대규모 캠퍼스 네트워크를 위한 ODBC 및 ISE DB(Custom Attribute)를 사용한 간소화된 액세스 정책

목차

소개

이 문서에서는 기능 및 보안 집행을 저하시키지 않는 대규모 캠퍼스 구축에 대해 설명합니다. Cisco의 엔드포인트 보안 솔루션인 ISE(Identity Services Engine)는 외부 ID 소스와의 통합을 통해 이러한 요구 사항을 해결합니다.

50개가 넘는 지리적 위치, 4000개가 넘는 다양한 사용자 프로필, 600,000개 이상의 엔드포인트를 보유한 대규모 네트워크의 경우, 기존의 IBN 솔루션은 모든 기능을 확장하든 기능 이상의 다른 관점에서 바라봐야 합니다. 오늘날의 기존 대규모 네트워크에서 IBN(Intent-Based Network) 솔루션을 사용하려면 기능뿐 아니라 확장성과 관리 용이성에 대한 추가적인 관심이 필요합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Dot1x/MAB 인증
- Cisco ISE(Identity Service Engine)
- Cisco TrustSec(CTS)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

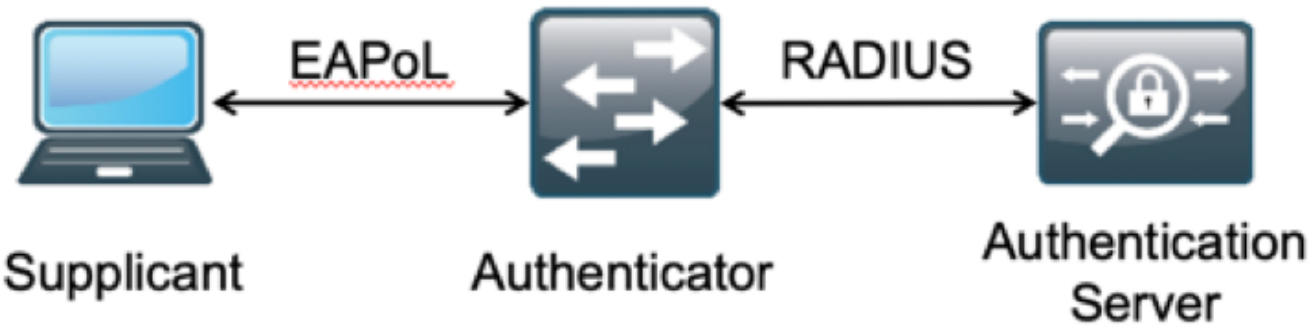
- Cisco ISE(Identity Services Engine) 버전 2.6 패치 2 및 버전 3.0
- Windows AD(Active Directory) Server 2008 릴리스 2
- Microsoft SQL Server 2012

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

배경 정보

IBN(Identity Based Network) 솔루션의 기본 요소는 AAA(Supplicant, Authenticator, Authentication) 서버입니다. 서 플리 컨 트는 네트워크 액세스에 대한 문제 발생 시 자격 증명을 제공 하는 엔드 포인트의 상담원 입니다. 인증자 또는 NAS(Network Access Server)는 액세스 레이어로, 자격 증명을 AAA 서버로 전송하는 네트워크 스위치 및 WLC로 구성됩니다. 인증 서버는 ID 저장소에 대해 사용자 인증 요청을 검증하고 access-accept 또는 access-reject를 사용하여 권한을 부여합니다. ID 저장소는 AAA 서버 내에 있거나 외부 전용 서버에 있을 수 있습니다.

이 그림에서는 기본 IBN 요소를 보여 줍니다.



RADIUS는 인증 및 권한 부여가 결합된 UDP(User Datagram Protocol) 기반 프로토콜입니다. Cisco의 엔터프라이즈 캠퍼스용 IBN 솔루션에서 ISE의 PSN(Policy Service Node) 페르소나는 엔터프라이즈 ID 저장소에 대해 엔드포인트를 인증하고 조건에 따라 권한을 부여하는 AAA 서버 역할을 합니다.

