Ejemplo de configuración de control de acceso basado en privilegios de la interfaz web 5760 con Cisco Access Control Server (ACS)

Contenido

Introducción

Este documento explicará cómo crear perfiles de autenticación y autorización de Cisco ACS Tacacacs+ con diferentes niveles de privilegio e integrarlos con 5760 para acceder a WebUI. Esta función se admite a partir de 3.6.3 (pero no en 3.7.x al momento de escribir este artículo).

Prerequisites

Requirements

Se supone que el lector está familiarizado con la configuración del Cisco ACS y del controlador de acceso convergente. Este documento se centra solamente en la interacción entre esos 2 componentes en el ámbito de la autorización de tacacs+.

Componentes Utilizados

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

- Cisco Converged Access 5760, versión 3.6.3

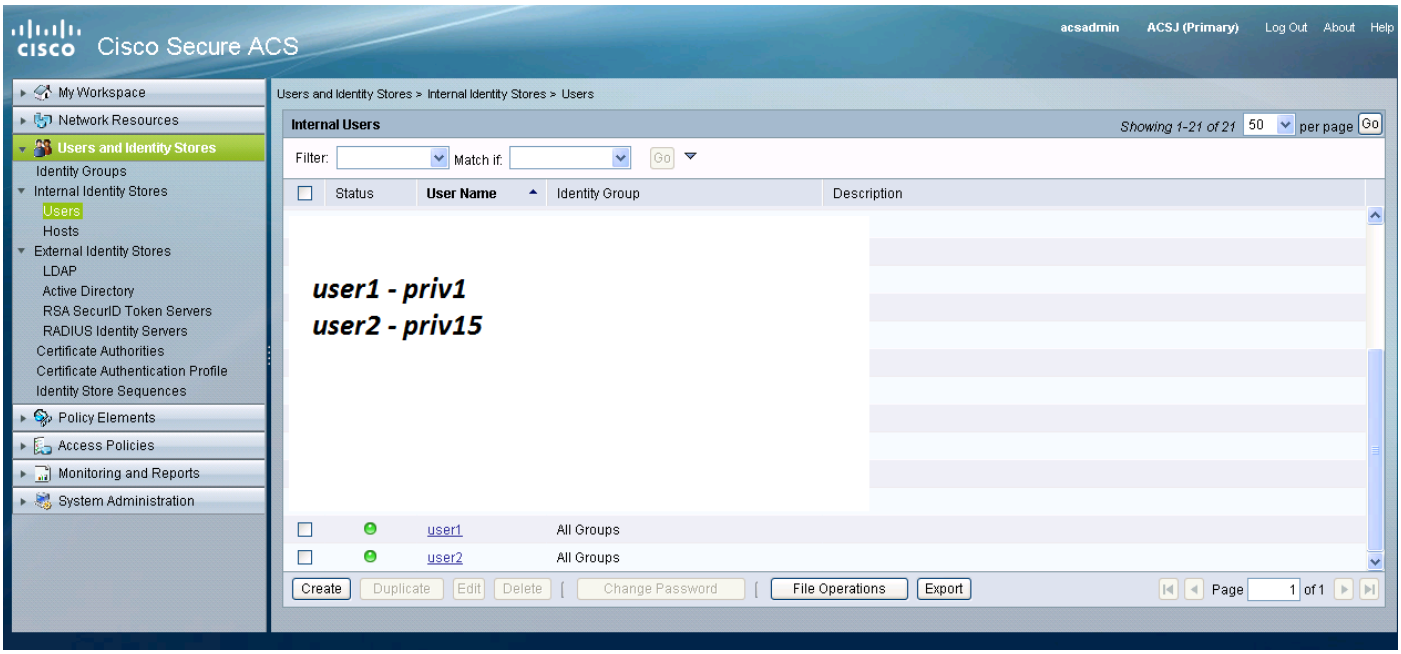
- Cisco Access Control Server (ACS) 5.2

Configuración

Crear unos pocos usuarios de prueba en ACS

Haga clic en "Users and Identity Stores" (Usuarios y almacenes de identidad) y, a continuación, seleccione "Users" (Usuarios).

Haga clic en "Crear" y configure algunos usuarios de prueba, como se muestra a continuación.



