5760 웹 인터페이스 권한 레벨 기반 액세스 제어 컨피그레이션 예(Cisco ACS)

목차

소개

이 문서에서는 권한 수준이 다른 Cisco ACS Tacacs+ 인증 및 권한 부여 프로파일을 생성하고 WebUI에 액세스하기 위해 5760과 통합하는 방법에 대해 설명합니다.이 기능은 3.6.3부터 지원됩니다(이 문서 작성 시 3.7.x에서는 지원되지 않음).

사전 요구 사항

요구 사항

판독기는 Cisco ACS 및 Converged Access 컨트롤러 컨피그레이션에 익숙하다고 가정합니다.이 문서에서는 tacacs+ 권한 부여 범위에서 두 구성 요소 간의 상호 작용에 대해서만 중점적으로 설명합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

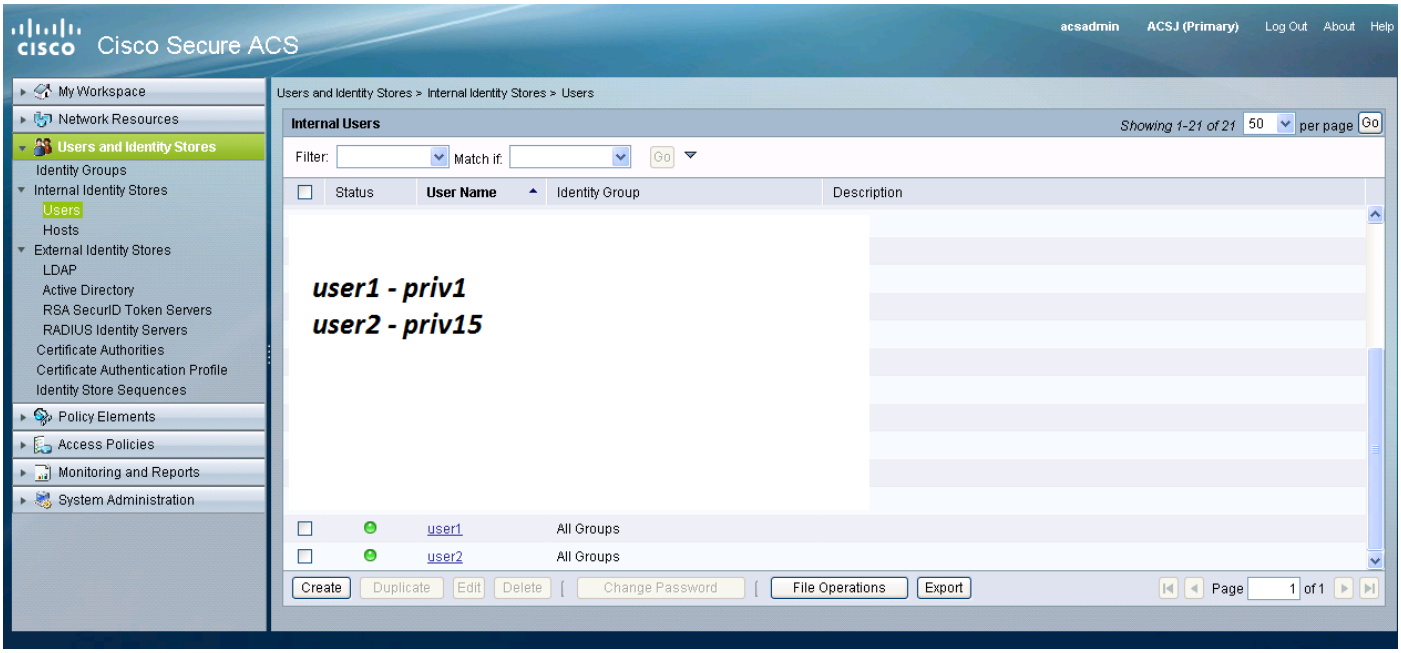
- Cisco Converged Access 5760, 릴리스 3.6.3
- Cisco ACS(Access Control Server) 5.2

구성

ACS에서 몇 명의 테스트 사용자 생성

"Users and Identity Stores(사용자 및 ID 저장소)"를 클릭한 다음 "Users(사용자)"를 선택합니다.

"Create(생성)"를 클릭하고 아래 그림과 같은 몇 가지 테스트 사용자를 구성합니다.



정책 요소 및 셸 프로파일 설정

2가지 액세스 유형에 대해 2개의 프로파일을 생성해야 합니다.cisco tacacs world에서 권한 15는 제한 없이 디바이스에 대한 전체 액세스를 제공하는 것을 의미합니다.반면 권한 1에서는 제한된 양의 명령만 로그인 및 실행할 수 있습니다.아래는 cisco에서 제공하는 액세스 레벨에 대한 간단한 설명입니다.