Cisco ISE에서 인증 및 권한 부여 정책은 이러한 요구 사항을 충족하도록 구성됩니다. 인증 정책은 유선 또는 무선 미디어 유형과 사용자 검증을 위한 EAP 프로토콜로 구성됩니다. 권한 부여 정책은 VLAN 또는 다운로드 가능한 ACL 또는 SGT(Secure Group Tag)일 수 있는 네트워크 액세스 결과와 일치하는 다양한 엔드포인트에 대한 기준을 정의하는 조건으로 구성됩니다. 이는 ISE에서 구성할

수 있는 정책의 최대 확장 번호입니다.

이 표는 Cisco ISE 정책 확장을 보여줍니다.

속성	척도 수
최대 인증 규칙 수	1000(정책 설정 모드)
최대 권한 부여 규칙 수	3,000(정책 설정 모드) 3,200개의 Authz 프로필

기술 트렌드

세그멘테이션은 오늘날의 엔터프라이즈 네트워크에서 실제 에지 네트워크가 필요 없는 핵심 보안 요소 중 하나가 되었습니다. 엔드포인트는 내부 네트워크와 외부 네트워크 사이에서 로밍할 수 있습니다. 세그멘테이션은 특정 세그먼트에 대한 보안 공격을 억제하여 네트워크 전반으로 확장하는 데 도움이 됩니다. Cisco ISE의 TrustSec을 통해 제공되는 오늘날의 SDA(Software-Defined Access) 솔루션은 고객의 비즈니스 모델에 따라 세분화하여 VLAN 또는 IP 서브넷과 같은 네트워크 요소에 의존하지 않도록 합니다.

문제

서로 다른 엔드포인트 프로파일이 500개 이상인 대규모 엔터프라이즈 네트워크에 대한 ISE 정책 컨피그레이션에서는 권한 부여 정책의 수가 관리 불가능한 지점으로 증가할 수 있습니다. Cisco ISE가 이러한 사용자 프로필의 볼륨에 맞추기 위해 전용 권한 부여 조건을 지원하더라도 관리자가 이러한 많은 수의 정책을 관리해야 하는 문제가 있습니다.

또한 고객은 관리 오버헤드를 방지하기 위해 전용 정책 대신 공통 권한 부여 정책을 필요로 할 수 있으며 해당 기준에 따라 엔드포인트에 대해 차별화된 네트워크 액세스를 가질 수 있습니다.

예를 들어, AD(Active Directory)가 있는 엔터프라이즈 네트워크**를** 신뢰할 **수 있는 소스로** 간주하고 엔드포인트의 고유한 차별화 요소는 AD의 특성 중 하나입니다. 그러한 경우, 기존의 정책 컨피그레이션 방식은 각 고유 엔드포인트 프로파일에 대해 더 많은 권한 부여 정책을 갖습니다.

이 방법에서 각 엔드포인트 프로파일은 domain.com의 AD 특성으로 구별됩니다. 따라서 전용 권한 부여 정책을 구성해야 합니다.

이 표에서는 기존 AuthZ 정책을 보여줍니다.

ABC-정책	AnyConnect가 User-AND-Machine-Both-Passed인 경우 및 AD-Group이 domain.com/groups/ABC인 경우 그런 다음 SGT:C2S-ABC 및 VLAN:1021
DEF-정책	AnyConnect가 User-AND-Machine-Both-Passed인 경우 및 AD-Group이 domain.com/groups/DEF인 경우 그런 다음 SGT:C2S-DEF 및 VLAN:1022
GHI 정책	AnyConnect가 User-AND-Machine-Both-Passed인 경우 및 AD-Group이 domain.com/groups/GHI인 경우 그런 다음

	SGT:C2S-GHI 및 VLAN:1023
	AnyConnect가 User-AND-Machine-Both-Passed인 경우
	및
XYZ 정책	AD-Group이 domain.com/groups/XYZ인 경우
	그런 다음
	SGT:C2S-XYZ 및 VLAN:1024

