# ISE 3.2의 패시브 ID 세션에 대한 권한 부여 흐름 구성

## 목차

[소개](#)
[배경 정보](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[설정](#)
[다음을 확인합니다.](#)
[문제 해결](#)

## 소개

이 문서에서는 세션에 SGT를 할당하기 위해 패시브 ID 이벤트에 대한 권한 부여 규칙을 구성하는 방법에 대해 설명합니다.

## 배경 정보

패시브 ID 서비스(패시브 ID)는 사용자를 직접 인증하지 않고 AD(Active Directory)(공급자로 알려짐)와 같은 외부 인증 서버에서 사용자 ID와 IP 주소를 수집한 다음 해당 정보를 가입자와 공유합니다.

ISE 3.2에는 Active Directory 그룹 멤버십을 기반으로 사용자에게 SGT(Security Group Tag)를 할당하도록 권한 부여 정책을 구성할 수 있는 새로운 기능이 도입되었습니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 3.X
- 모든 공급자와 수동 ID 통합
- AD(Active Directory) 관리
- 세그멘테이션(Trustsec)
- PxGrid(플랫폼 교환 그리드)

### 사용되는 구성 요소

- ISE(Identity Service Engine) 소프트웨어 버전 3.2
- 마이크로소프트 액티브 디렉토리
- Syslog

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

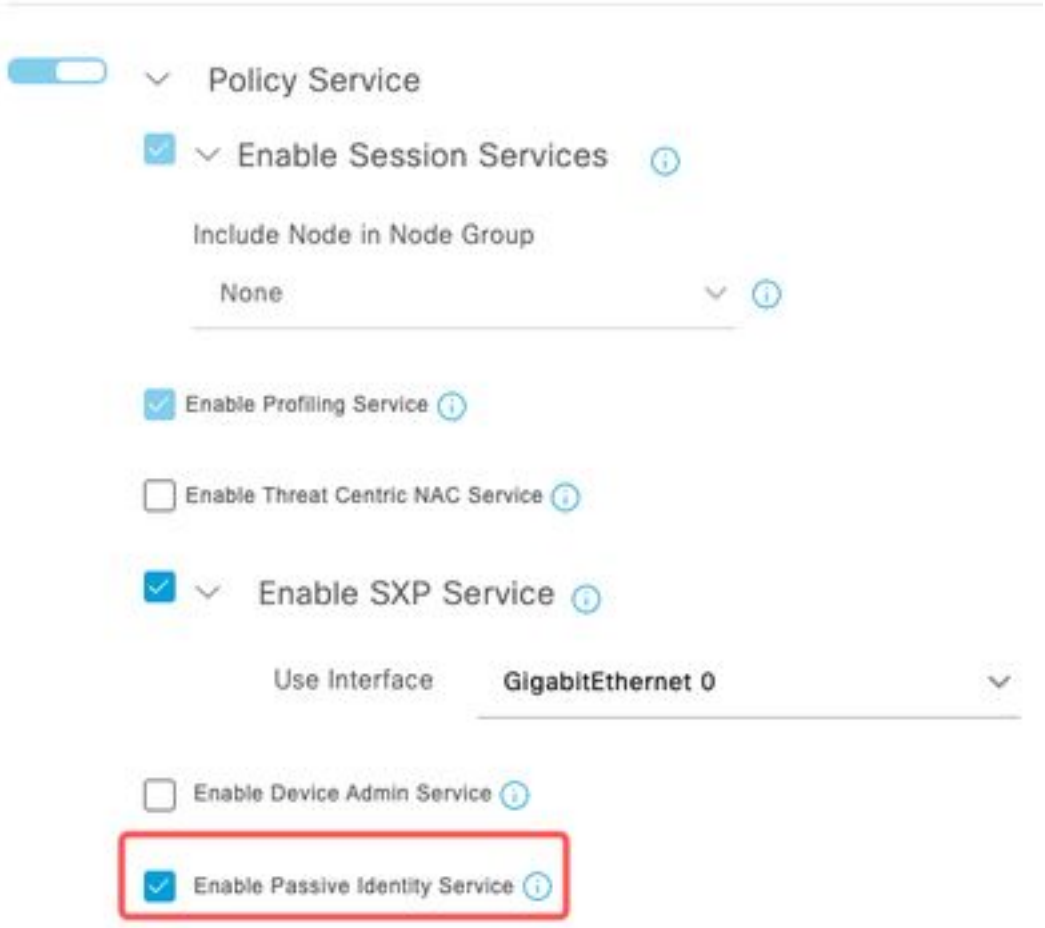
이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 설정

1단계. ISE 서비스를 활성화합니다.

