Esempio di configurazione del controllo di accesso basato su privilegi dell'interfaccia Web 5760 con Cisco Access Control Server (ACS)

Sommario

Introduzione

In questo documento viene spiegato come creare profili di autenticazione e autorizzazione Cisco ACS Tacacs+ con diversi livelli di privilegi e come integrarlo con 5760 per l'accesso a WebUI. Questa funzione è supportata a partire dalla versione 3.6.3 (ma non dalla versione 3.7.x al momento della scrittura).

Prerequisiti

Requisiti

Si presume che il lettore abbia familiarità con la configurazione di Cisco ACS e del Converged Access Controller. Il presente documento si concentra esclusivamente sull'interazione tra questi due componenti nell'ambito dell'autorizzazione TACACS+.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

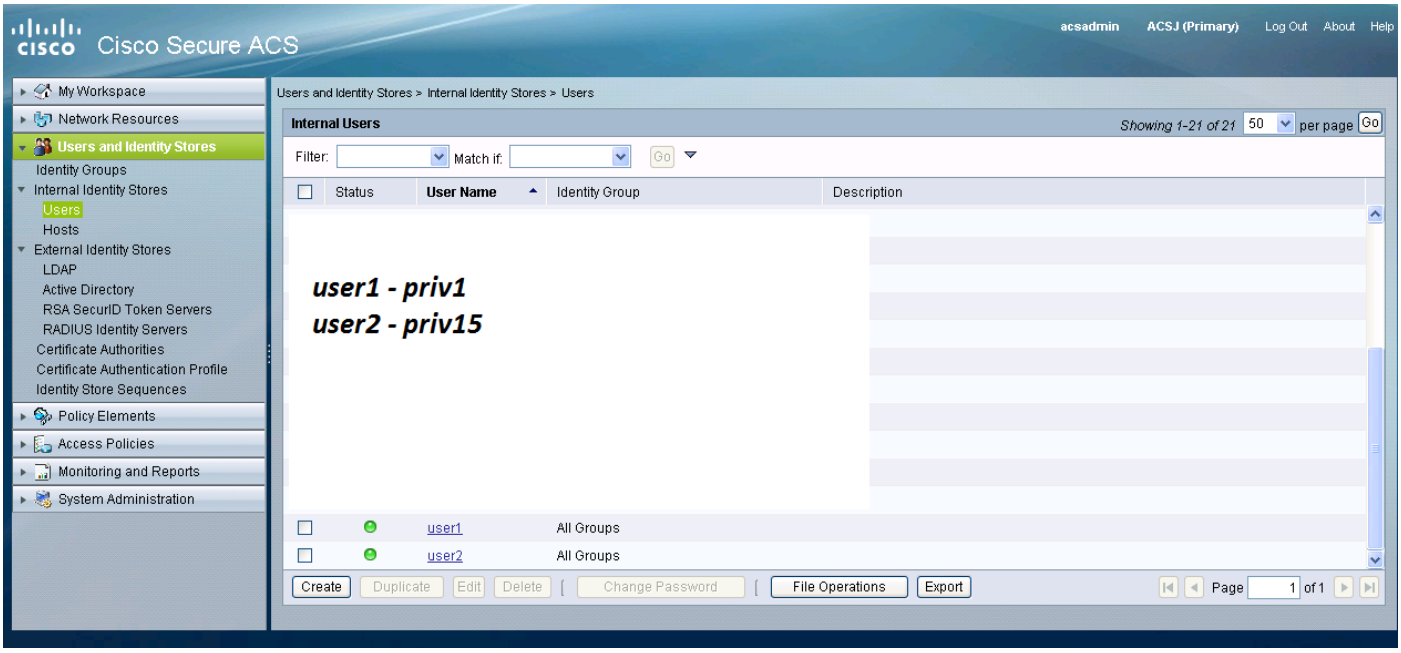
- Cisco Converged Access 5760, versione 3.6.3
- Cisco Access Control Server (ACS) 5.2

Configurazione

Creare alcuni utenti di test in ACS

Fare clic su "Utenti e archivi identità", quindi selezionare "Utenti".

Fare clic su "Crea" e configurare alcuni utenti di prova come illustrato di seguito.