제안 솔루션

Cisco ISE에서 지원되는 최대 확장 가능한 권한 부여 정책 수에 대한 보안 침해를 피하기 위해, 제안된 솔루션은 특성에서 가져온 권한 부여 결과와 함께 각 엔드 포인트를 권한 부여하는 외부 DB를 사용 하는 것입니다. 예를 들어 AD가 권한 부여를 위한 외부 DB로 사용되는 경우, 사용하지 않는 사용자 특성(예: 부서 또는 Pin 코드)을 참조하여 SGT 또는 VLAN과 매핑된 권한 부여 결과를 제공할 수 있습니다.

이는 Cisco ISE를 외부 DB와 통합하거나 사용자 지정 특성으로 구성된 ISE의 내부 DB 내에서 구현할 수 있습니다. 이 섹션에서는 다음 2가지 시나리오의 구축에 대해 설명합니다.

> **참고:** 두 옵션 모두에서 DB는 **user-id를** 포함하지만 DOT1X **엔드포인트**의 비밀번호는 포함하지 않습니다. DB는 **권한 부여** 지점으로만 사용됩니다. 인증은 여전히 대부분의 경우 AD(Active Directory) 서버에 있는 고객의 ID 저장소로 유지될 수 있습니다.

외부 DB를 사용한 컨피그레이션

Cisco ISE는 엔드포인트 자격 증명 검증을 위해 외부 DB와 통합됩니다.

이 표에서는 검증된 외부 ID 소스를 보여줍니다.