권한 레벨 1 = 비권한(프롬프트: 라우터>), 로그인하기 위한 기본 레벨

권한 수준 15 = 권한(프롬프트는 라우터 번호), 활성화 모드로 전환한 후 레벨

privilege level 0 = 거의 사용되지 않지만 다음 5개의 명령을 포함합니다.**비활성화**, **활성화**, **종료**, **도움말** 및 **로그아웃**

5760에서 레벨 2-14는 레벨 1과 동일하게 간주됩니다. 레벨 1과 동일한 권한이 부여됩니다. **5760에서 특정 명령에 대해 tacacs 권한 레벨을 구성하지 마십시오**.탭당 UI 액세스는 5760에서 지원되지 않습니다.전체 액세스 권한(priv15) 또는 모니터 탭(priv1)에만 액세스할 수 있습니다. 또한 권한 수준이 0인 사용자는 로그인할 수 없습니다.

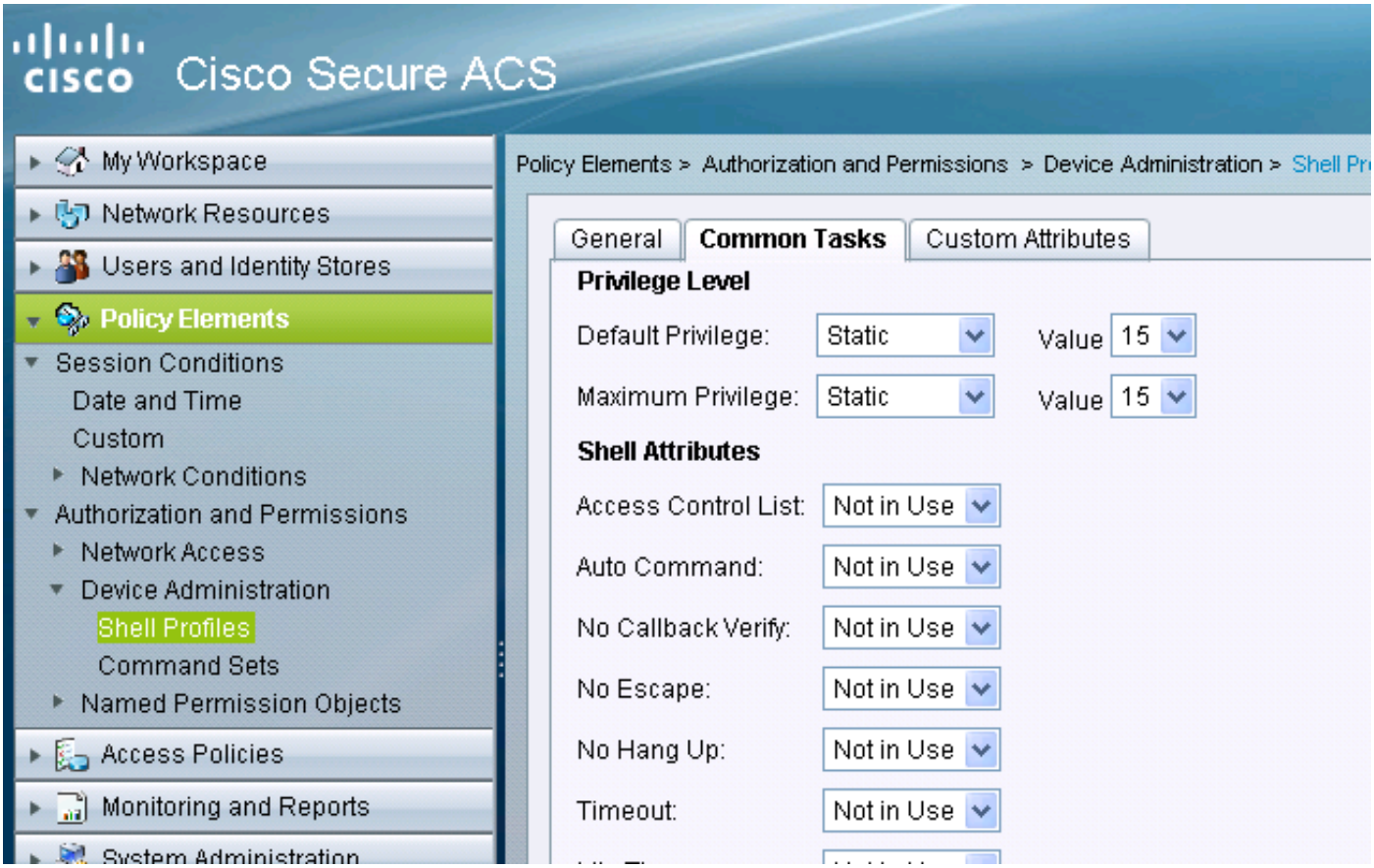
권한 15 레벨 셸 액세스 프로필 생성

아래 인쇄 화면을 사용하여 해당 프로파일을 생성합니다.

"Policy Elements(정책 요소)"를 클릭합니다. "셸 프로파일"을 클릭합니다.