1. ISE에서 Administration(관리) > Deployment(구축)로 **이동하고 ISE 노드**를 선택한 다음 Edit(편집)를 클릭하고 **Policy Service(정책 서비스)를 활성화하고 Enable Passive Identity Service(수동 ID 서비스** 활성화)를 선택합니다**.** 패시브 ID 세션을 통해 게시해야 하는 경우 SXP 및 PxGrid를 활성화할 수 있습니다(선택 사항). 저장을 **클릭합니다**.

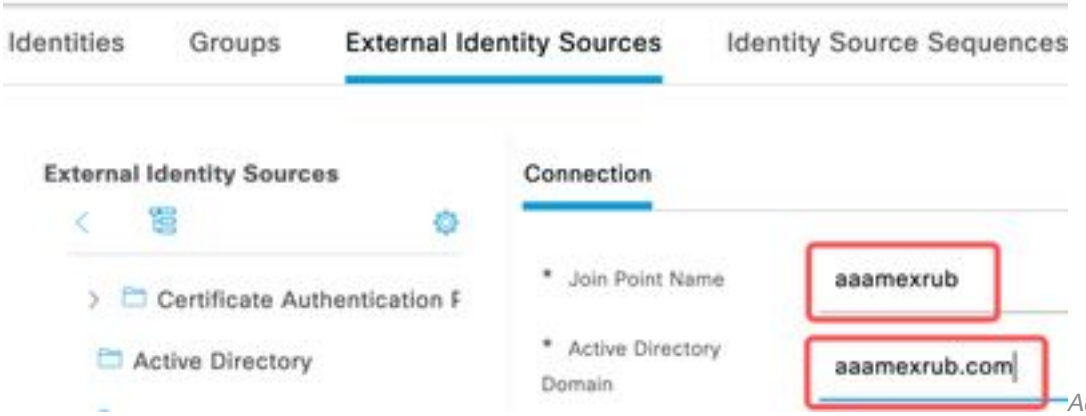
   **경고:** API 제공자에 의해 인증된 PassiveID 로그인 사용자의 SGT 세부 정보는 SXP에 게시할 수 없습니다. 그러나 이러한 사용자의 SGT 세부사항은 pxGrid 및 pxGrid Cloud를 통해 게시할 수 있습니다.




*활성화된 서비스*

2단계. Active Directory를 구성합니다.

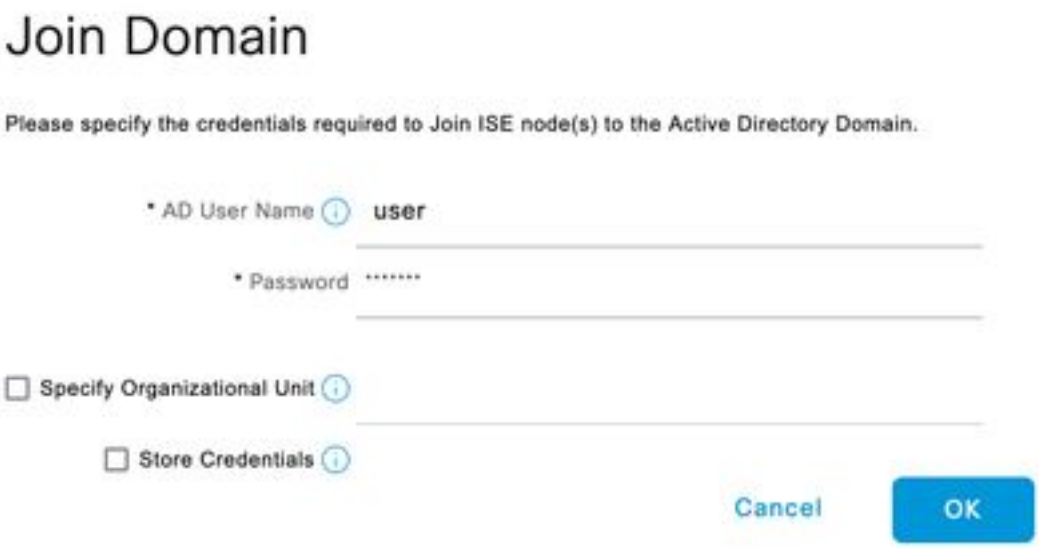
1. Administration(관리) > **Identity Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동하고 Active directory**를 선택한 다음 Add(추가) **버튼을 클릭합니다.**
2. **가입 포인트 이름** 및 **Active Directory 도메인**을 입력합니다. Submit(제출)**을 클릭합니다**.