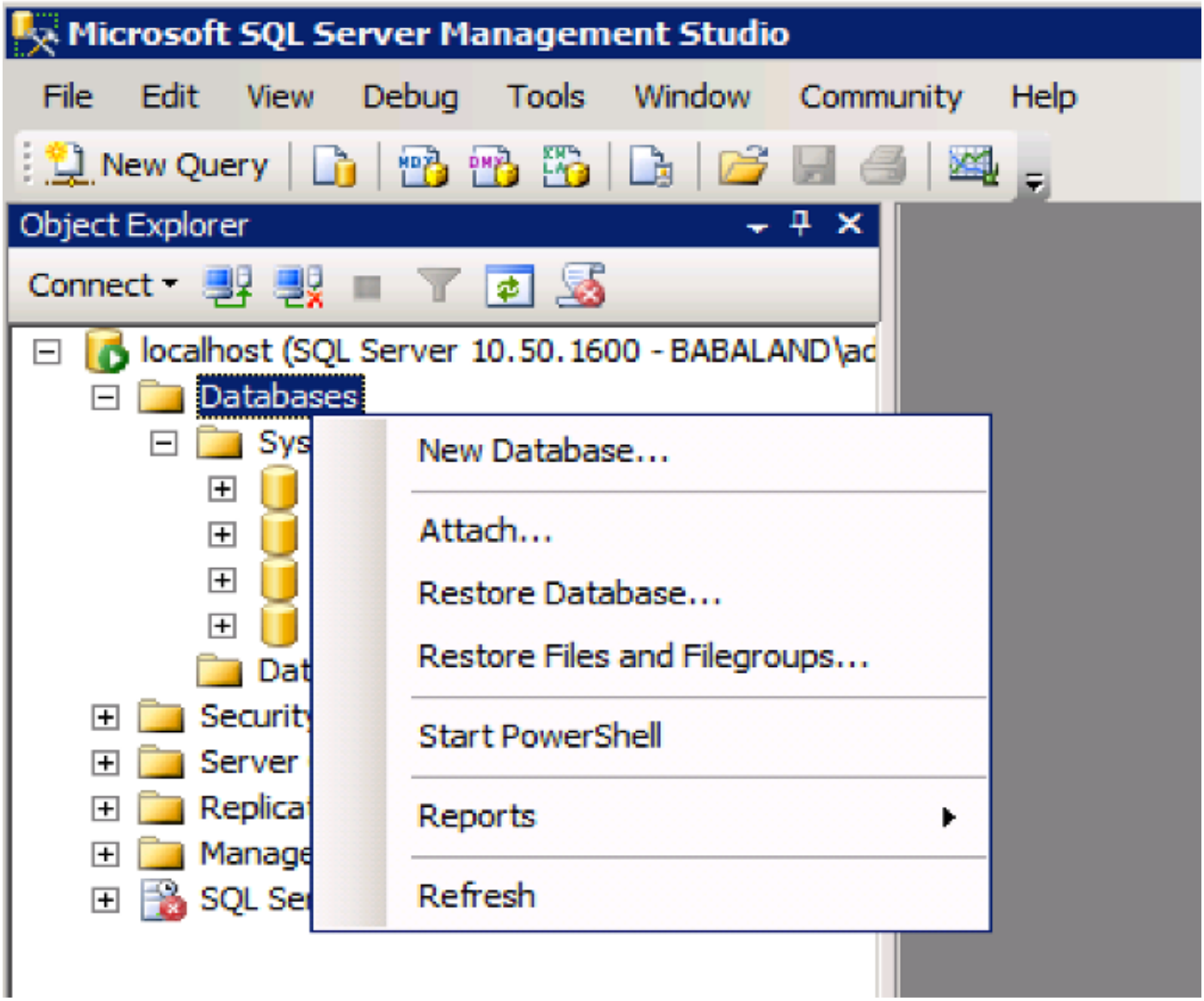
외부 ID 소스	OS/버전
액티브 디렉토리	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—
LDAP 서버	
SunONE LDAP 디렉토리 서버	버전 5.2
OpenLDAP 디렉토리 서버	버전 2.4.23
모든 LDAP v3 호환 서버	—
토큰 서버	
RSA ACE/서버	6.x 시리즈
RSA 인증 관리자	7.x 및 8.x 시리즈
모든 RADIUS RFC 2865 호환 토큰 서버	—
SAML(Security Assertion Markup Language) SSO(Single Sign-On)	
Microsoft Azure	—
OAM(Oracle Access Manager)	버전 11.1.2.2.0
OIF(Oracle Identity Federation)	버전 11.1.1.2.0
PingFederate 서버	버전 6.10.0.4
PingOne 클라우드	—

보안 인증	8.1.1
모든 SAMLv2 호환 ID 공급자	—
ODBC(Open Database Connectivity) ID 소스	
Microsoft SQL Server(MS SQL)	Microsoft SQL Server 2012 Enterprise Edition 릴리스
오라클	12.1.0.2.0
PostgreSQL	9
사이베이스	16
마이sql	6.3
소셜 로그인(게스트 사용자 계정용)	
페이스북	—

