Cisco RADIUS(Identity Service Engine)를 사용한 AsyncOS 외부 인증

목차

소개

이 문서에서는 RADIUS를 통한 외부 인증을 성공적으로 구현하기 위해 ESA(Email Security Appliance)/SMA(Security Management Appliance)와 Cisco ISE(Identity Services Engine) 간에 필요한 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AAA(Authentication, Authorization, and Accounting)
- RADIUS CLASS 특성.
- Cisco ISE ID 관리 및 권한 부여 정책.
- Cisco ESA/SMA 사용자 역할.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0
- Cisco SMA 13.6.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

관련 제품

사용된 구성 요소 섹션에 나열된 버전 이외의 버전은 테스트되지 않았습니다.

배경 정보

Radius CLASS 특성

어카운팅에 사용되는 이 값은 RADIUS 서버가 모든 어카운팅 패킷에 포함하는 임의의 값입니다.

클래스 특성은 ISE(RADIUS)에서 그룹 단위로 구성됩니다.

사용자가 25 속성이 연결된 ISE/VPN 그룹의 일부로 간주되면 NAC는 ISE(Identity Services Engine) 서버에서 구성된 매핑 규칙을 기반으로 정책을 적용합니다.

구성

네트워크 다이어그램

Identity Service Engine은 ESA/SMA의 인증 요청을 수락하고 사용자 ID 및 그룹과 일치시킵니다.

1단계. 인증을 위한 ID 그룹을 만듭니다.

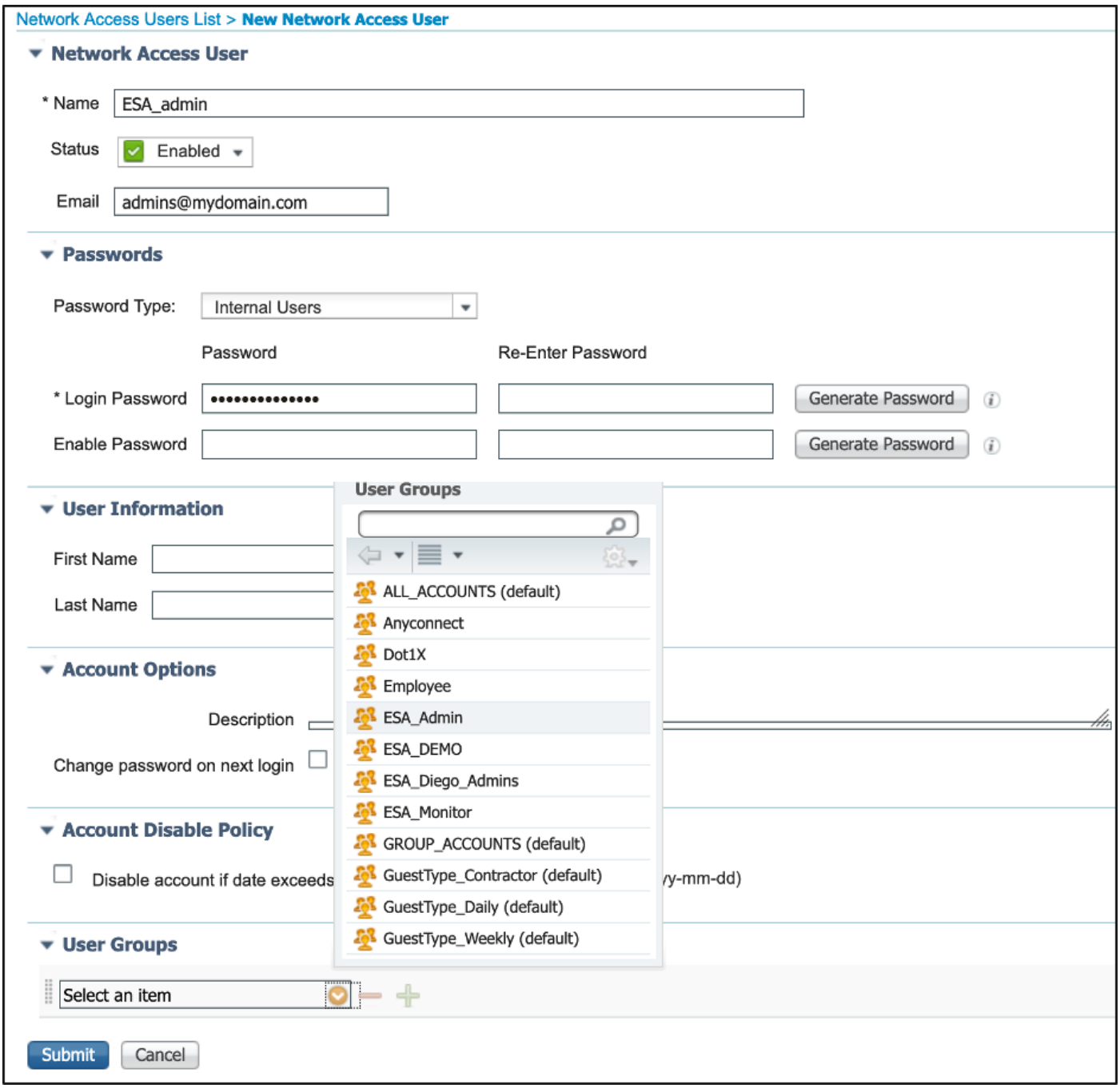
ISE 서버에 로그인하고 ID 그룹 생성:

Administration->Identity Management->Groups->User Identity Group으로 이동합니다.이미지에 표시된 대로

참고: Cisco는 할당된 각 ESA/SMA 역할에 대해 ISE의 ID 그룹을 권장합니다.

2단계. 인증을 위한 로컬 사용자를 생성합니다.

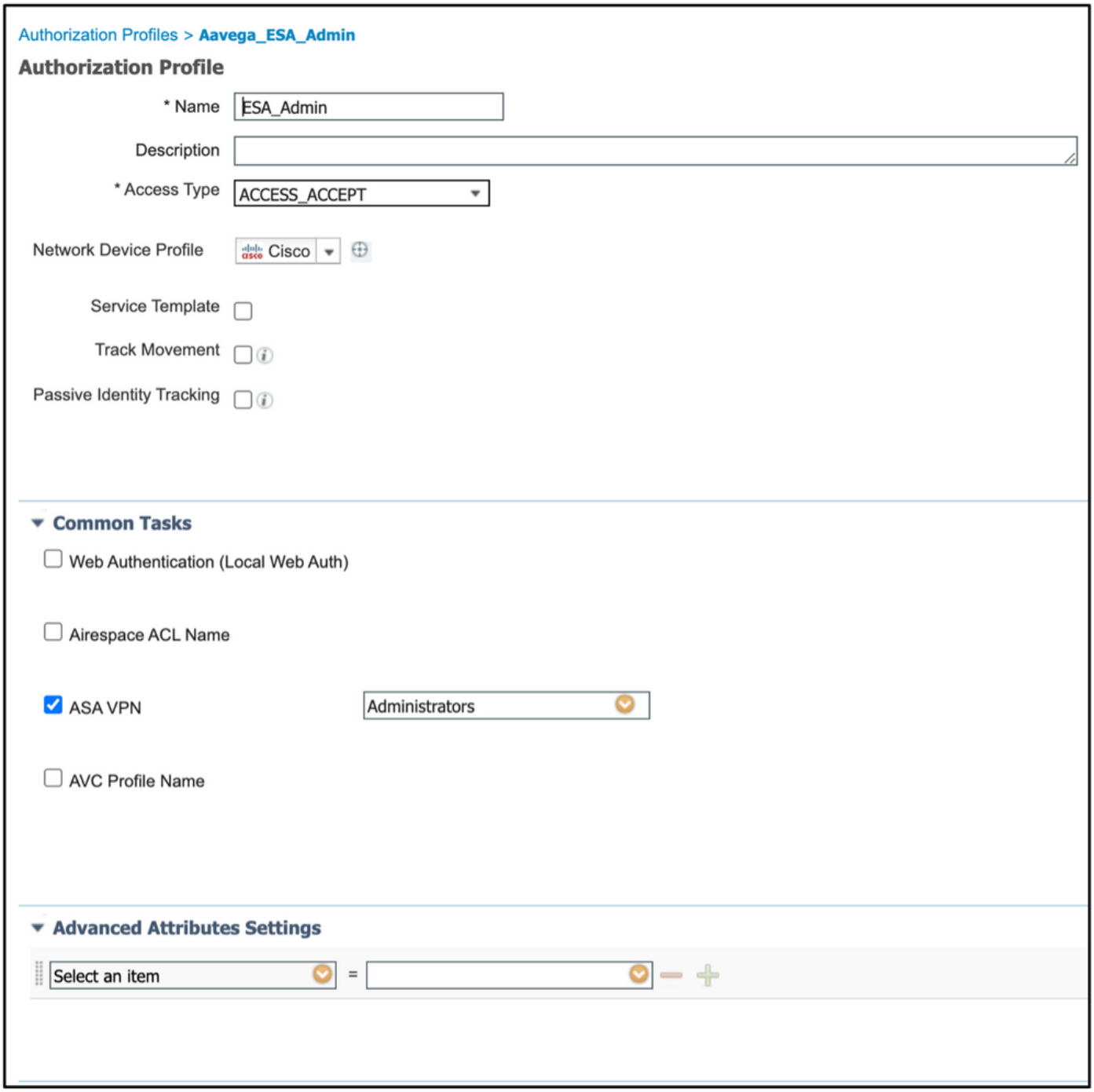
이 단계에서는 새 사용자를 생성하거나 1단계에서 생성한 ID 그룹에 이미 있는 사용자를 할당합니다. ISE에 로그인하고 Administration(관리) **->Identity Management(ID 관리)->Identities(ID)로 이동하여** 새 사용자를 생성하거나 생성한 그룹의 사용자에게 할당하십시오.이미지에 표시된 대로