*Active Directory 추가*

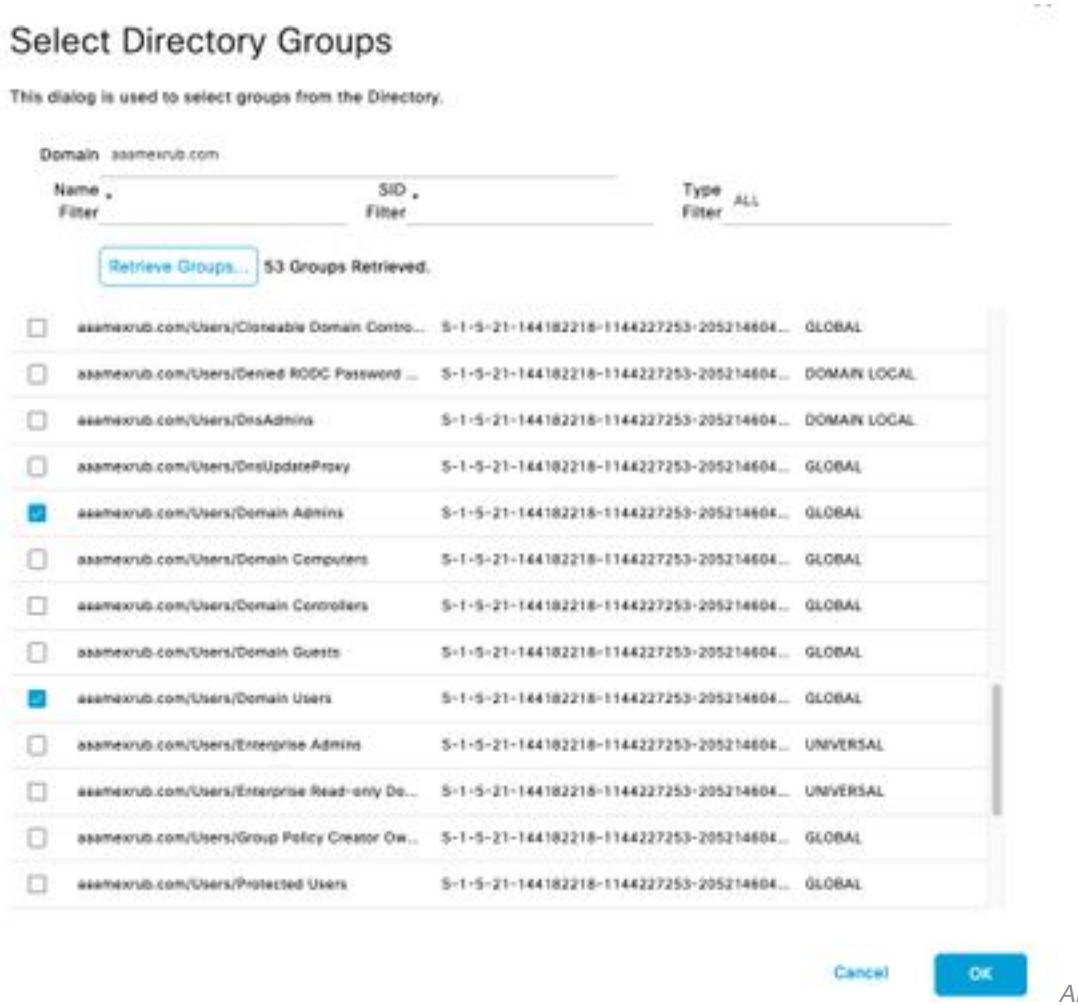
3. ISE를 AD에 추가하는 팝업이 나타납니다. Yes(**예**)를 **클릭합니다**. 사용자 이름과 **비밀번호**를 **입력합니다**. OK(확인)를 클릭합니다.


