ISE 2.x에 대해 Prime 3.1 TACACS 인증 구성

목차

소개

이 문서에서는 ISE 2.x에서 TACACS를 통해 인증하도록 Prime Infrastructure를 구성하는 방법에 대해 설명합니다.

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Identity Services Engine(ISE)
- Prime Infrastructure

구성

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 이상.

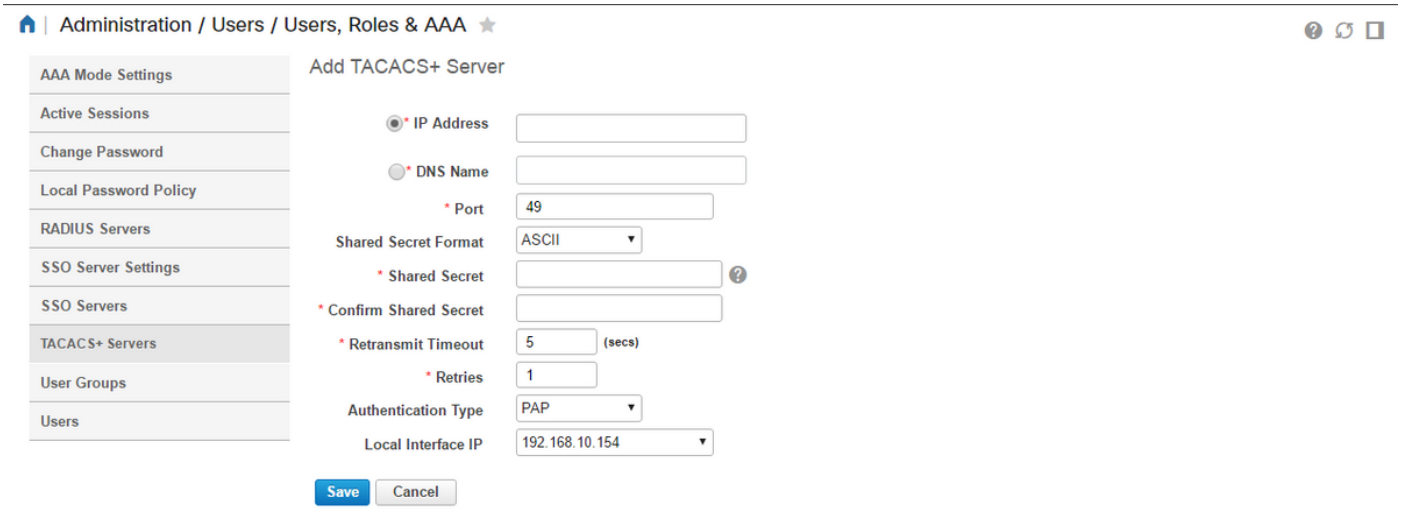
(참고: ISE는 버전 2.0부터 시작하는 TACACS만 지원하지만 Prime에서 Radius를 사용하도록 구성할 수 있습니다. Prime에는 이전 버전의 ISE 또는 서드파티 솔루션과 함께 Radius를 사용하려는 경우 TACACS 외에도 Radius 특성 목록이 포함됩니다.)

Prime 컨피그레이션

Administration(관리) / Users(사용자)/ Users(사용자), Roles(역할) 및 AAA(AAA) 화면으로 이동합니다(아래 참조).

그런 다음 TACACS+ Servers(TACACS+ 서버) 탭을 선택한 다음 오른쪽 상단 모서리에서 Add TACACS+ Server(TACACS+ 서버 추가) 옵션을 선택하고 go(이동)를 선택합니다.

다음 화면에서는 TACACS 서버 항목의 컨피그레이션을 사용할 수 있습니다(개별 TACACS 서버마다 수행해야 함)



