** - ACS determina se il comando elaborato corrisponde a un comando elencato nel set di autorizzazioni dei comandi. Se il comando non corrisponde, l'autorizzazione del comando è determinata dall'impostazione Comandi non corrispondenti: *permettere* o *negare*. In caso contrario, se il comando viene individuato, la valutazione continua.
2. **Corrispondenza argomenti**: ACS determina se gli argomenti del comando presentati corrispondono agli argomenti elencati nel set di autorizzazioni del comando.Se uno degli argomenti non corrisponde, l'autorizzazione del comando viene determinata dall'attivazione o meno dell'opzione Permit Unmatched Args. Se sono consentiti argomenti non corrispondenti, il comando viene autorizzato e la valutazione termina; in caso contrario, il comando non viene autorizzato e la valutazione termina.Se tutti gli argomenti corrispondono, la valutazione continua.
3. **Criteri argomento**: una volta che ACS determina che gli argomenti del comando corrispondono agli argomenti del set di autorizzazioni del comando, ACS determina se ogni argomento del comando è consentito in modo esplicito. Se tutti gli argomenti sono consentiti in modo esplicito, ACS concede l'autorizzazione per il comando. Se uno o più argomenti non sono consentiti, ACS nega l'autorizzazione del comando.

Aggiungere un set di autorizzazioni per i comandi della shell

In questa sezione sono inclusi gli scenari seguenti che descrivono come aggiungere un set di

autorizzazioni per i comandi:

- Scenario 1: Privilegio per accesso in lettura/scrittura o accesso completo
- Scenario 2: Privilegio di accesso in sola lettura
- Scenario 3: Privilegio per accesso limitato

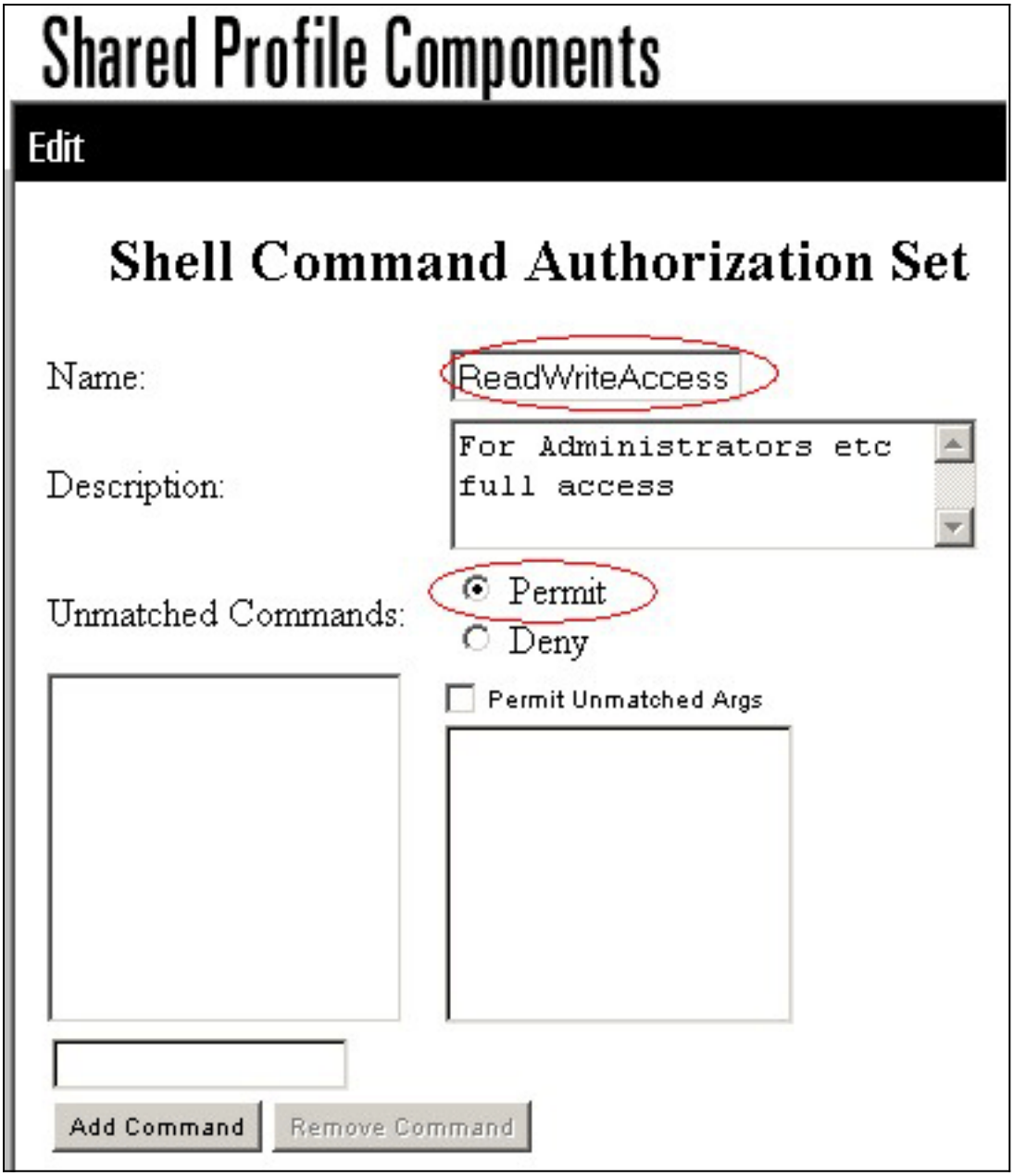
Nota: per ulteriori informazioni su come creare i set di autorizzazioni dei comandi, consultare la sezione Aggiunta di un set di autorizzazioni dei comandi della Guida dell'utente di Cisco Secure Access Control Server 4.1. Per ulteriori informazioni su come modificare ed eliminare i set di autorizzazioni dei comandi, consultare il documento sulla modifica di un set di autorizzazioni dei comandi e sull'eliminazione di un set di autorizzazioni dei comandi.

Scenario 1: Privilegio per accesso in lettura/scrittura o accesso completo

In questi scenari, agli utenti viene concesso l'accesso in lettura/scrittura (o completo).

Nell'area Set di autorizzazioni comandi shell della finestra Componenti profilo condiviso configurare le impostazioni seguenti:

1. Nel campo Name (Nome), immettere **ReadWriteAccess** come nome del set di autorizzazioni del comando.
2. Nel campo Descrizione immettere una descrizione per il set di autorizzazioni del comando.
3. Fare clic sul pulsante di opzione **Autorizza** e quindi su **Invia**.