Configuración de elementos de política y perfiles de shell

Debe crear 2 perfiles para los 2 tipos diferentes de acceso .Privilege 15 en el mundo de cisco tacacs significa proporcionar acceso completo al dispositivo sin ninguna restricción. Por otra parte, el privilegio 1 le permitirá iniciar sesión y ejecutar sólo una cantidad limitada de comandos. A continuación se ofrece una breve descripción de los niveles de acceso proporcionados por cisco.

nivel de privilegio 1 = no privilegiado (el mensaje es router>), el nivel predeterminado para iniciar sesión

nivel de privilegio 15 = privilegiado (la solicitud es router#), el nivel luego de pasar al modo de activación

nivel de privilegio 0 = rara vez se utiliza, pero incluye 5 comandos: **inhabilitar**, **habilitar**, **salir**, **ayudar** y **cerrar sesión**

En el 5760, los niveles 2-14 se consideran iguales al nivel 1. Se les otorga el mismo privilegio que a 1. **No configure los niveles de privilegio de tacacs para ciertos comandos en el 5760**. El acceso a la interfaz de usuario por pestañas no se admite en 5760. Puede tener acceso completo (priv15) o sólo acceso a la ficha Monitor (priv1). Además, los usuarios con el nivel de privilegio 0 no pueden iniciar sesión.

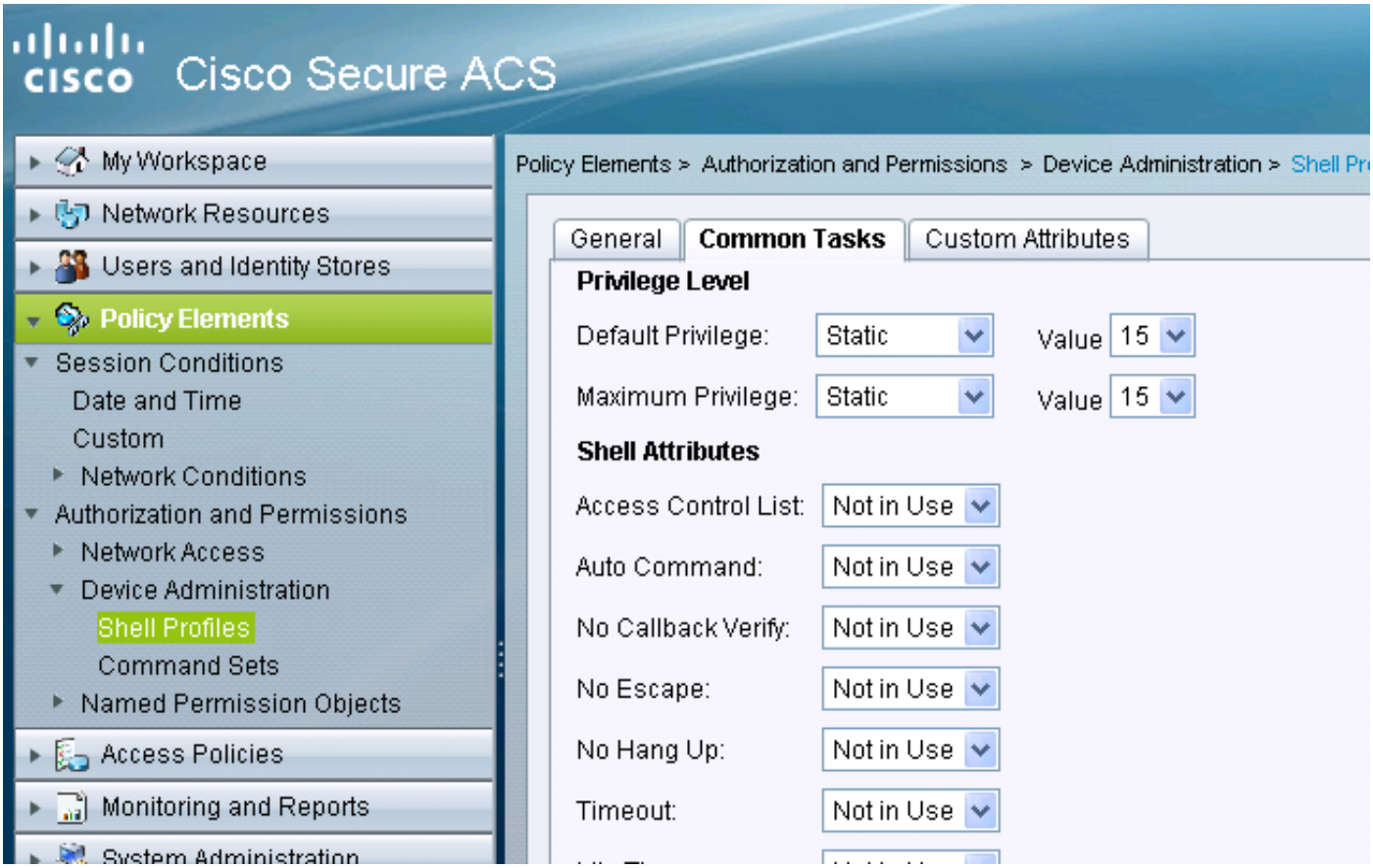
Creación del perfil de acceso al shell de 15 niveles de privilegio

Mediante la siguiente pantalla de impresión, cree ese perfil:

Haga clic en "Elementos de política". Haga clic en "Perfiles de Shell".