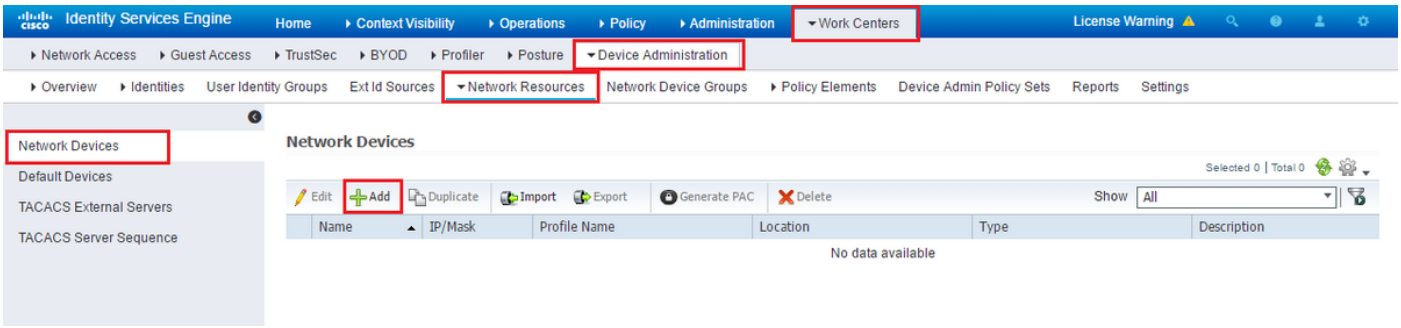
여기서 서버의 IP 주소 또는 DNS 주소와 공유 비밀 키를 입력해야 합니다. 또한 사용하려는 로컬 인터페이스 IP에 유의하십시오. 나중에 ISE에서 AAA 클라이언트에 대해 동일한 IP 주소를 사용해야 합니다.

Prime에서 컨피그레이션을 완료하려면 Administration(관리)/Users(사용자)/Users(사용자)/Users(사용자), Roles(역할) 및 AAA(AAA 모드 설정) 탭 아래에서 TACACS를 활성화해야 합니다.

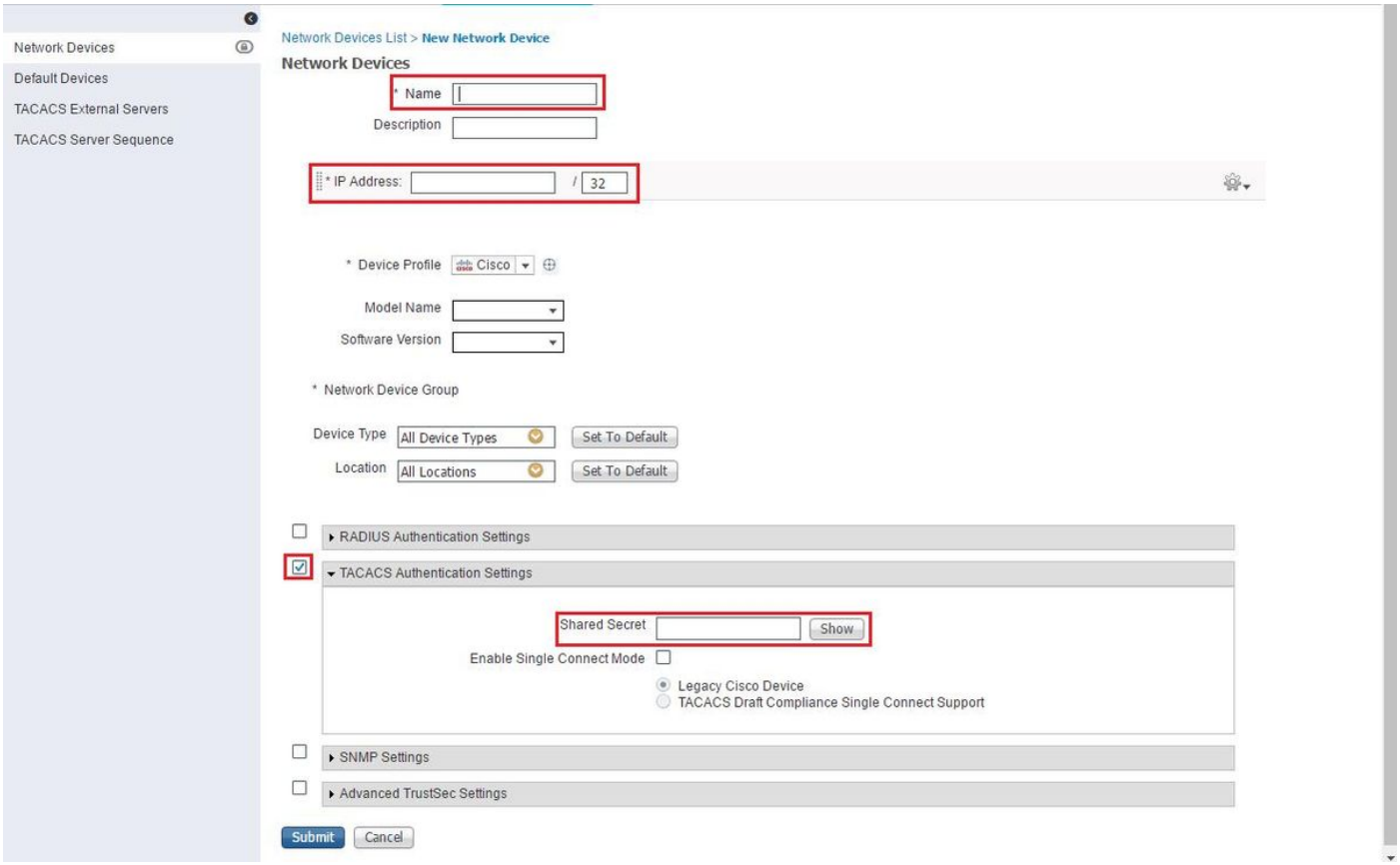
(참고: 특히 컨피그레이션을 테스트할 때는 Enable fallback to Local(로컬로 대체 활성화) 옵션을 ONLY on no server response(서버 응답이 없는 경우에만) 또는 On no response or failure(응답 또는 실패 응답이 없는 경우에만) 옵션과 함께 선택하는 것이 좋습니다.)