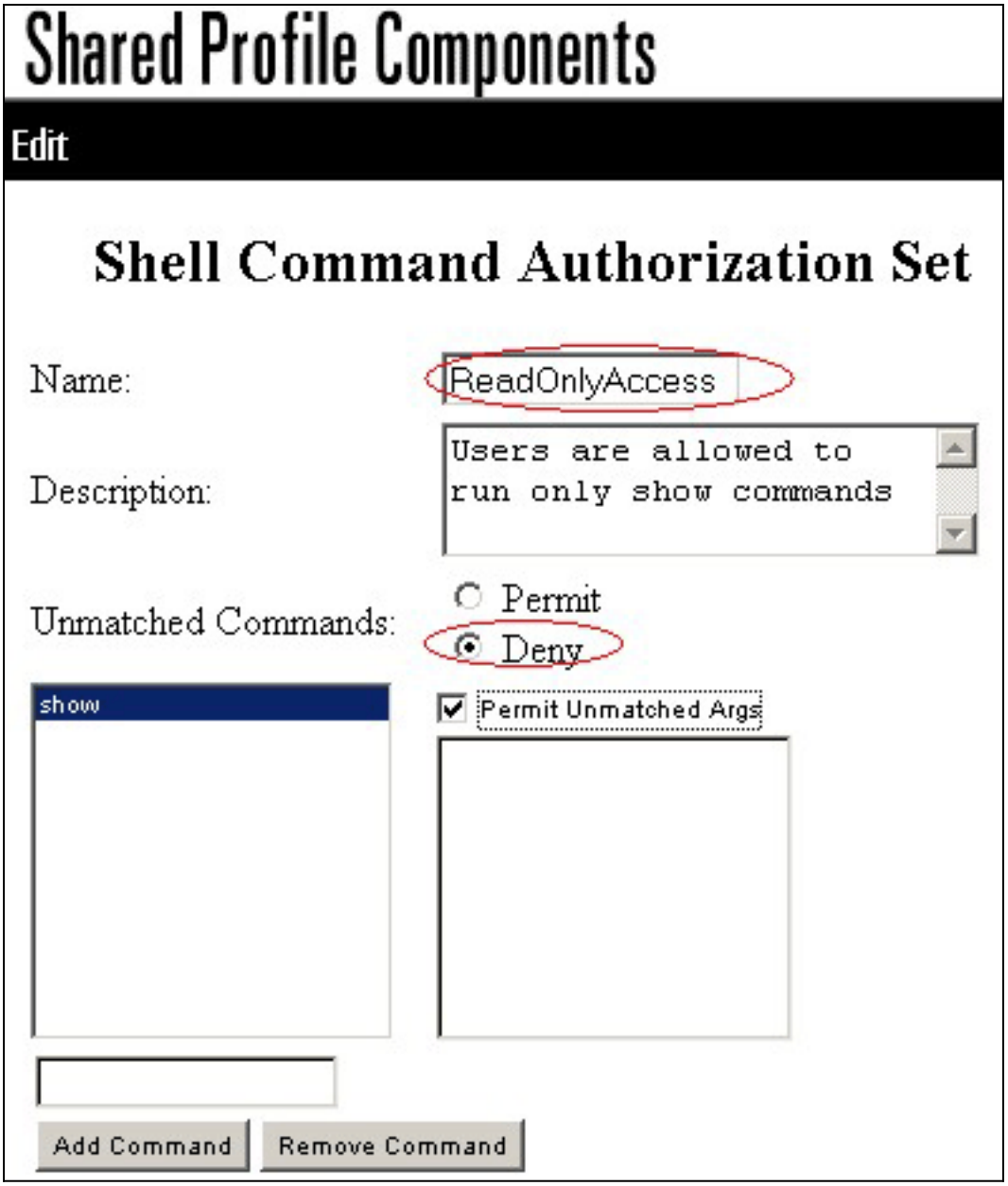


Scenario 2: Privilegio di accesso in sola lettura

In questi scenari, gli utenti possono utilizzare solo i comandi **show**.

Nell'area Set di autorizzazioni comandi shell della finestra Componenti profilo condiviso configurare le impostazioni seguenti:

1. Nel campo Name (Nome), immettere **ReadOnlyAccess** come nome del set di autorizzazioni del comando.
2. Nel campo Descrizione immettere una descrizione per il set di autorizzazioni del comando.
3. Fare clic sul pulsante di opzione **Nega**.
4. Immettere il comando **show** nel campo sopra il pulsante Add Command, quindi fare clic su **Add Command**.
5. Selezionare la casella di controllo **Consenti argomenti senza corrispondenza** e fare clic su **Invia**

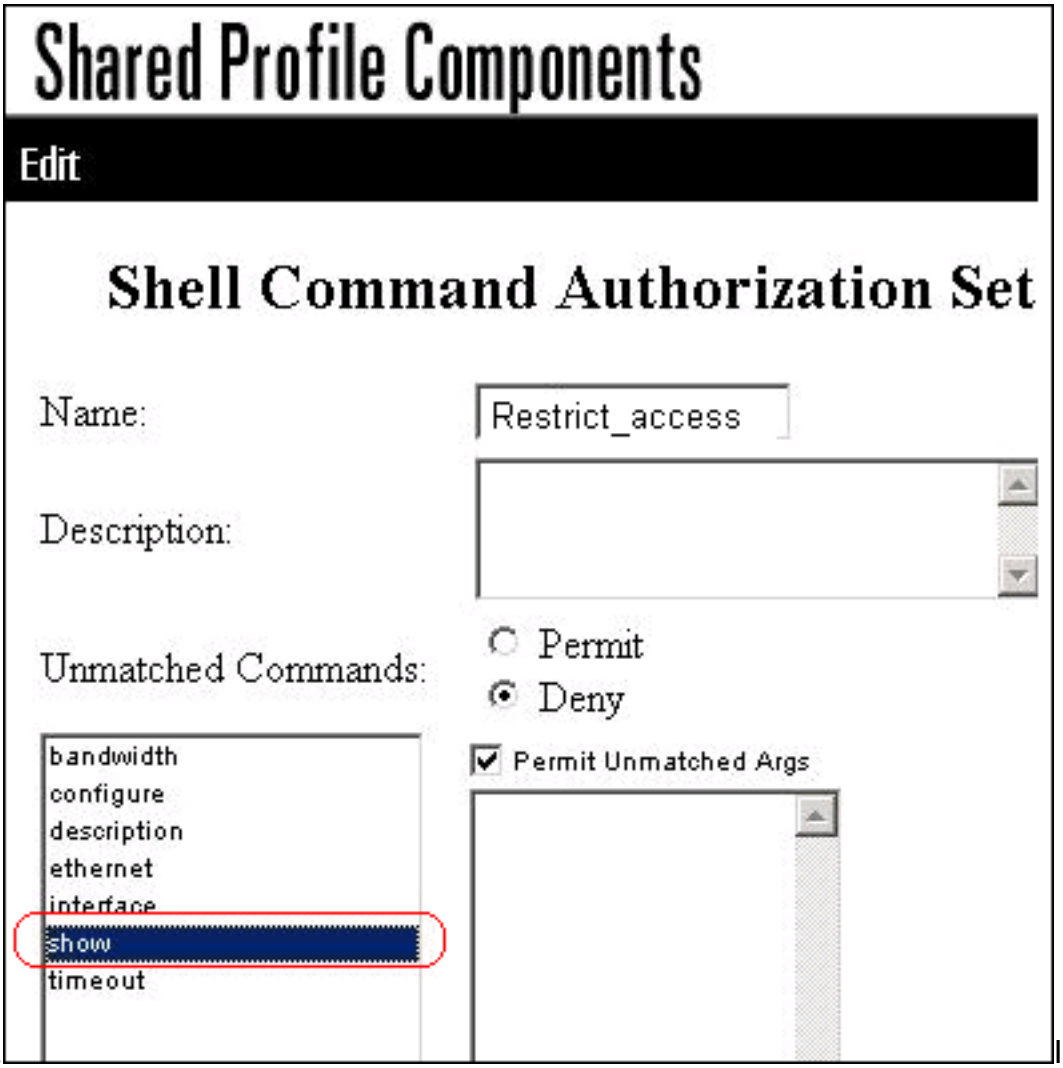


Scenario 3: Privilegio per accesso limitato

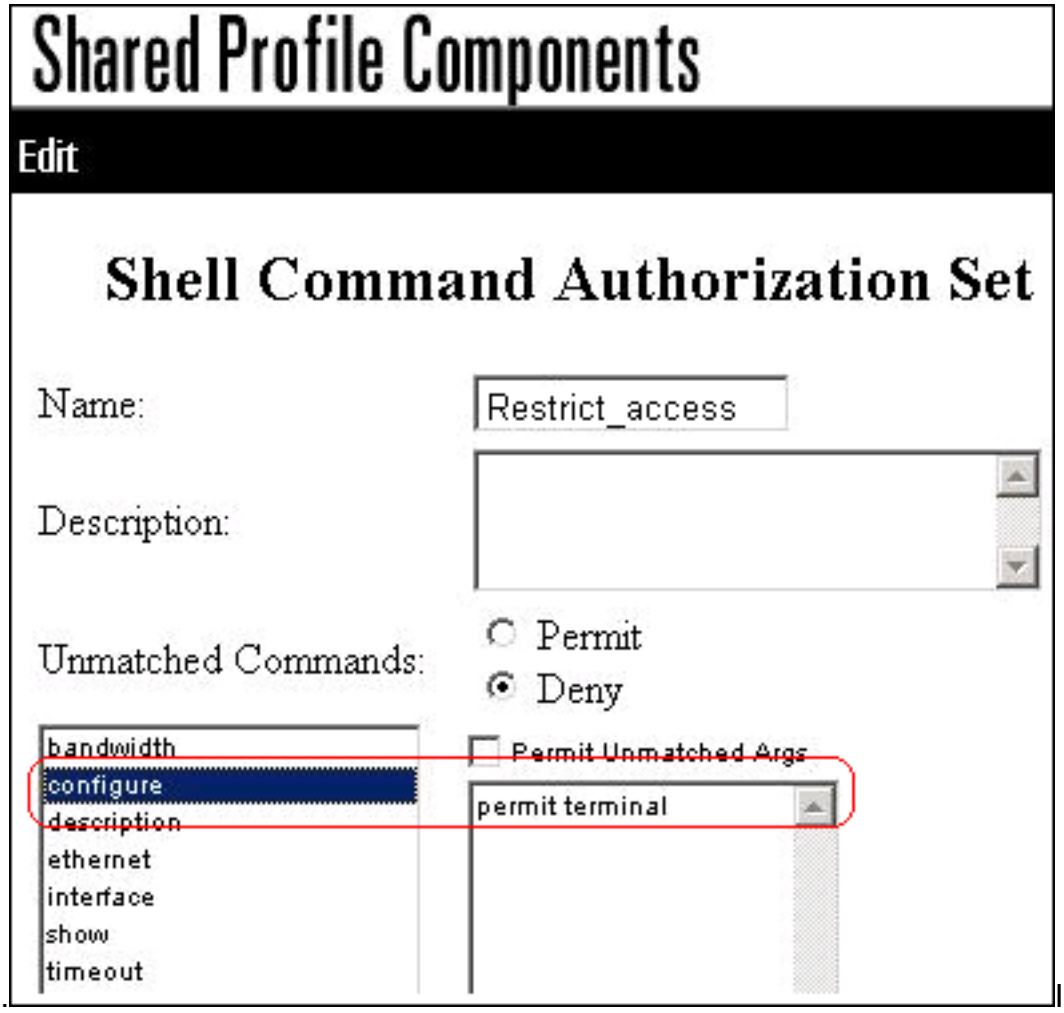
In questo scenario, gli utenti possono utilizzare comandi selettivi.