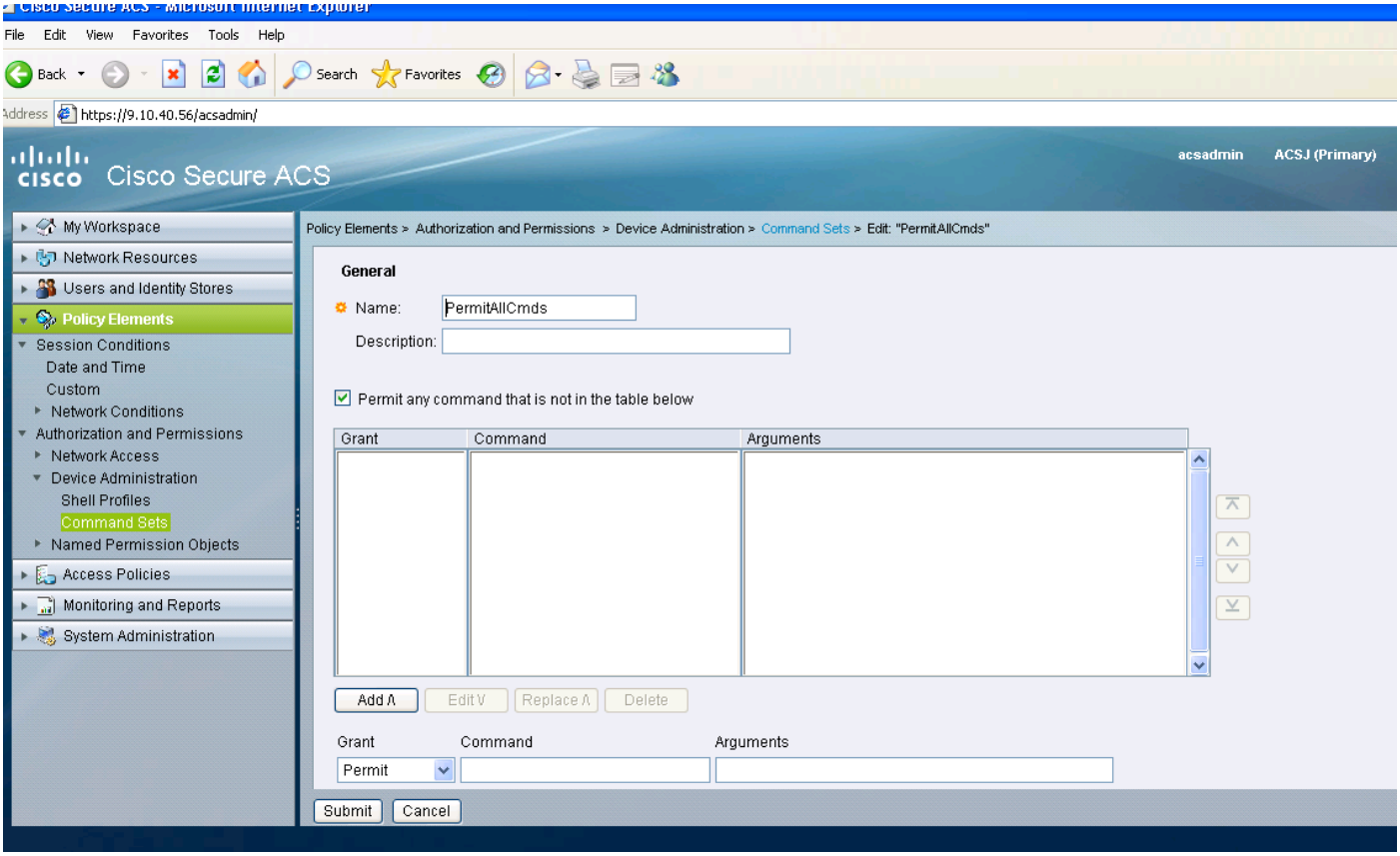
Cree uno nuevo.

Vaya a la ficha "Tareas comunes" y establezca los niveles de privilegio predeterminado y máximo en 15.



