Konfigurationsbeispiel für die Zugriffskontrolle auf Berechtigungsebene der Webschnittstelle 5760 mit Cisco Access Control Server (ACS)

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie Authentifizierungs- und Autorisierungsprofile für Cisco ACS TACACS+ mit unterschiedlichen Berechtigungsebenen erstellen und in 5760 für den Zugriff auf die WebUI integrieren. Diese Funktion wird ab 3.6.3 unterstützt (jedoch nicht ab 3.7.x zum Zeitpunkt dieser Veröffentlichung).

Voraussetzungen

Anforderungen

Es wird davon ausgegangen, dass der Leser mit der Konfiguration des Cisco ACS und des Converged Access Controllers vertraut ist. Dieses Dokument konzentriert sich nur auf die Interaktion zwischen diesen beiden Komponenten im Rahmen der takacs+-Autorisierung.

Verwendete Komponenten

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

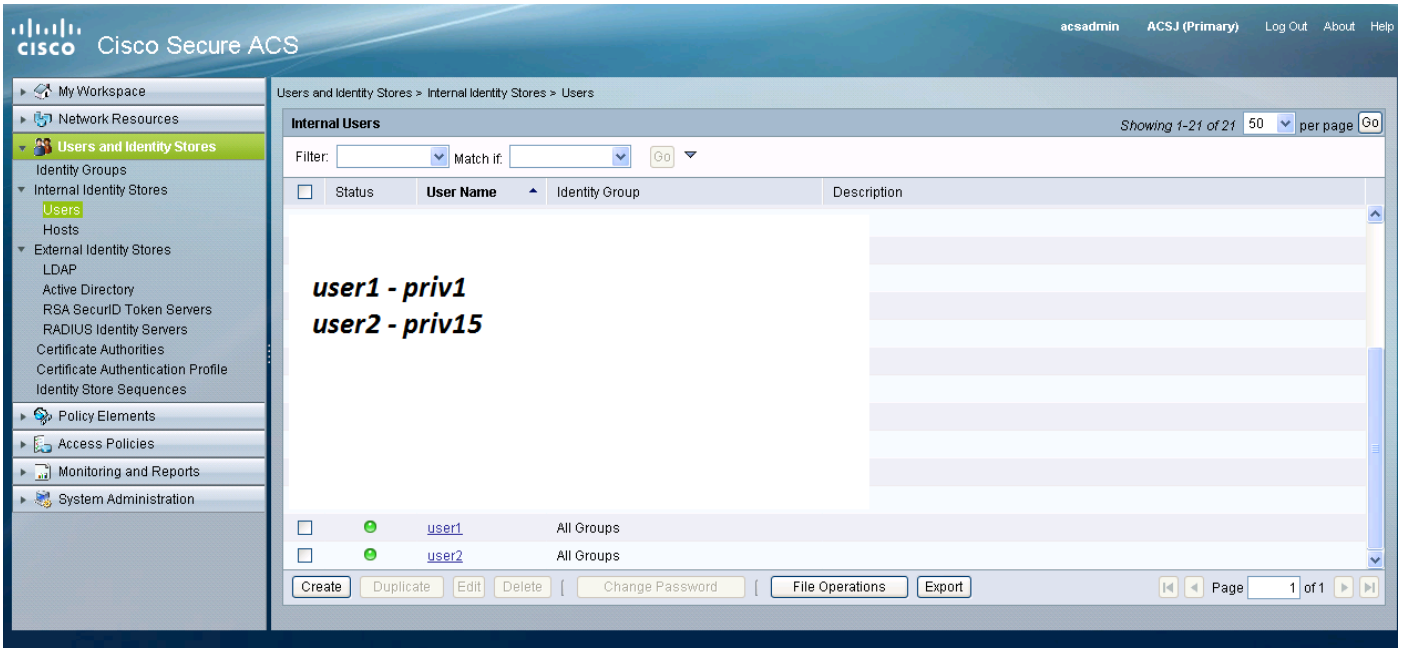
- Cisco Converged Access 5760, Version 3.6.3
- Cisco Access Control Server (ACS) 5.2

Konfiguration

Erstellen Sie einige Testbenutzer im ACS.

Klicken Sie auf "Benutzer und Identitätsdatenbanken" und wählen Sie "Benutzer" aus.

Klicken Sie auf "Erstellen", und konfigurieren Sie einige Testbenutzer, wie unten gezeigt.



Einrichten von Richtlinienelementen und Shell-Profilen

Sie müssen zwei Profile für die beiden verschiedenen Zugriffstypen erstellen.Berechtigung 15 in der Cisco-Takakonie bedeutet, dass der uneingeschränkte Zugriff auf das Gerät ohne Einschränkungen möglich ist. Privilege 1 dagegen ermöglicht Ihnen, sich anzumelden und nur eine begrenzte Anzahl von Befehlen auszuführen. Nachfolgend finden Sie eine kurze Beschreibung der von cisco bereitgestellten Zugriffsebenen.