Nell'area Set di autorizzazioni comandi shell della finestra Componenti profilo condiviso configurare le impostazioni seguenti:

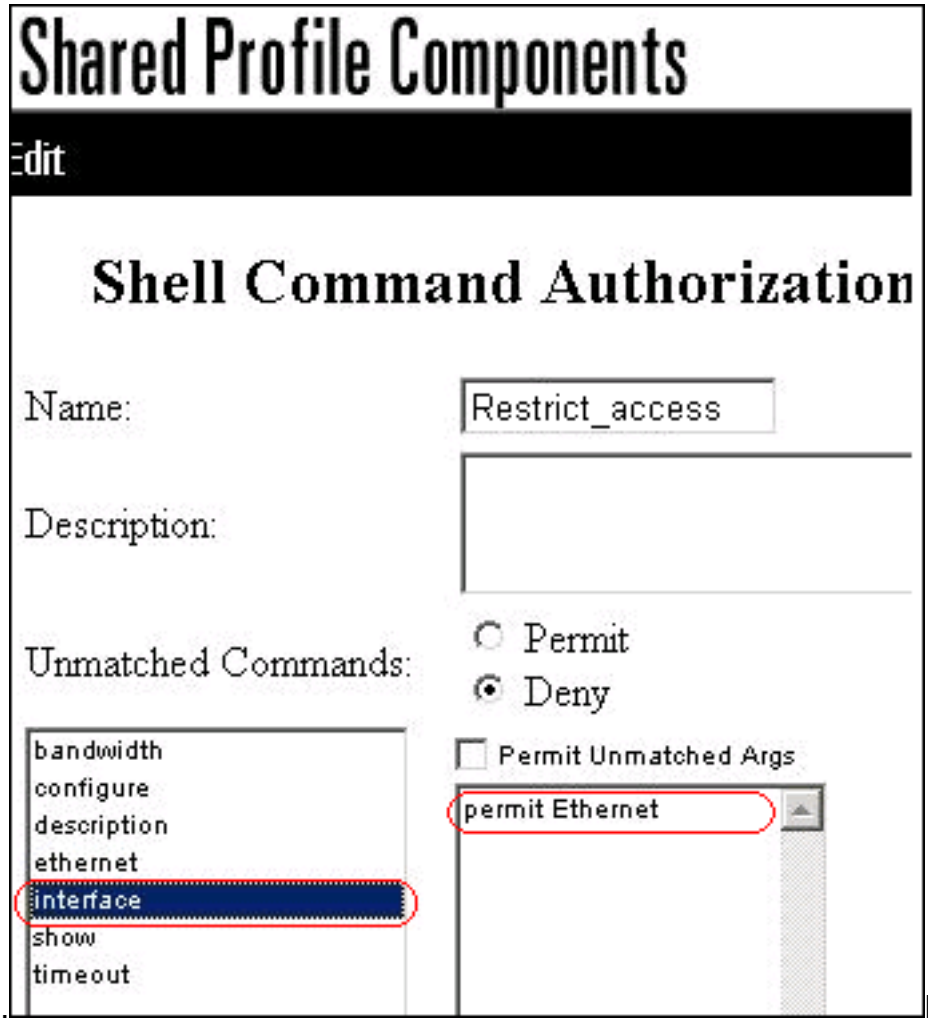
1. Nel campo Name (Nome), immettere **Restrict_access** come nome del set di autorizzazioni del comando.
2. Fare clic sul pulsante di opzione **Nega**.
3. Immettere i comandi che si desidera consentire ai client AAA.Nel campo situato sopra il pulsante Aggiungi comando, immettere il comando **show** e fare clic su **Aggiungi**



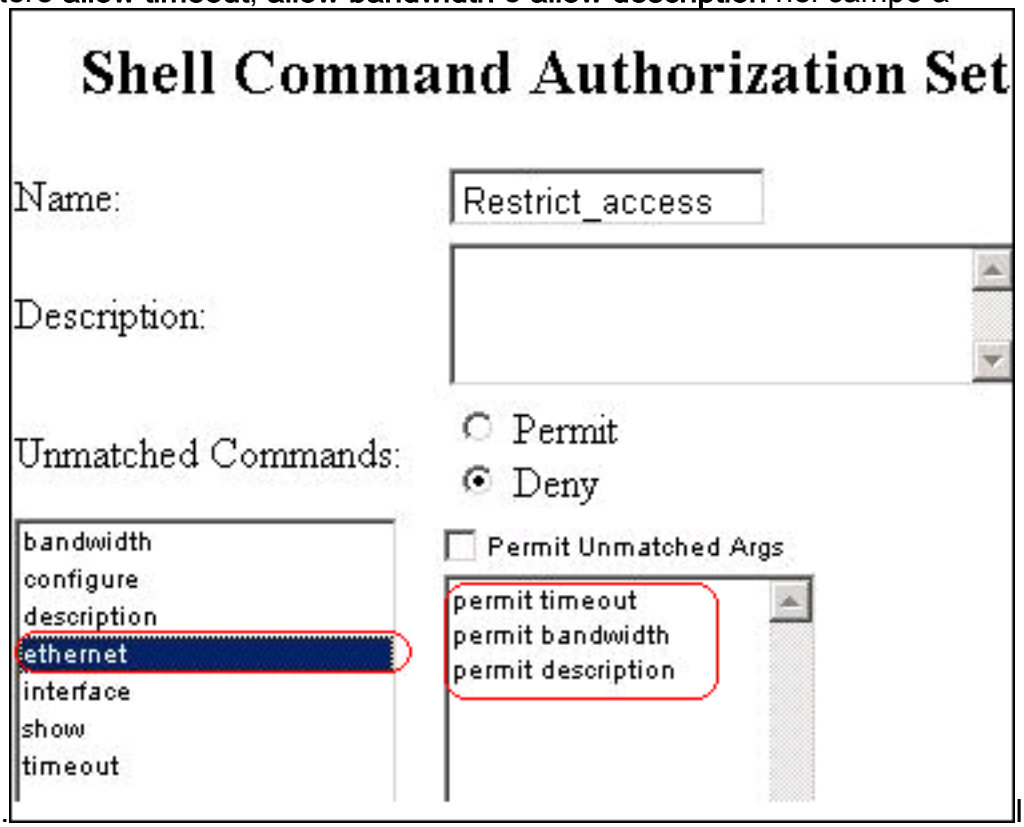
comando.Immettere il comando **configure** e fare clic su **Add Command**.Selezionare il comando **configure** e immettere **allow terminal** nel campo a