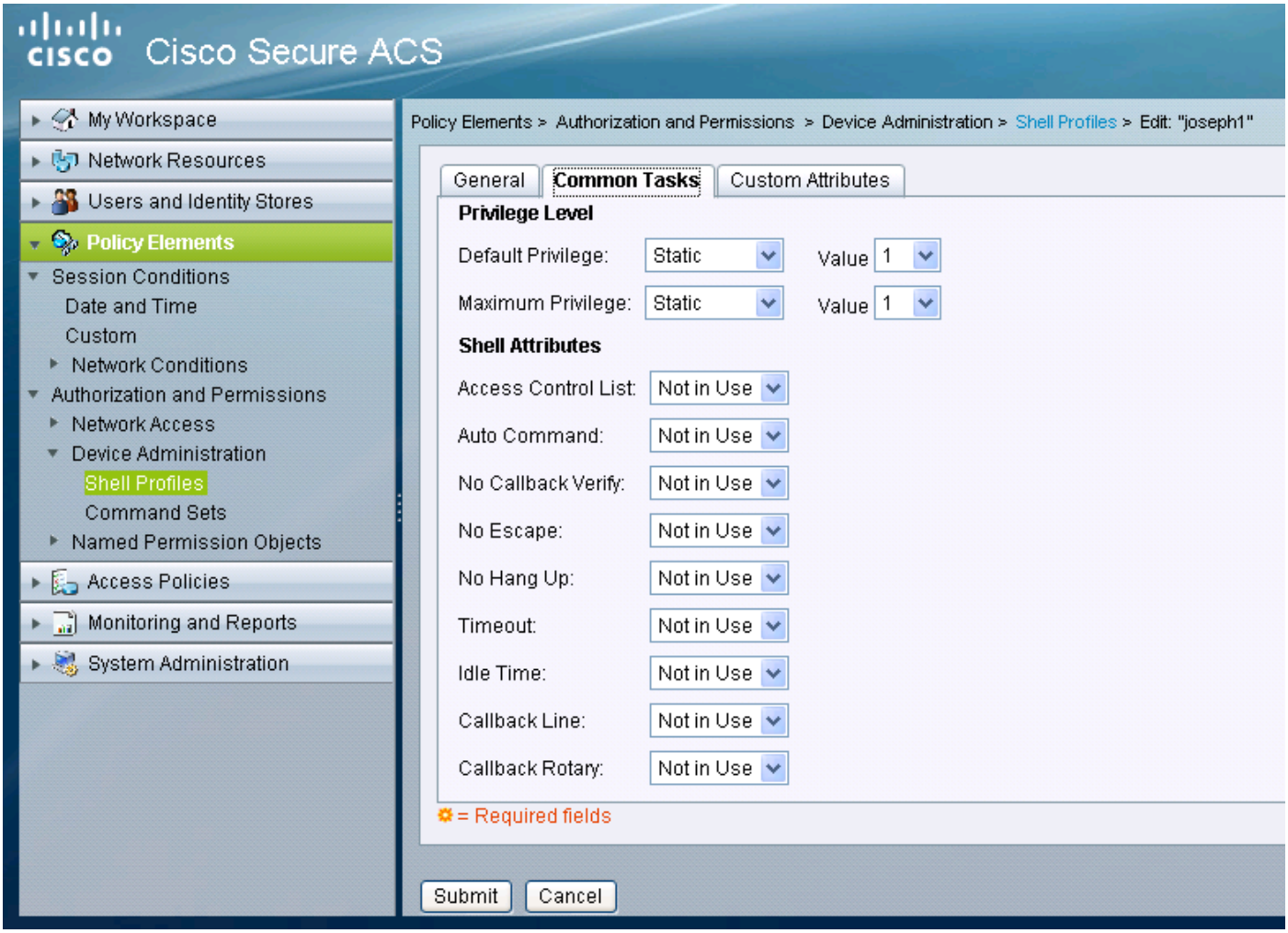
Creación de conjuntos de comandos para el usuario administrador

Los conjuntos de comandos son conjuntos de comandos que utilizan todos los dispositivos tacacs.Se pueden utilizar para restringir los comandos que un usuario puede utilizar si se le asigna ese perfil específico. Dado que en el 5760, la restricción se realiza en el código de Webui en función del nivel de privilegio pasado, los conjuntos de comandos para el nivel de privilegio 1 y 15 son los mismos.



