5760 web interface op basis van toegangscontrole-configuratievoorbeeld met Cisco Access Control Server (ACS)

Inhoud

Inleiding

Dit document zal uitleggen hoe u Cisco ACS TACACS+ verificatie- en autorisatieprofielen kunt maken met verschillende voorkeursniveaus en hoe u dit kunt integreren met 5760 voor toegang tot WebUI. Deze optie wordt ondersteund vanaf 3.6.3 (maar niet op 3.7.x ten tijde van het schrijven).

Voorwaarden

Vereisten

Aangenomen wordt dat de lezer bekend is met de configuratie van Cisco ACS en geconvergeerde toegangscontroller. Dit document richt zich uitsluitend op de interactie tussen deze twee componenten in het kader van de goedkeuring van tacacs+.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

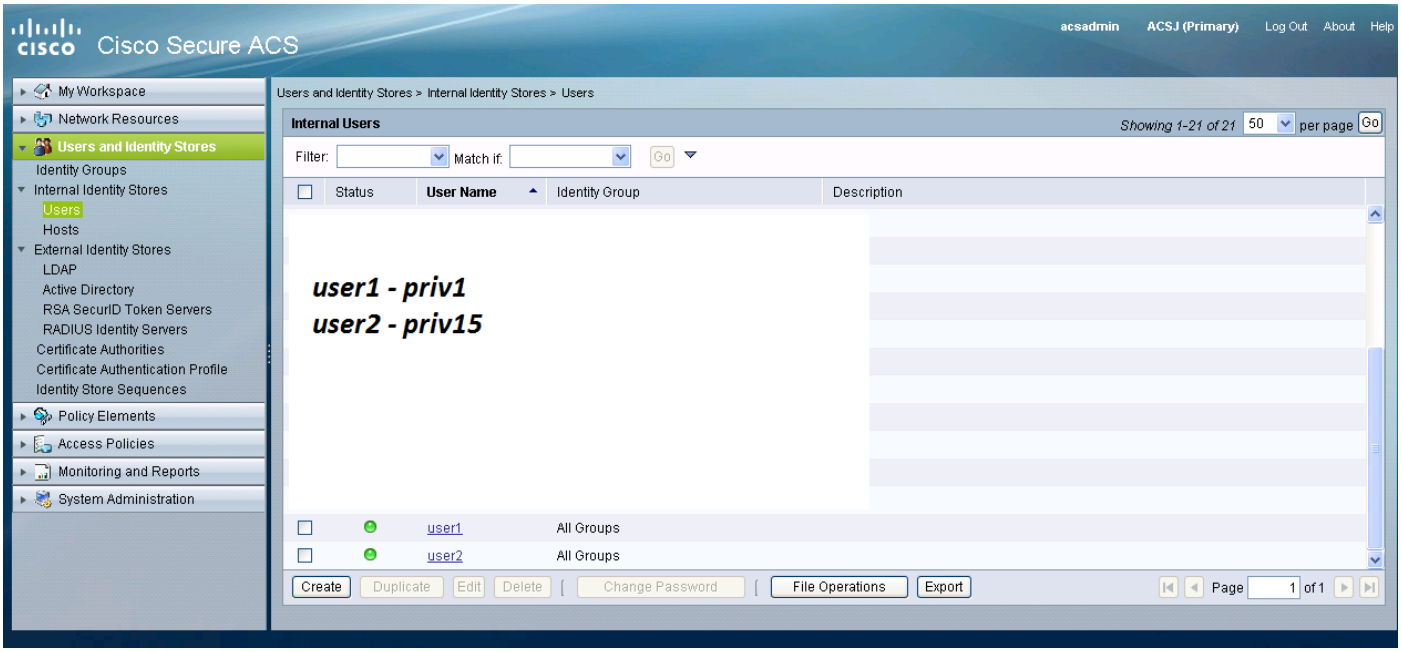
- Cisco geconvergeerde access point 5760, release 3.6.3
- Cisco Access Control Server (ACS) 5.2

Configuratie

Maak een paar testgebruikers in ACS

Klik op "Gebruikers en identiteitsopslag" en selecteer vervolgens "Gebruikers".

Klik op "Maken" en stel een paar testgebruikers in zoals hieronder wordt weergegeven.



Beleidselementen en shell-profielen instellen

U moet twee profielen maken voor de 2 verschillende soorten toegang. Voorrecht 15 in de wereld van de tacs van Cisco betekent volledige toegang tot het apparaat zonder enige beperking. Voorbeeld 1 daarentegen biedt u de mogelijkheid om alleen een beperkte hoeveelheid opdrachten in te loggen en uit te voeren. Hieronder vindt u een korte beschrijving van de toegangsniveaus van cisco.

bevoorrecht niveau 1 = niet bevoorrecht (de vraag is router>), het standaard niveau voor het registreren in

bevoorrecht niveau 15 = bevoorrecht (de vraag is router#), het niveau na het gaan in toelaten modus

bevoorrecht niveau 0 = zelden gebruikt, maar omvat 5 opdrachten: **Uitschakelen**, **inschakelen**, **afsluiten**, **helpen** en **uitloggen**

Op 5760 worden de niveaus 2-14 geacht hetzelfde te zijn als niveau 1. Zij krijgen hetzelfde voorrecht als 1. **Configureer de tacs privilege-niveaus voor bepaalde opdrachten op de 5760 niet**. UI-toegang per tabbladen wordt niet ondersteund in 5760. U kunt volledige toegang (priv15) hebben of alleen toegang tot het tabblad Monitor (priv1). Gebruikers met voorkeursniveau 0 mogen ook niet inloggen.