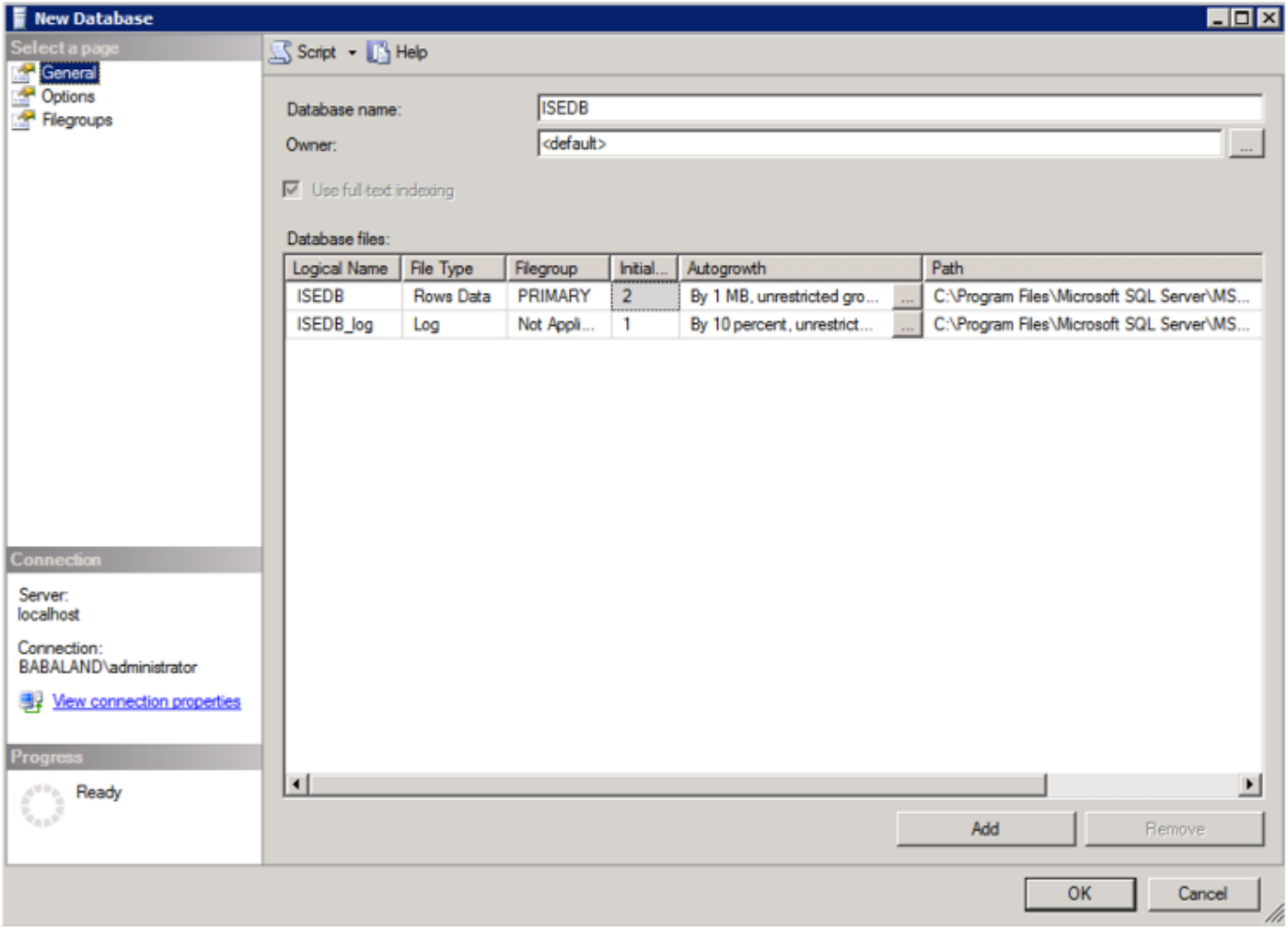
ODBC 샘플 컨피그레이션

이 컨피그레이션은 Microsoft SQL에서 솔루션을 빌드하기 위해 수행됩니다.