ISE 구성

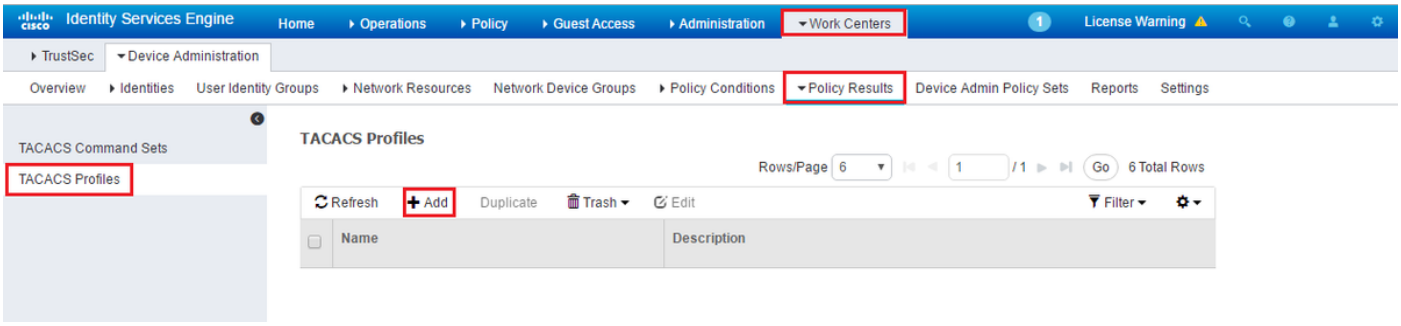
Work Centers(작업 센터)/Device Administration(디바이스 관리)/Network Resources(네트워크 리소스)/Network Devices(네트워크 디바이스)/Add(추가)에서 ISE의 AAA 클라이언트로 Prime 구성