Impostazione di elementi di criteri e profili shell

È necessario creare 2 profili per i 2 diversi tipi di accesso. Il privilegio 15 nel mondo dei TACACS di cisco significa fornire un accesso completo al dispositivo senza alcuna restrizione. Il privilegio 1, d'altra parte, consente di accedere ed eseguire solo una quantità limitata di comandi. Di seguito è riportata una breve descrizione dei livelli di accesso forniti da cisco.

livello di privilegio 1 = non privilegiato (il prompt è router>), il livello predefinito per l'accesso

livello di privilegio 15 = privilegiato (il prompt è il numero del router), il livello dopo l'attivazione della modalità di abilitazione

livello di privilegio 0 = utilizzato raramente, ma include 5 comandi: **disabilita**, **abilita**, **esci**, **guida** e **disconnetti**

Sugli switch 5760, i livelli da 2 a 14 sono considerati uguali al livello 1. Ad essi viene concesso lo stesso privilegio di 1. **Non configurare i livelli di privilegi TACACS per alcuni comandi sullo switch 5760**. l'accesso tramite interfaccia utente per schede non è supportato in 5760. È possibile accedere in modalità completa (priv1) o solo alla scheda Monitor (priv1). Inoltre, agli utenti con il livello di privilegio 0 non è consentito eseguire l'accesso.

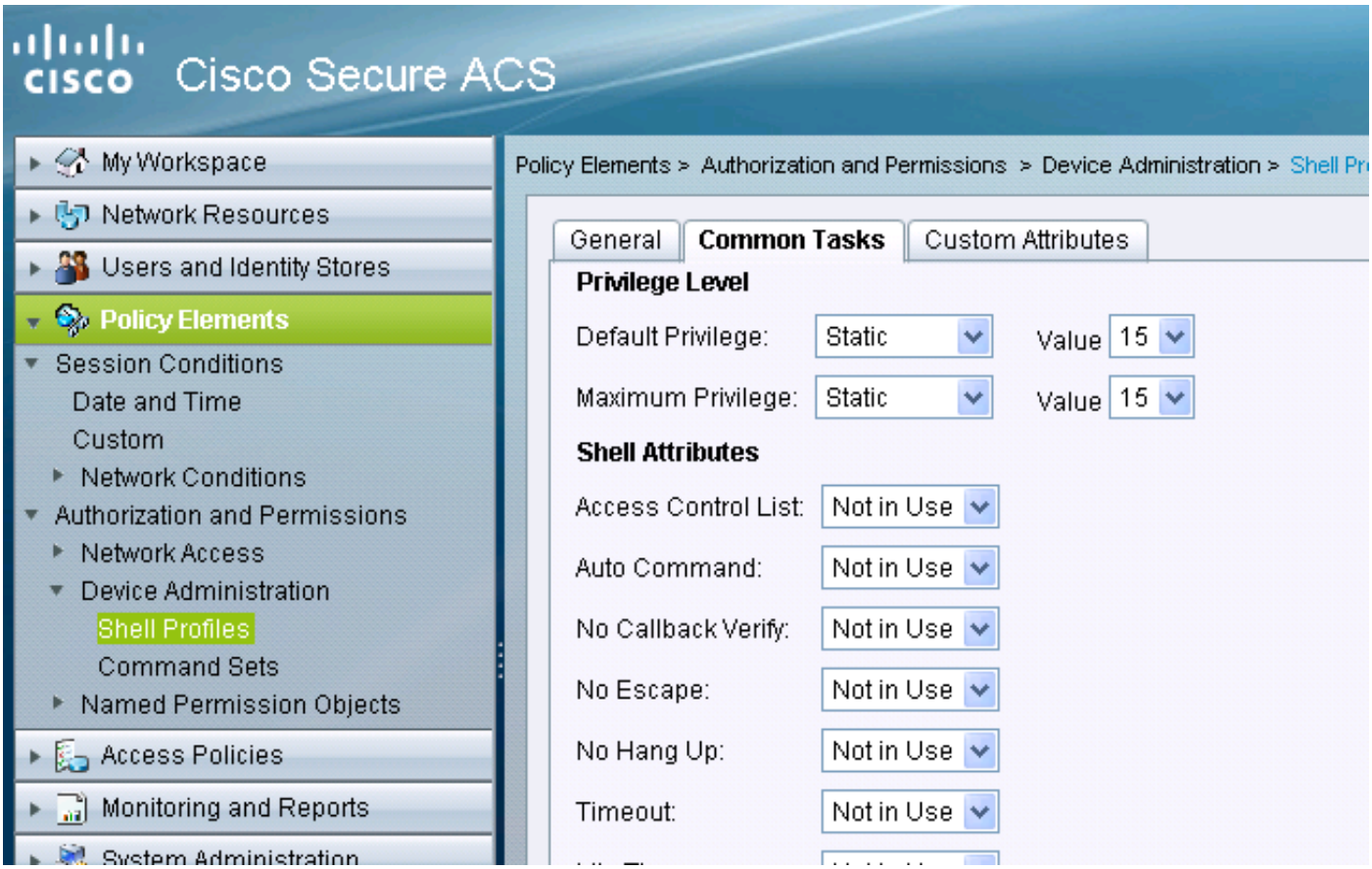
Creazione del profilo di accesso alla shell di livello 15 per il privilegio

Utilizzare la schermata di stampa seguente per creare il profilo:

Fare clic su "Elementi criteri". Fare clic su "Profili shell".