3단계. 권한 부여 프로파일을 생성합니다.

RADIUS 인증은 권한 부여 프로파일 없이 성공적으로 완료할 수 있지만 역할을 할당할 수는 없습니다.설정을 완료하려면 Policy(정책) **->Policy Elements(정책 요소)->Results(결과)->Authorization(권한 부여)->Authorization(권한 부여) 프로필로 이동하십시오.**

참고:할당할 역할당 하나의 권한 부여 프로파일을 생성합니다.



참고:radius 클래스 특성 25를 사용하고 이름을 지정합니다.이 이름은 AsyncOS(ESA/SMA)의 컨피그레이션과 일치해야 합니다. 그림 3에서 관리자는 CLASS 특성 이름입니다.

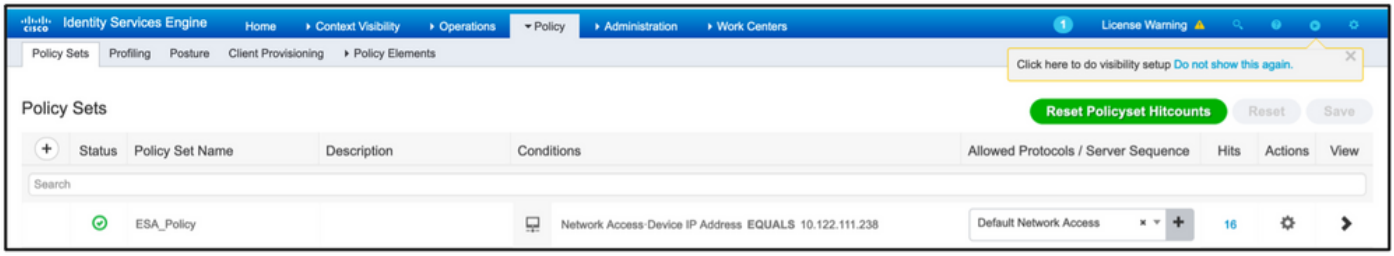
4단계. 권한 부여 정책을 생성합니다.