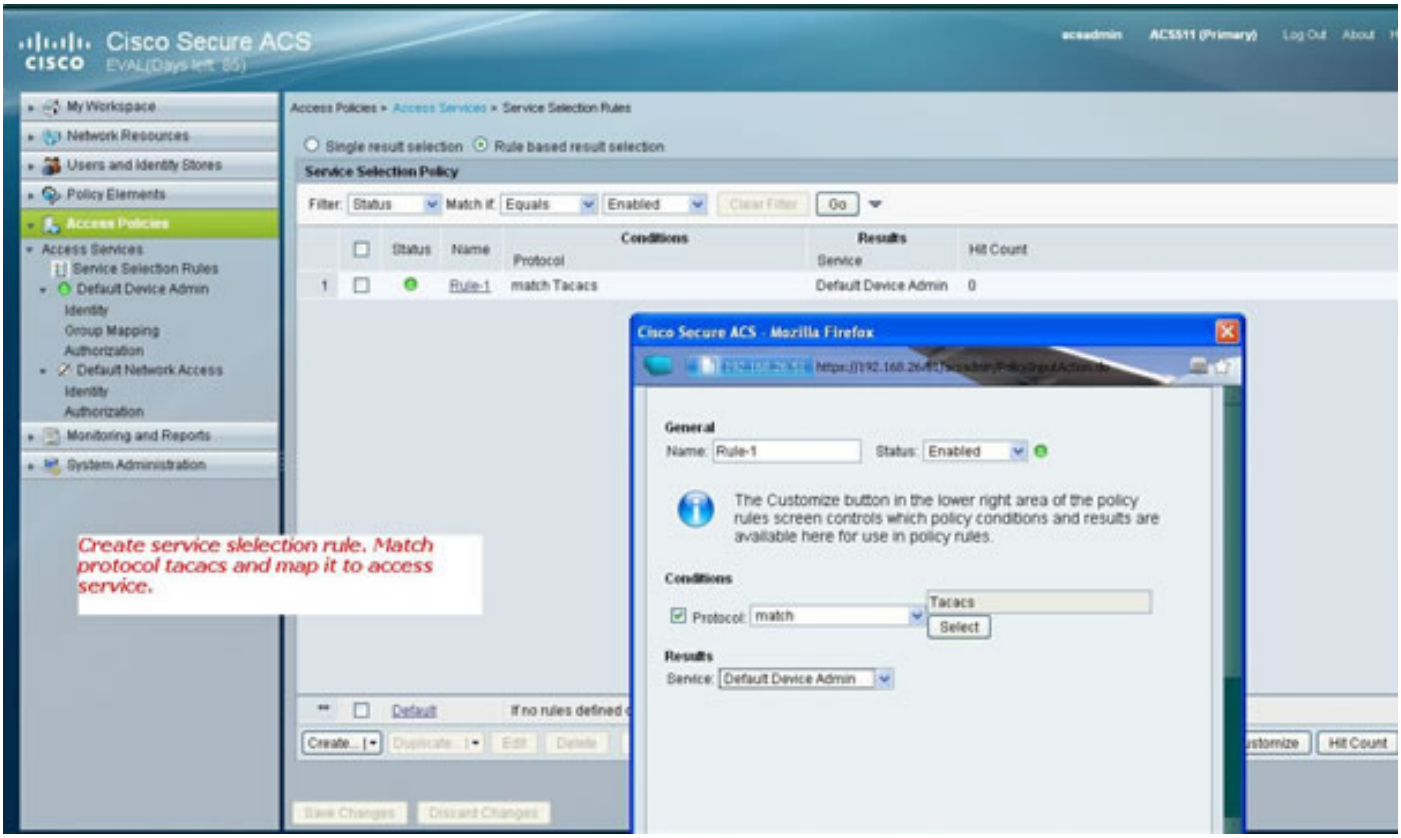
Creación de perfiles de shell para usuarios de sólo lectura

Cree otro perfil de shell para usuarios de sólo lectura. Este perfil se diferenciará por el hecho de que los niveles de privilegio se establecen en 1.