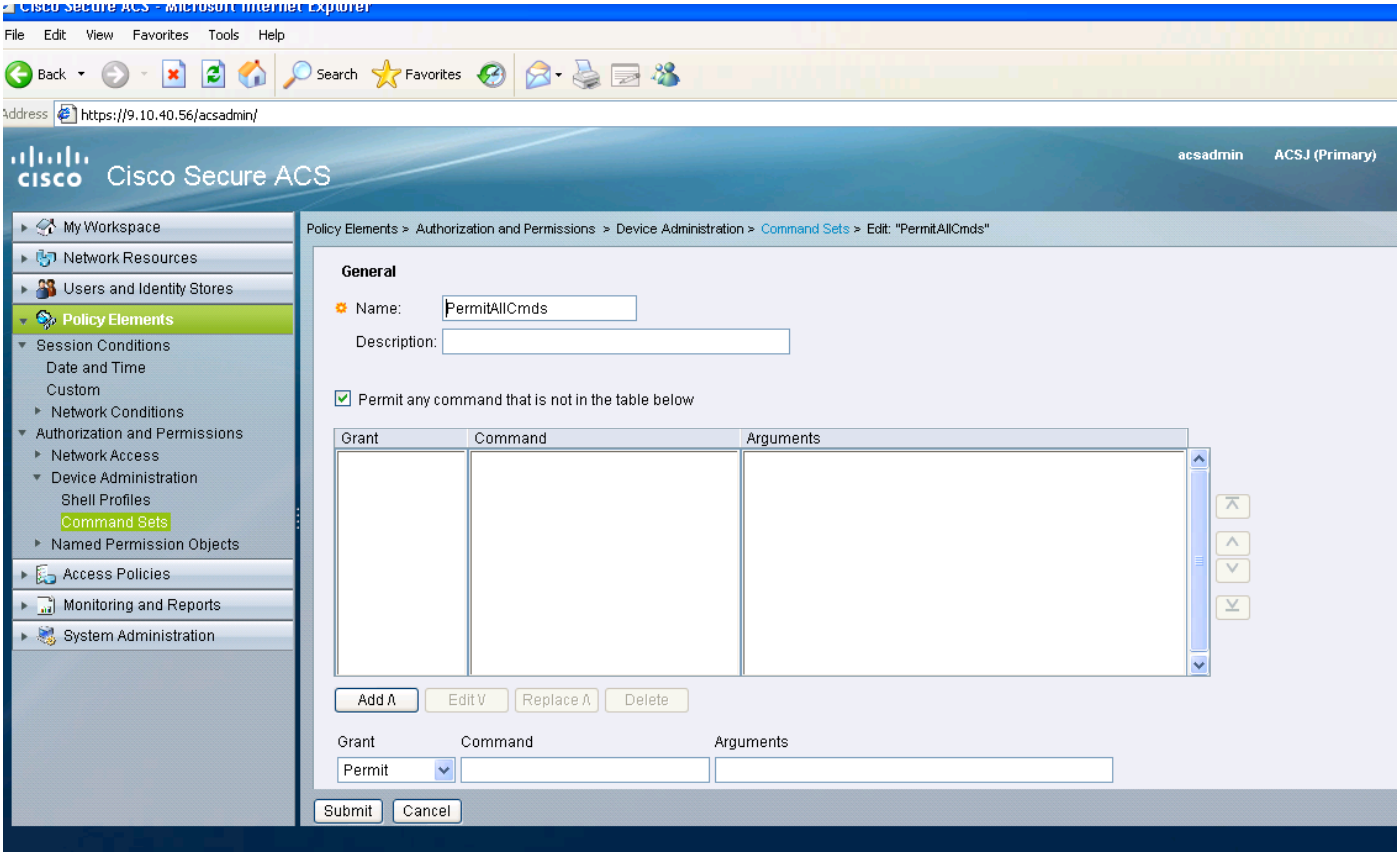
Crearne uno nuovo.

Nella scheda "Operazioni comuni" impostare il livello di privilegi predefinito e massimo su 15.