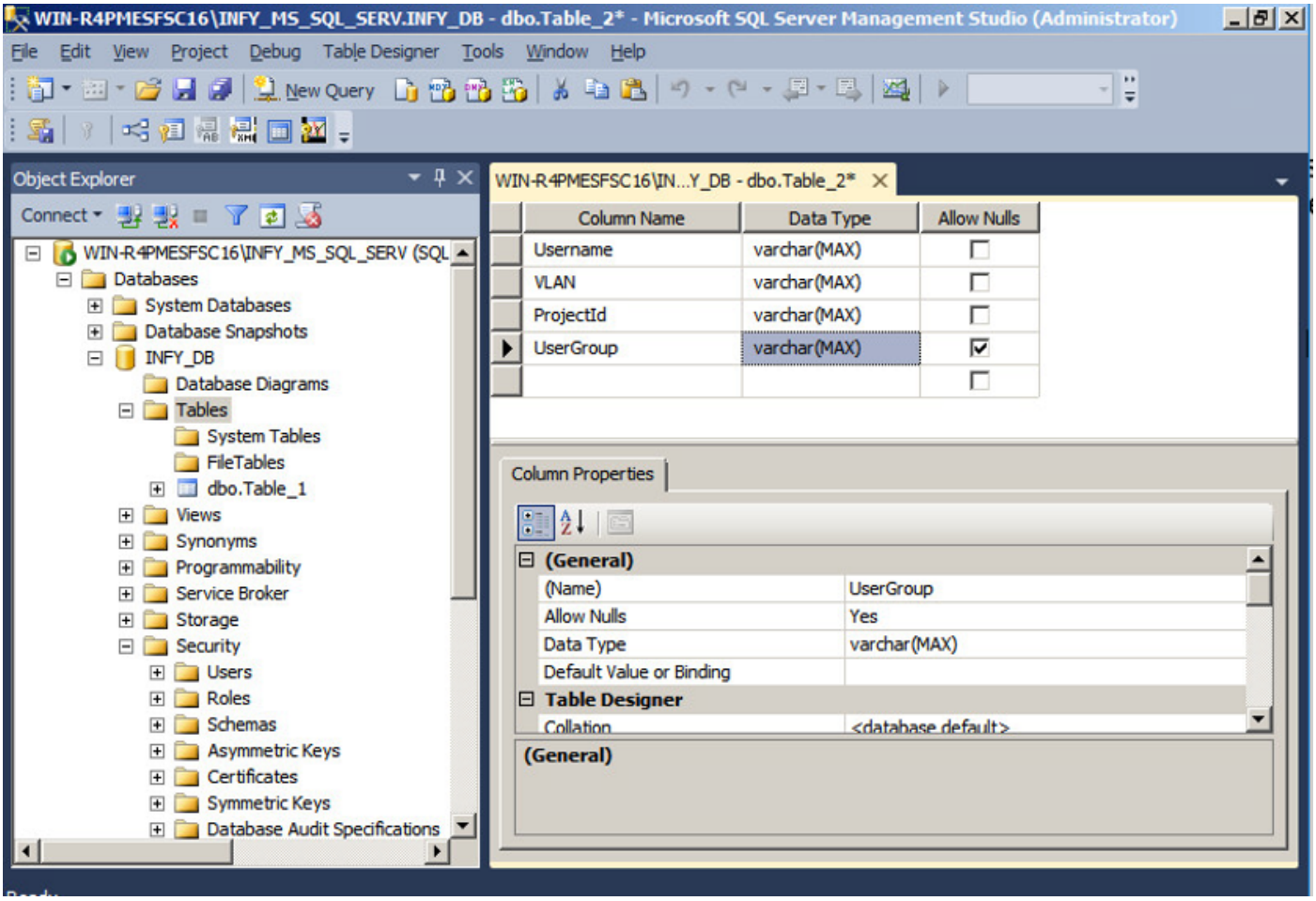
1단계. SQL Server Management Studio(**시작 메뉴 > Microsoft SQL Server**)를 열어 데이터베이스를 만듭니다.