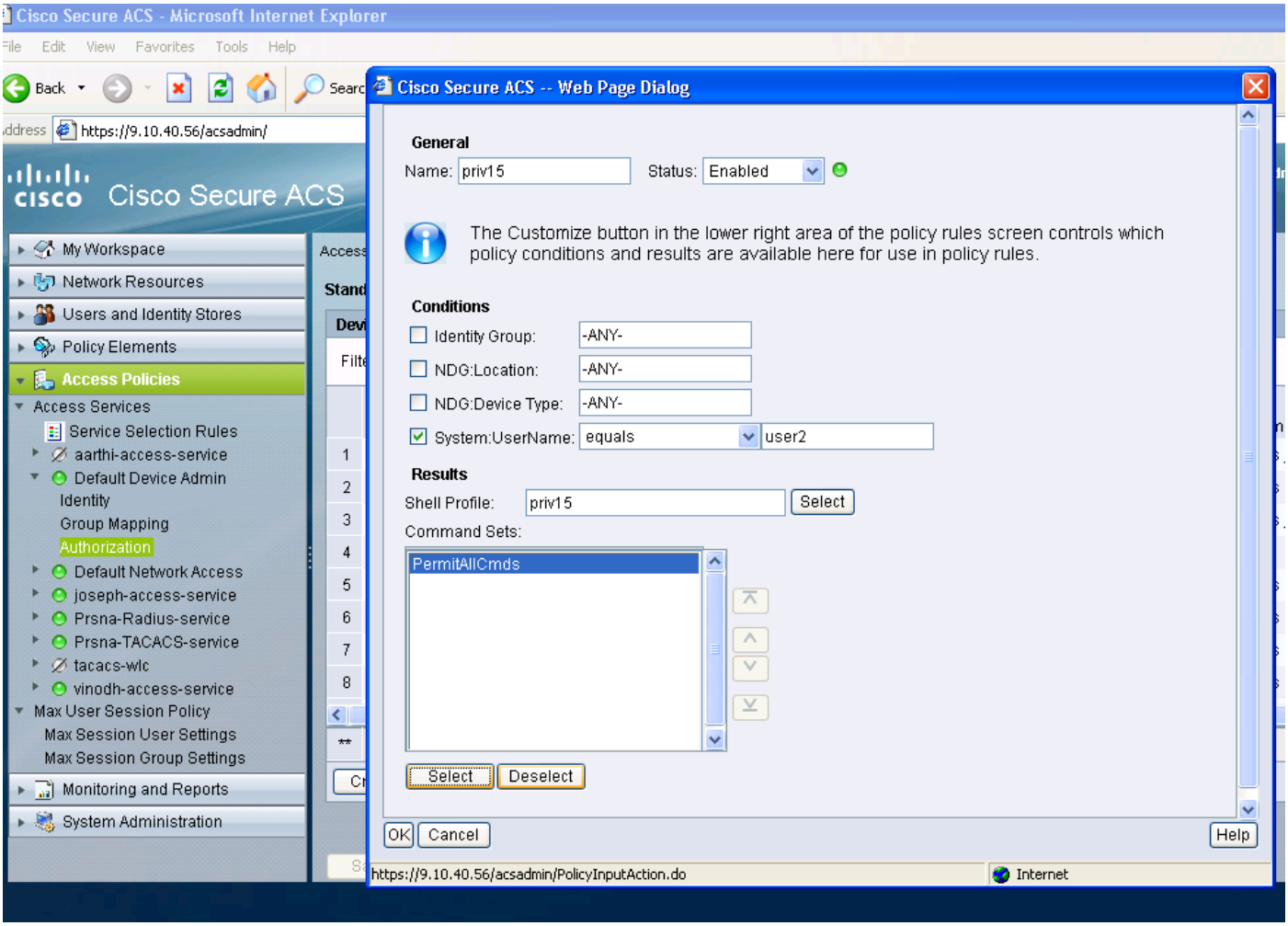
Cree una regla de selección de servicio para que coincida con el protocolo tacacs

En función de las políticas y la configuración, asegúrese de que dispone de una táctica de coincidencia de reglas que proviene del modelo 5760.