Berechtigungsstufe 1 = nicht privilegiert (Eingabeaufforderung ist Router>), die Standardstufe für die Anmeldung

Berechtigungsstufe 15 = privilegiert (Eingabeaufforderung ist Router#), die Ebene nach dem Wechseln in den Aktivierungsmodus

Berechtigungsstufe 0 = selten verwendet, beinhaltet jedoch 5 Befehle: **Deaktivieren**, **Aktivieren**, **Beenden**, **Hilfe** und **Abmelden**

Beim 5760 werden die Stufen 2-14 als mit Stufe 1 identisch betrachtet. Sie erhalten das gleiche Privileg wie 1. **Konfigurieren Sie keine takacs-Berechtigungsebenen für bestimmte Befehle auf dem 5760**. Der 5760 unterstützt keinen Benutzeroberflächenzugriff auf Registerkarten. Sie können entweder vollständigen Zugriff (priv15) oder nur Zugriff auf die Registerkarte Monitor (priv1) haben. Benutzer mit der Berechtigungsstufe 0 dürfen sich nicht anmelden.

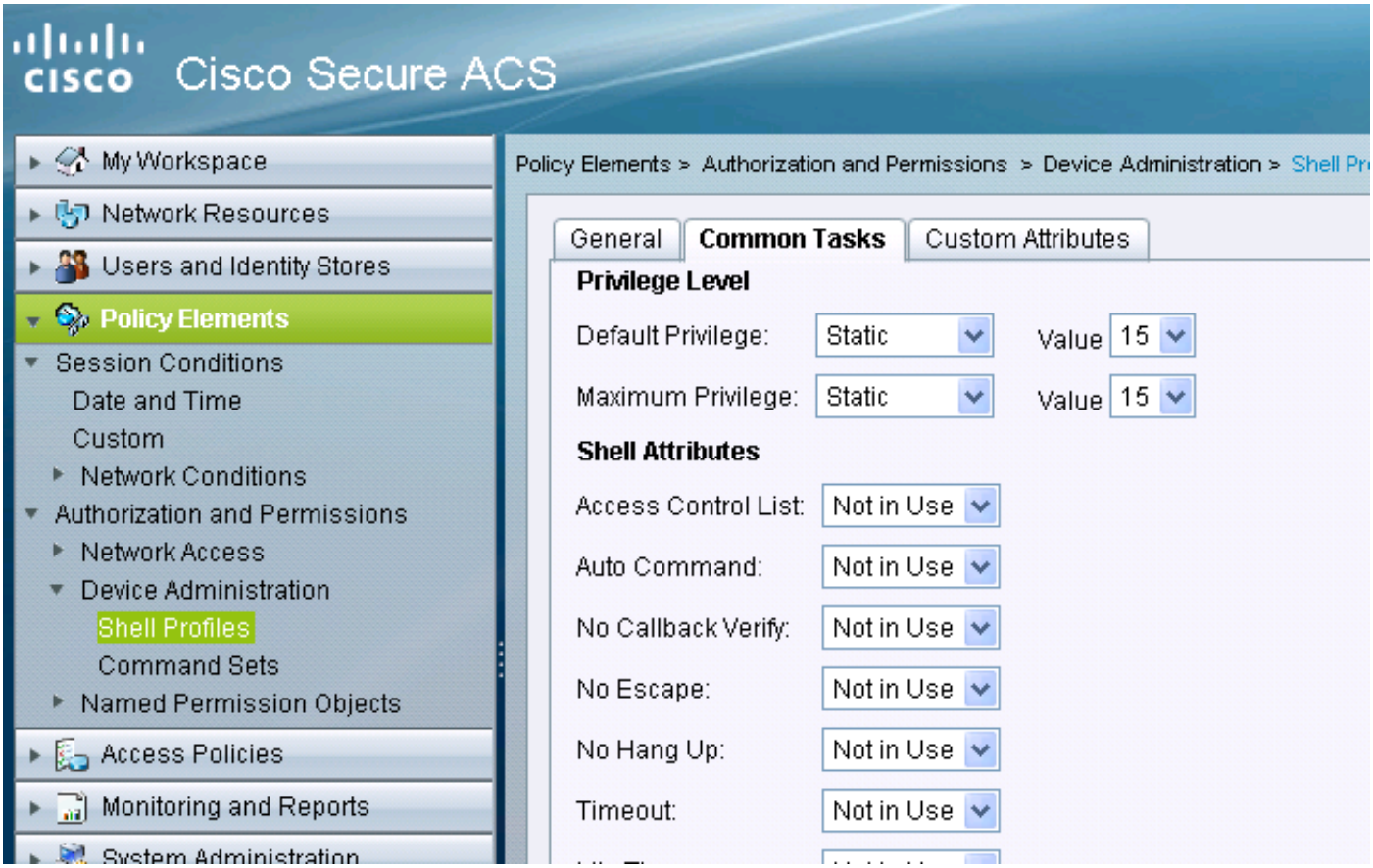
Erstellen eines privilegierten Zugriffsprofils auf 15-Ebenen-Shell

Erstellen Sie dieses Profil mithilfe des unten stehenden Druckbildschirms:

Klicken Sie auf "Richtlinienelemente". Klicken Sie auf "Shell-Profile".