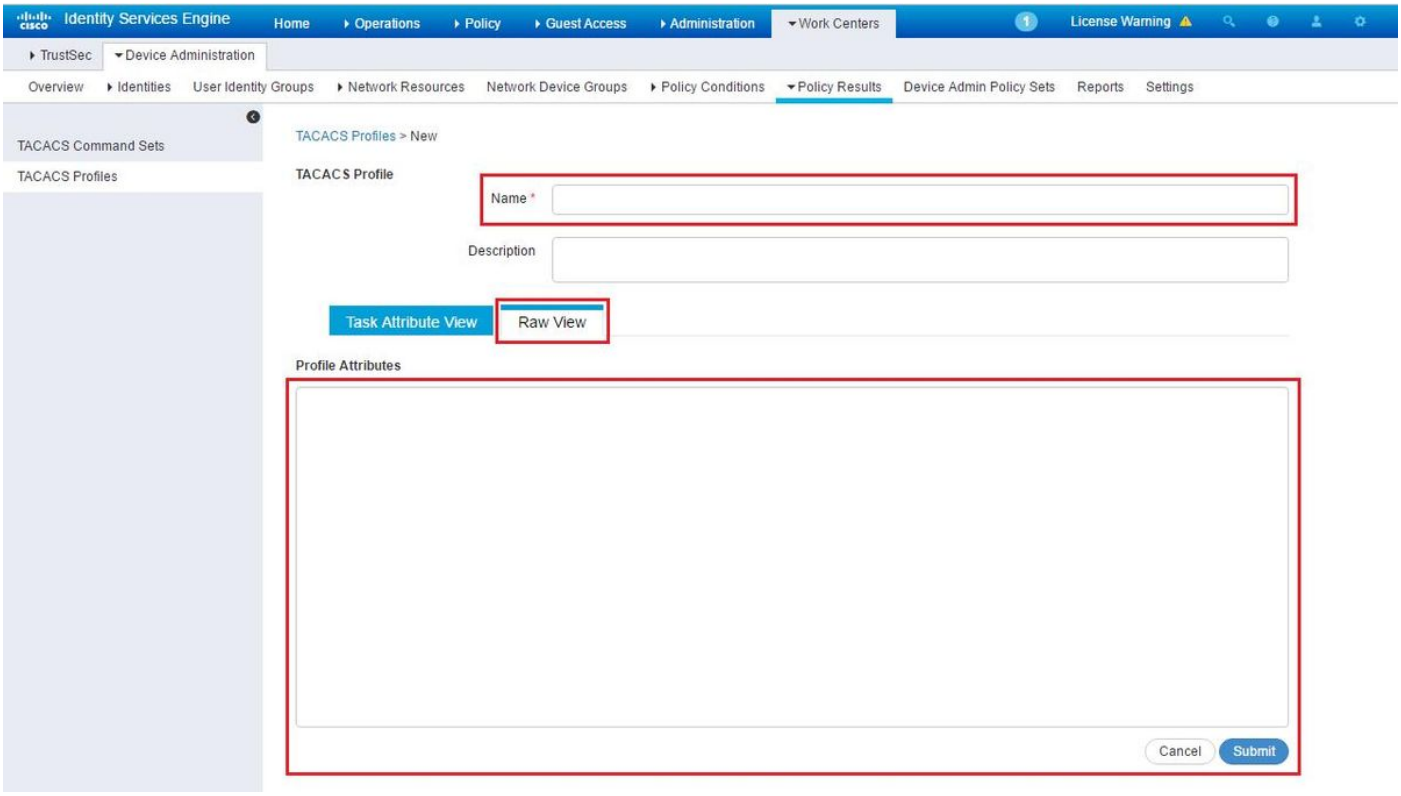
Prime 서버에 대한 정보를 입력합니다. 포함해야 할 필수 특성은 Name(이름), IP address(IP 주소)입니다. TACACS 및 Shared Secret(공유 암호)에 대한 옵션을 선택합니다. 나중에 권한 부여 규칙 또는 기타 정보의 조건으로 사용하기 위해 Prime에 대해 Device Type(디바이스 유형)을 추가로 추가할 수 있지만 이는 선택 사항입니다.



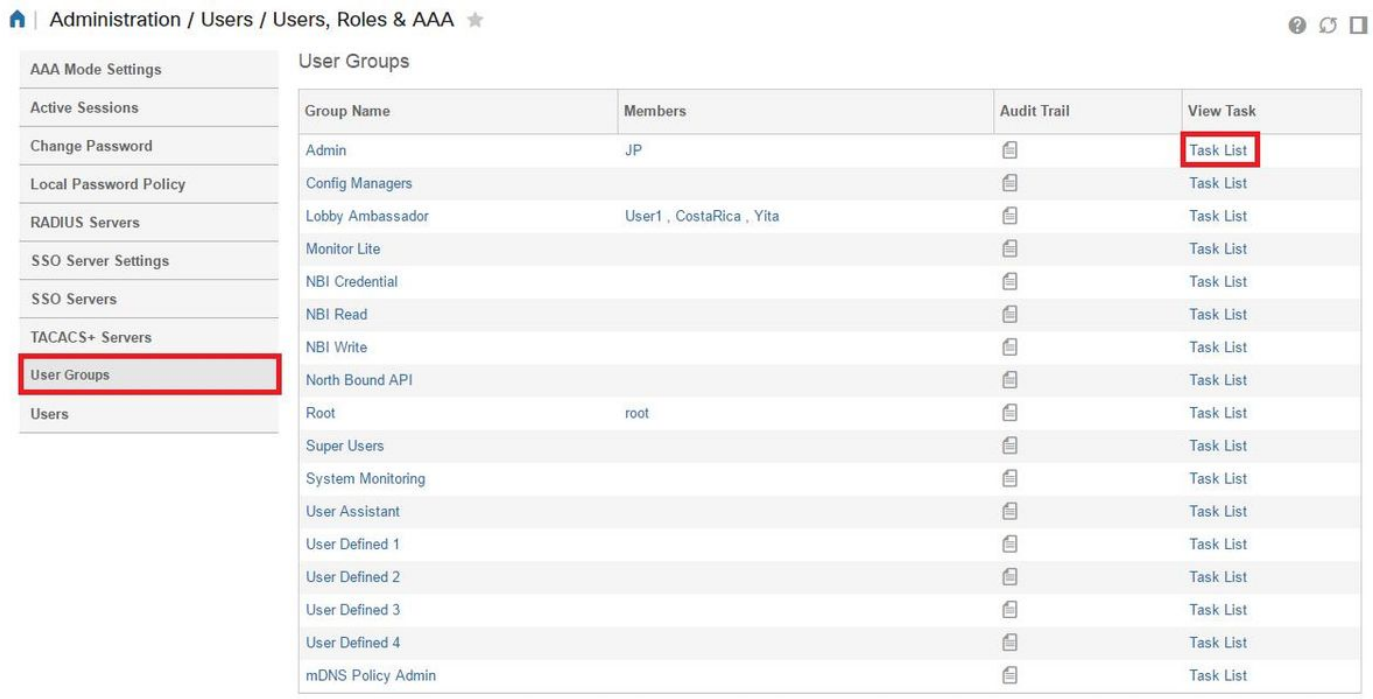
그런 다음 TACACS 프로필 결과를 생성하여 필요한 특성을 ISE에서 Prime으로 전송하여 올바른 액세스 수준을 제공합니다. Work Centers(작업 센터)/Policy Results(정책 결과)/Tacacs Profiles(Tacacs 프로필)로 이동하고 Add(추가) 옵션을 선택합니다.