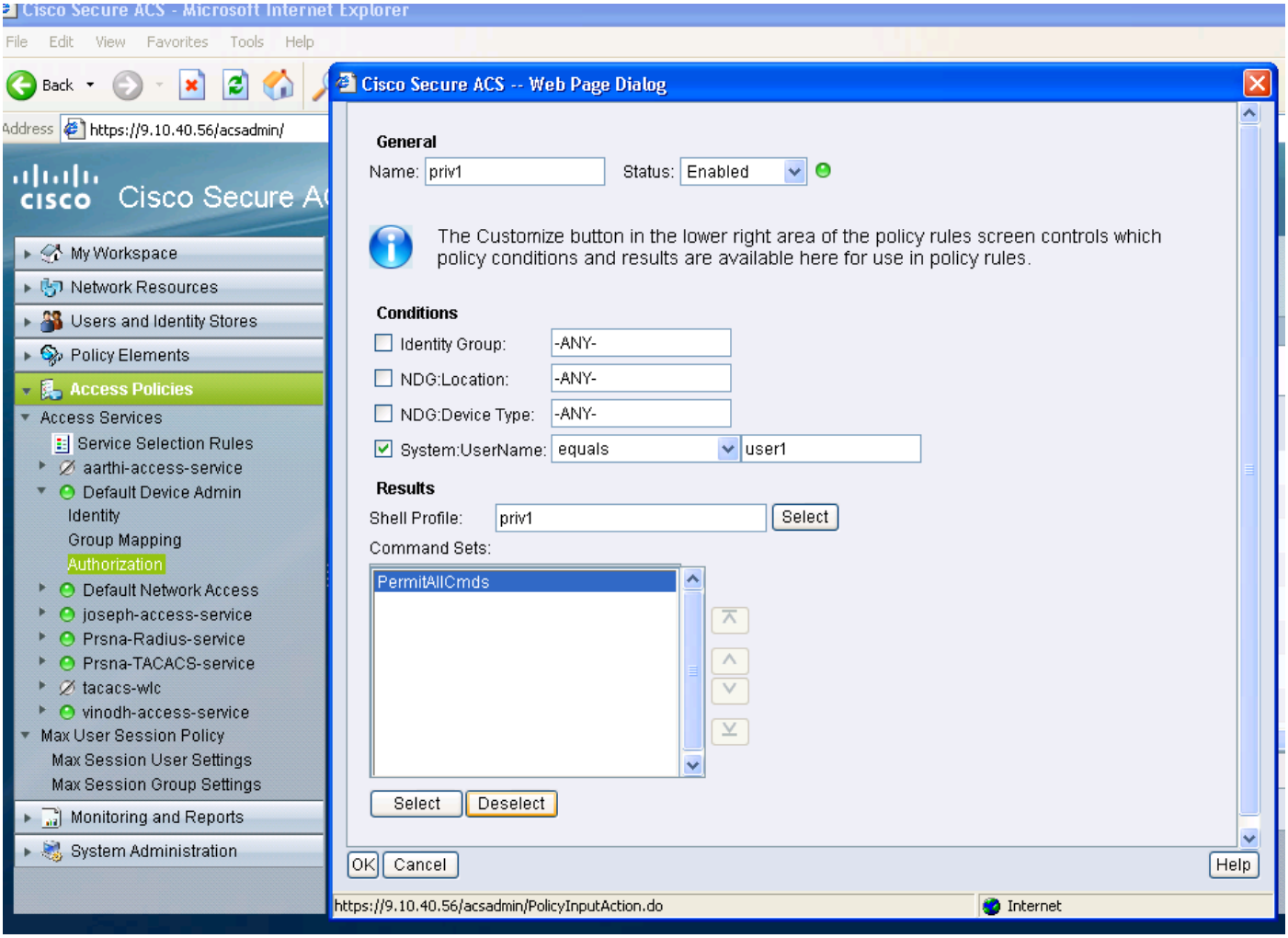
Cree una política de autorización para el acceso completo a la administración.

La política de administración de dispositivos predeterminada utilizada con la selección del protocolo tacacs se selecciona como parte del proceso de política de evaluación. Cuando se utiliza el protocolo tacacs para la autenticación, la política de servicio seleccionada se denomina política de administración de dispositivos predeterminada. Esa política en sí misma comprende dos secciones. Identidad significa quién es el usuario y a qué grupo pertenece (local o externo) y a qué se le permite hacer según el perfil de autorización configurado. Asigne el conjunto de comandos relacionado con el usuario que está configurando.



Cree una política de autorización para el acceso de administración de sólo lectura.

Lo mismo se hace para los usuarios de sólo lectura. Estos ejemplos configuran el perfil de shell de nivel de privilegio 1 para el usuario 1 y el privilegio 15 para el usuario 2.



Configuración del 5760 para tacacs

1. Es necesario configurar el servidor Radius/Tacacs.

tacacs server tac_acct

address ipv4 9.1.0.100

clave cisco

2. Configurar el grupo de servidores

aaa group server tacacs+ gtac

nombre del servidor tac_acct

No hay ningún requisito previo hasta el paso anterior.

3. configurar listas de métodos de autenticación y autorización

aaa authentication login <method-list> group <srv-grp>

aaa authorization exec <method-list> group srv-grp>

aaa authorization exec default group <srv-grp> —à workparfor get tacacs on http.

Los 3 comandos anteriores y todos los demás parámetros de autenticación y autorización deben

utilizar la misma base de datos, ya sea radius/tacacs o local

Por ejemplo, si la autorización de comandos debe habilitarse, también debe apuntar a la misma base de datos.

Por ejemplo:

aaa authorization, comandos 15 <method-list> group <srv-grp> —> el grupo de servidores que apunta a la base de datos (tacacs/radius o local) debe ser el mismo.