*ISE에 계속 참여*

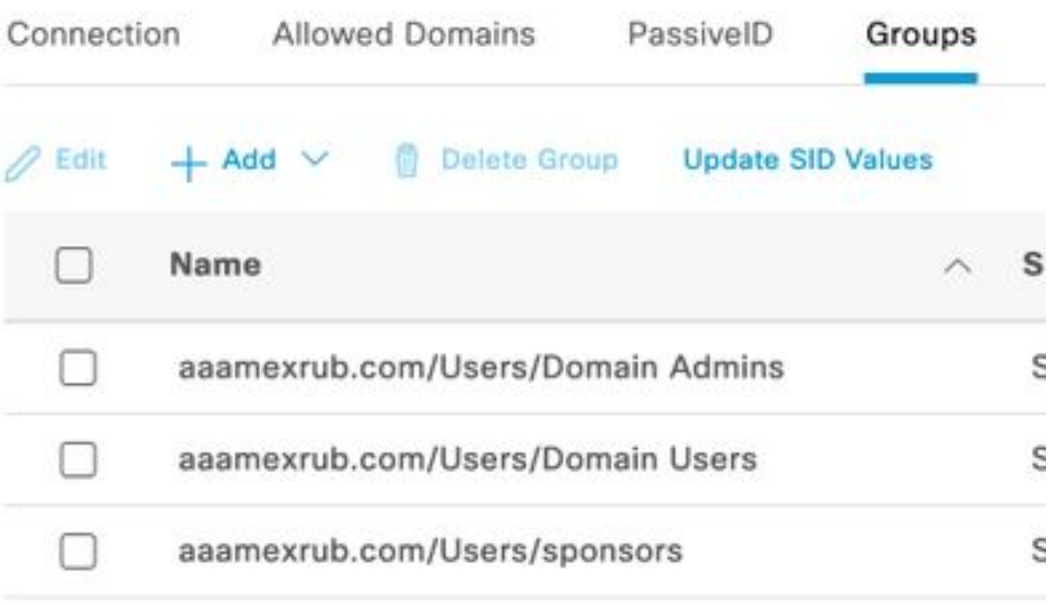



*Active Directory 가입*

4. AD 그룹을 검색합니다. Groups(**그룹**)로 **이동하여 Add(추가)**를 클릭한 다음 Retrieve Groups(**그룹 검색**)를 클릭하고 원하는 그룹을 모두 선택한 다음 **OK(확인)를** 클릭합니다.

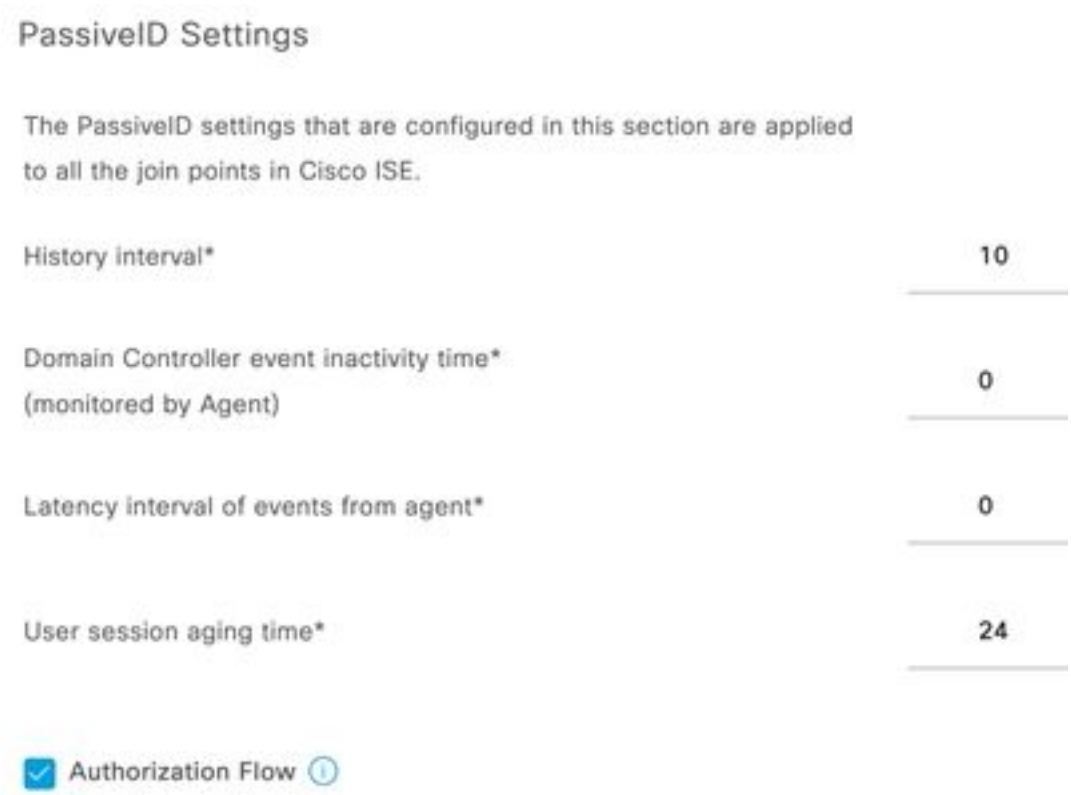



*AD 그룹 검색*




*검색된 그룹*

5. Authorization Flow를 활성화합니다. **Advance Settings(고급 설정)**로 이동하고 PassiveID Settings(**PassiveID 설정) 섹션**에서 **Authorization Flow(권한 부여 플로우) 확인란을** 선택합니다. 저장을 **클릭합니다**.