이 마지막 단계에서는 ISE 서버가 사용자 로그인 시도를 식별하고 올바른 권한 부여 프로파일에 매핑할 수 있습니다.

권한 부여가 성공적으로 완료되면 ISE는 권한 부여 프로파일에 정의된 CLASS 값을 따라 액세스 승인을 반환합니다.

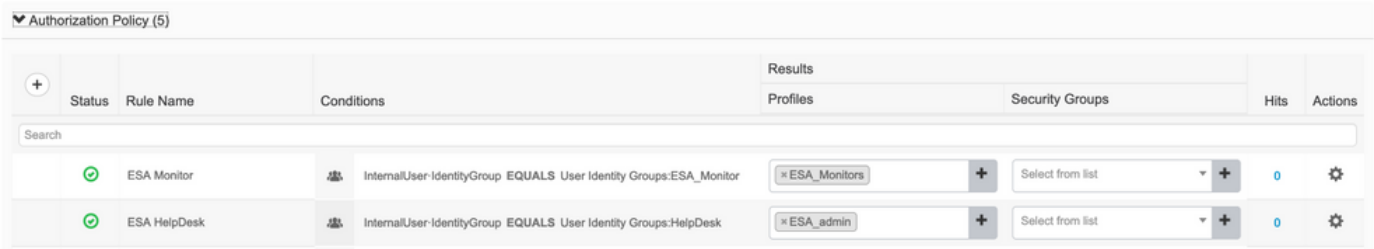
Policy(정책) > Policy Sets(정책 집합) > Add(추가)(+ 기호)로 이동합니다.

이름을 지정하고 더하기 기호를 선택하여 필요한 조건을 추가합니다.이 실습 환경은 Radius를 사용합니다.NAS-IP 주소.새 정책을 저장합니다.



권한 부여 요청과 올바르게 일치하려면 조건을 추가해야 합니다.**선택**  아이콘을 클릭하고 조건을 추가합니다.

랩 환경은 InternalUser-IdentityGroup을 사용하며 각 권한 부여 프로파일과 일치합니다.