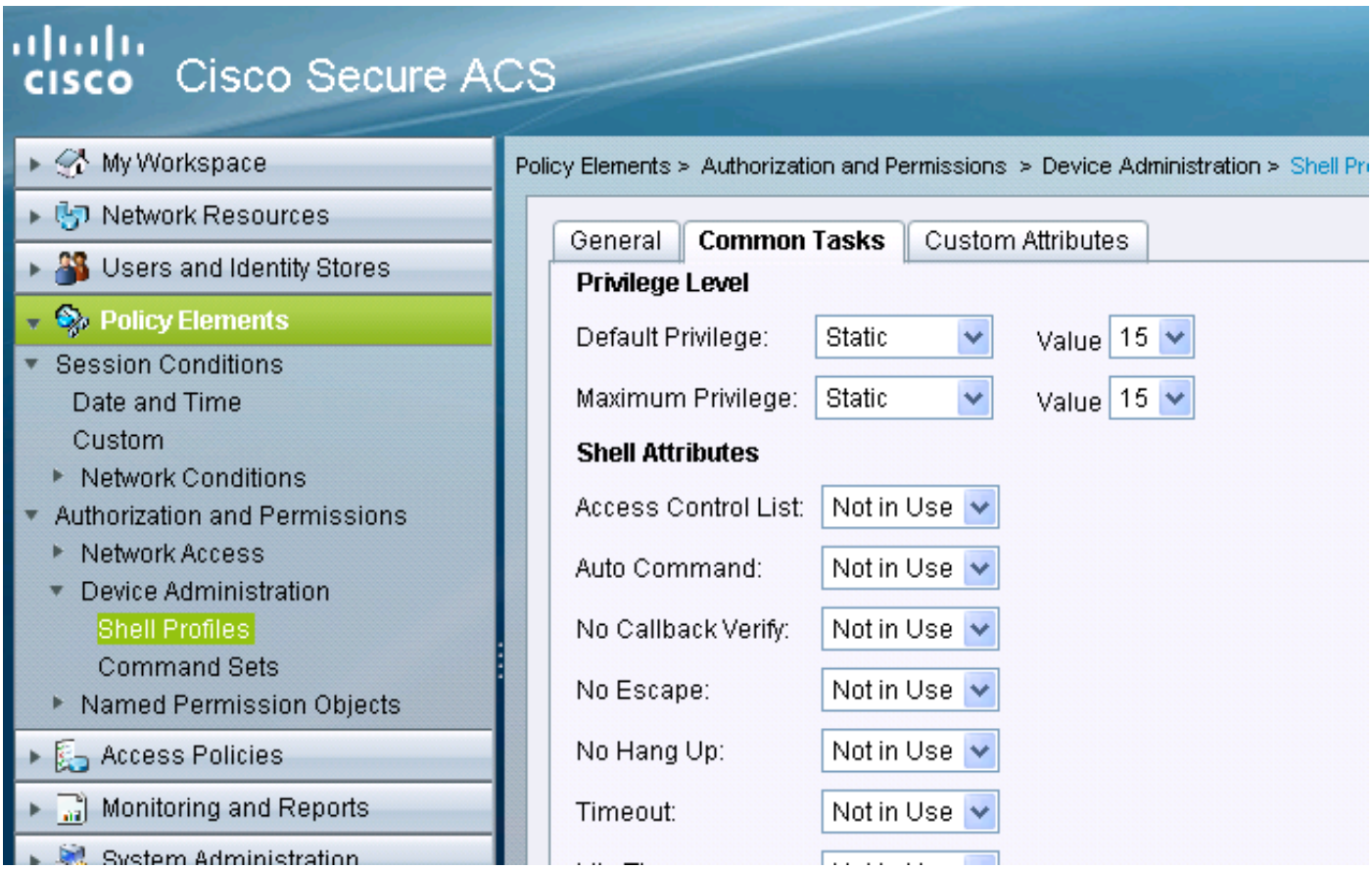
Toegangsprofiel met 15 niveaus voor schelpen maken

Maak dat profiel met het onderstaande afdrukscherm:

Klik op "Beleidselementen". Klik op "Shell profielen".