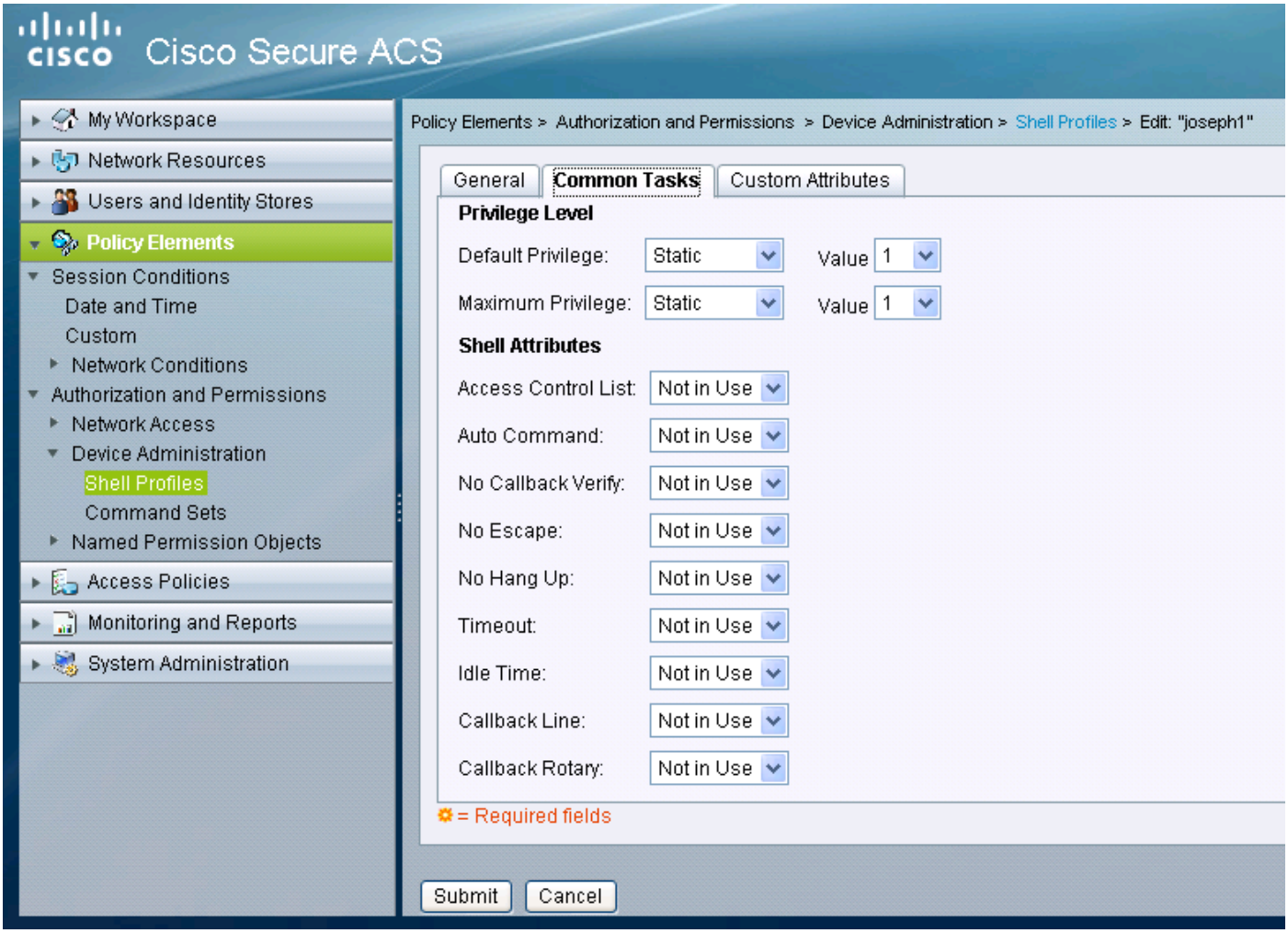
Creazione di set di comandi per l'utente amministratore

I set di comandi sono set di comandi utilizzati da tutti i dispositivi TACACS. Possono essere utilizzati per limitare i comandi che un utente può usare se gli è stato assegnato quel profilo specifico. Poiché sullo switch 5760 le restrizioni vengono applicate al codice Webui in base al livello di privilegio passato, i set di comandi per il livello di privilegio 1 e 15 sono gli stessi.