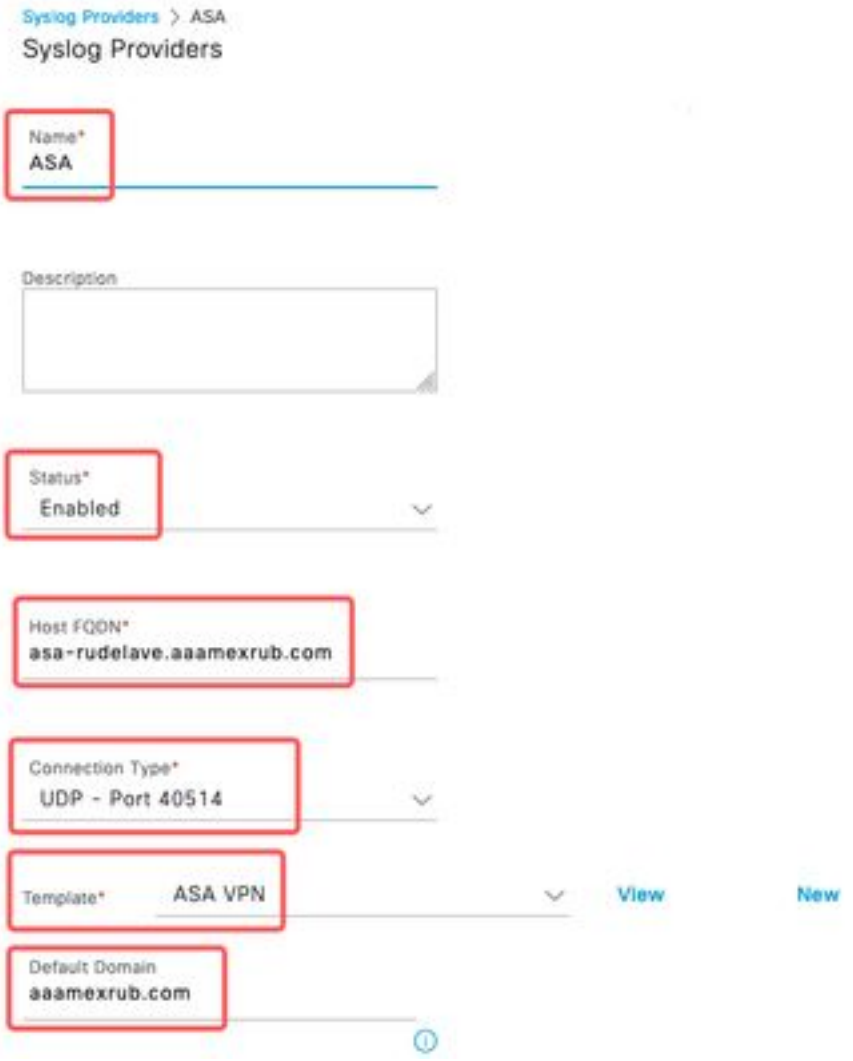



*Enable Authorization Flow(권한 부여 흐름 활성화)*

3단계. Syslog 공급자를 구성합니다.

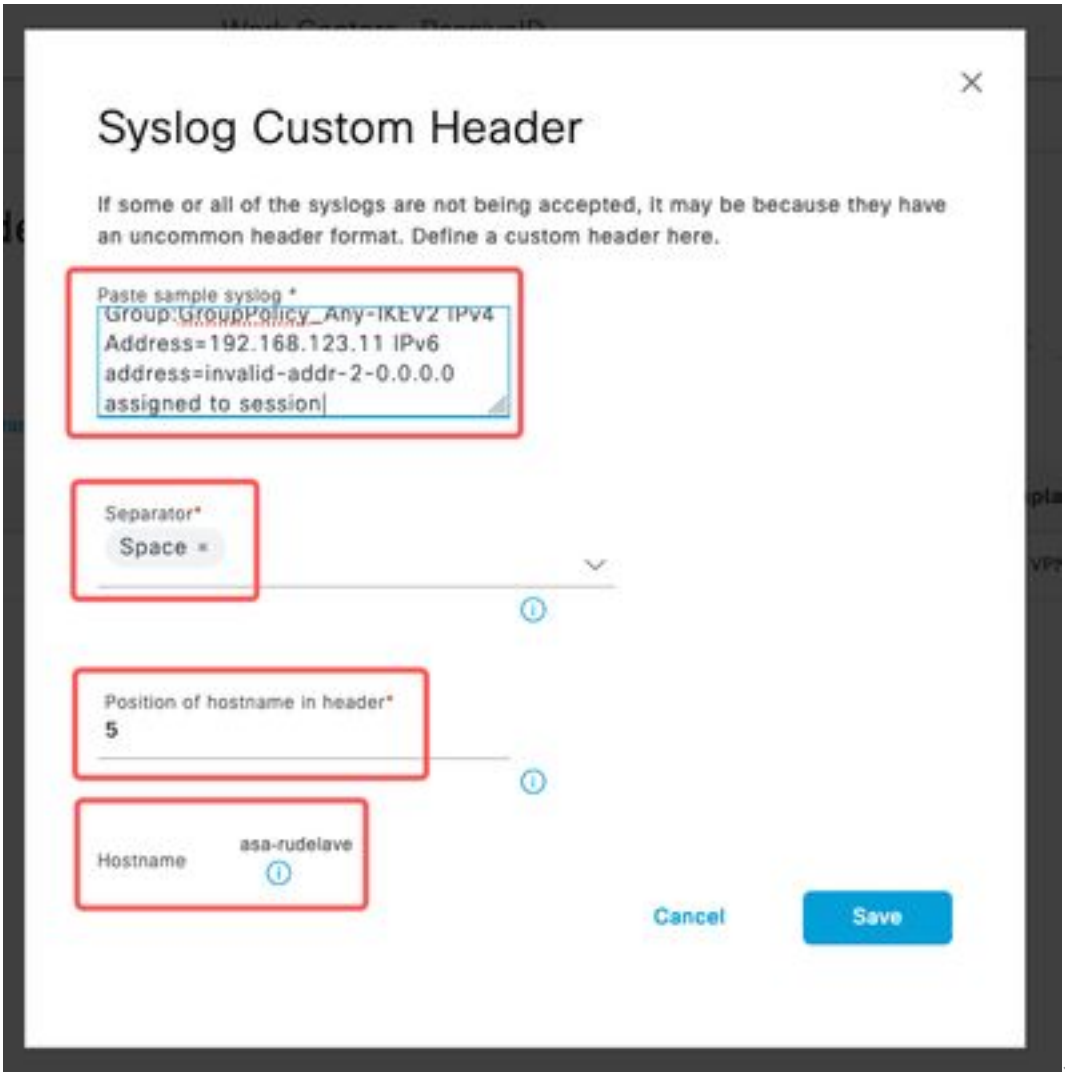
1. Work Centers(작업 센터) > **PassiveID > Providers(제공자)로 이동하고 Syslog Providers(Syslog 제공자)**를 선택하고 Add(추가)를 클릭한 **다음 정보를 완료합니다.** Save(저장)를 클릭합니다.