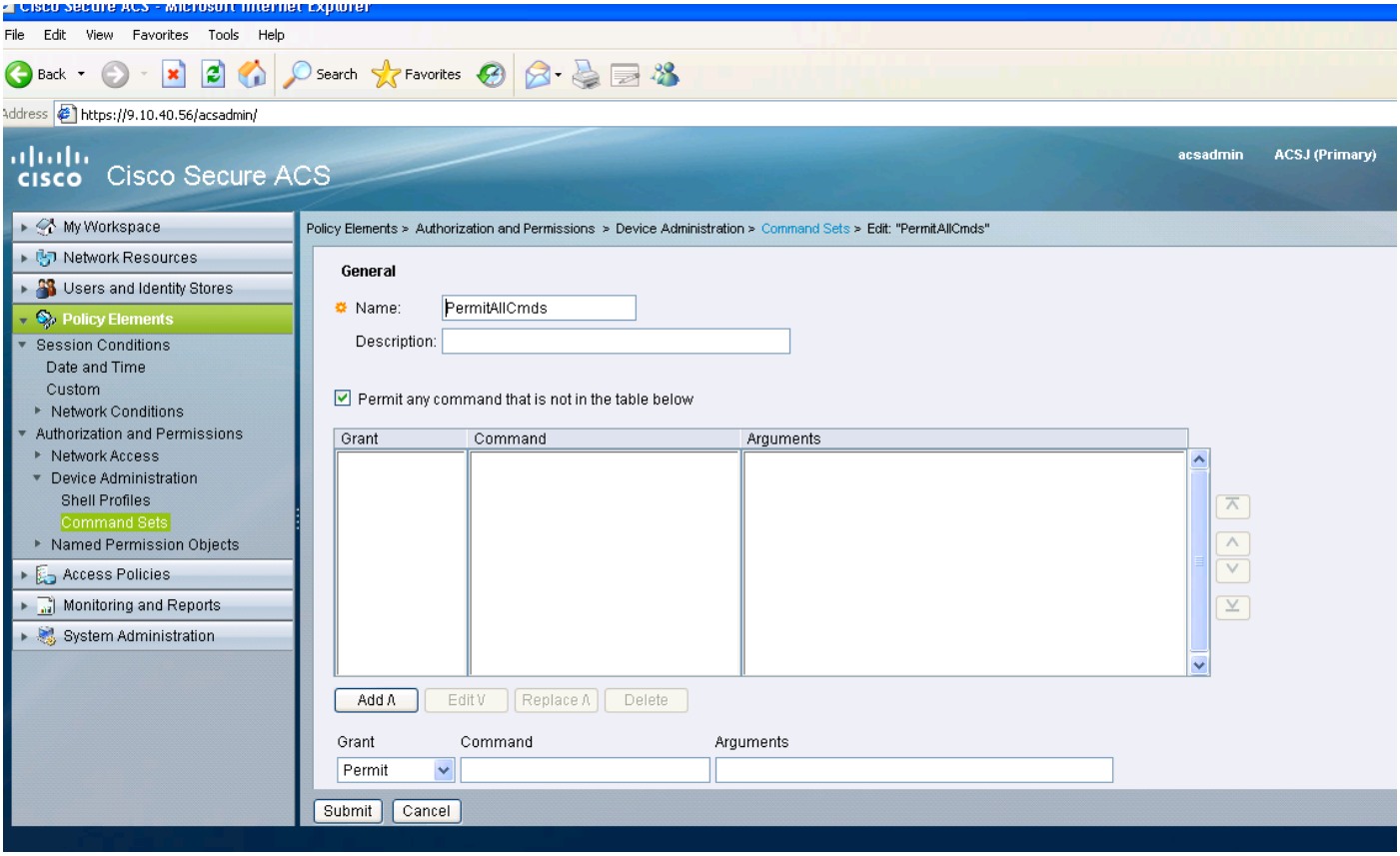
Maak een nieuwe.

Ga in het tabblad "Gemeenschappelijke taken" en stel de standaard- en de maximale voorrechten in op 15.