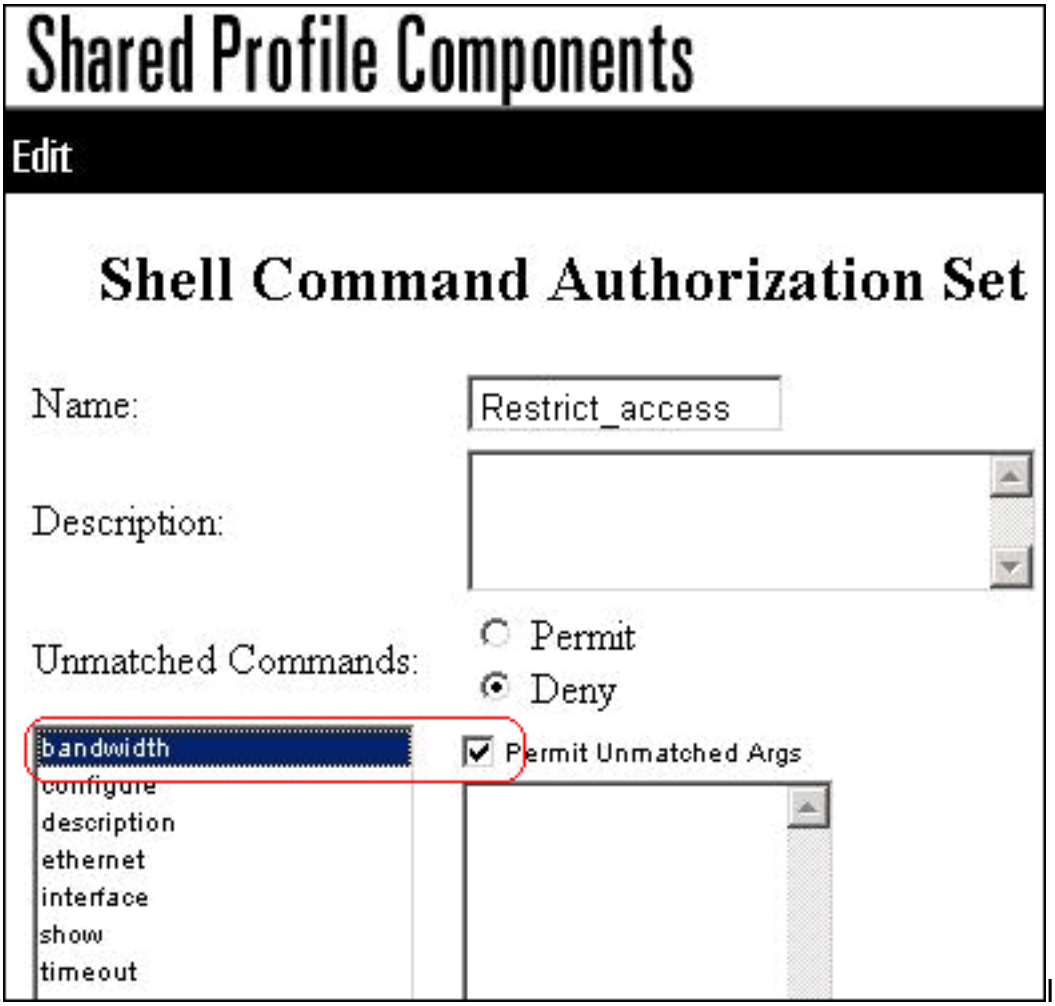
destra.Immettere il comando **interface** e fare clic su **Add Command**.Selezionare il comando **interface** e immettere **allow Ethernet** nel campo a



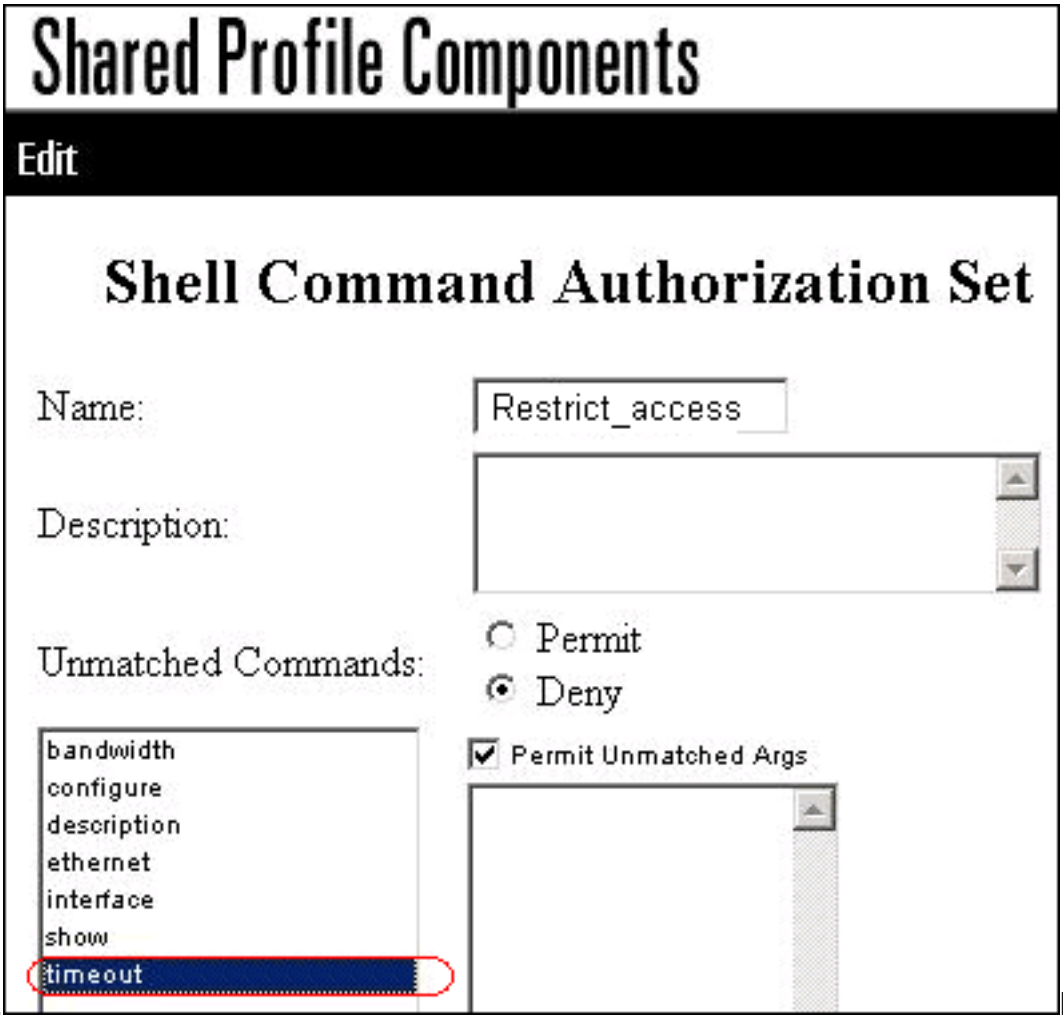
destra.Immettere il comando **ethernet** e fare clic su **Aggiungi comando**.Selezionare il comando **interface** e immettere **allow timeout**, **allow bandwidth** e **allow description** nel campo a



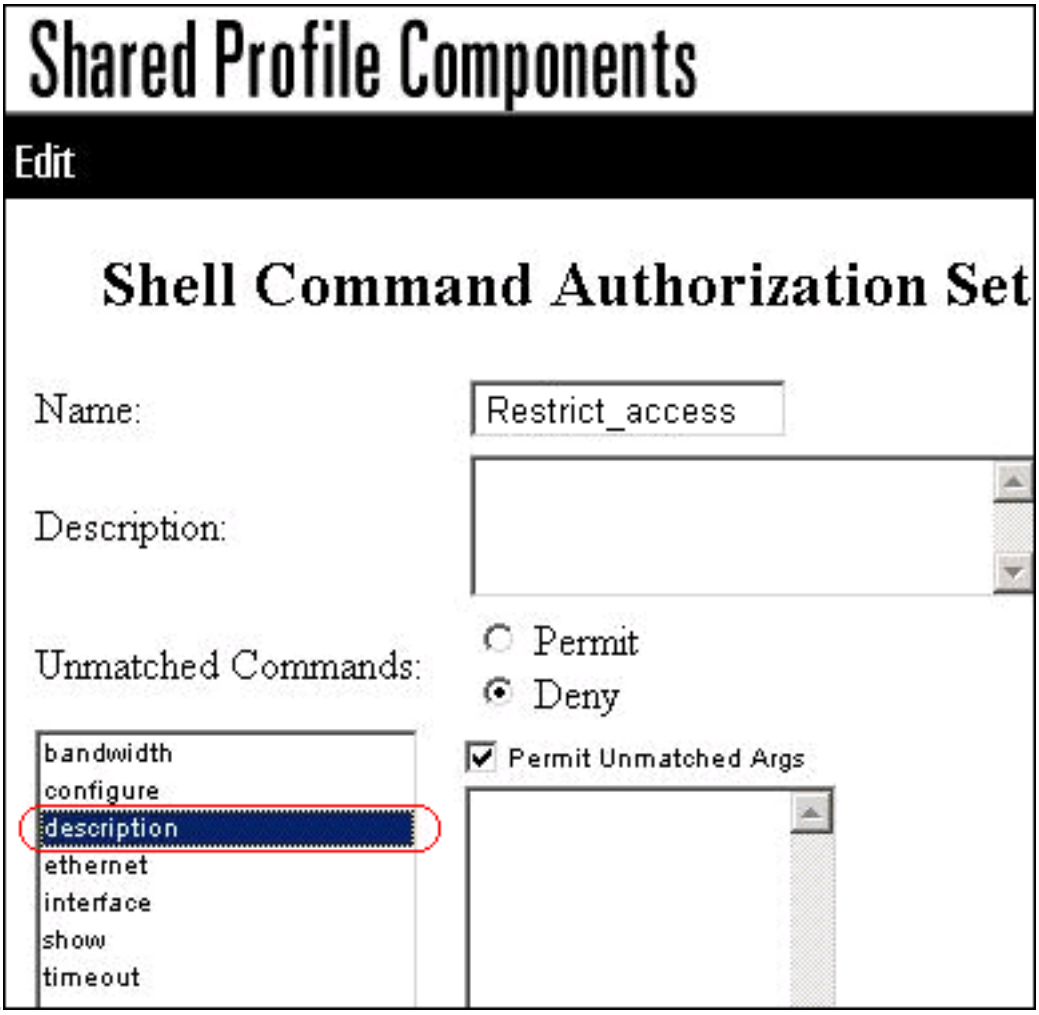
destra.Immettere il comando **bandwidth** e fare clic su **Add**



Command.Immettere il comando **timeout** e fare clic su **Add**



Command. Immettere il comando **description** e fare clic su **Add**



Command.