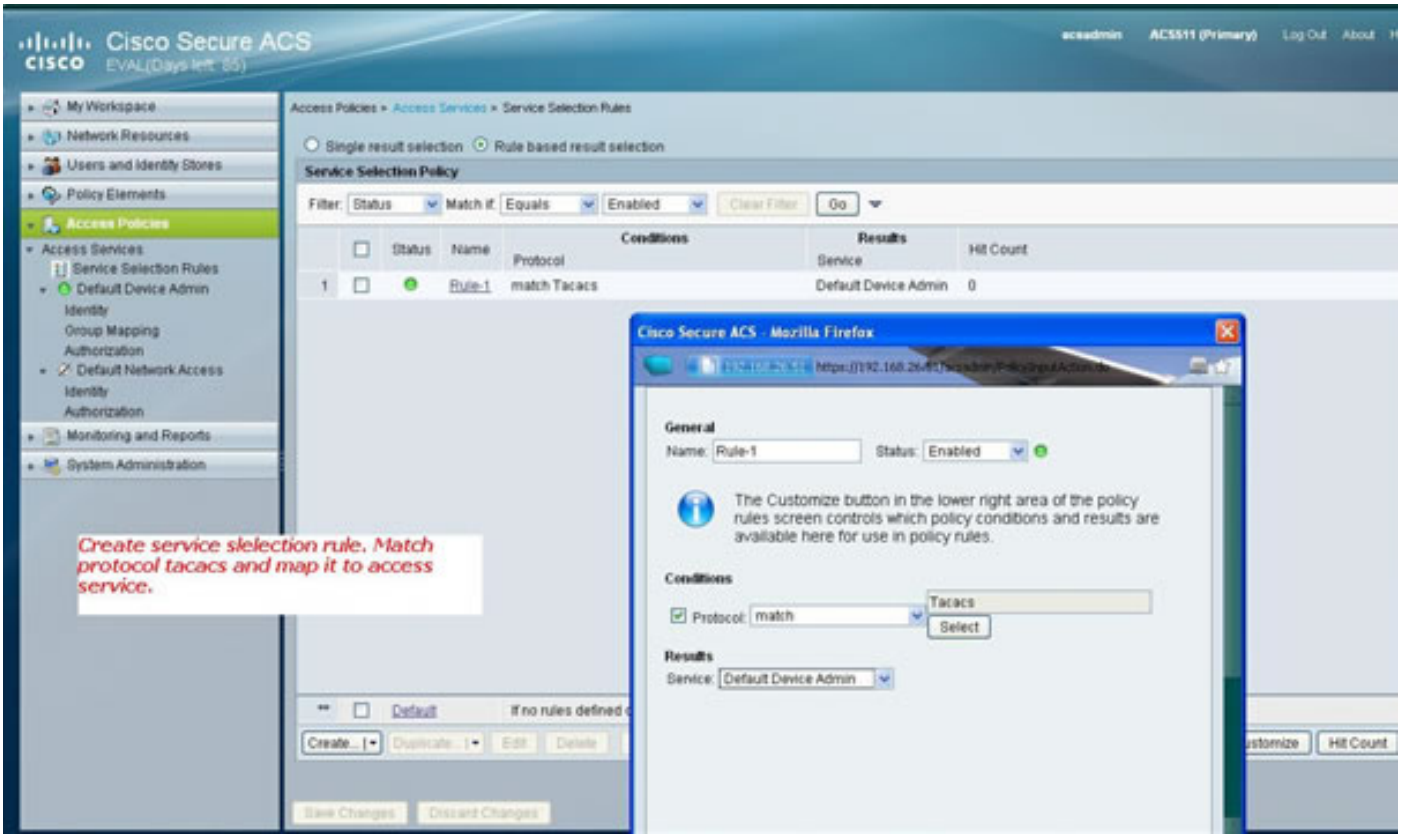
Creazione del profilo shell per l'utente di sola lettura

Creare un altro profilo shell per gli utenti di sola lettura. Questo profilo si differenzia per il fatto che i livelli di privilegio sono impostati su 1.