4. configure http para utilizar las listas de métodos anteriores

ip http authentication aaa login-auth <method-list> —> la lista de métodos debe especificarse explícitamente aquí, incluso si la lista de métodos es "default"

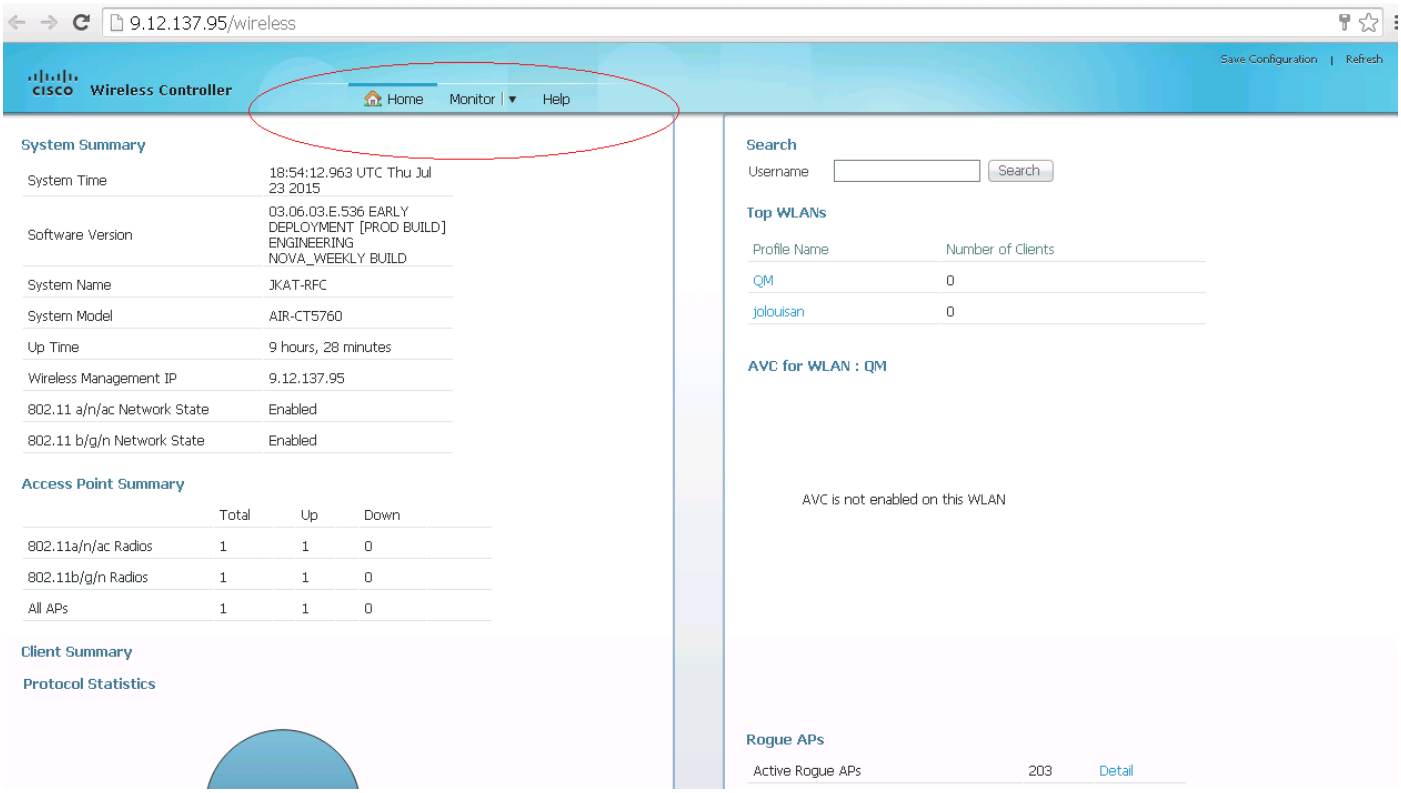
ip http authentication aaa exec-auth <method-list>

** Puntos a tener en cuenta

- No configure ninguna lista de métodos en los parámetros de configuración "line vty". Si los pasos anteriores y la línea vty tienen configuraciones diferentes, las configuraciones vty de línea tendrían prioridad.
- La base de datos debe ser la misma en todos los tipos de configuración de administración como ssh/telnet y webui.
- La autenticación HTTP debe tener la lista de métodos definida explícitamente.

Acceso al mismo 5760 con los 2 perfiles diferentes

A continuación se muestra un acceso desde un usuario de nivel de privilegio 1 donde se proporciona acceso limitado



A continuación se muestra un acceso desde un usuario de nivel de privilegio 15 donde se le da acceso completo