使用思科存取控制伺服器(ACS)的5760 Web介面許可權級型存取控制組態範例

目錄

簡介

本文檔將介紹如何建立具有不同許可權級別的Cisco ACS Tacacs+身份驗證和授權配置檔案，以及如何將其與5760整合以訪問WebUI。從3.6.3開始（但在撰寫本文時不在3.7.x上）支援此功能。

必要條件

需求

假設讀卡器熟悉思科ACS和融合接入控制器配置。本檔案只會重點說明在tacacs+授權範圍中的這兩個元件之間的互動。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

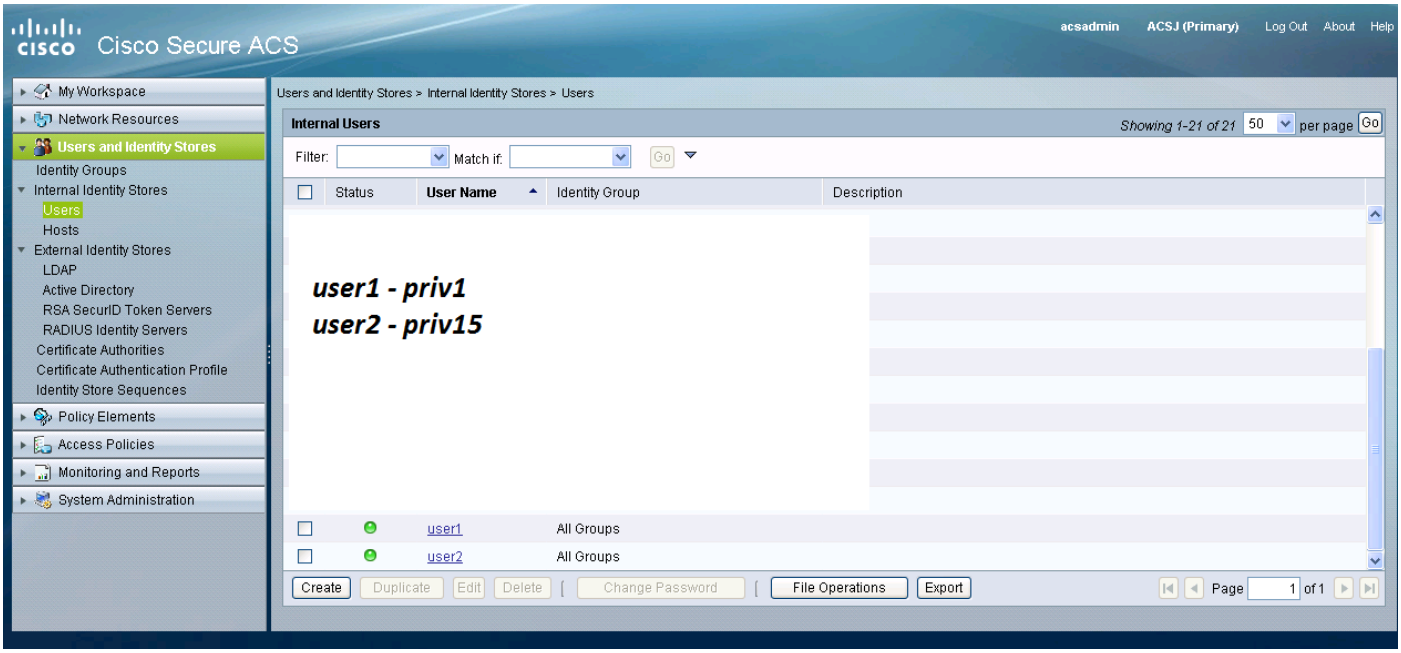
- 思科融合接入5760，版本3.6.3
- 思科存取控制伺服器(ACS)5.2

組態

在ACS中建立幾個測試使用者

按一下「使用者和身份庫」，然後選擇「使用者」。

按一下「建立」並配置幾個測試使用者，如下圖所示。



設定策略元素和殼配置檔案

您需要為2種不同型別的訪問建立2個配置檔案。在cisco tacacs世界中，特權15意味著提供裝置的完全訪問許可權，沒有任何限制。另一方面，特權1僅允許您登入並執行有限數量的命令。下面簡要介紹思科提供的訪問級別。

許可權級別1 =非特權（提示符為router>），登入的預設級別

許可權級別15 =特權（提示為router#），進入啟用模式後的級別

許可權級別0 =很少使用，但包括5個命令：**disable**、**enable**、**exit**、**help**和**logout**

在5760**上**，2-14級被視作與1級相同。它們被授予與1級相同的許可權。請不要為5760上的某些命令配置tacacs許可權級**別**。5760不支援每個頁籤的UI訪問。您可以擁有完全訪問許可權(priv15)或只能訪問Monitor頁籤(priv1)。 此外，許可權級別為0的使用者不能登入。