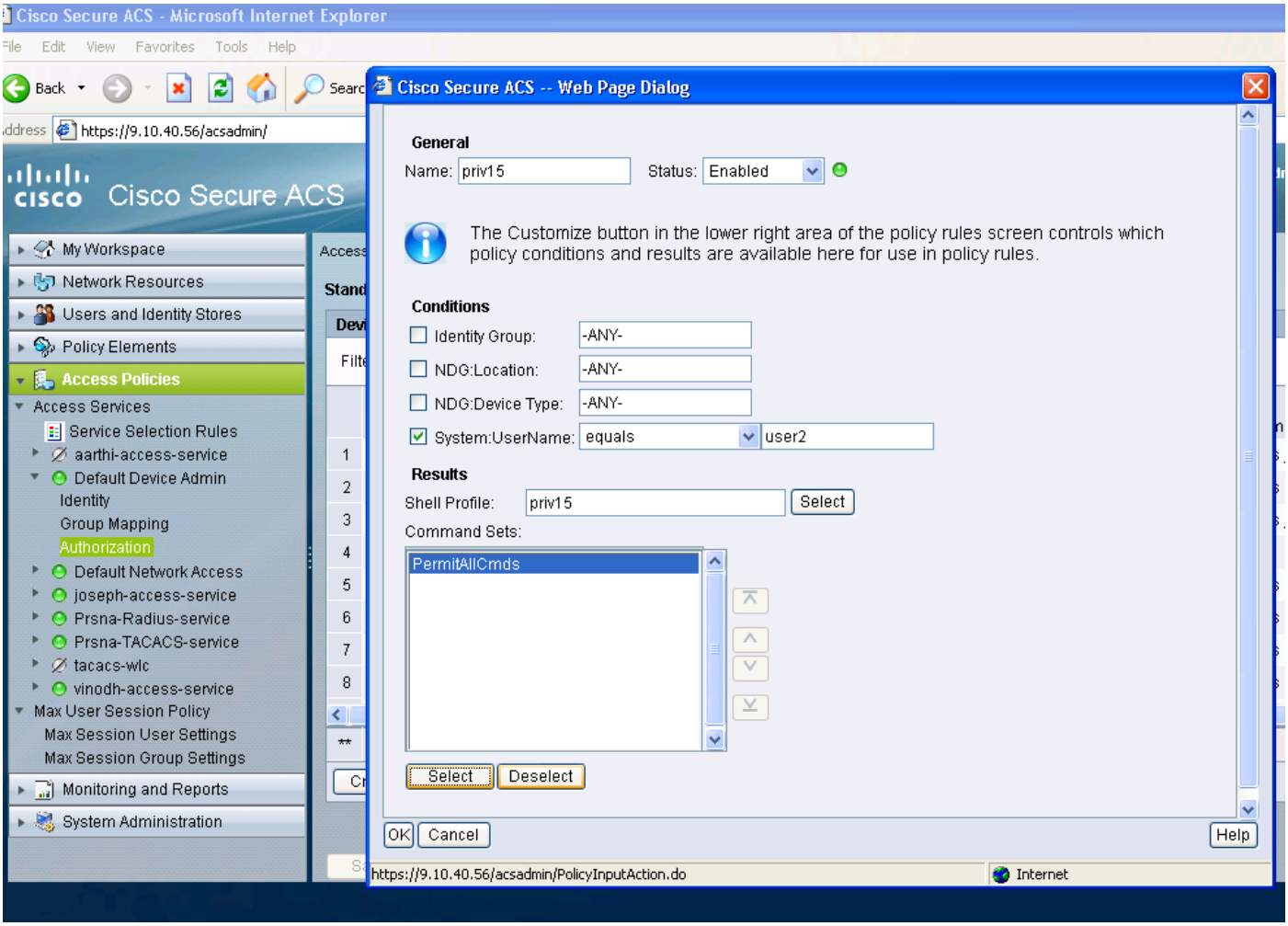
Crea una regola di selezione del servizio corrispondente al protocollo TACACS

A seconda delle policy e della configurazione, accertarsi di avere una regola corrispondente ai tacac provenienti dallo switch 5760.