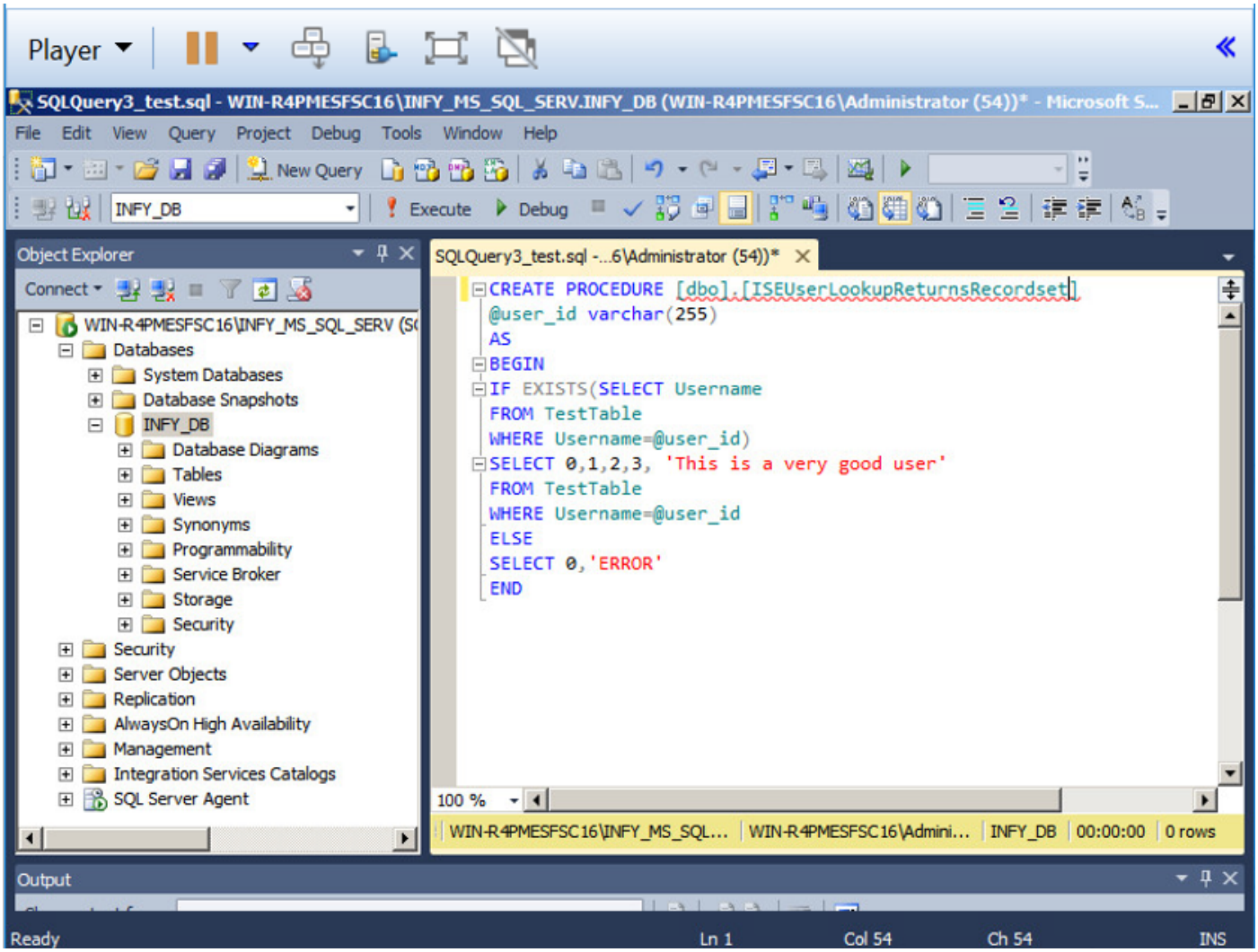
2단계. 이름을 입력하고 데이터베이스를 만듭니다.