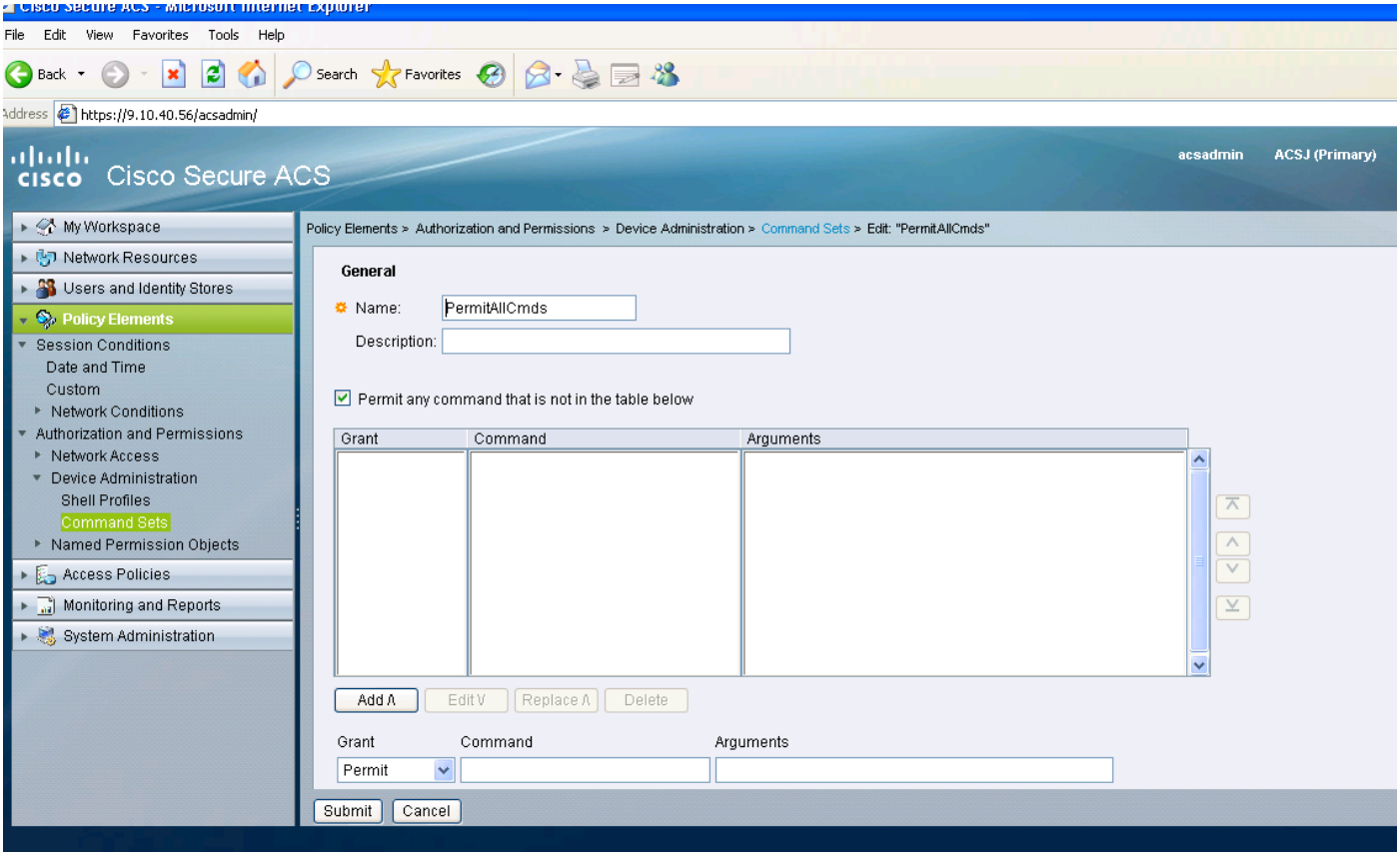
새 항목을 만듭니다.

"Common Tasks(공통 작업)" 탭으로 이동하여 기본 및 최대 권한 레벨을 15로 설정합니다.