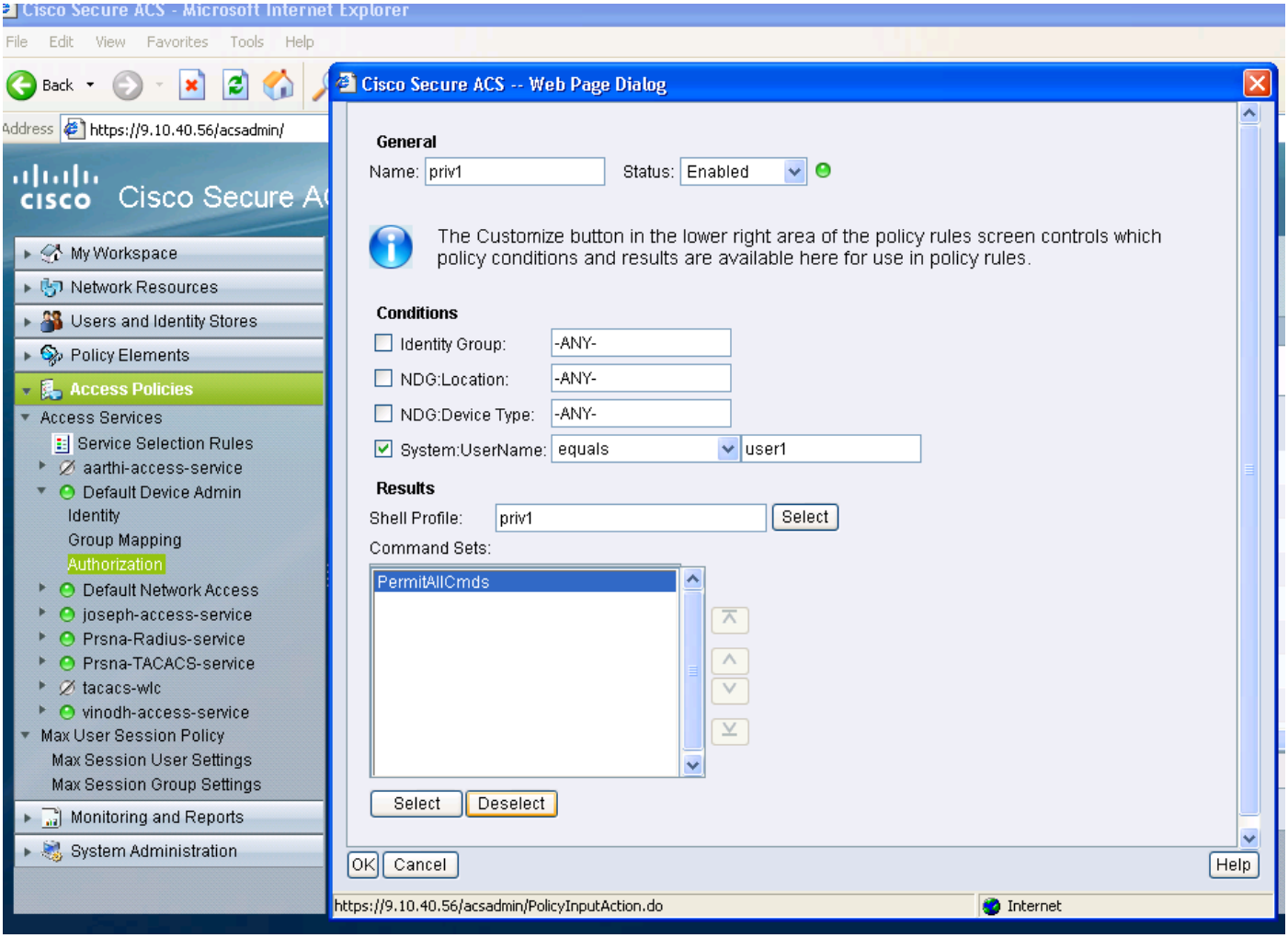
Creare criteri di autorizzazione per l'accesso amministrativo completo.

Il criterio di amministrazione del dispositivo predefinito utilizzato con la selezione del protocollo TACACS è selezionato come parte del processo del criterio di valutazione. Quando si utilizza il protocollo TACACS per l'autenticazione, il criterio di servizio selezionato è denominato Criterio predefinito di amministrazione del dispositivo. Tale politica comprende di per sé due sezioni . Identità indica chi è l'utente, a quale gruppo appartiene (locale o esterno) e cosa può fare in base al profilo di autorizzazione configurato. Assegnare il set di comandi relativo all'utente che si sta configurando.



Creare criteri di autorizzazione per l'accesso amministrativo di sola lettura.

La stessa operazione viene eseguita per gli utenti di sola lettura. In questo esempio vengono configurati il profilo della shell di livello 1 per l'utente 1 e il privilegio 15 per l'utente 2.



Configurazione di 5760 per TACACS

1. È necessario configurare il server Radius/Tacacs.

tac_acct server tacacs

indirizzo ipv4 9.1.0.100

chiave cisco

2. Configurare il gruppo di server

gtac acs+ gruppo server aaa

nome server tac_acct

Non esistono prerequisiti fino al passaggio precedente.

3. configurare gli elenchi dei metodi di autenticazione e autorizzazione

aaa authentication login <elenco metodi> group <srv-grp>

aaa authorization exec <elenco-metodi> group srv-grp>

aaa authorization exec default group <srv-grp> - à soluzione alternativa per ottenere tacacs su http.

I 3 comandi indicati sopra e tutti gli altri parametri di autenticazione e autorizzazione devono utilizzare lo stesso database, radius/tacacs o locale

Ad esempio, se l'autorizzazione dei comandi deve essere attivata, è necessario che faccia riferimento allo stesso database.

Per Esempio:

i comandi di autorizzazione aaa 15 <method-list> group <srv-grp> —> il gruppo di server che punta al database (tacacs/radius o locale) deve essere lo stesso.