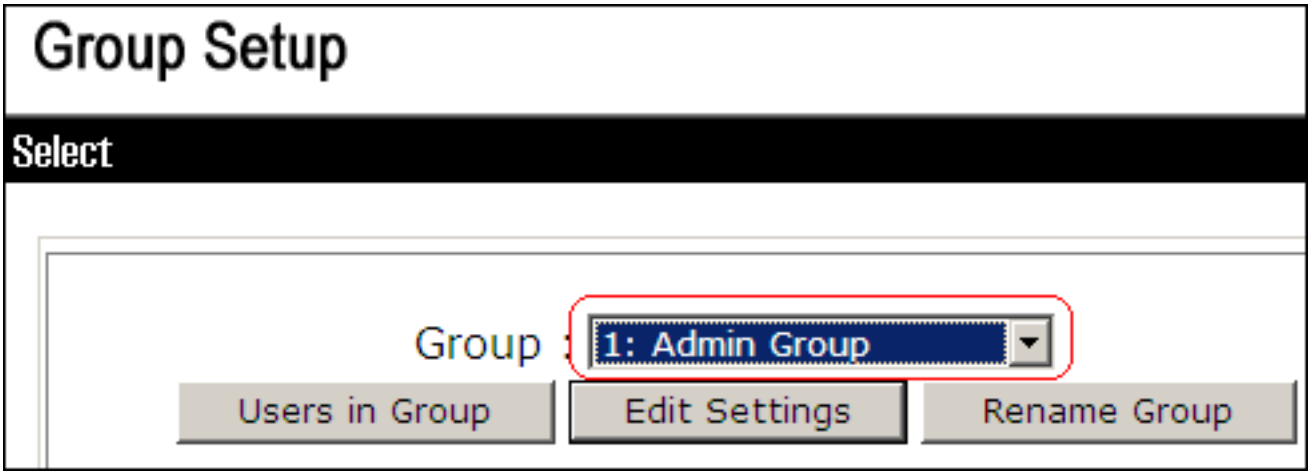
4. Fare clic su **Invia**.

Associa il set di autorizzazioni dei comandi della shell al gruppo di utenti

Per ulteriori informazioni su come configurare la configurazione del set di autorizzazioni dei comandi della shell per i gruppi di utenti, consultare la sezione Configurazione di un set di autorizzazioni dei comandi della shell per un gruppo di utenti della Guida per l'utente di Cisco Secure Access Control Server 4.1.

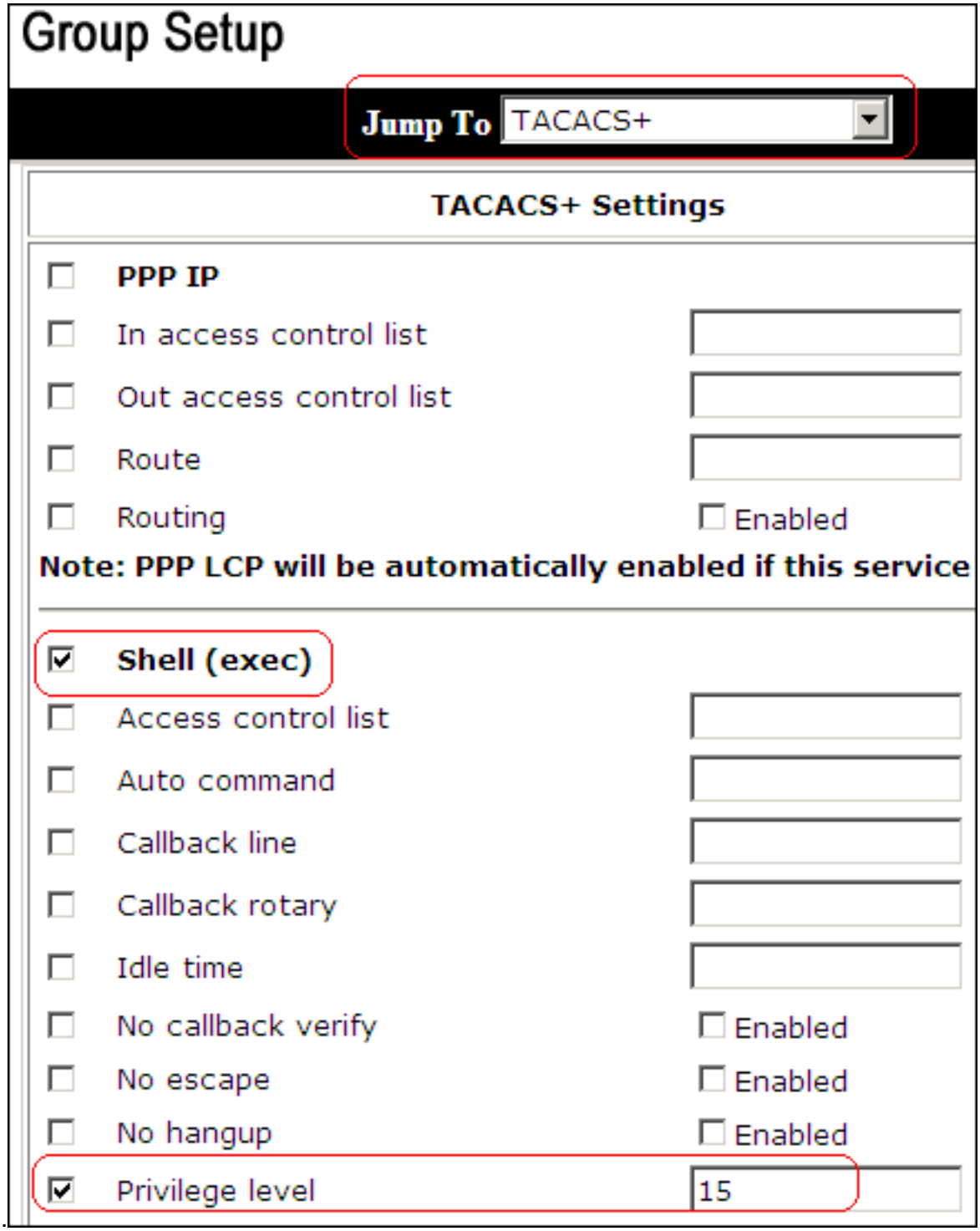
Associa il set di autorizzazioni dei comandi della shell (accesso in lettura/scrittura) al gruppo di utenti (gruppo amministrativo)

1. Nella finestra ACS, fare clic su **Group Setup**, quindi selezionare **Admin Group** dall'elenco a discesa
Group.



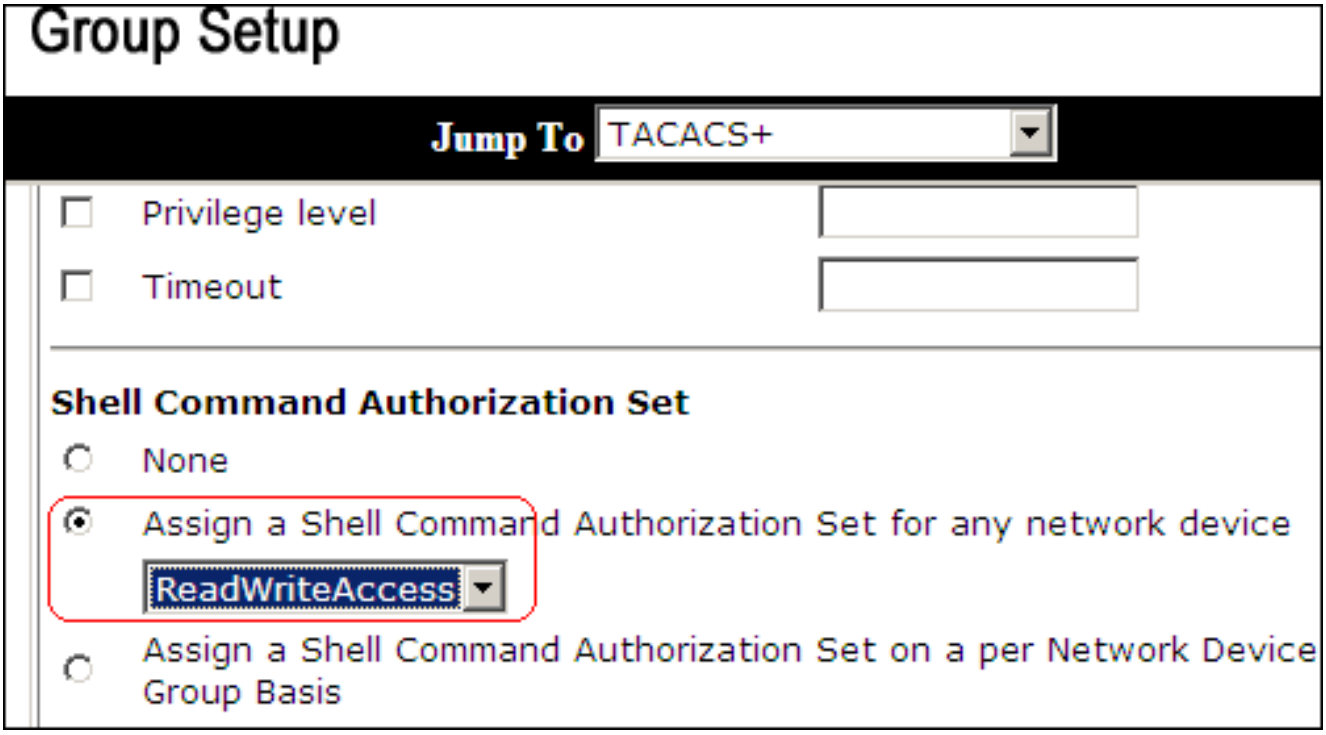
2. Fare clic su **Modifica impostazioni**.
3. Dall'elenco a discesa Vai a, scegliere **Abilita opzioni**.
4. Nell'area Enable Options (Abilita opzioni), fare clic sul pulsante di scelta **Max Privilege for any AAA client** (Privilegio massimo per qualsiasi client AAA), quindi selezionare **Level 15** (Livello 15) dall'elenco a discesa.