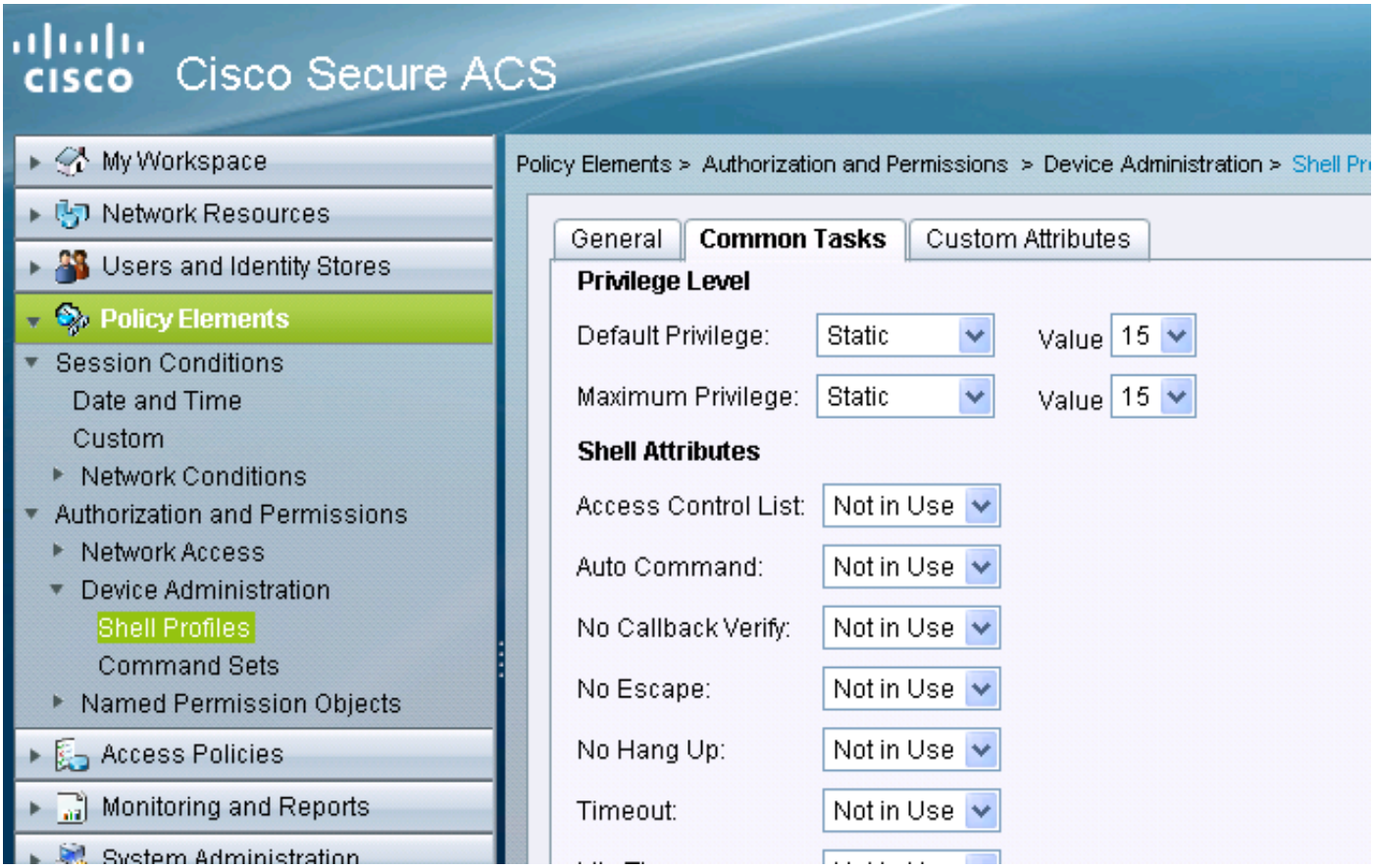
建立許可權15級外殼訪問配置檔案

使用下面的列印螢幕建立該配置檔案：

按一下「Policy Elements」（策略元素）。 按一下「Shell Profiles」。

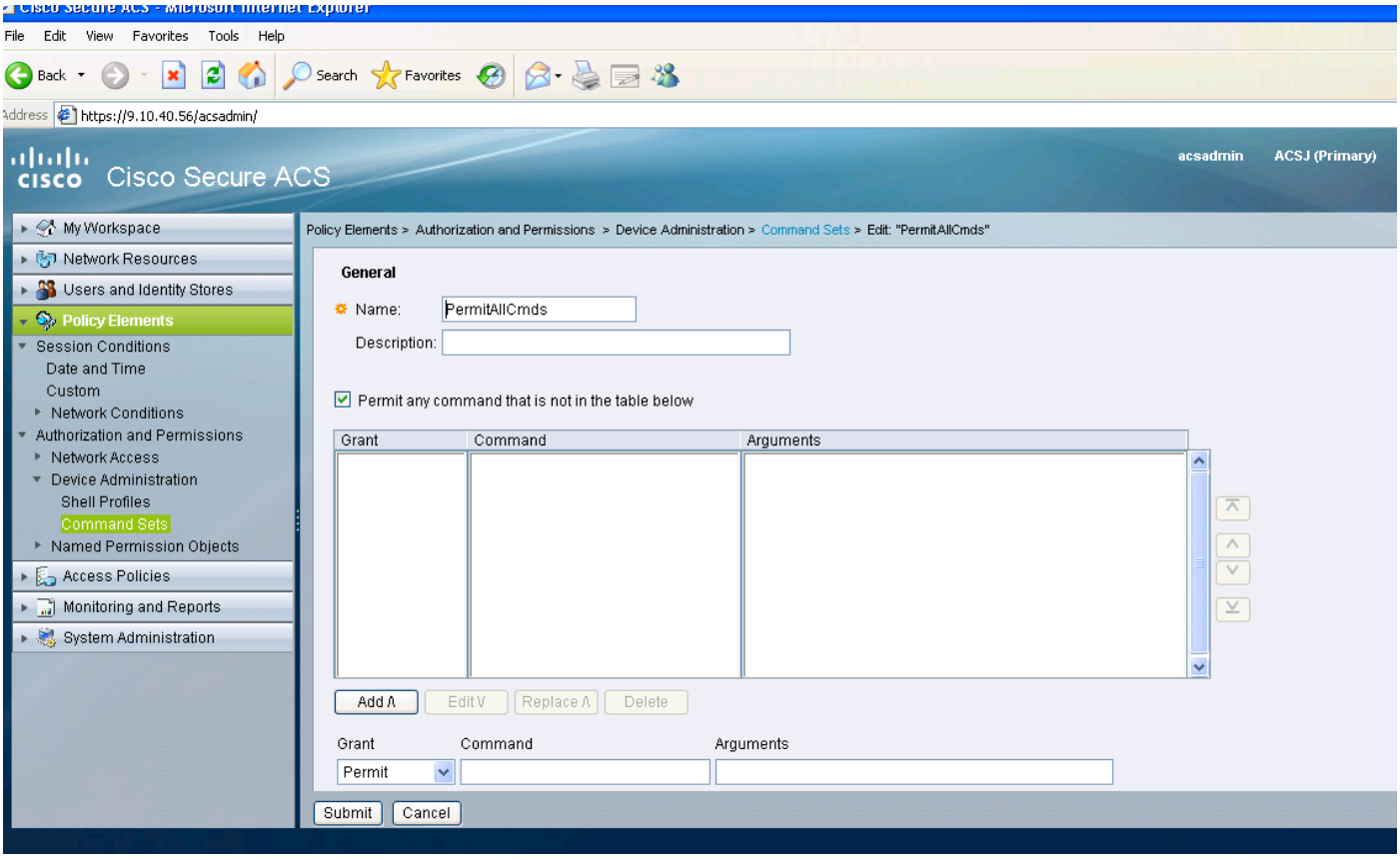
新建一個。