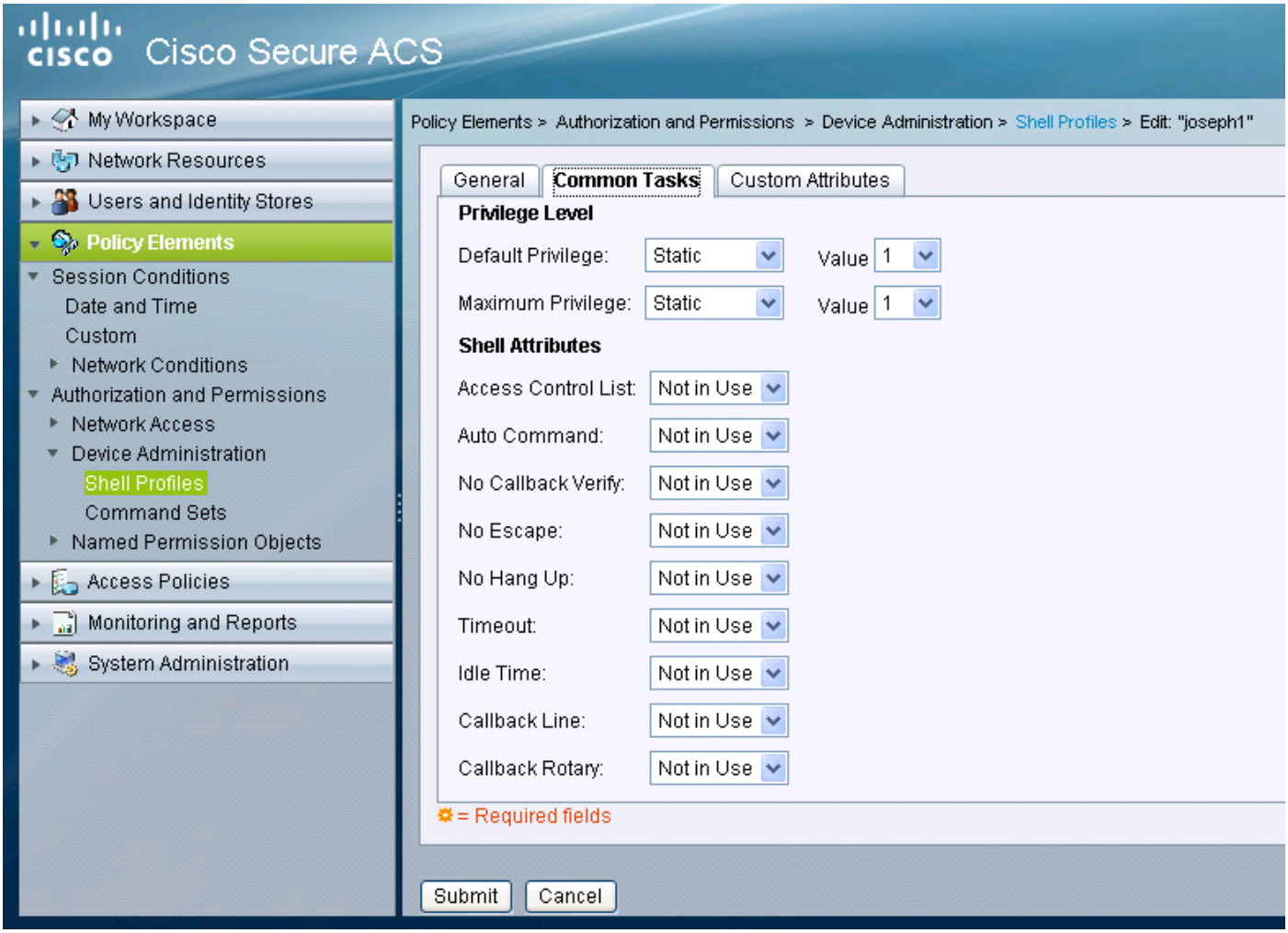
관리자 사용자에 대한 명령 집합 생성

명령 집합은 모든 tacacs 디바이스에서 사용하는 명령 집합입니다. 이러한 명령 집합을 사용하여 특정 프로파일을 할당한 경우 사용자가 사용할 수 있는 명령을 제한할 수 있습니다.5760에서는 전달된 권한 수준에 따라 Webui 코드에 대한 제한이 수행되므로 권한 레벨 1과 15에 대한 명령 집합이 동일합니다.