5. Dall'elenco a discesa Vai a, scegliere **TACACS+**.
6. Nell'area Impostazioni TACACS+, selezionare la casella di controllo **Shell (exec)**, selezionare la casella di controllo **Livello di privilegio** e immettere **15** nel campo Livello di



privilegio.

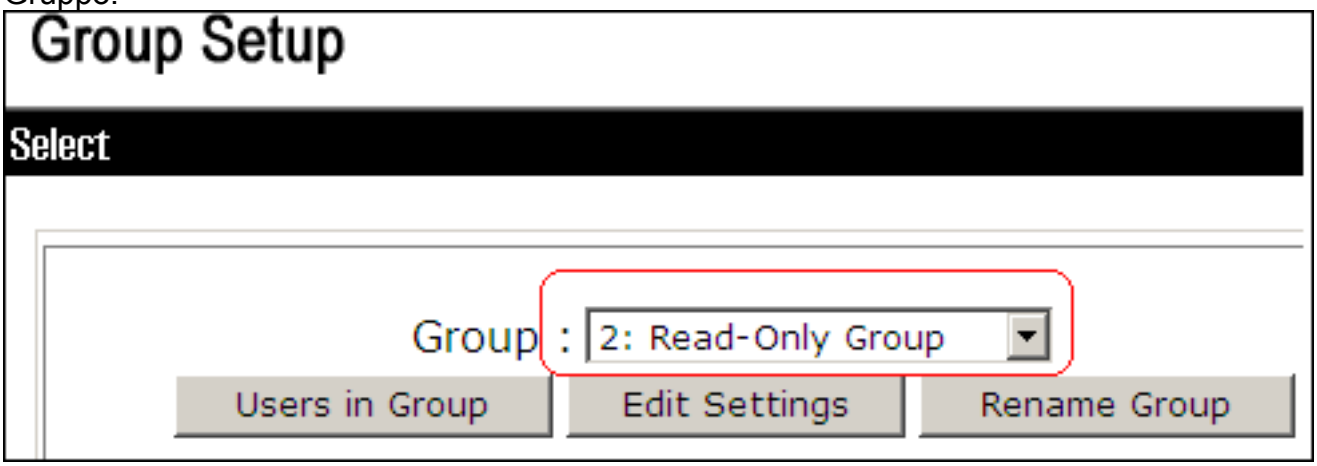
7. Nell'area Set di autorizzazioni dei comandi della shell, fare clic sul pulsante di scelta **Assegna un set di autorizzazioni dei comandi della shell per qualsiasi dispositivo di rete** e scegliere **ReadWriteAccess** dall'elenco a discesa.



8. Fare clic su **Submit (Invia).**

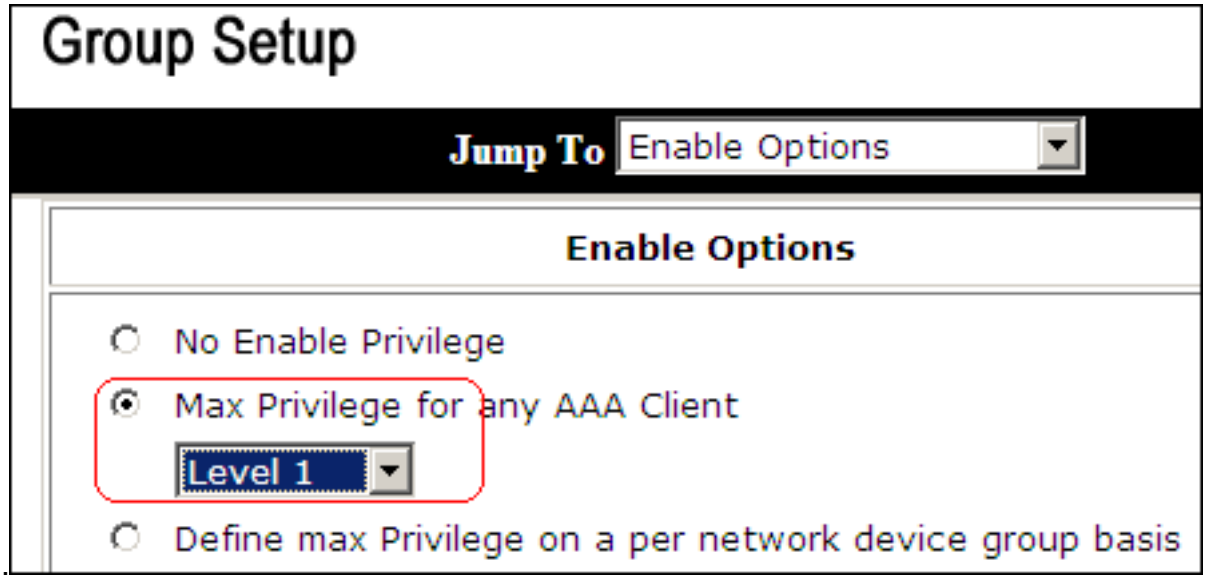
Associa il set di autorizzazioni dei comandi della shell (accesso in sola lettura) al gruppo di utenti (gruppo di sola lettura)

1. Nella finestra ACS, fare clic su **Configurazione gruppo**, quindi scegliere **Gruppo di sola lettura** dall'elenco a discesa
   Gruppo.