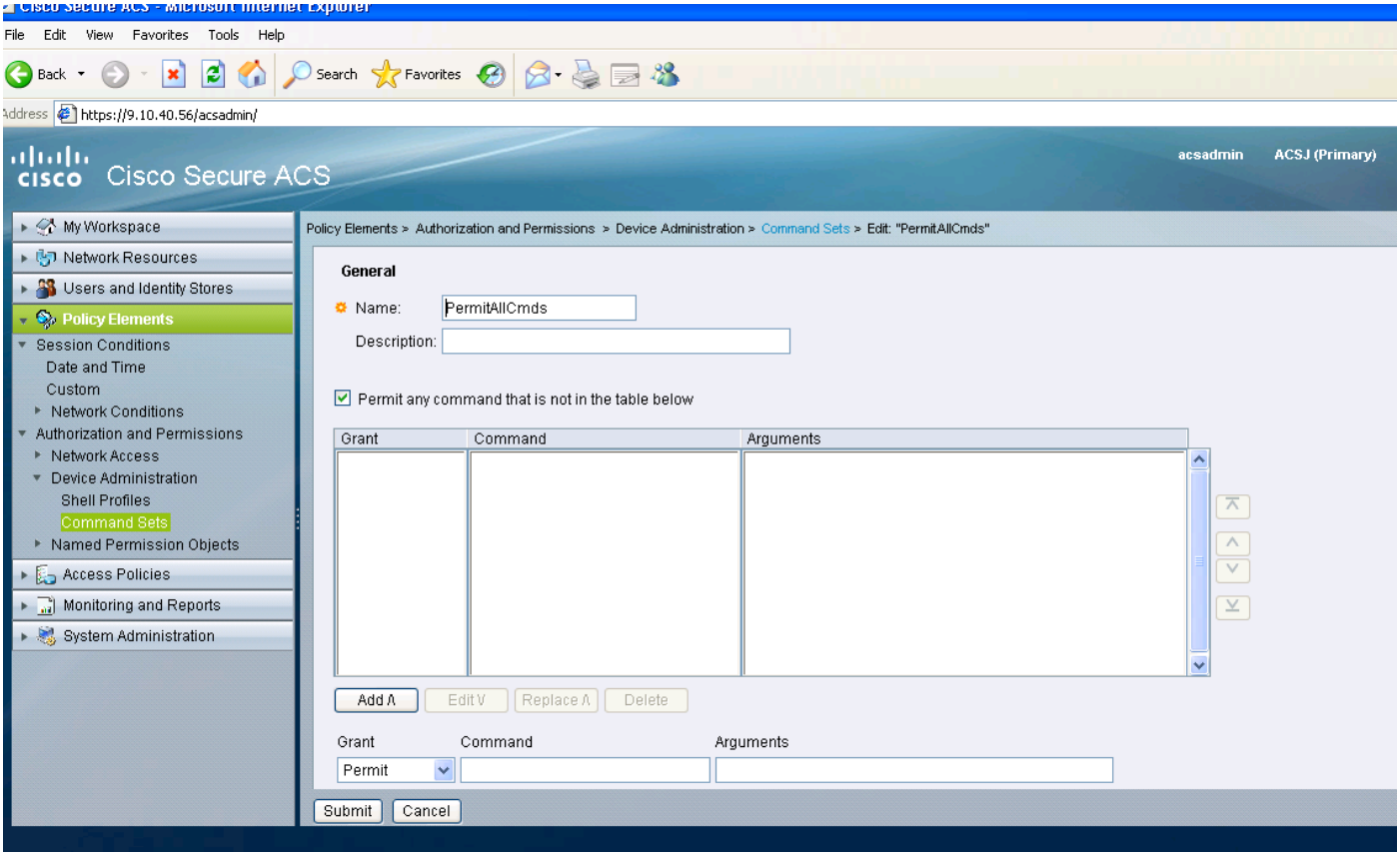
Erstellen Sie eine neue.

Wechseln Sie zur Registerkarte "Allgemeine Aufgaben", und legen Sie die Standard- und die maximale Berechtigungsstufe auf 15 fest.