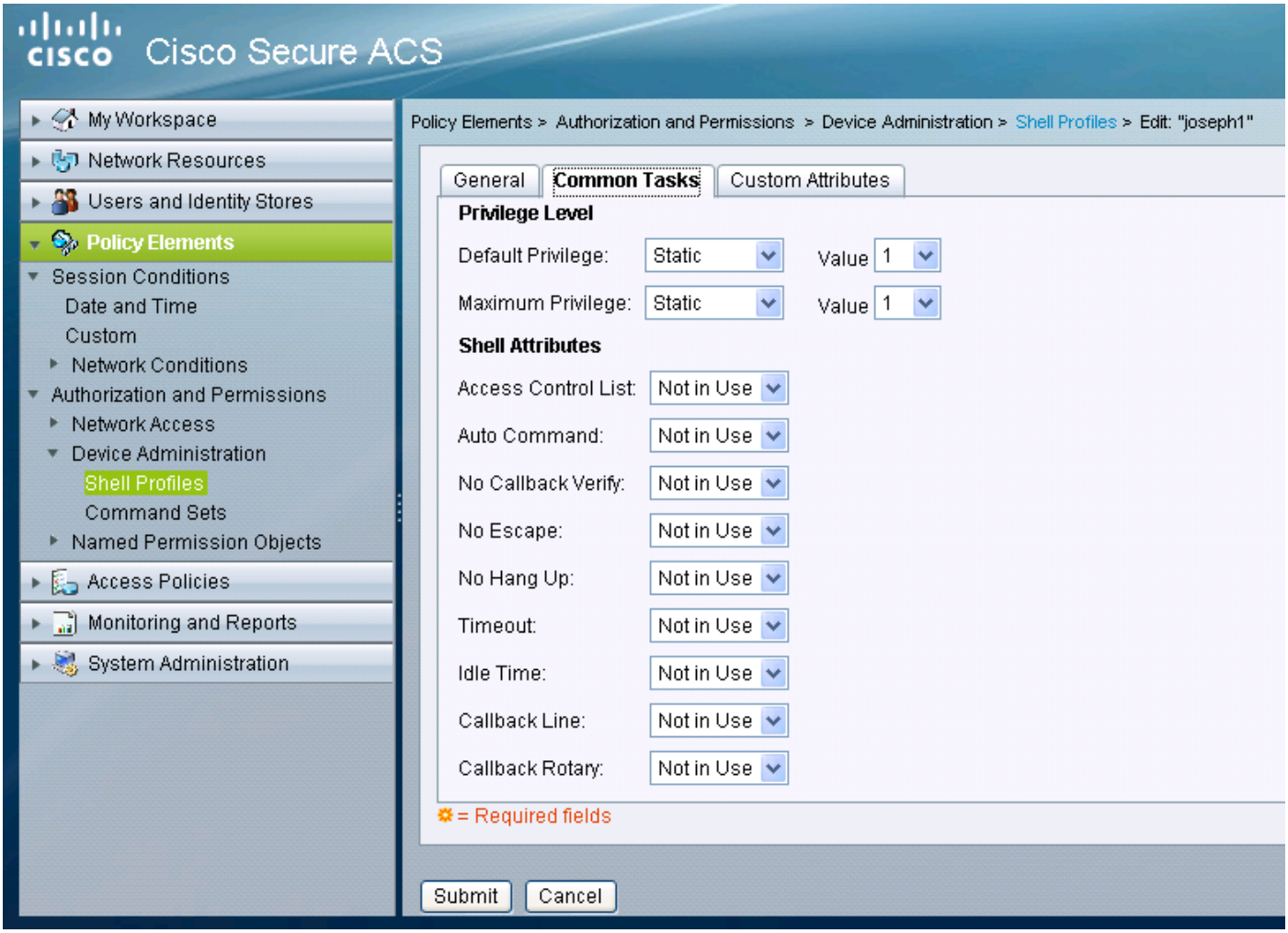
Opdrachtsets maken voor beheerder-gebruiker

Opdrachtsets zijn reeksen opdrachten die door alle tacacs-apparaten worden gebruikt.Ze kunnen worden gebruikt om de opdrachten te beperken die een gebruiker mag gebruiken indien dat specifieke profiel is toegewezen. Aangezien op de 5760-regel beperkingen worden opgelegd aan de Webui-code op basis van het goedgekeurde privilege-niveau, zijn de commando's voor zowel privilege-niveau1 als 15 hetzelfde.



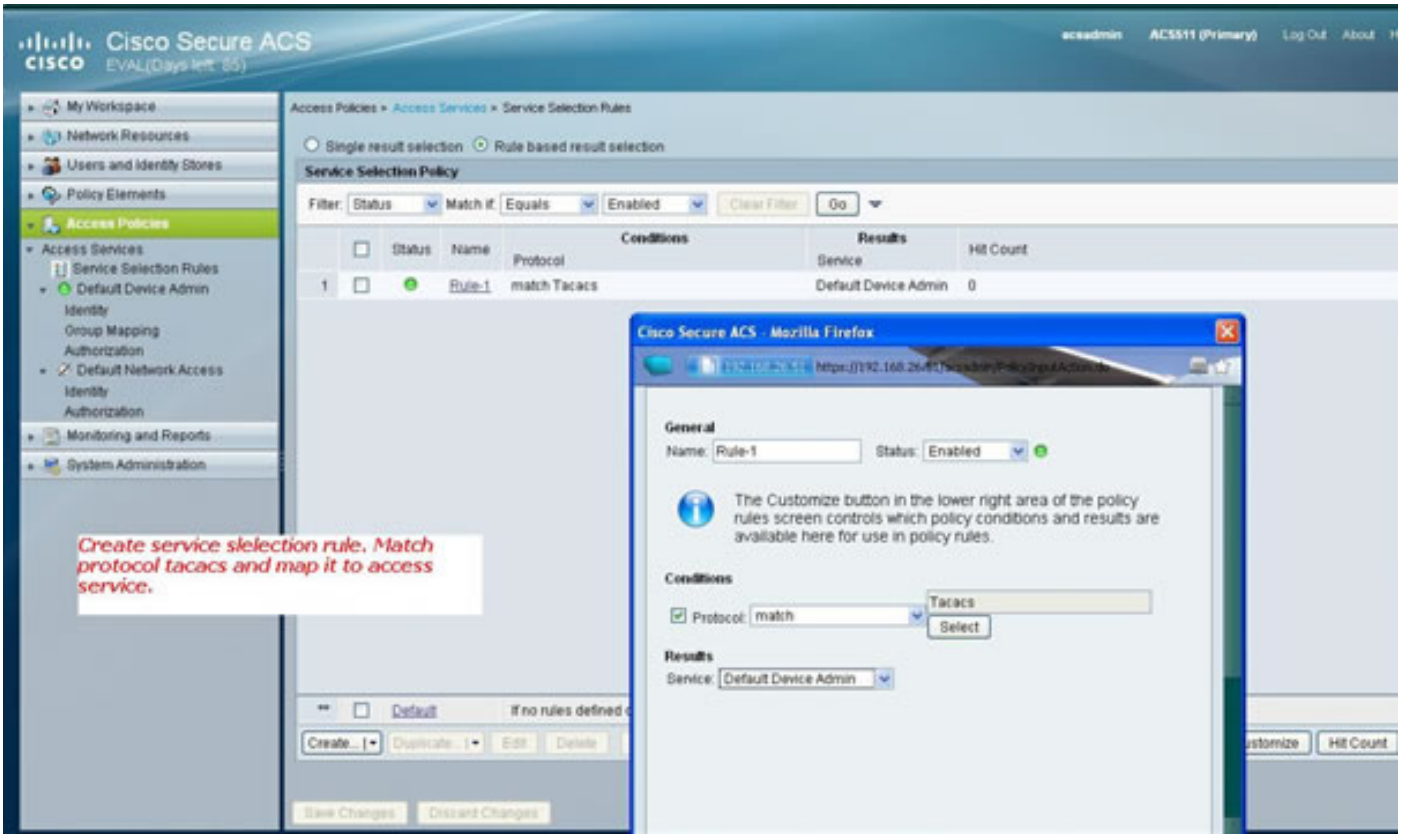
shell-profiel maken voor alleen lezen gebruiker