4. configurare http per l'utilizzo degli elenchi di metodi precedenti

ip http authentication aaa login-auth <elenco metodi> —> è necessario specificare qui in modo esplicito l'elenco metodi, anche se l'elenco è "default"

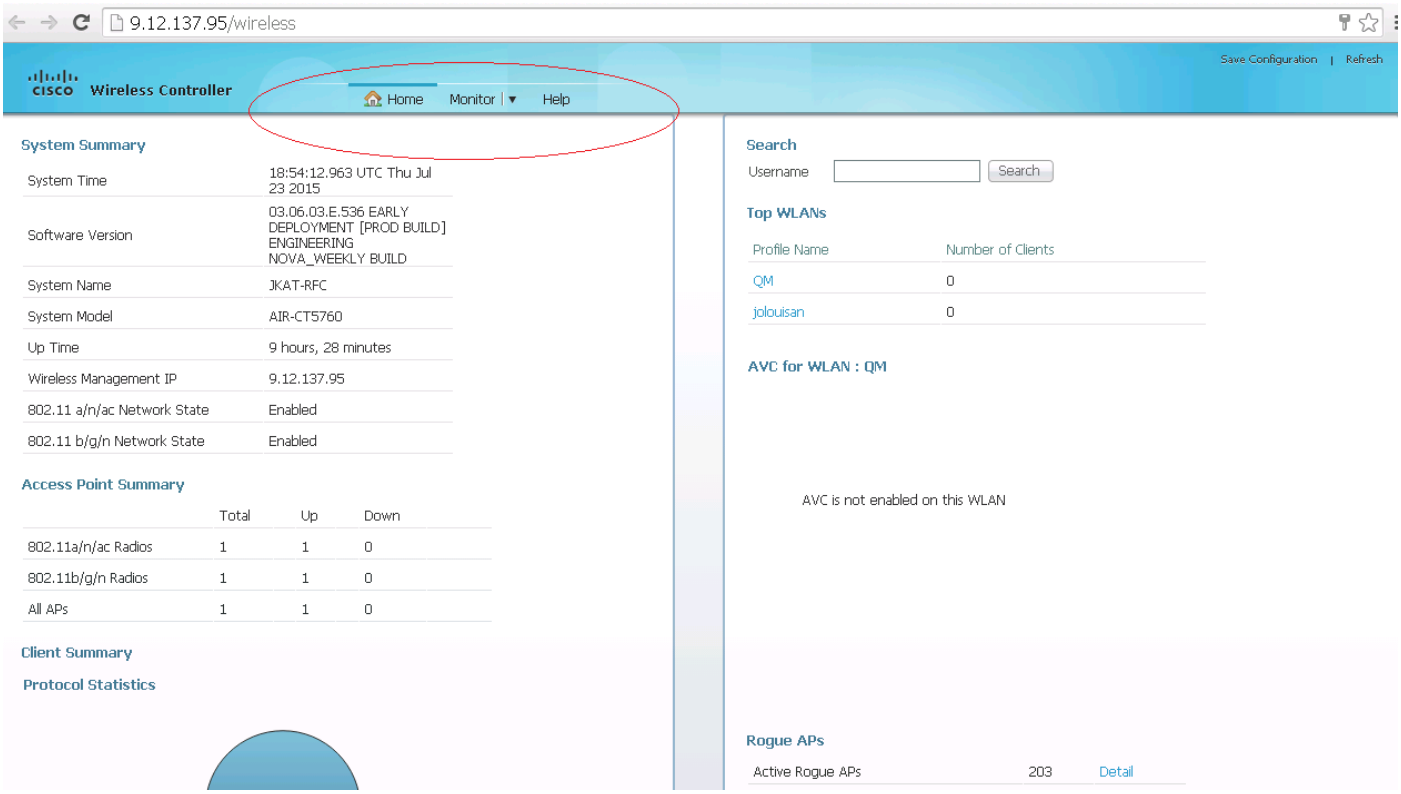
ip http authentication aaa exec-auth <elenco metodi>

** Note

- Non configurare alcun elenco di metodi sui parametri di configurazione "line vty". Se i passi precedenti e la vty di linea hanno configurazioni diverse, le configurazioni vty di linea avranno la precedenza.
- Il database deve essere lo stesso per tutti i tipi di configurazione della gestione, ad esempio ssh/telnet e webui.
- Per l'autenticazione HTTP l'elenco dei metodi deve essere definito in modo esplicito.

Accesso allo stesso switch 5760 con due profili diversi

Di seguito viene riportato l'accesso da parte di un utente con privilegi di livello 1 a cui viene concesso un accesso limitato



Di seguito viene riportato un accesso da un utente con livello di privilegio 15 al quale è stato concesso l'accesso completo