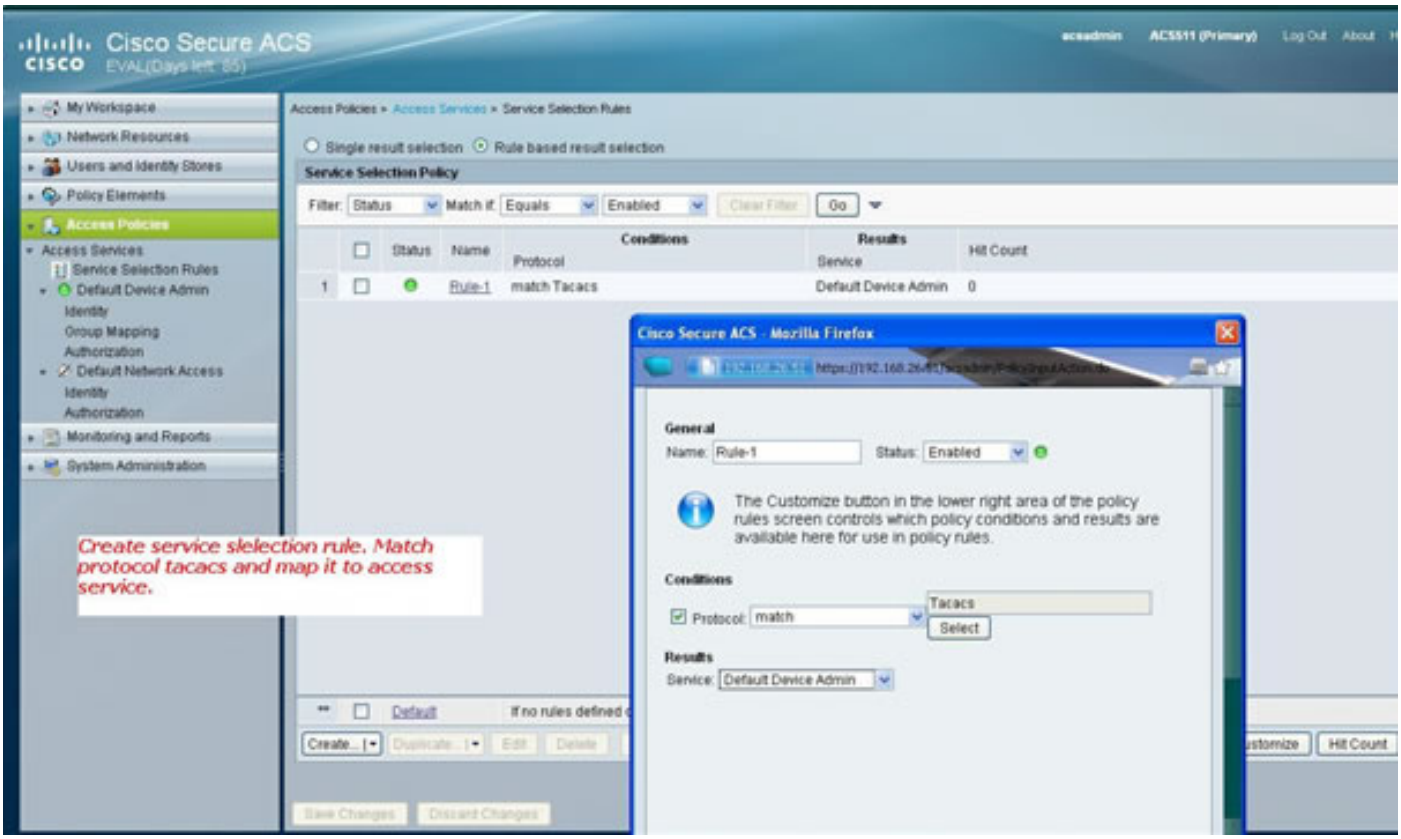
읽기 전용 사용자에 대한 셸 프로필을 만드는 중

읽기 전용 사용자를 위해 다른 셸 프로필을 만듭니다.이 프로파일은 권한 레벨이 1로 설정된다는 사실에 따라 달라집니다.