   **주의:** 이 경우 ISE는 ASA에서 성공한 VPN 연결로부터 syslog 메시지를 수신하지만 이 문서에서는 해당 컨피그레이션에 대해 설명하지 않습니다.




*Syslog 공급자 구성*

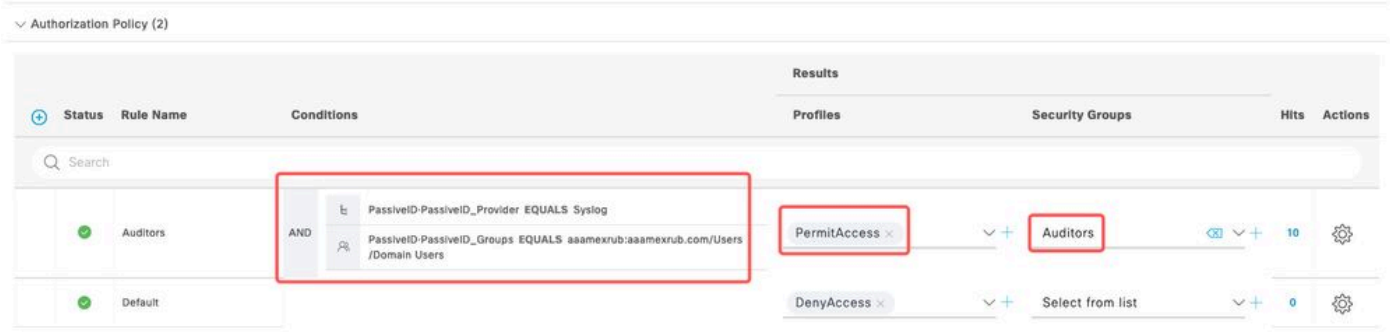
2. Custom Header(**사용자 지정 헤더)를 클릭합니다**. 샘플 syslog를 붙여넣은 다음 Separator 또는 Tab을 사용하여 디바이스 호스트 이름을 찾습니다. 올바른 경우 Hostname(호스트 이름)이 표시됩니다. Save(저장)를 클릭합니다.




*사용자 지정 헤더 구성*

4단계. 권한 부여 규칙 구성

1. **Policy > Policy Sets로** 이동합니다. 이 경우 Default(기본) 정책을 사용합니다. Default(기본) **정책을** 클릭합니다. Authorization **Policy(권한 부여 정책**)에서 새 규칙을 추가합니다. PassiveID 정책에서 ISE는 모든 공급자를 가집니다. 이 ID를 PassiveID 그룹과 결합할 수 있습니다. Permit **Access as** Profile(**액세스**를 프로필로 허용)을 선택하고 **Security Groups(보안 그룹)**에서 need it SGT(필요 SGT)를 선택합니다.