轉到「常見任務」頁籤，將預設和最大許可權級別設定為15。



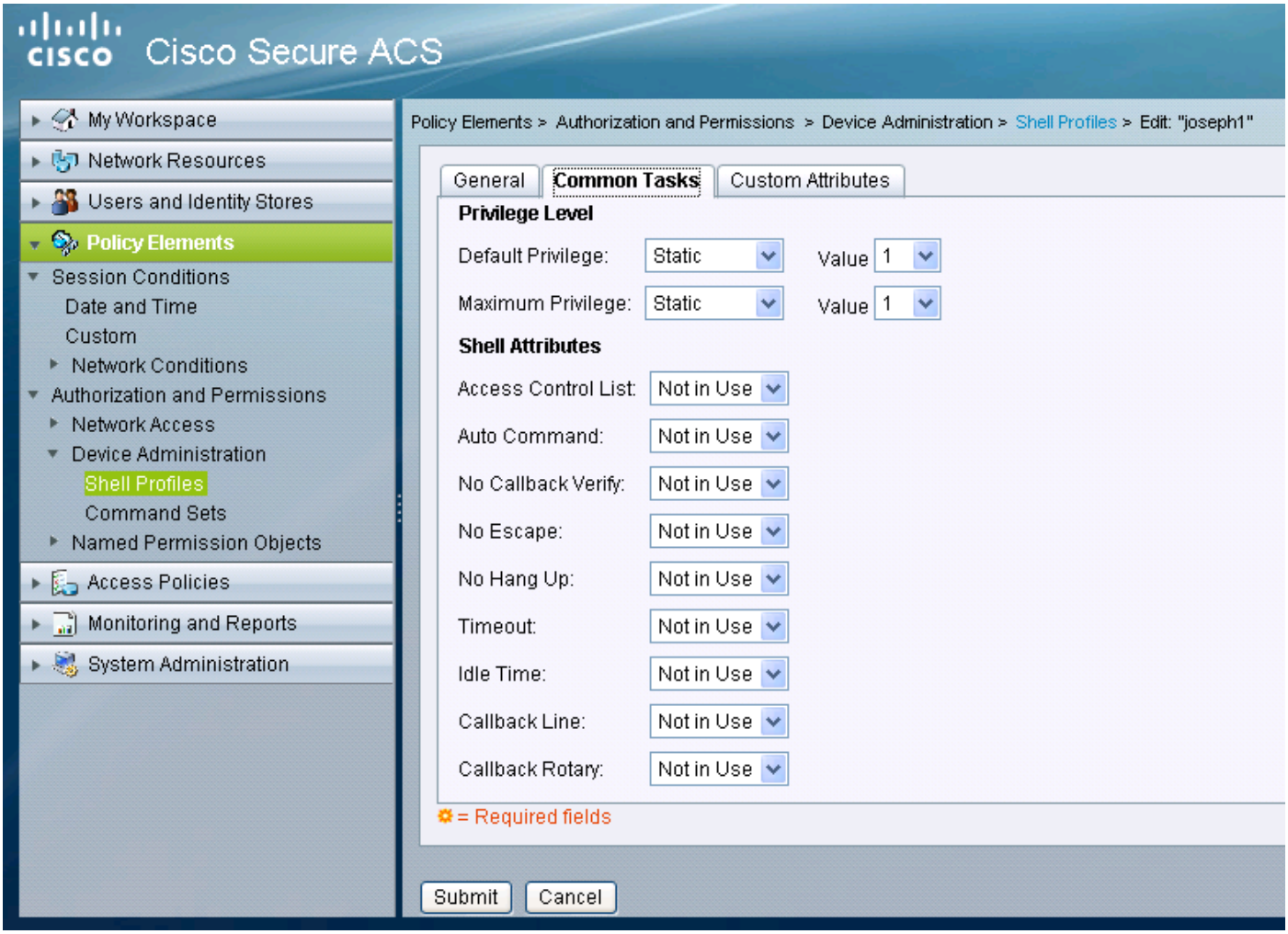
為管理員使用者建立命令集

命令集是所有tacacs裝置使用的命令集。如果指定了特定的配置檔案，則可以使用命令集來限制允許使用者使用的命令。由於在5760上，基於所傳遞的許可權級別對Webui代碼進行限制，因此許可權級別1和15的命令集是相同的。