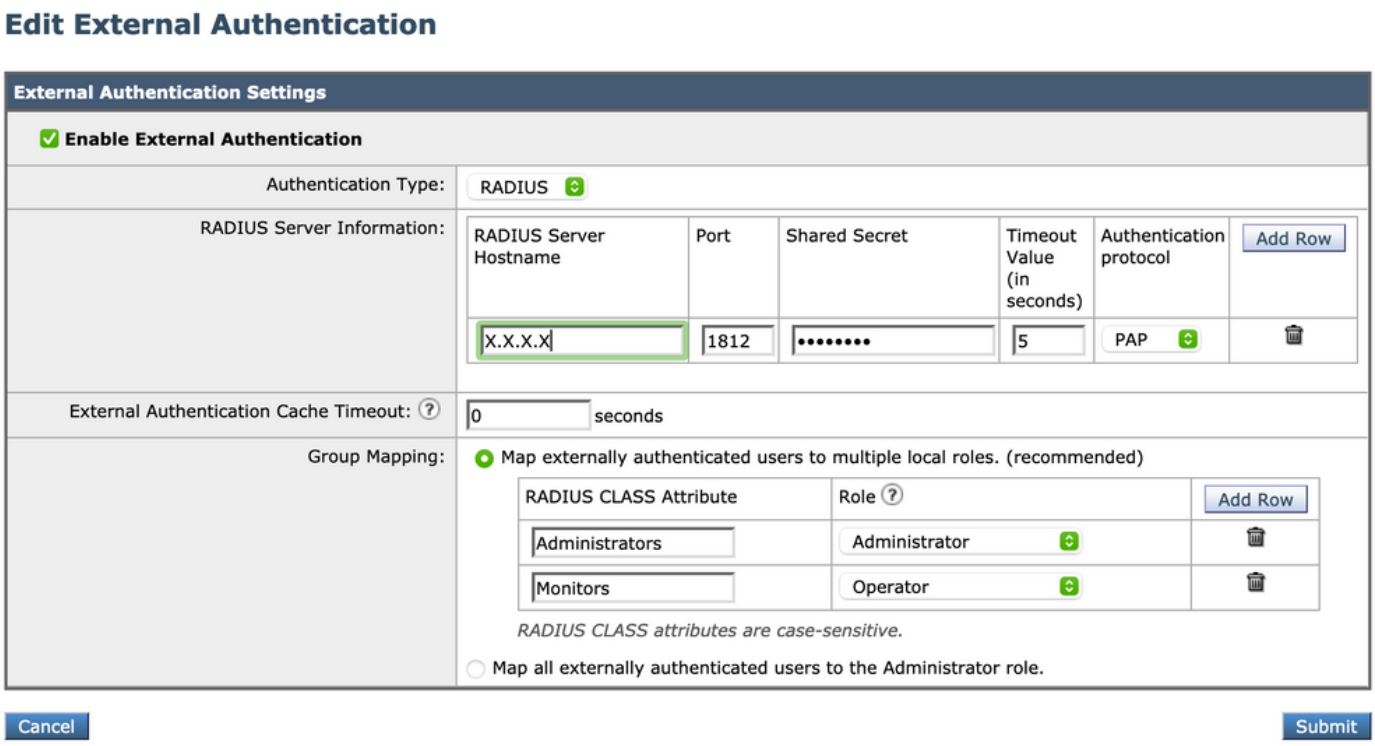
5단계. AsyncOS ESA/SMA에 대한 외부 인증을 활성화합니다.

AsyncOS 어플라이언스(ESA/SMA/WSA)에 로그인합니다. System **Administration(시스템 관리) > Users(사용자) > External Authentication(외부 인증) > Enable External Authentication on ESA(ESA에서 외부 인증 활성화)로** 이동합니다.

다음 값을 제공합니다.