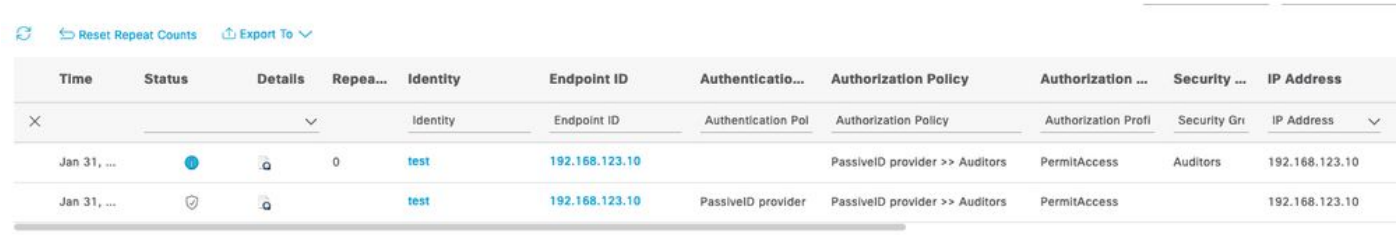



*권한 부여 규칙 구성*

# 다음을 확인합니다.

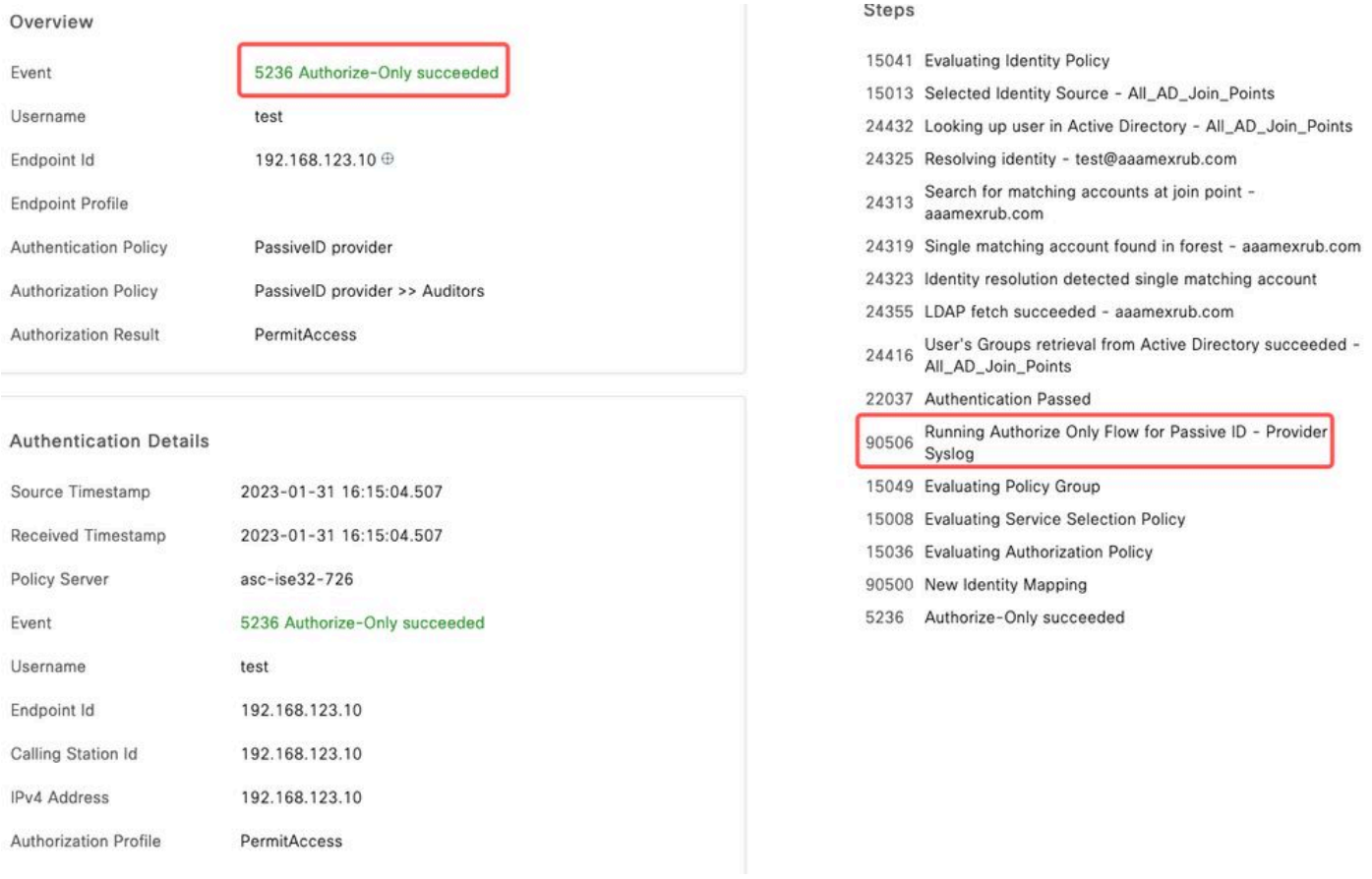
ISE가 Syslog를 수신하면 Radius Live Logs(Radius 라이브 로그)를 확인하여 권한 부여 플로우를 볼 수 있습니다. Operations(운영) **>** Radius(**반경) > Live logs(라이브 로그)로 이동합니다**.