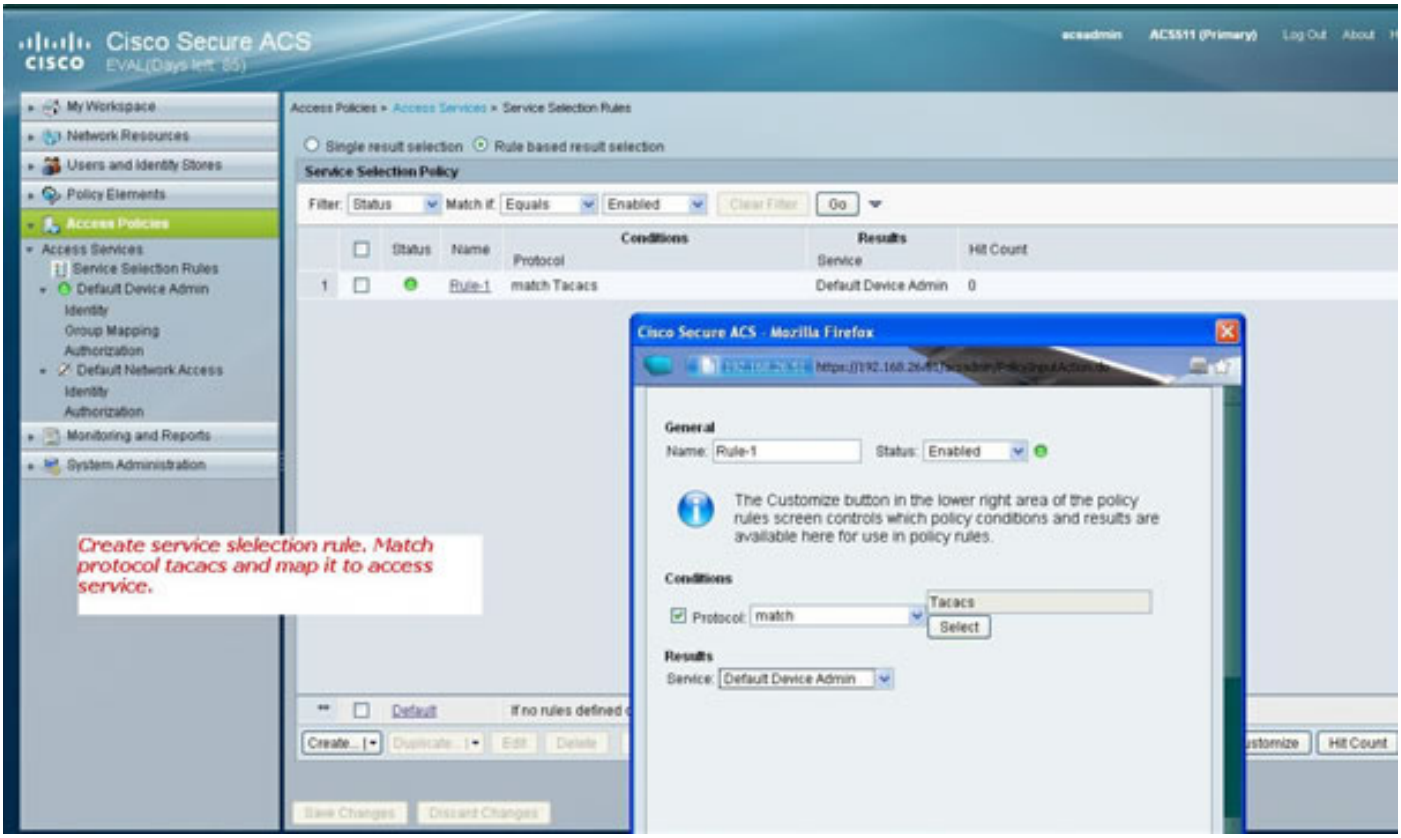
為只讀使用者建立外殼配置檔案

為只讀使用者建立另一個外殼配置檔案。此配置檔案將因許可權級別設定為1而有所不同。



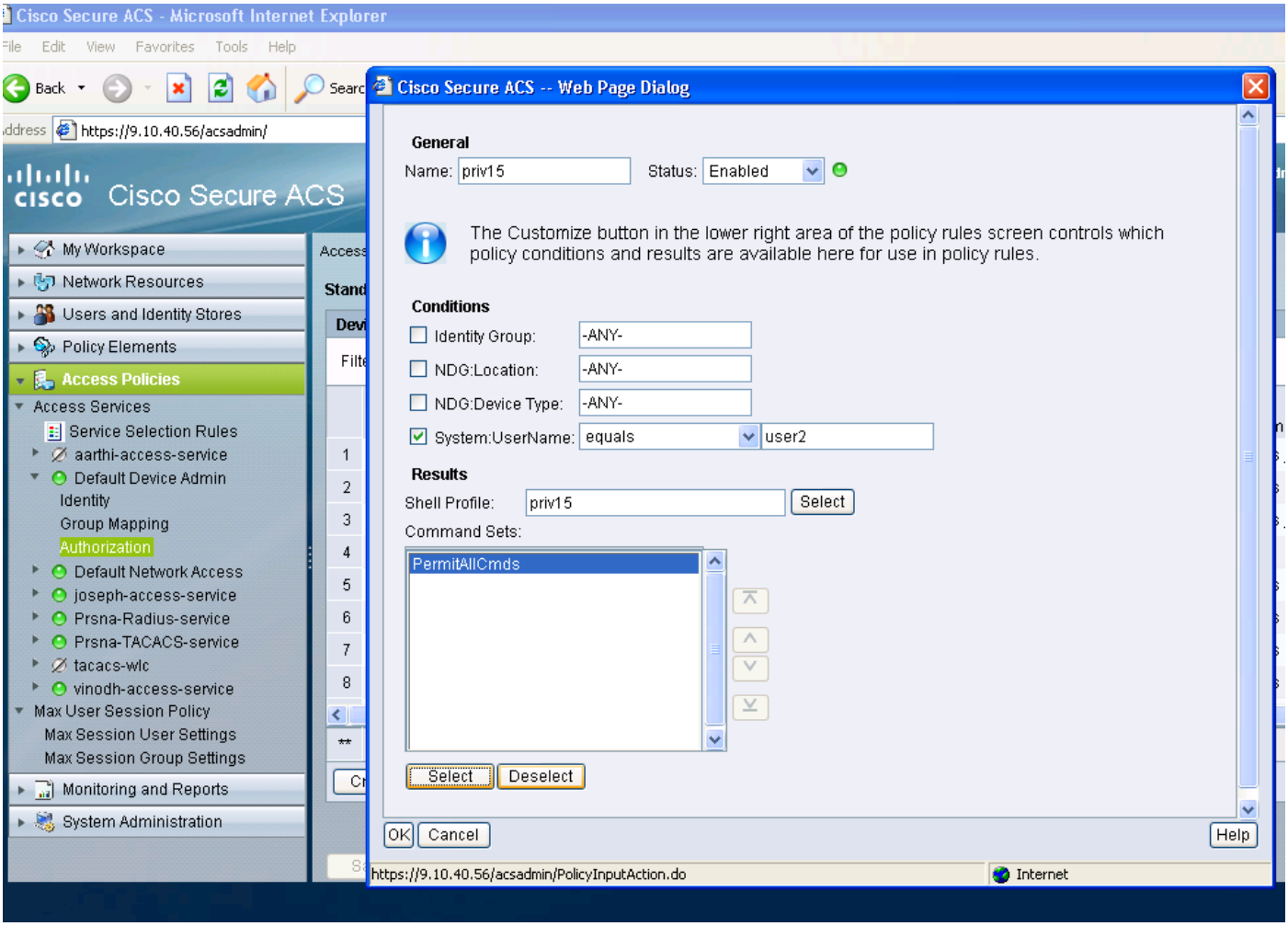