Een ander shell-profiel maken voor alleen-lezen gebruikers Dit profiel zal verschillen door het feit dat de voorrechten zijn ingesteld op 1.



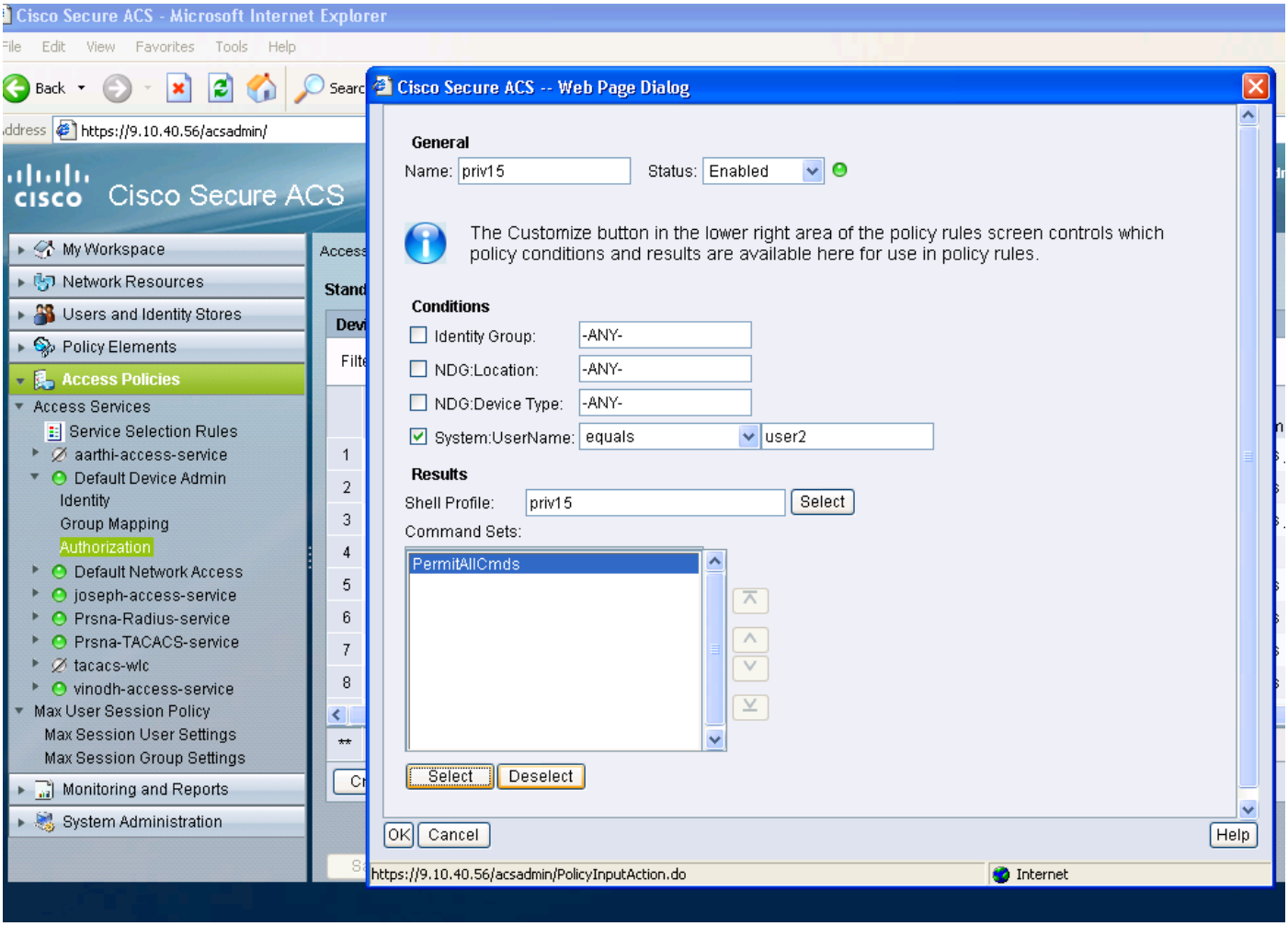
Maak een selectieregel voor de service die overeenkomt met het tacacs-protocol