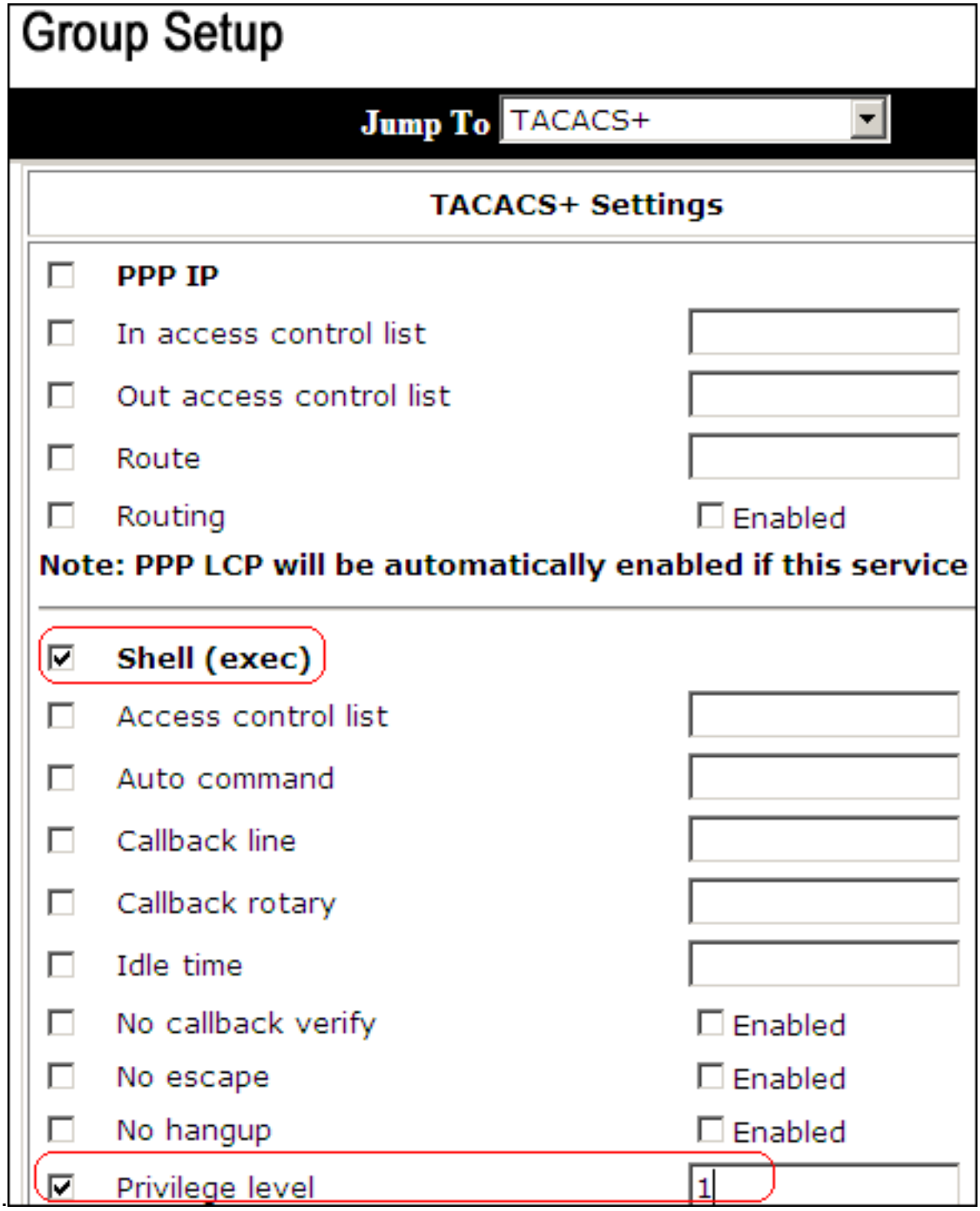


2. Fare clic su **Modifica impostazioni**.
3. Dall'elenco a discesa Vai a, scegliere **Abilita opzioni**.
4. Nell'area Enable Options (Abilita opzioni), fare clic sul pulsante di opzione **Max Privilege for any AAA client**, quindi selezionare **Level 1 (Livello 1)** dall'elenco a

discesa.



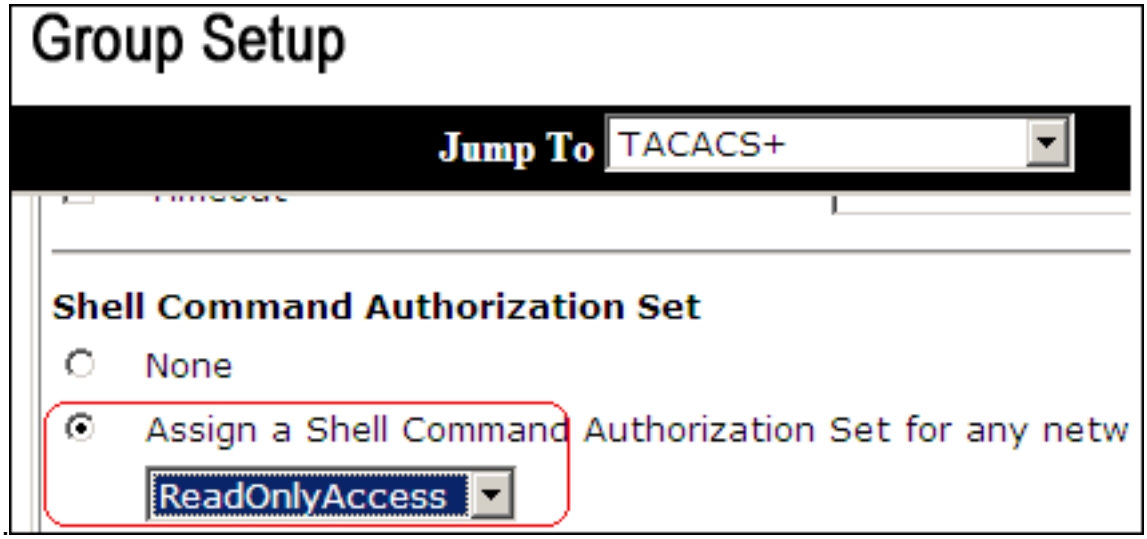
5. Nell'area Impostazioni TACACS+ selezionare la casella di controllo **Shell (exec)**, selezionare la casella di controllo **Livello di privilegio** e immettere **1** nel campo Livello di



privilegio.

6. Nell'area Set di autorizzazioni dei comandi della shell, fare clic sul pulsante di opzione **Assegna un set di autorizzazioni dei comandi della shell per qualsiasi dispositivo di rete** e scegliere **ReadOnlyAccess** dall'elenco a

discesa.



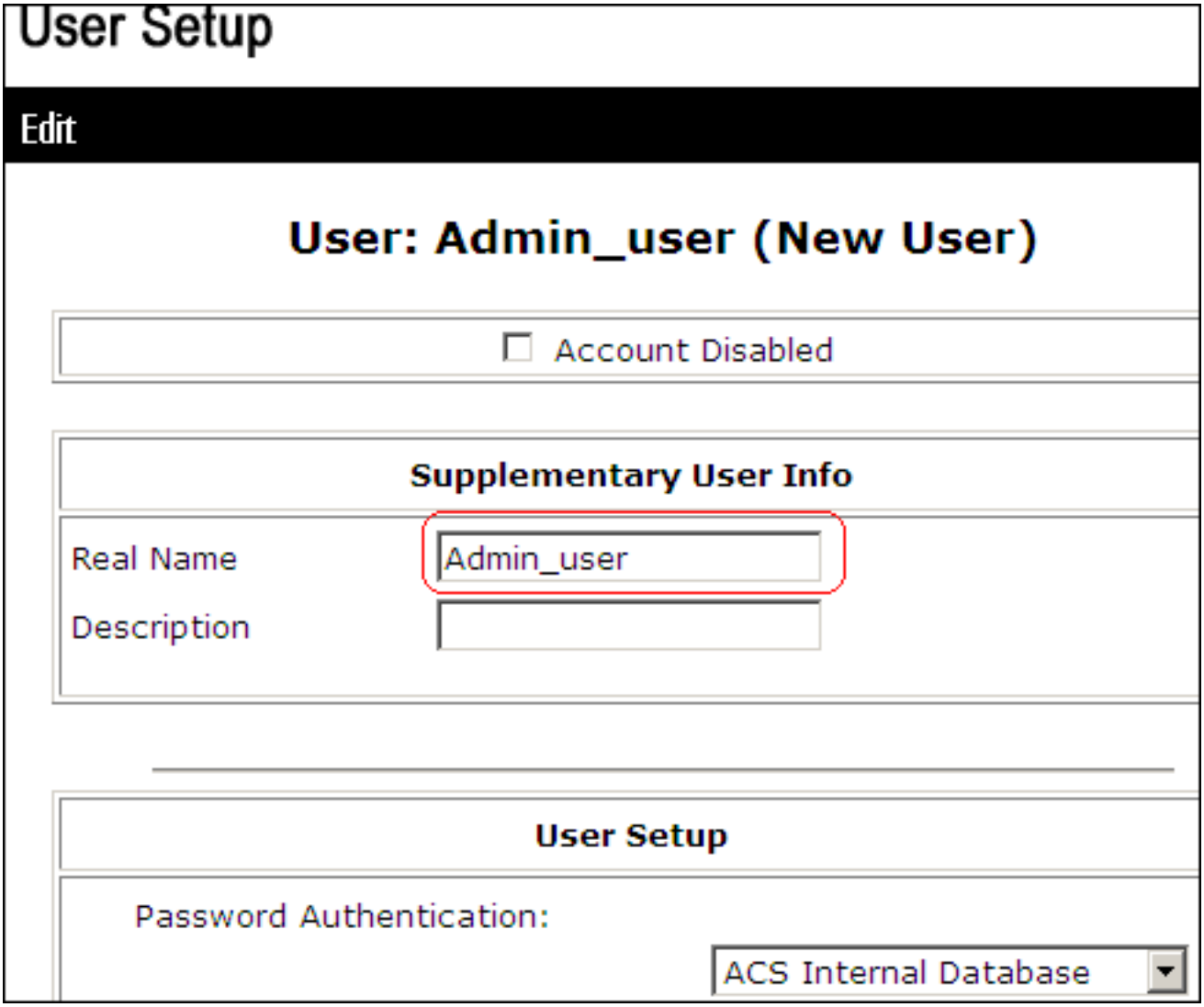
7. Fare clic su **Submit (Invia).**

Associa il set di autorizzazioni dei comandi della shell (Restrict_access) all'utente