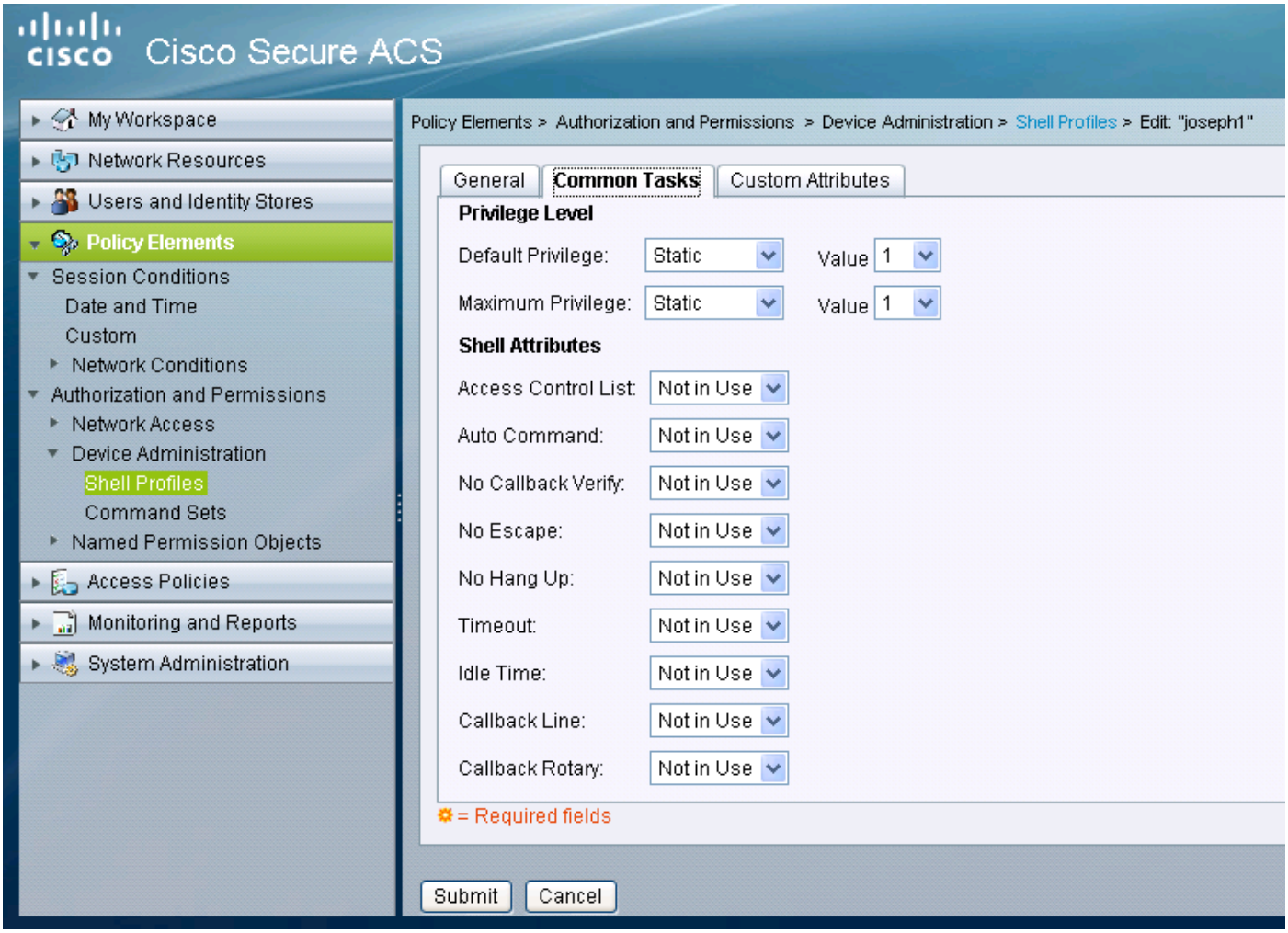
Erstellen von Befehlssätzen für Admin-Benutzer

Befehlssätze sind Befehlssätze, die von allen takacs-Geräten verwendet werden.Sie können verwendet werden, um die Befehle zu beschränken, die ein Benutzer verwenden darf, wenn ihm dieses spezifische Profil zugewiesen wird. Da auf dem 5760 die Einschränkung auf dem Webui-Code basierend auf der übergebenen Berechtigungsebene erfolgt, sind die Befehlssätze für die beiden Berechtigungsebenen 1 und 15 identisch.