Afhankelijk van uw beleid en configuratie, zorg ervoor dat u een regel hebt die aansluit bij de tac's die uit de 5760 komen.



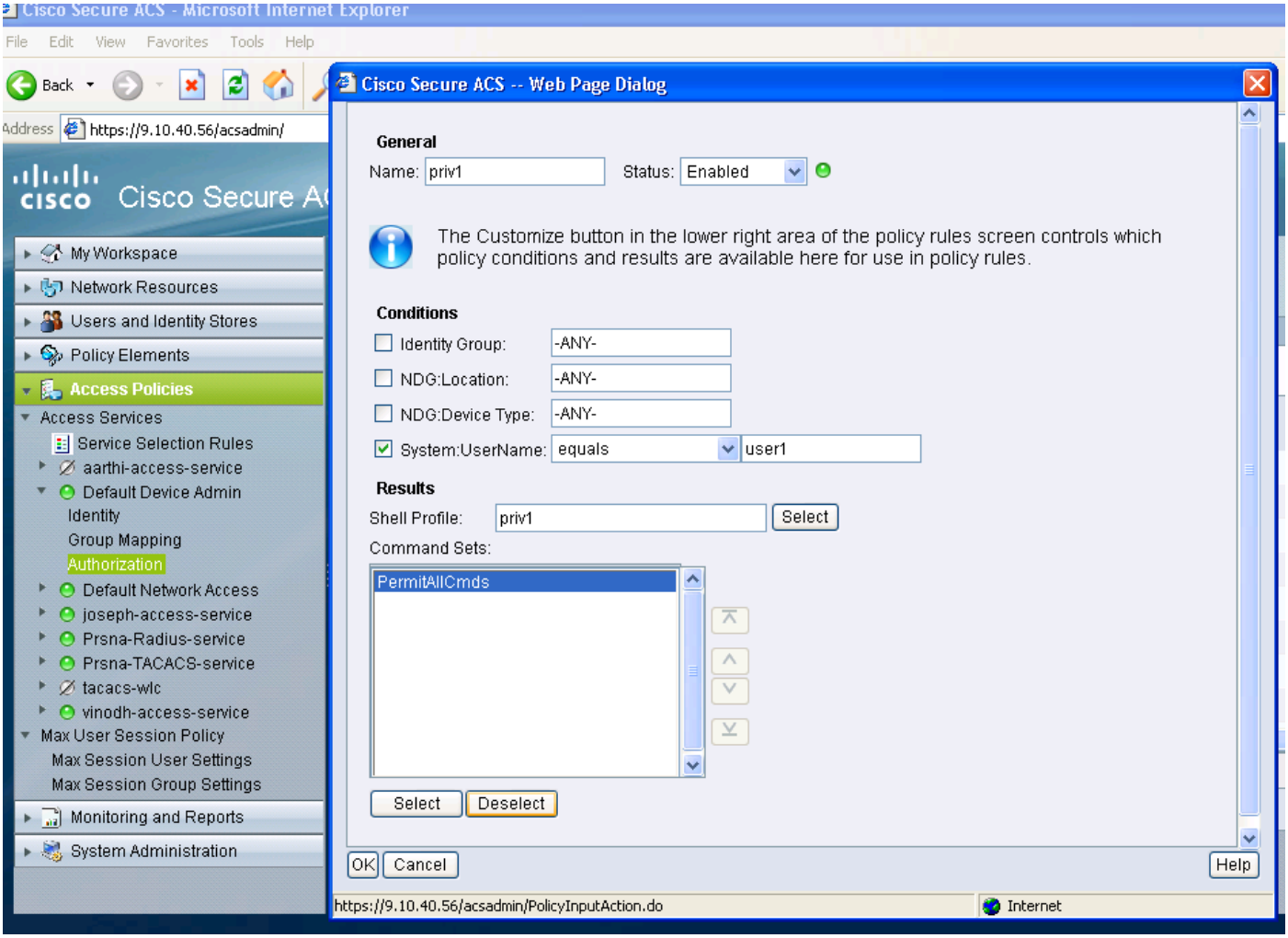
Opzetten van een vergunningenbeleid voor volledige administratieve toegang.