建立與tacacs協定匹配的服務選擇規則

根據您的策略和配置，確保您有與5760提供的tacacs匹配的規則。



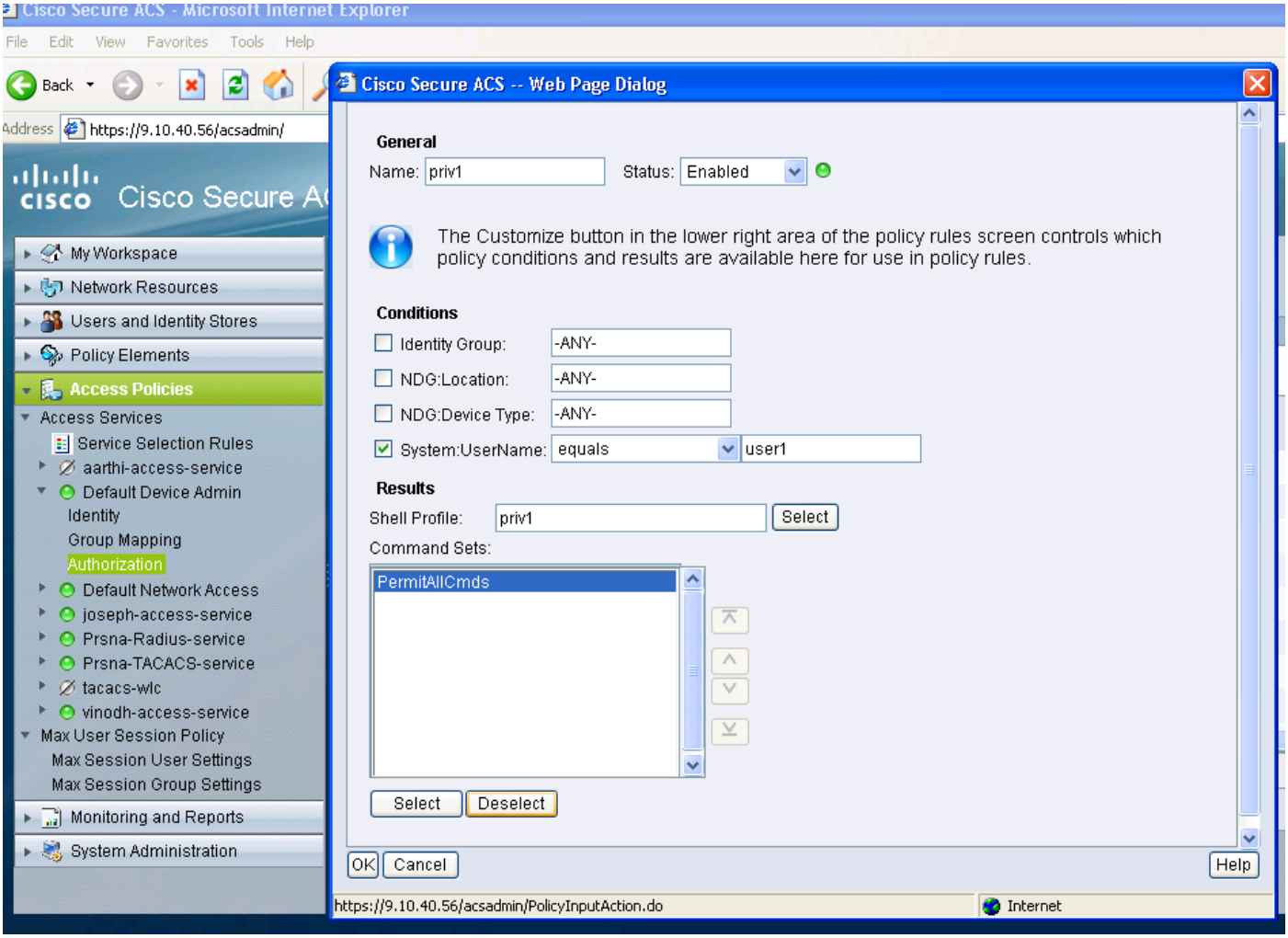
為完全管理訪問建立授權策略。

選擇與tacacs協定選擇一起使用的預設裝置管理策略作為評估策略過程的一部分。使用tacacs協定進行身份驗證時，選定的服務策略稱為預設裝置管理策略。該策略本身包含兩個部分。身份是指根據配置的授權配置檔案，使用者身份以及使用者所屬的組（本地或外部）以及允許使用者執行哪些操作。分配與您正在配置的使用者相關的命令集。