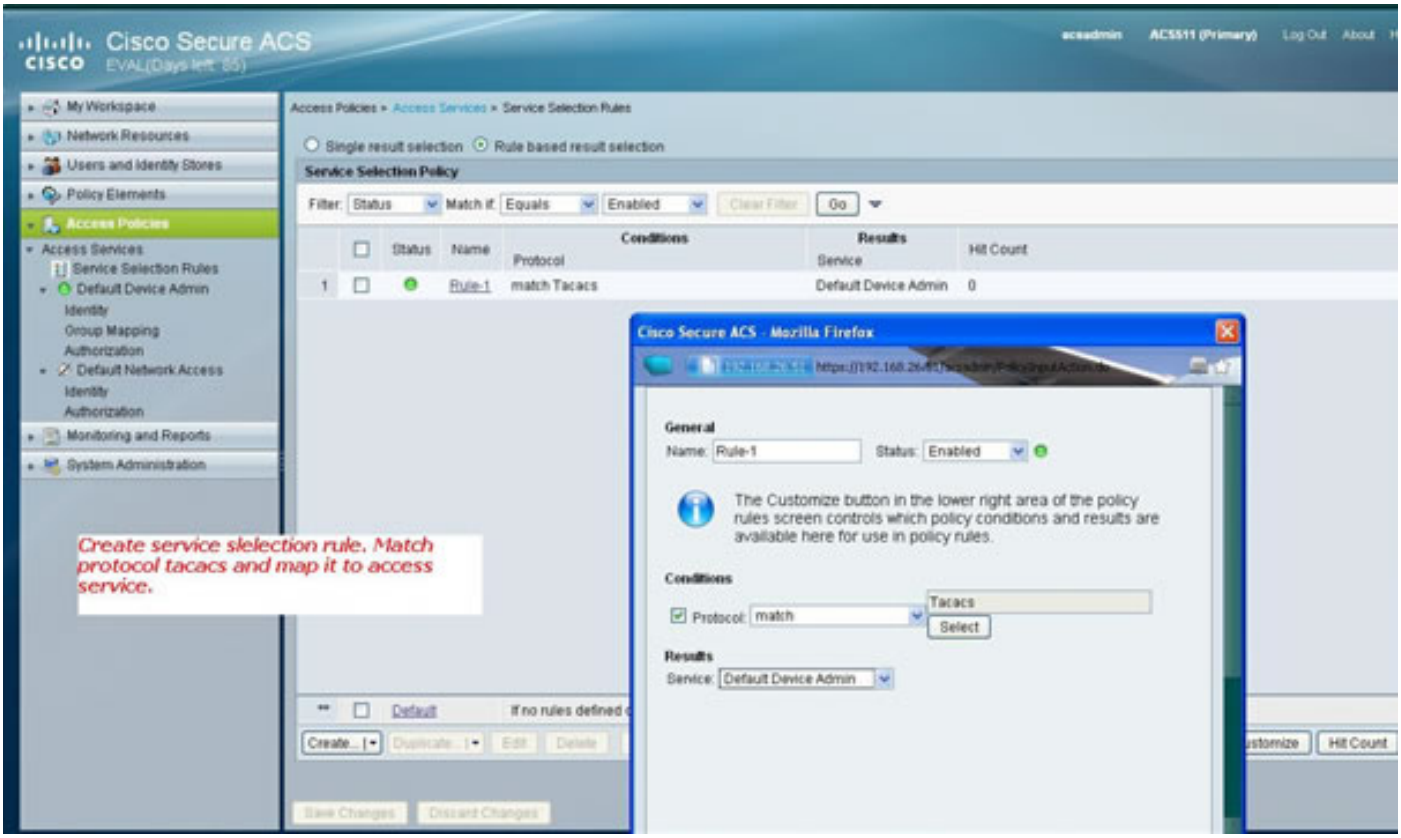
Erstellen eines Shell-Profils für schreibgeschützten Benutzer

Erstellen Sie ein anderes Shell-Profil für schreibgeschützte Benutzer. Dieses Profil unterscheidet sich dadurch, dass die Berechtigungsstufen auf 1 festgelegt sind.