Het standaard beleid voor apparaatbeheer dat wordt gebruikt voor de selectie van tacs-protocollen wordt geselecteerd als onderdeel van het evaluatiebeleidsproces. Wanneer u het tacacs-protocol gebruikt om echt te maken, wordt het geselecteerde servicebeleid het beleid Default Devices Admin genoemd. Dit beleid omvat op zichzelf 2 delen. Identificatie betekent wie de gebruiker is en tot welke groep hij behoort (lokaal of extern) en wat hij mag doen volgens het ingestelde autorisatieprofiel. Pas de opdrachtset aan met betrekking tot de gebruiker die u configureren.



Creëer een autorisatiebeleid voor alleen leesbare administratieve toegang.

Dit geldt ook voor alleen-lezen gebruikers. Deze voorbeelden vormen het privilege niveau 1 shell-profiel voor gebruiker 1 en het privilege 15 aan gebruiker 2.



De 5760 configureren voor tacs

1. Radius/tacacs-server moet worden geconfigureerd.

tacacs server tac_acct

adres ipv4 9.1.0.100

cisco

2. De servergroep configureren

AAA groepsserver tacacs+ gtac

servernaam tac_acct

Er is geen enkele voorwaarde voor de bovengenoemde stap.

3. Verificatie- en autoriteitslijsten configureren

aanmelding bij verificatie <methode-list> groep <srv-grp>

Aandacht voor de toekenning van een vergunning voor de groep srv-grp>

een autorisatie exec default group <srv-grp> —à workround om tacacs op http. te krijgen.

Bovenstaande 3 opdrachten en alle andere authenticatie- en autorisatieparameters dienen

dezelfde database te gebruiken, ofwel de straal-/tacacs of lokale

Bijvoorbeeld, als commandoautorisatie moet worden ingeschakeld, moet het ook naar dezelfde database wijzen.

Voor EX:

aaa autorisatie-opdrachten 15 <methode-list> groep <srv-grp> —> de servergroep die naar de database wijst (tacacs/straal of lokaal) moet hetzelfde zijn.

4. vorm http om de bovenstaande methodelijsten te gebruiken

ip http: / inlognaam-auth <methode-list> —> de methodelijst moet hier expliciet worden gespecificeerd, zelfs als de methodelijst "default" is