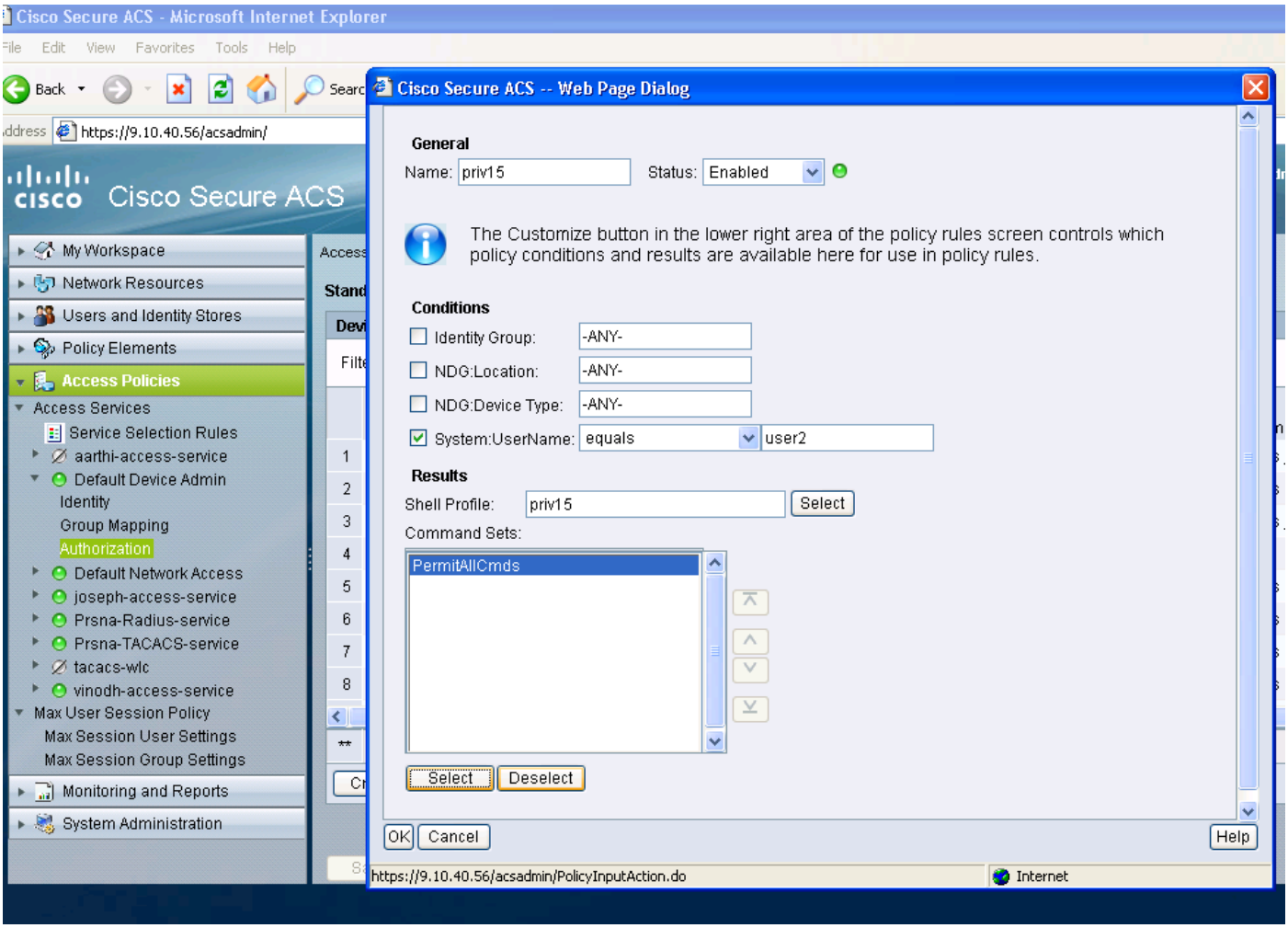
tacacs 프로토콜과 일치하는 서비스 선택 규칙 생성

정책 및 컨피그레이션에 따라 5760에서 오는 tacacs와 일치하는 규칙이 있는지 확인합니다.



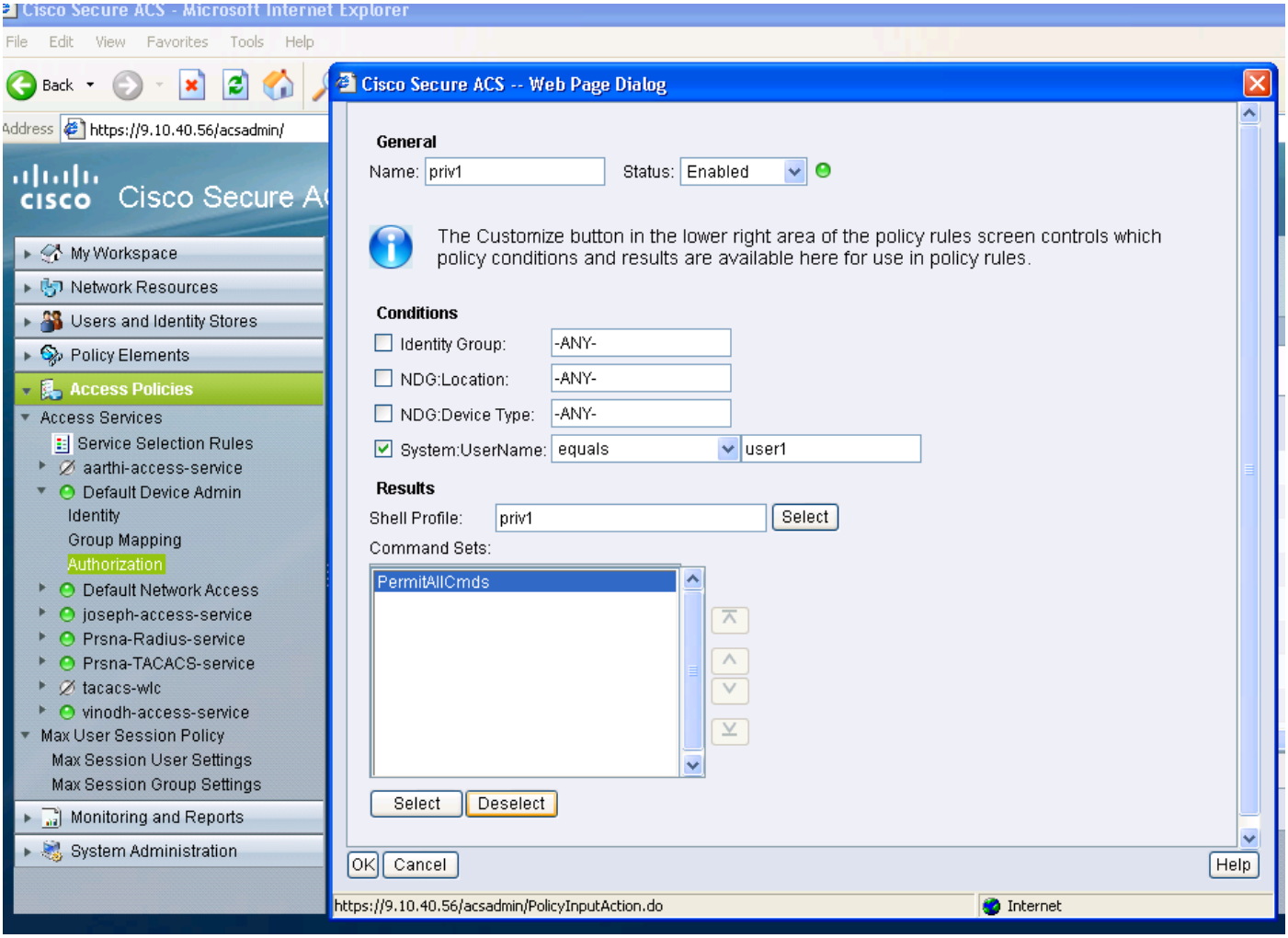
전체 관리 액세스를 위한 권한 부여 정책을 생성합니다.

tacacs 프로토콜 선택에 사용된 기본 디바이스 관리 정책은 평가 정책 프로세스의 일부로 선택됩니다.tacacs 프로토콜을 사용하여 인증할 경우 선택한 서비스 정책을 Default Device Admin 정책이라고 합니다.그 정책 자체는 2개의 섹션으로 구성됩니다.ID는 사용자가 누구인지, 어떤 그룹(로컬 또는 외부)에 속하는지, 그리고 구성된 권한 부여 프로필에 따라 어떤 작업을 수행할 수 있는지 의미합니다.구성 중인 사용자와 관련된 명령 집합을 할당합니다.