為只讀管理訪問建立授權策略。

只讀使用者也一樣。此示例為使用者1配置許可權級別1外殼配置檔案，為使用者2配置許可權15。



為tacacs配置5760

1. 需要配置Radius/Tacacs伺服器。
tacacs伺服器tac_acct

地址ipv4 9.1.0.100

主要cisco

2. 配置伺服器組
aaa群組伺服器tacacs+ gtac

伺服器名稱tac_acct

在上述步驟之前，沒有任何先決條件。

3. 配置身份驗證和授權方法清單
aaa authentication login <method-list> group <srv-grp>

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

aaa authorization exec default group <srv-grp> ----à解決方法以獲取http上的tacacs。

上述3個命令及所有其他驗證和授權引數應使用相同的資料庫（radius/tacacs或本地）

例如，如果需要啟用命令授權，則還需要指向同一資料庫。

例如：

aaa authorization commands 15 <method-list> group <srv-grp> —>指向資料庫的伺服器組（tacacs/radius或local）應相同。

4. 配置http以使用上述方法清單

ip http authentication aaa login-auth <method-list> —>即使方法清單是「default」，也需要在此處顯式指定方法清單

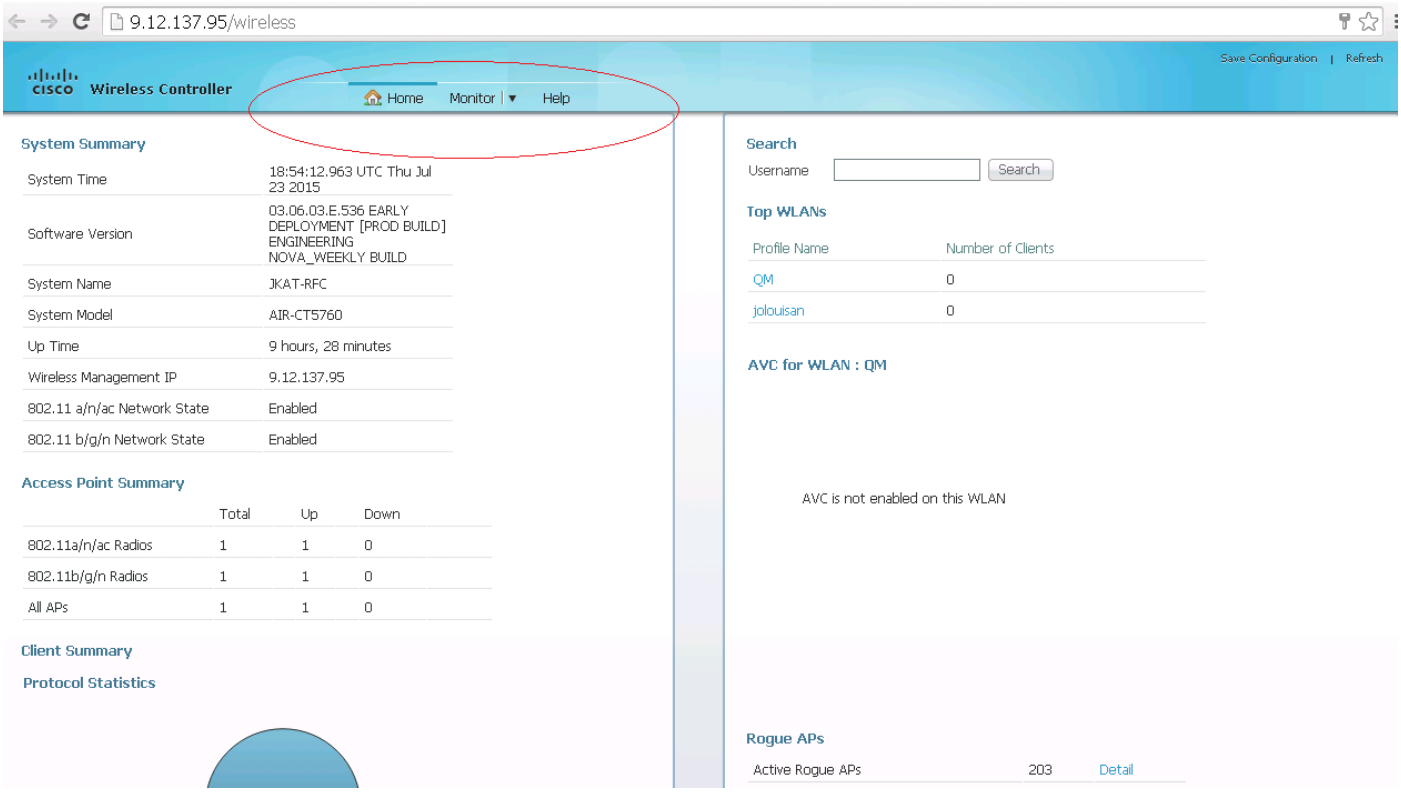
ip http authentication aaa exec-auth <method-list>