- RADIUS 서버 호스트 이름
- 포트
- 공유 암호
- 시간 초과 값(초)
- 인증 프로토콜

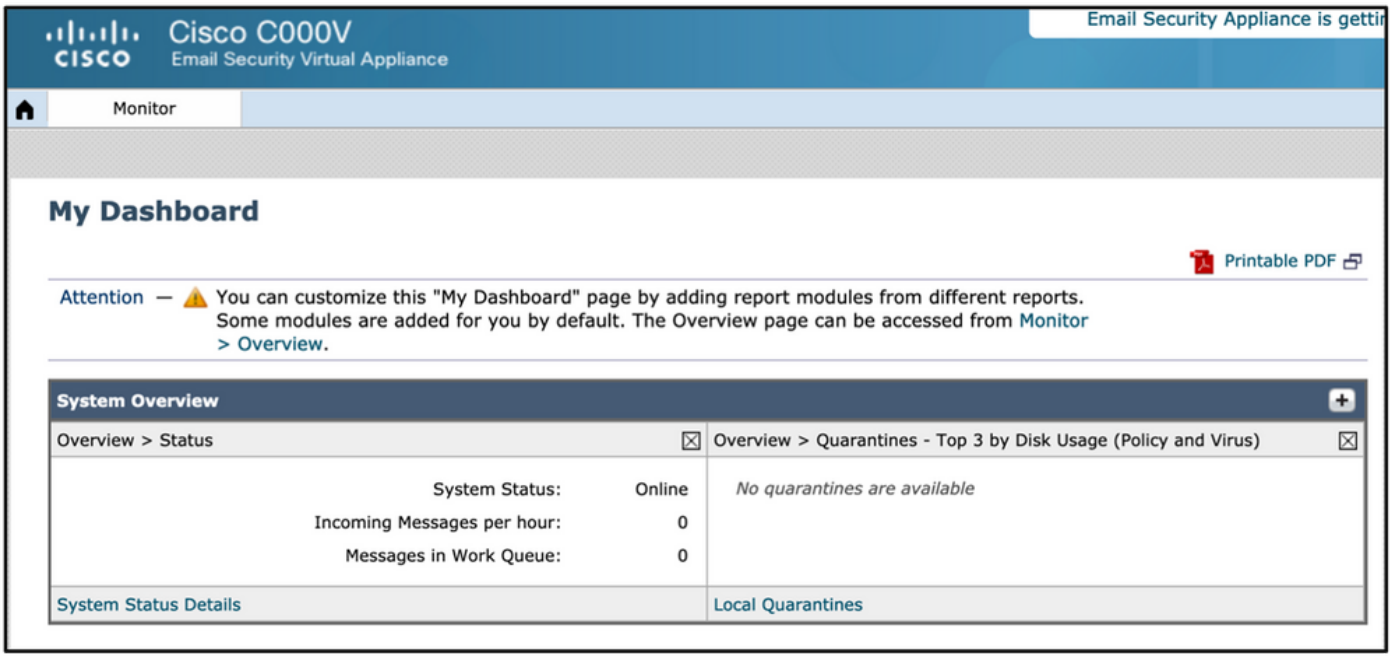
Map externally **authenticated users to multiple local roles(외부 인증 사용자를 여러 로컬 역할에 매핑)를 선택합니다(권장)**. 이미지에 표시된 대로



참고:RADIUS CLASS 특성은 3단계에서 정의된 특성 Name과 일치해야 합니다(ASA VPN으로 매핑된 일반 작업 아래).

다음을 확인합니다.

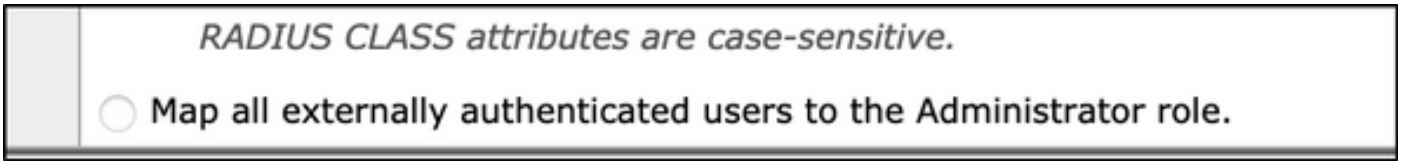
AsyncOS 어플라이언스에 로그인하고 액세스 권한이 부여되었으며 할당된 역할이 올바르게 할당되었는지 확인하십시오.이미지에 게스트 사용자 역할이 나와 있습니다.



문제 해결

로그인 시도가 ESA에서 "Invalid username or password(잘못된 사용자 이름 또는 비밀번호)" 메시지와 함께 작동하지 않을 경우.권한 부여 정책에 문제가 있을 수 있습니다.

ESA에 로그인하고 External Authentication(외부 인증)에서 Map all externally authenticated users to the Administrator role(외부에서 인증된 모든 사용자를 관리자 역할에 매핑)을 선택합니다.



변경 사항을 제출하고 커밋합니다.새 로그인을 시도합니다.성공적으로 로그인하면 ISE Radius 권한 부여 프로파일(CLASS 특성 25) 및 권한 부여 정책 설정을 다시 확인합니다.

- ISE 2.4
- AsyncOS