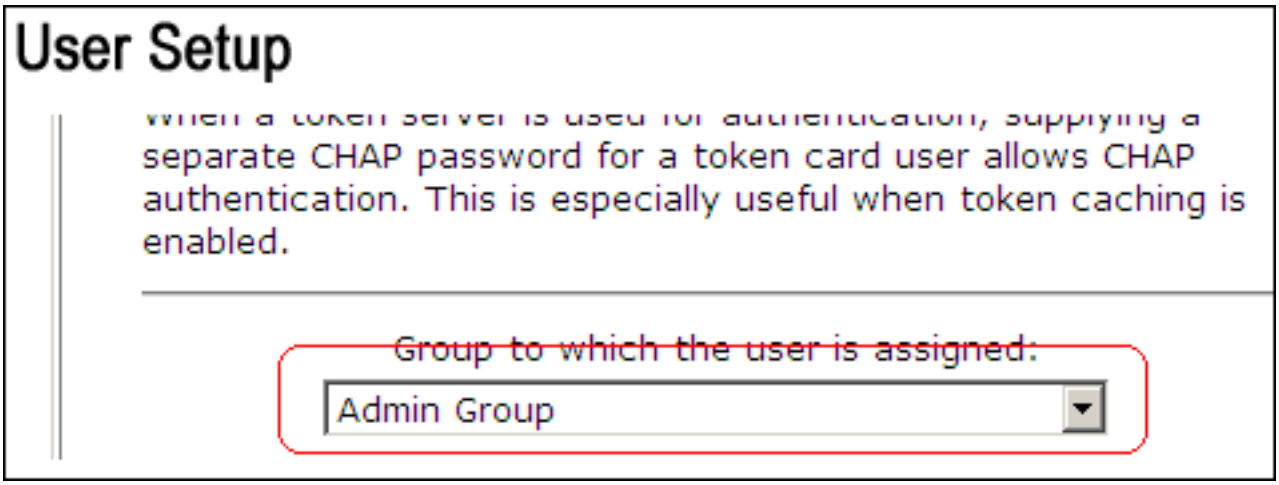
Per ulteriori informazioni su come configurare il set di autorizzazioni dei comandi della shell per gli utenti, consultare la sezione Configurazione del set di autorizzazioni dei comandi della shell per l'utente della Guida dell'utente di Cisco Secure Access Control Server 4.1.

Nota: le impostazioni a livello di utente sostituiscono le impostazioni a livello di gruppo in ACS. Ciò significa che se l'utente ha impostato l'autorizzazione per il comando della shell nelle impostazioni a livello di utente, le impostazioni a livello di gruppo verranno sostituite.

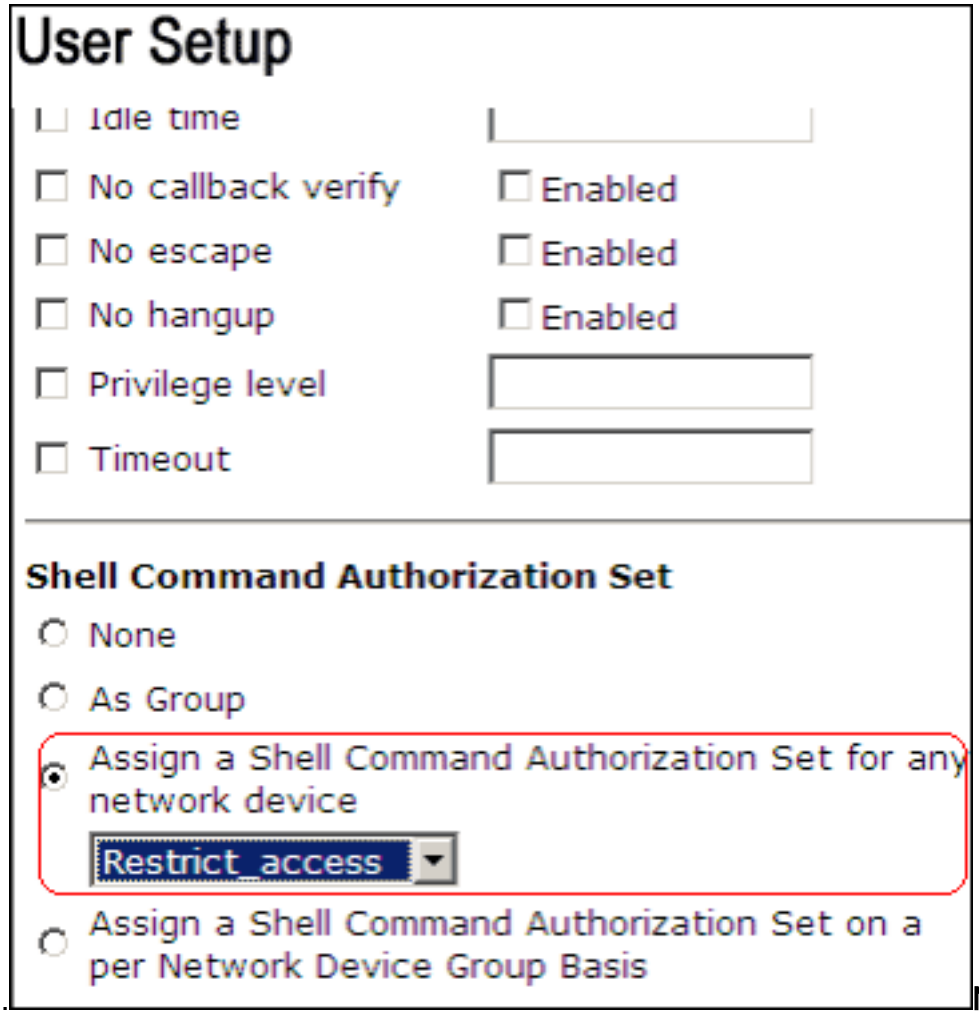
1. Fare clic su **User Setup > Add/Edit** (Impostazione utente > Aggiungi/Modifica) per creare un nuovo utente denominato *Admin_user* da includere nel gruppo Admin.



2. Dall'elenco a discesa del gruppo a cui è assegnato l'utente, scegliere **Gruppo amministratori**.



3. Nell'area Set di autorizzazioni dei comandi della shell, fare clic sul pulsante di opzione **Assegna un set di autorizzazioni dei comandi della shell per qualsiasi dispositivo di rete** e scegliere **Limita_accesso** dall'elenco a discesa.**Nota:** in questo scenario, l'utente fa parte del gruppo Admin. Il set di autorizzazioni della shell *Restrict_access* è applicabile. il set di autorizzazioni della shell di *accesso in lettura/scrittura* non è



applicabile.**Nota:** nella sezione TACACS+ (Cisco) dell'area Configurazione interfaccia, verificare che l'opzione **Shell (exec)** sia selezionata nella colonna Utente.

Configurazione router IOS

Oltre alla configurazione predefinita, questi comandi sono richiesti su un router o su uno switch IOS per implementare l'autorizzazione dei comandi tramite un server ACS:

```
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
```

Configurazione ASA/PIX/FWSM

Oltre alla configurazione predefinita, questi comandi sono richiesti su ASA/PIX/FWSM per implementare l'autorizzazione dei comandi tramite un server ACS:

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

Nota: non è possibile utilizzare il protocollo RADIUS per limitare l'accesso degli utenti ad ASDM

per scopi di sola lettura. Poiché i pacchetti RADIUS contengono contemporaneamente l'autenticazione e l'autorizzazione, tutti gli utenti autenticati nel server RADIUS dispongono di un livello di privilegio di 15. È possibile ottenere questo risultato tramite TACACS con l'implementazione di set di autorizzazione dei comandi.

Nota: l'esecuzione di ciascun comando digitato su ASA/PIX/FWSM richiede molto tempo, anche se ACS non è disponibile per l'autorizzazione del comando. Se ACS non è disponibile e l'appliance ASA ha configurato l'autorizzazione del comando, l'appliance richiederà comunque l'autorizzazione del comando per ciascun comando.

Risoluzione dei problemi

Errore: autorizzazione comando non riuscita

Problema

Dopo aver effettuato l'accesso al firewall tramite la registrazione TACACS, i comandi non funzionano. Quando si immette un comando, viene visualizzato questo errore: `autorizzazione del comando non riuscita`.

Soluzione

Per risolvere il problema, completare i seguenti passaggi:

1. Assicurarsi che venga utilizzato il nome utente corretto e che tutti i privilegi richiesti siano assegnati all'utente.
2. Se il nome utente e i privilegi sono corretti, verificare che l'appliance ASA sia connessa all'appliance ACS e che l'appliance sia attiva.

Nota: questo errore può verificarsi anche se l'amministratore ha configurato in modo errato l'autorizzazione del comando per gli utenti locali e TACACS. In questo caso, eseguire un recupero della password per risolvere il problema.

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Pagina di supporto di Cisco Secure Control Access Control Server
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).