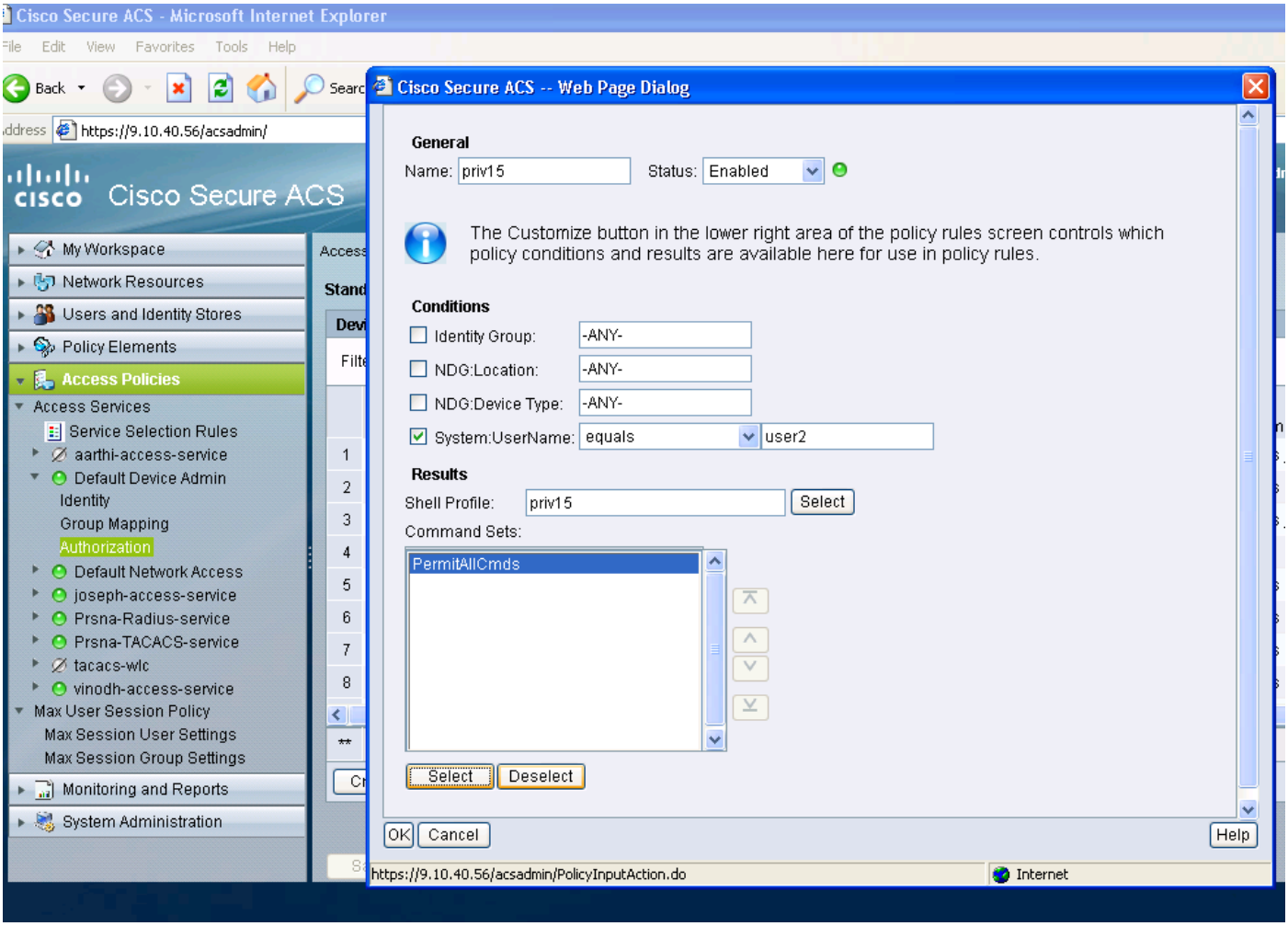
Erstellen einer Serviceauswahlregel, die dem Protokoll "takacs" entspricht

Stellen Sie je nach Richtlinie und Konfiguration sicher, dass Sie über Regelabstimmungstaktiken aus dem 5760 verfügen.