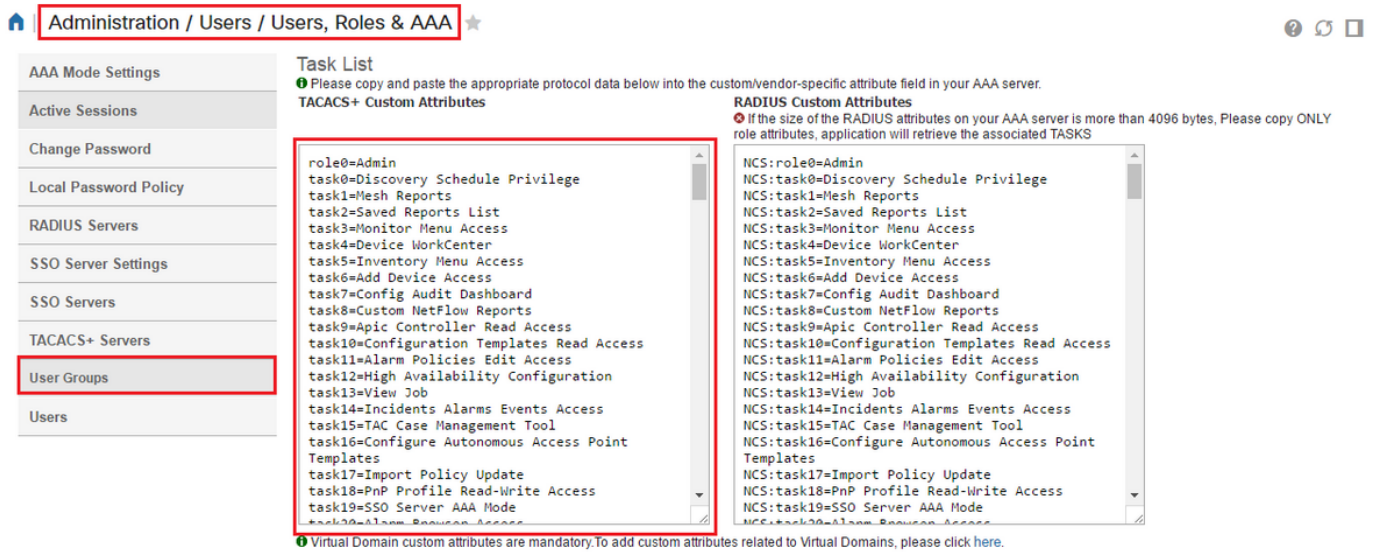
이름을 구성하고 Profile attributes(프로필 특성) 상자에 특성을 입력하려면 Raw View(원시 보기) 옵션을 사용합니다. 특성은 primer 서버 자체에서 가져옵니다.