**記要點

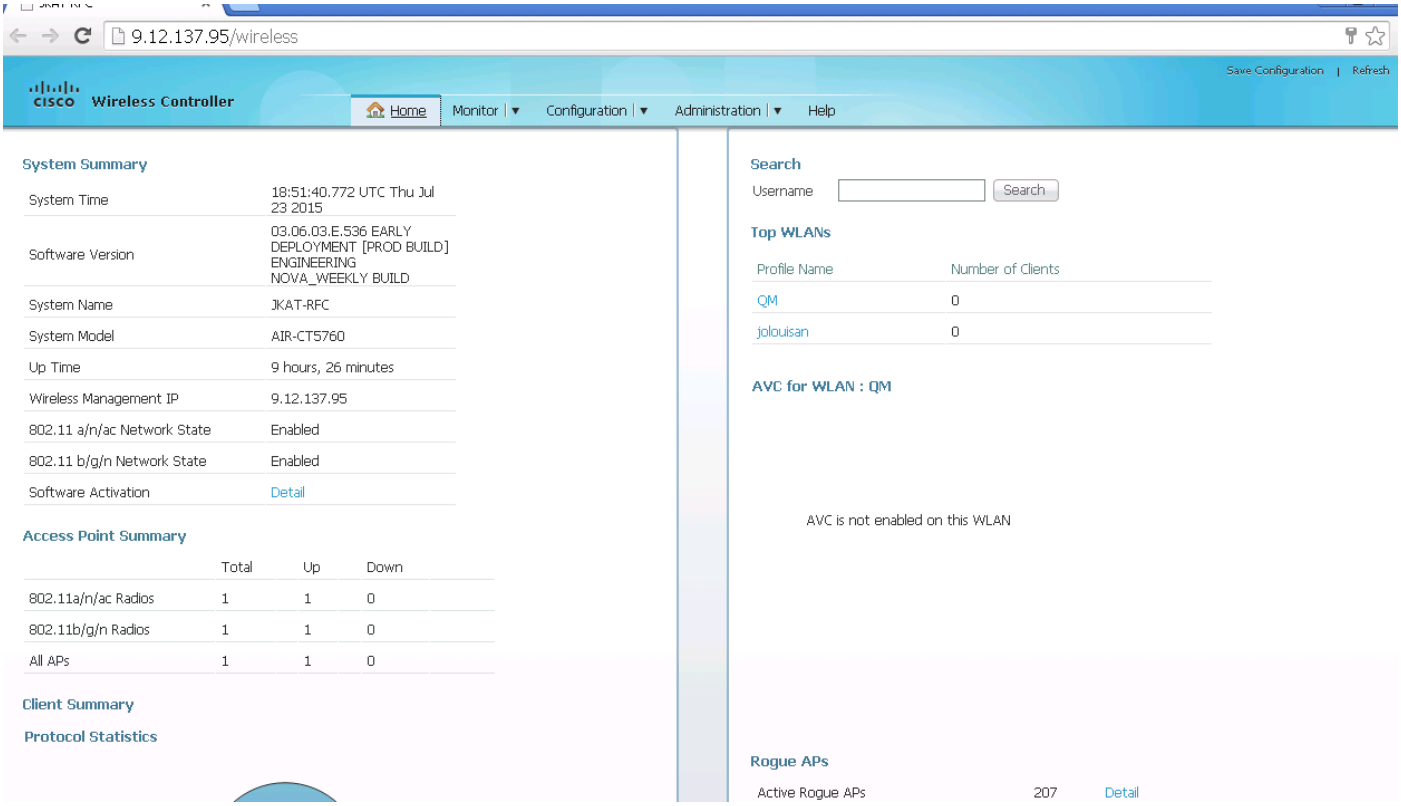
- 請勿在「line vty」配置引數上配置任何方法清單。如果上述步驟和線路vty具有不同的配置，則線路vty配置將優先。
- 所有管理配置型別（如ssh/telnet和webui）中的資料庫應該相同。
- Http身份驗證應顯式定義方法清單。

使用2個不同的配置檔案訪問相同的5760

下面是來自許可權級別1使用者的訪問，其中授予了有限的訪問許可權



下面是來自許可權級別15使用者的訪問許可權，您可在其中獲得完全訪問許可權


9.12.137.95/wireless
Wireless Controller
Save Configuration | Refresh
Home
Monitor
Configuration
Administration
Help
System Summary
System Time 18:51:40.772 UTC Thu Jul 23 2015
Software Version 03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name JKAT-RFC
System Model AIR-CT5760
Up Time 9 hours, 26 minutes
Wireless Management IP 9.12.137.95
802.11 a/n/ac Network State Enabled
802.11 b/g/n Network State Enabled
Software Activation Detail
Access Point Summary
Total Up Down
802.11a/n/ac Radios 1 1 0
802.11b/g/n Radios 1 1 0
All APs 1 1 0
Client Summary
Protocol Statistics
Search
Username
Search
Top WLANs
Profile Name Number of Clients
QM 0
jolouisan 0
AVC for WLAN : QM
AVC is not enabled on this WLAN
Rogue APs
Active Rogue APs 207 Detail