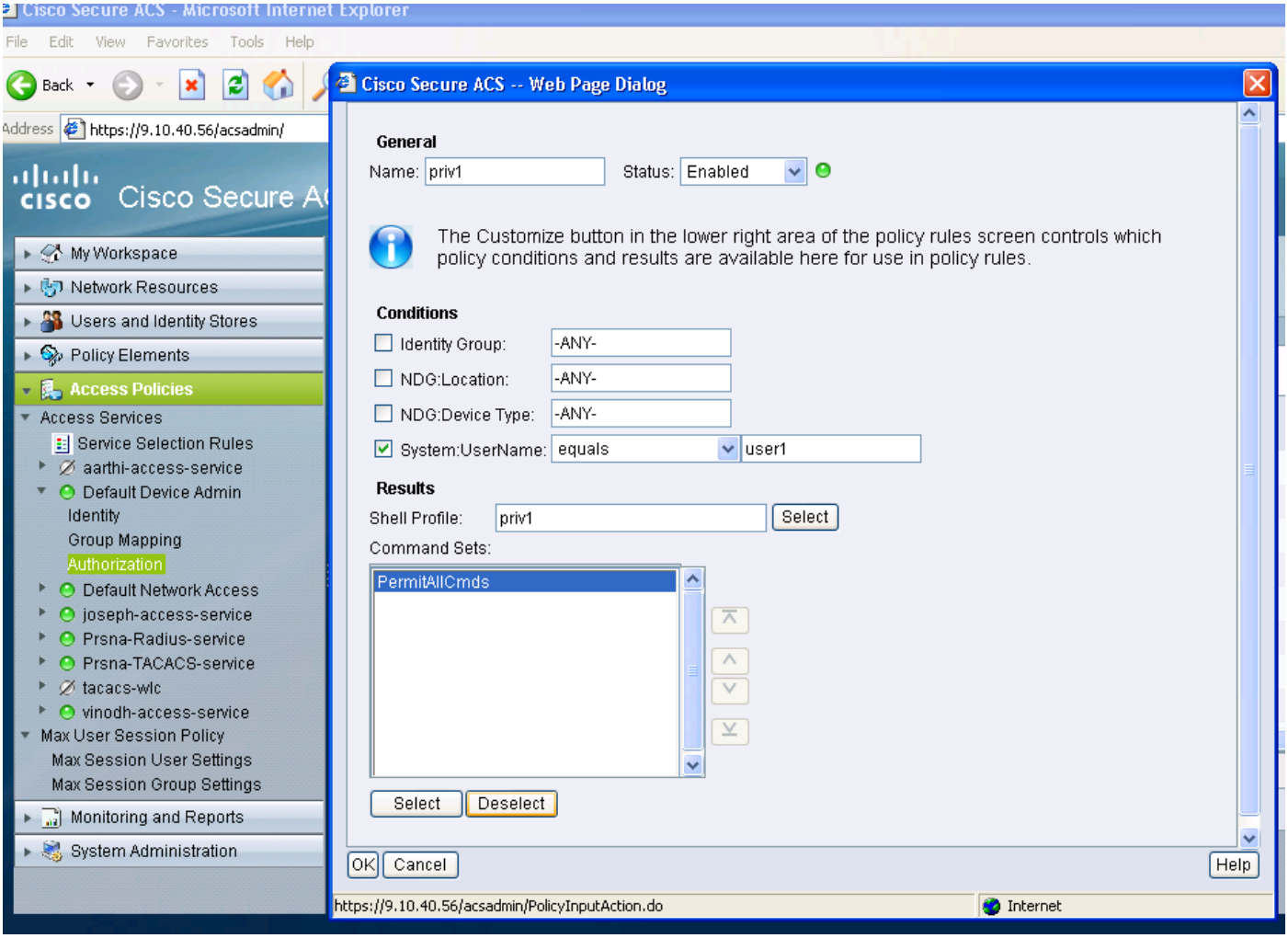
Erstellen Sie eine Autorisierungsrichtlinie für den vollständigen Administratorzugriff.

Im Rahmen des Evaluierungsrichtlinienprozesses wird die mit der takacs-Protokollauswahl verwendete Standard-Geräteadministratorrichtlinie ausgewählt. Wenn Sie das takacs-Protokoll für die Authentifizierung verwenden, wird die gewählte Dienstrichtlinie als Standard-Geräteadministratorrichtlinie bezeichnet. Diese Richtlinie besteht aus zwei Abschnitten. Identiy (Identifikation) bedeutet, wer der Benutzer ist und zu welcher Gruppe er gehört (lokal oder extern) und was er gemäß dem konfigurierten Autorisierungsprofil tun darf. Weisen Sie den Befehlssatz für den Benutzer zu, den Sie konfigurieren.



Erstellen Sie eine Autorisierungsrichtlinie für schreibgeschützten Administrationszugriff.

Dasselbe gilt für schreibgeschützte Benutzer. In diesem Beispiel wird das Shell-Profil der Berechtigungsstufe 1 für Benutzer 1 und die Berechtigung 15 für Benutzer 2 konfiguriert.



Konfigurieren des 5760 für Takaks

1. Radius/TACACS-Server müssen konfiguriert werden.

takacs server tac_acct

address ipv4 9.1.0.100

Schlüssel Cisco

2. Servergruppe konfigurieren

aaa group server tacacs+ gtac

Servername tac_acct

Bis zum oben beschriebenen Schritt gibt es keine Voraussetzung.

3. Konfiguration von Authentifizierungs- und Autorisierungsmethodenlisten

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

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

aaa authorized exec default group <srv-grp> —à workaround, um Taktiken auf http abzurufen.

Die drei oben genannten Befehle und alle anderen Authentifizierungs- und

Autorisierungsparameter sollten dieselbe Datenbank verwenden, entweder Radius/Takacs oder lokal

Wenn beispielsweise die Befehlsautorisierung aktiviert werden muss, muss sie auch auf dieselbe Datenbank verweisen.

Beispiel:

aaa authorized befehle 15 <method-list> group <srv-grp> —> Die Servergruppe, die auf die Datenbank verweist (takacs/radius oder local), sollte die gleiche sein.