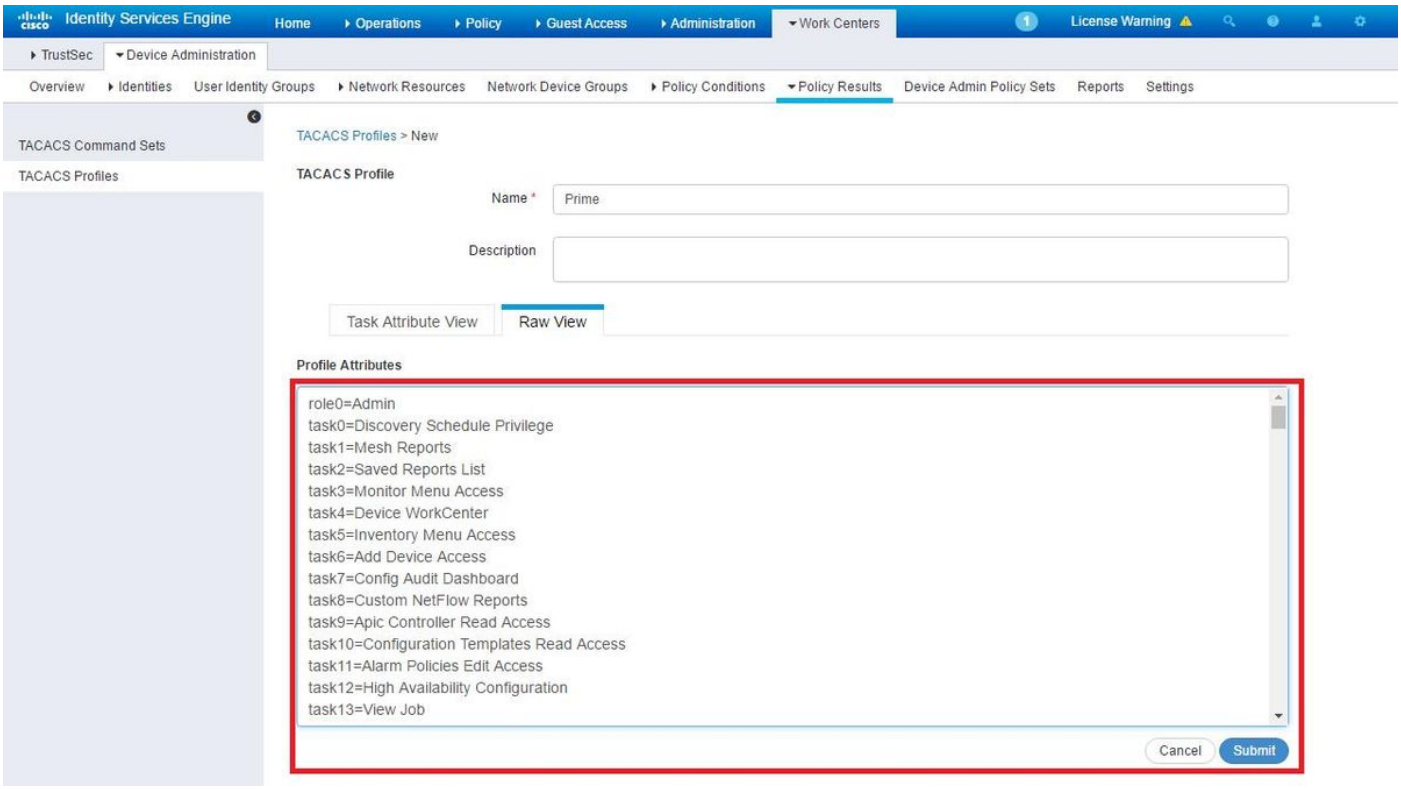
Administration(관리) / Users(사용자)/ Users(사용자), Roles(역할) 및 AAA(AAA) 화면에서 특성을 가져오고 User Groups(사용자 그룹) 탭을 선택합니다. 여기서 제공하려는 액세스 그룹 수준을 선택합니다. 이 예에서는 관리자 액세스 권한이 왼쪽에 있는 적절한 작업 목록을 선택하여 제공됩니다.



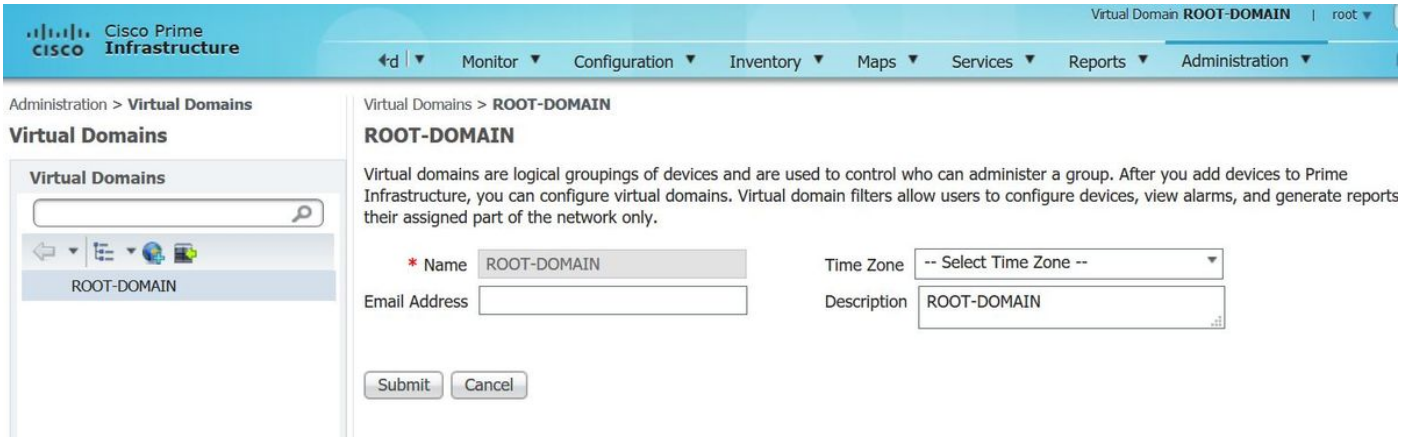
모든 TACACS 사용자 지정 특성을 복사합니다.