읽기 전용 관리 액세스를 위한 권한 부여 정책을 만듭니다.

읽기 전용 사용자도 마찬가지입니다.다음 예에서는 사용자 1에 대한 권한 레벨 1 셸 프로파일 및 사용자 2에 대한 권한 15를 구성합니다.



tacacs에 대한 5760 구성

1. Radius/Tacacs 서버를 구성해야 합니다.
tacacs 서버 tac_acct

주소 ipv4 9.1.0.100

cisco

2. 서버 그룹 구성
aaa 그룹 서버 tacacs+ gtac

서버 이름 tac_acct

위 단계까지는 사전 요건이 없습니다.

3. 인증 및 권한 부여 방법 목록 구성
aaa 인증 로그인 <method-list> 그룹 <srv-grp

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

aaa authorization exec default group <srv-grp> - http에서 tacacs를 가져오는 해결 방법

위의 3 명령과 다른 모든 인증 및 권한 부여 매개변수는 동일한 데이터베이스(radius/tacacs 또는

local)를 사용해야 합니다.

예를 들어 명령 권한 부여를 활성화해야 하는 경우 동일한 데이터베이스를 가리켜야 합니다.

예:

aaa authorization 명령 15 <method-list> group <srv-grp> —> 데이터베이스를 가리키는 서버 그룹 (tacacs/radius 또는 local)은 동일해야 합니다.

4. 위의 메서드 목록을 사용하도록 http 구성

ip http authentication aaa login-auth <method-list> —> 메서드 목록이 "default"인 경우에도 여기서 메서드 목록을 명시적으로 지정해야 합니다.

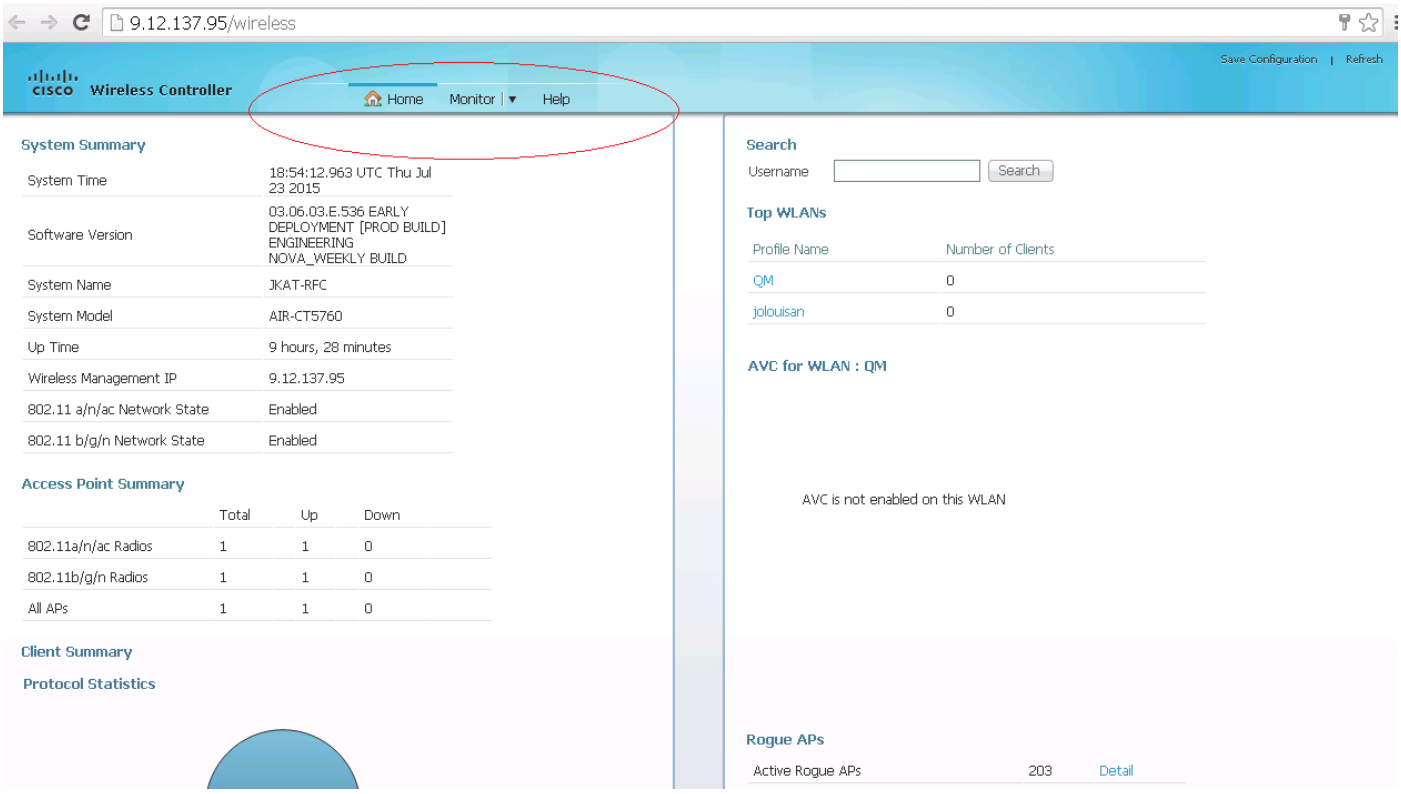
ip http authentication aaa exec-auth <method-list>