로그에서 Authorization 이벤트를 볼 수 있습니다. 여기에는 사용자 이름, 권한 부여 정책 및 그와 연결된 보안 그룹 태그가 포함됩니다.




*Radius 라이브 로그*

자세한 내용을 확인하려면 Detail **Report**를 **클릭합니다**. SGT를 할당하기 위해 정책을 평가하는 Authorize-Only(권한 부여 전용) 흐름을 확인할 수 있습니다.




*Radius 라이브 로그 보고서*

# 문제 해결

이 경우 패시브 ID 세션과 권한 부여 플로우의 두 가지 플로우를 사용합니다. 디버그를 활성화하려면 **Operations(운영)** > Troubleshoot(문제 **해결)** > Debug Wizard(**디버그 마법사)** > Debug Log Configuration(**디버그 로그 컨피그레이션)으로 이동한 다음 ISE 노드**를 선택합니다.

PassiveID의 경우 다음 구성 요소를 DEBUG **레벨로** 활성화합니다.

- 수동 ID

수동 ID 제공자를 기반으로 이 시나리오를 확인할 파일을 검사하려면 다른 제공자에 대해 passiveid-syslog.log **파일**을 검토해야 합니다.

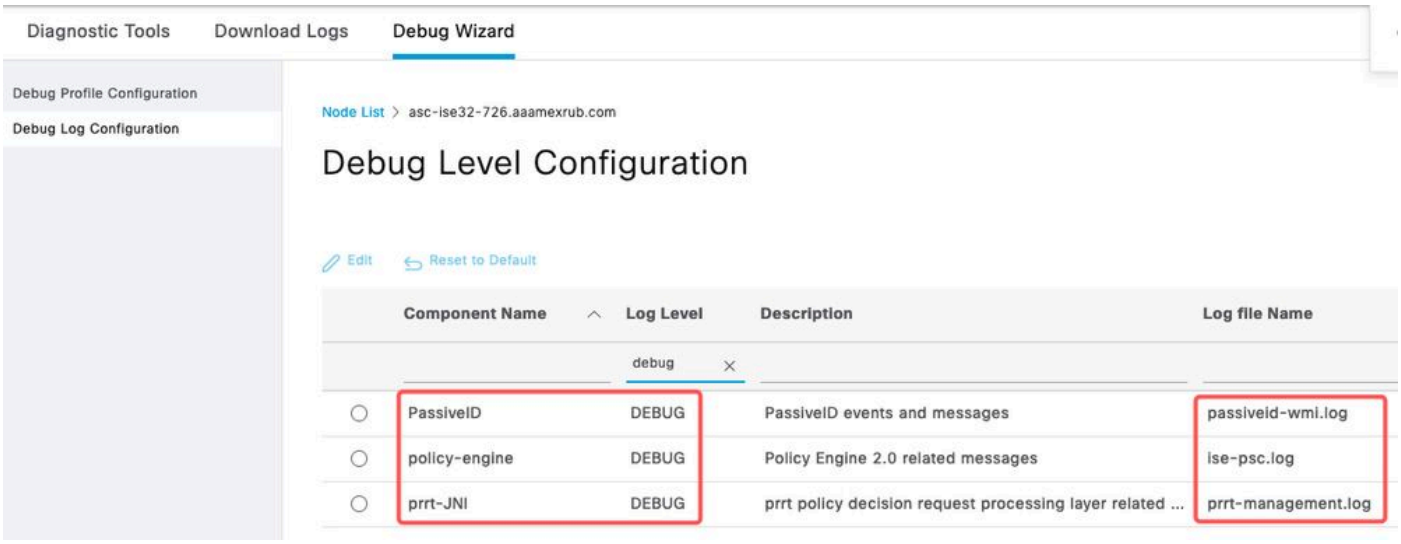
- passiveid-agent.log

- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Authorization Flow(권한 부여 플로우)에서 다음 구성 요소를 DEBUG **레벨로** 활성화합니다.

- 정책 엔진
- 포트-JNI

예:




*디버그 사용*

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.