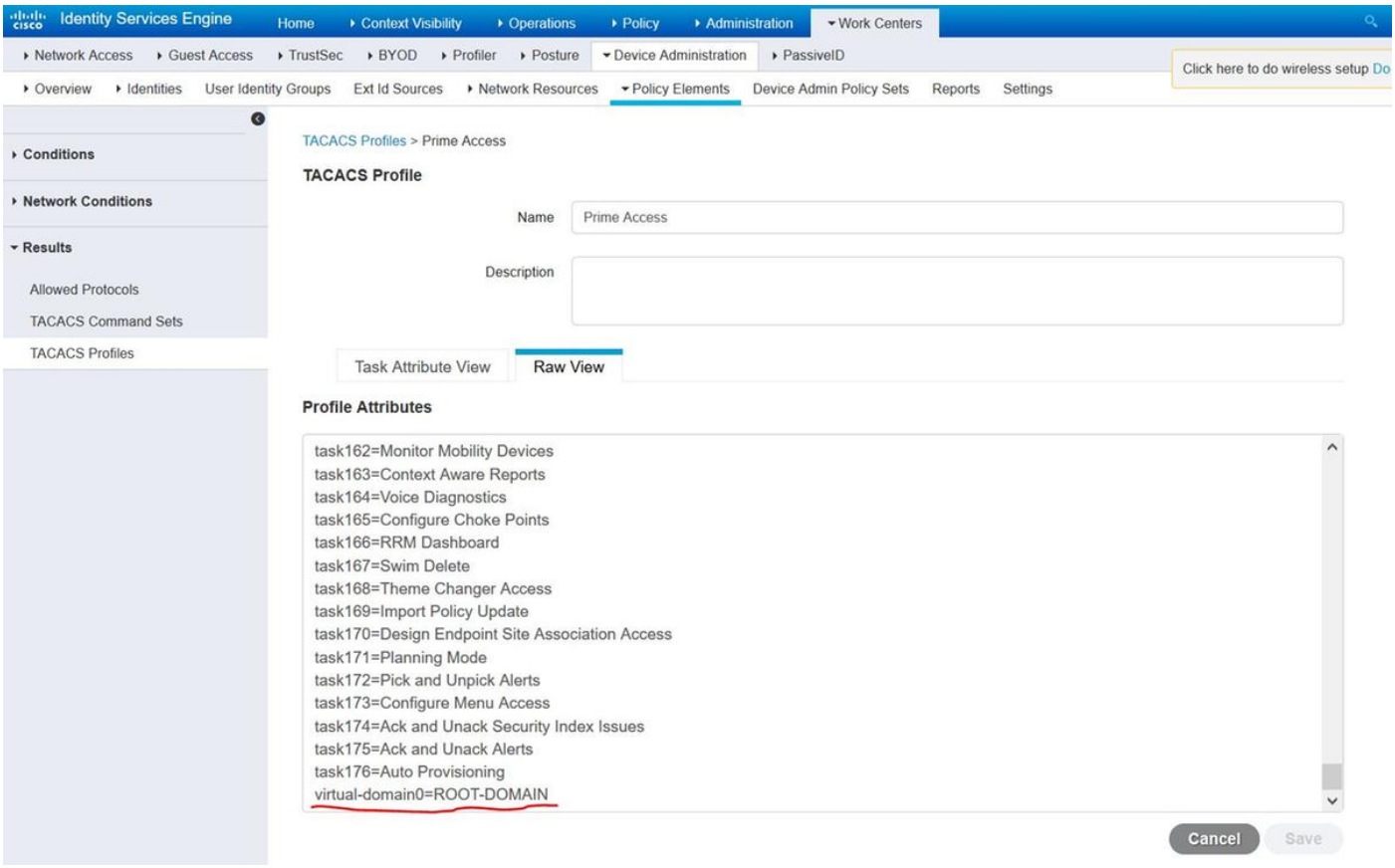
그런 다음 ISE의 Profile(프로파일)의 Raw View(원시 보기) 섹션에 붙여넣습니다.