** 참고 사항

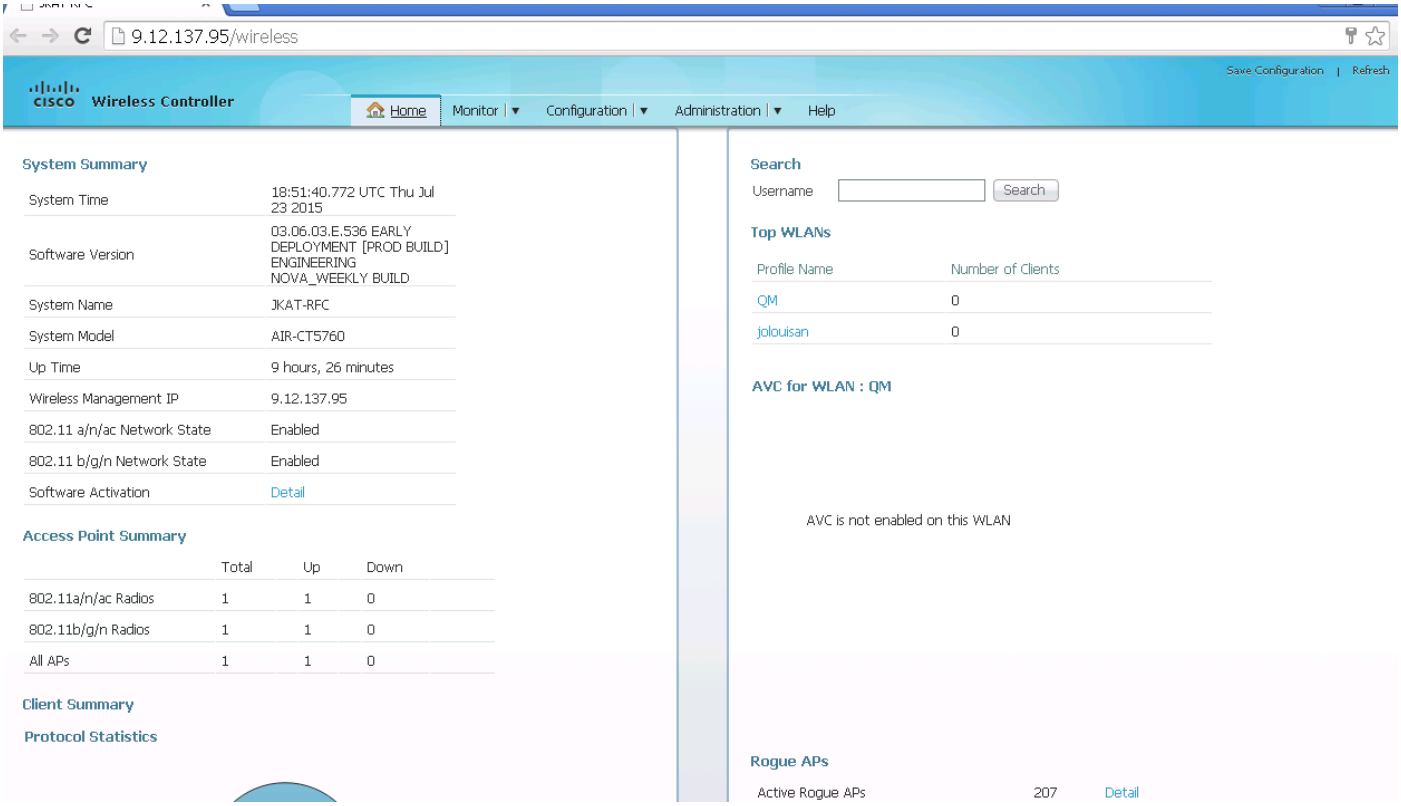
- "line vty" 컨피그레이션 매개변수에서 method-list를 구성하지 마십시오.위의 단계와 행 vty에 다른 컨피그레이션이 있는 경우 라인 vty 컨피그레이션이 우선합니다.
- ssh/telnet 및 webui와 같은 모든 관리 구성 유형에서 데이터베이스는 동일해야 합니다.
- Http 인증에는 명시적으로 정의된 메서드 목록이 있어야 합니다.

서로 다른 2개의 프로필을 사용하여 동일한 5760에 액세스

아래는 제한된 액세스 권한이 부여된 권한 수준 1 사용자의 액세스 권한입니다



아래는 권한 레벨 15 사용자로부터 전체 액세스 권한을 부여받은 액세스 권한입니다


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