4. Konfigurieren von http für die Verwendung der obigen Methodenlisten

ip http authentication aa login-auth <method-list> —> Die Methodenliste muss hier explizit angegeben werden, selbst wenn die Methodenliste "default" lautet.

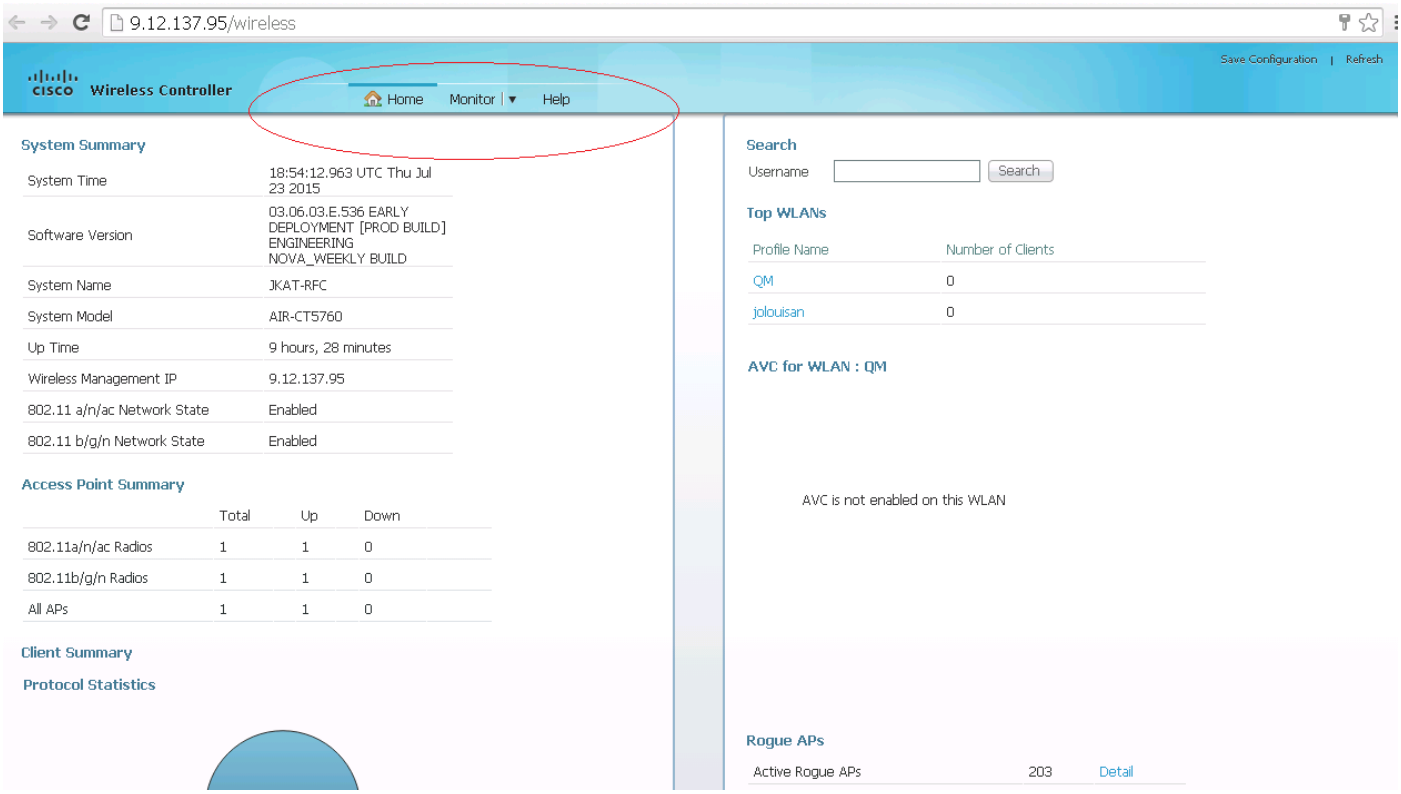
ip http authentication aaa exec-auth <method-list>

** Hinweis

- Konfigurieren Sie keine Methodenlisten für die Konfigurationsparameter "line vty". Wenn die oben genannten Schritte und die Posten-VTY unterschiedliche Konfigurationen haben, haben die VTY-Posten Vorrang.
- Die Datenbank sollte für alle Management-Konfigurationsarten wie ssh/telnet und webui identisch sein.
- Bei der HTTP-Authentifizierung sollte die Methodenliste explizit definiert sein.

Zugriff auf denselben 5760 mit den beiden unterschiedlichen Profilen

Im Folgenden sehen Sie einen Zugriff von einem Benutzer der Privilegienstufe 1, der begrenzten Zugriff erhält.



Im Folgenden sehen Sie einen Zugriff von einem Benutzer der Berechtigungsstufe 15, für den Sie vollständigen Zugriff erhalten.