가상 도메인 사용자 지정 특성은 필수입니다. 루트 도메인 정보는 Prime Administration(기본 관리) -> Virtual Domains(가상 도메인)에서 찾을 수 있습니다.

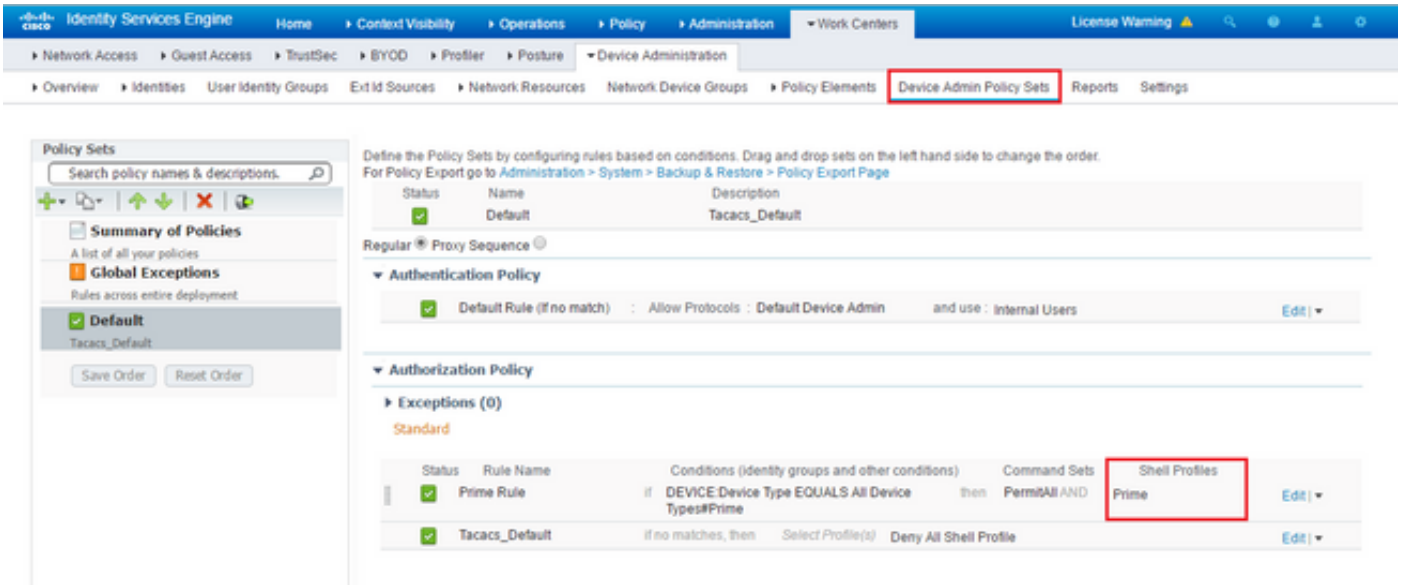


Prime Virtual Domain의 이름을 attribute virtual-domain0="virtual domain name"으로 추가해야 합니다.



그런 다음 이전 단계에서 생성한 셸 프로필을 할당하는 규칙을 Work Centers/Device Administration/Device Admin Policy Sets(작업 센터/디바이스 관리/디바이스 관리 정책 집합) 아래에 생성하기만 하면 됩니다

(참고: "조건"은 구축에 따라 달라지지만, 이 규칙에서 요청을 제대로 필터링하도록 Prime에 대해 특별히 "Device Type"을 사용하거나 Prime IP 주소와 같은 다른 유형의 필터를 "조건" 중 하나로 사용할 수 있습니다.)



이 시점에서 컨피그레이션이 완료되어야 합니다.

문제 해결

이 컨피그레이션이 실패하고 Prime에서 로컬 폴백 옵션이 활성화된 경우 Prime의 IP 주소를 제거하여 ISE에서 장애 조치를 강제로 수행할 수 있습니다. 그러면 ISE가 응답하지 않고 로컬 자격 증명을 강제로 사용하게 됩니다. 거부 시 로컬 폴백이 수행되도록 구성된 경우 로컬 어카운트는 여전히 작동하며 고객에게 액세스 권한을 제공합니다.

ISE가 성공적인 인증을 표시하고 올바른 규칙과 일치하지만 Prime이 요청을 계속 거부하는 경우 프로필에서 특성이 올바르게 구성되었으며 추가 특성이 전송되지 않았음을 다시 확인하고자 할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.