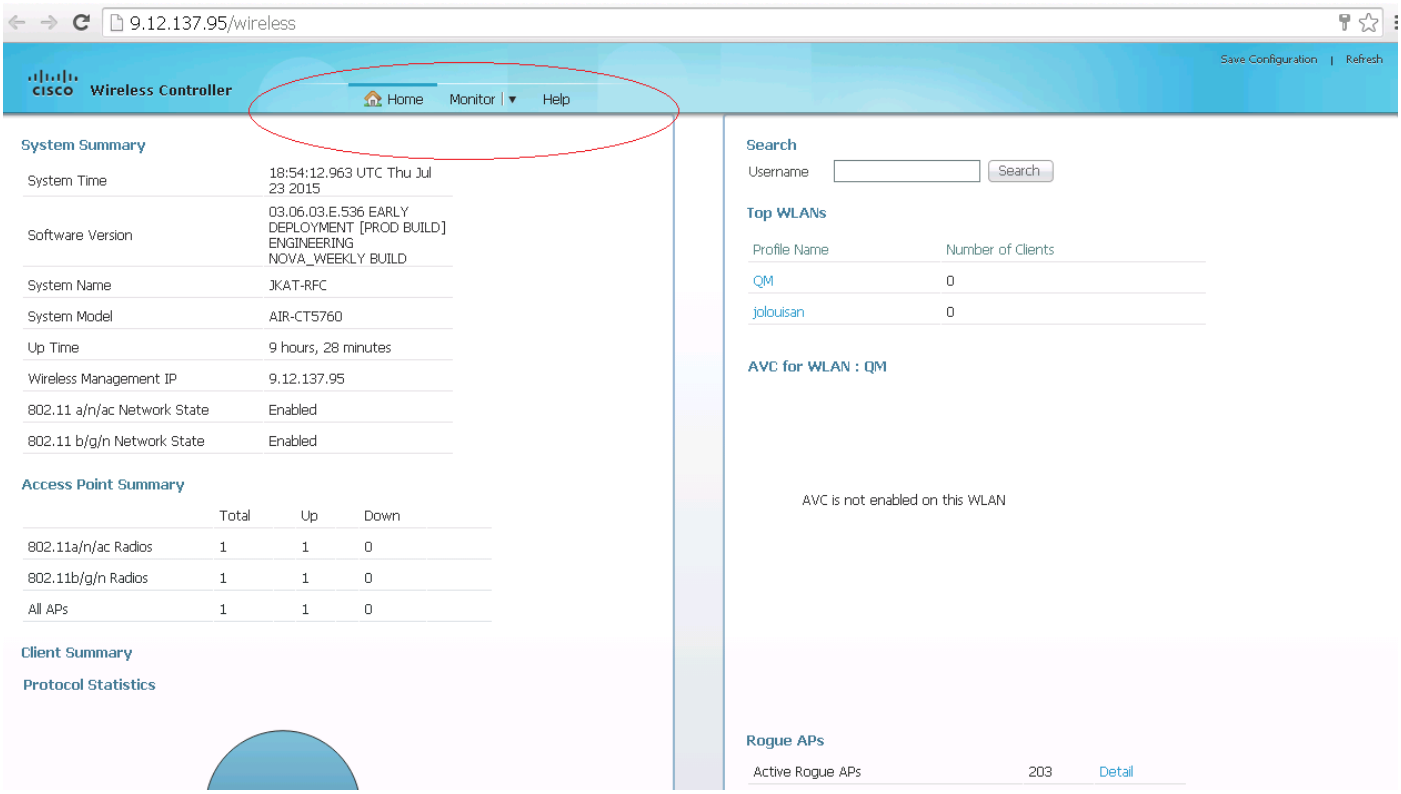
ip http: / exec-auth <methode-list>

** Opmerkingen

- Configureer geen methodelijsten op de "line vty" configuratieparameters. Als de bovenstaande stappen en de lijn vty verschillende configuraties hebben, dan zullen de line vty configuratie voorrang krijgen.
- De database moet gelijk zijn voor alle beheerconfiguratietypen zoals ssh/telnet en webui.
- Voor de HTTP-verificatie moet de methodelijst expliciet worden gedefinieerd.

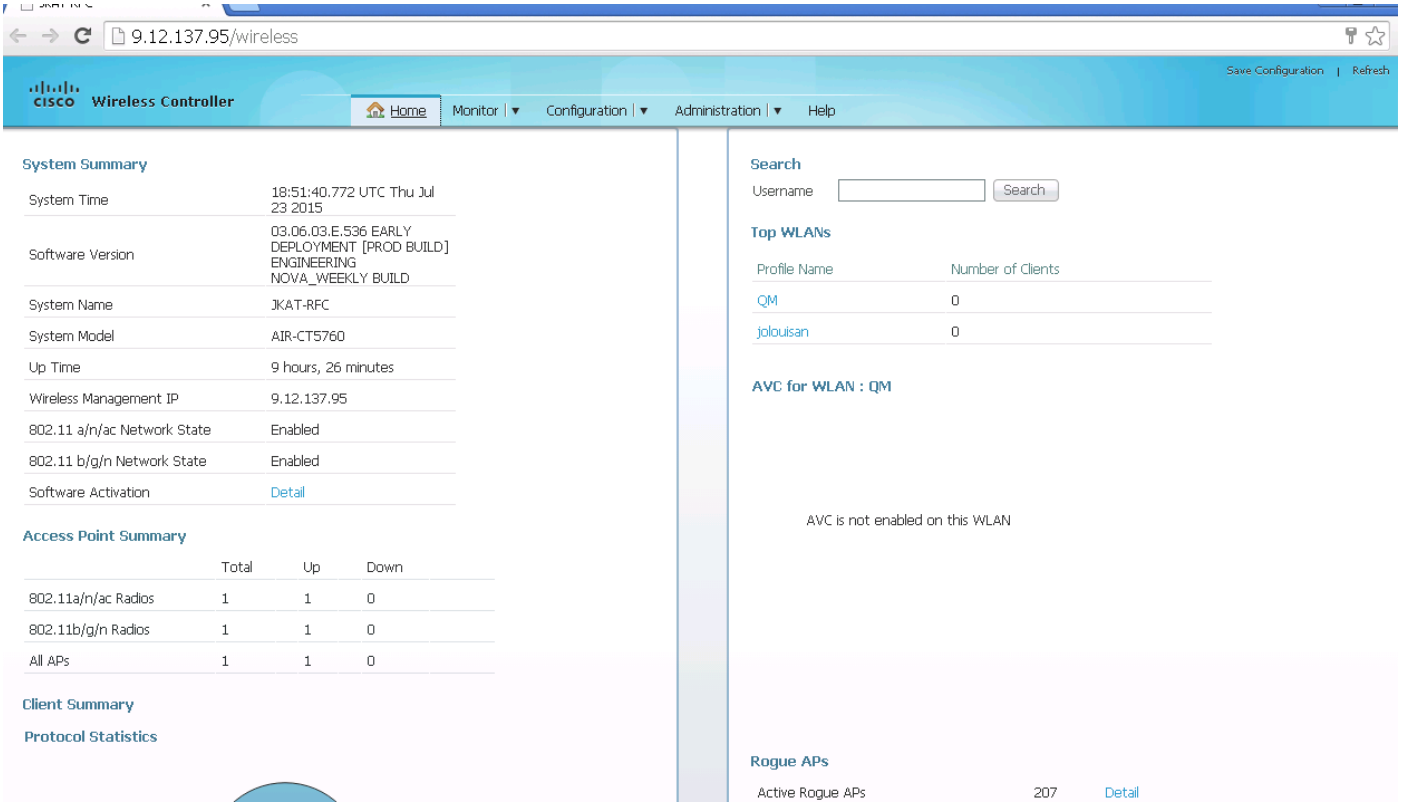
Dezelfde 5760 gebruiken met de 2 verschillende profielen

Hieronder volgt een toegang van een gebruiker van voorkeursniveau 1 waar beperkte toegang wordt verleend



Hieronder volgt een toegang van een bevoorrecht niveau 15-gebruiker waar u volledige toegang

hebt


9.12.137.95/wireless
Save Configuration | Refresh
Wireless Controller
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