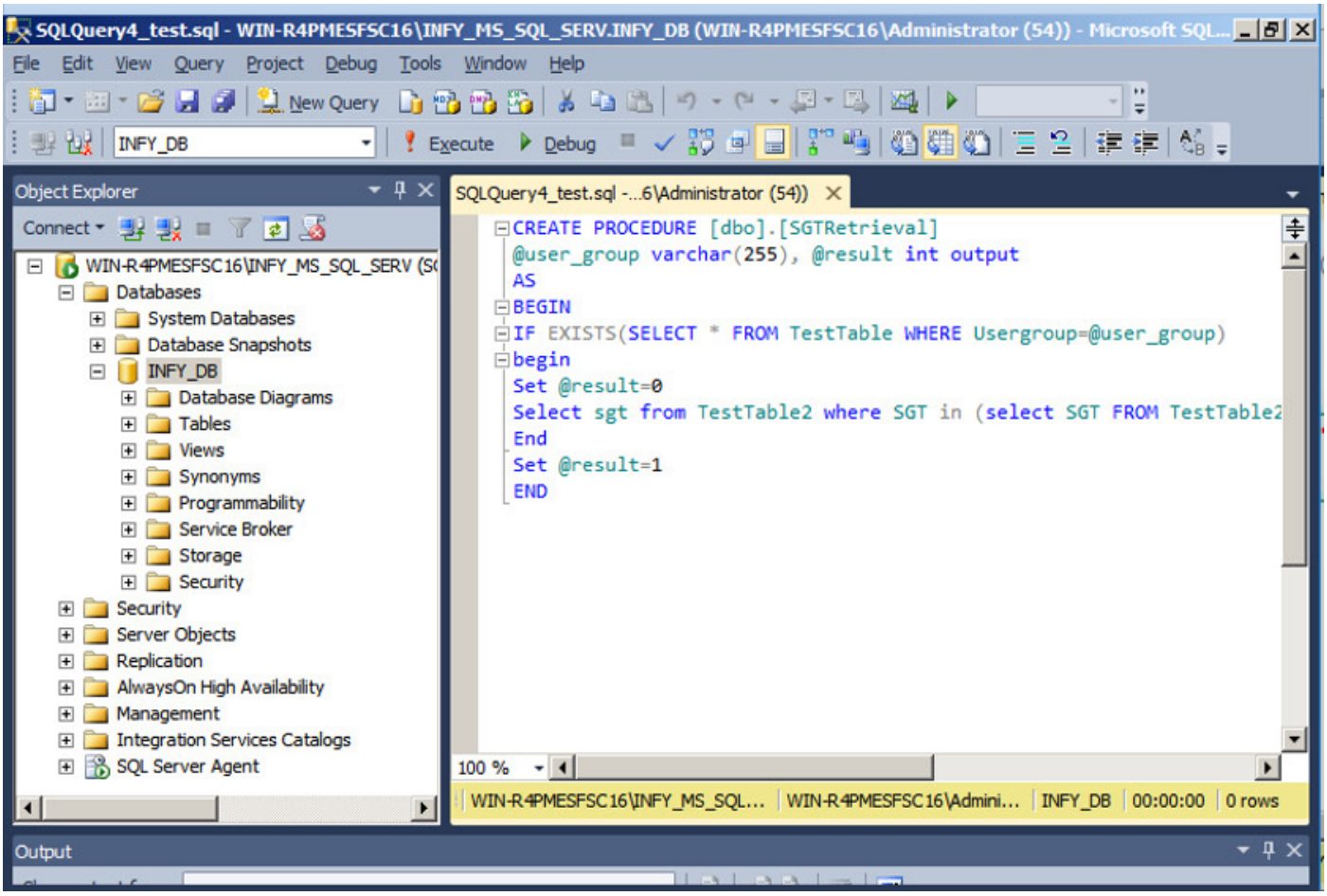
3단계. 권한 부여를 위해 엔드포인트에 대한 매개 변수로 필요한 열이 포함된 새 테이블을 생성합니다.



4단계. 사용자 **이름**이 있는지 확인하는 절차를 생성합니다.



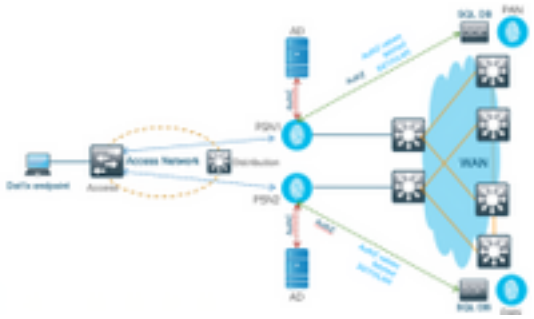
5단계. 테이블에서 속성(SGT)을 가져오는 절차를 생성합니다.

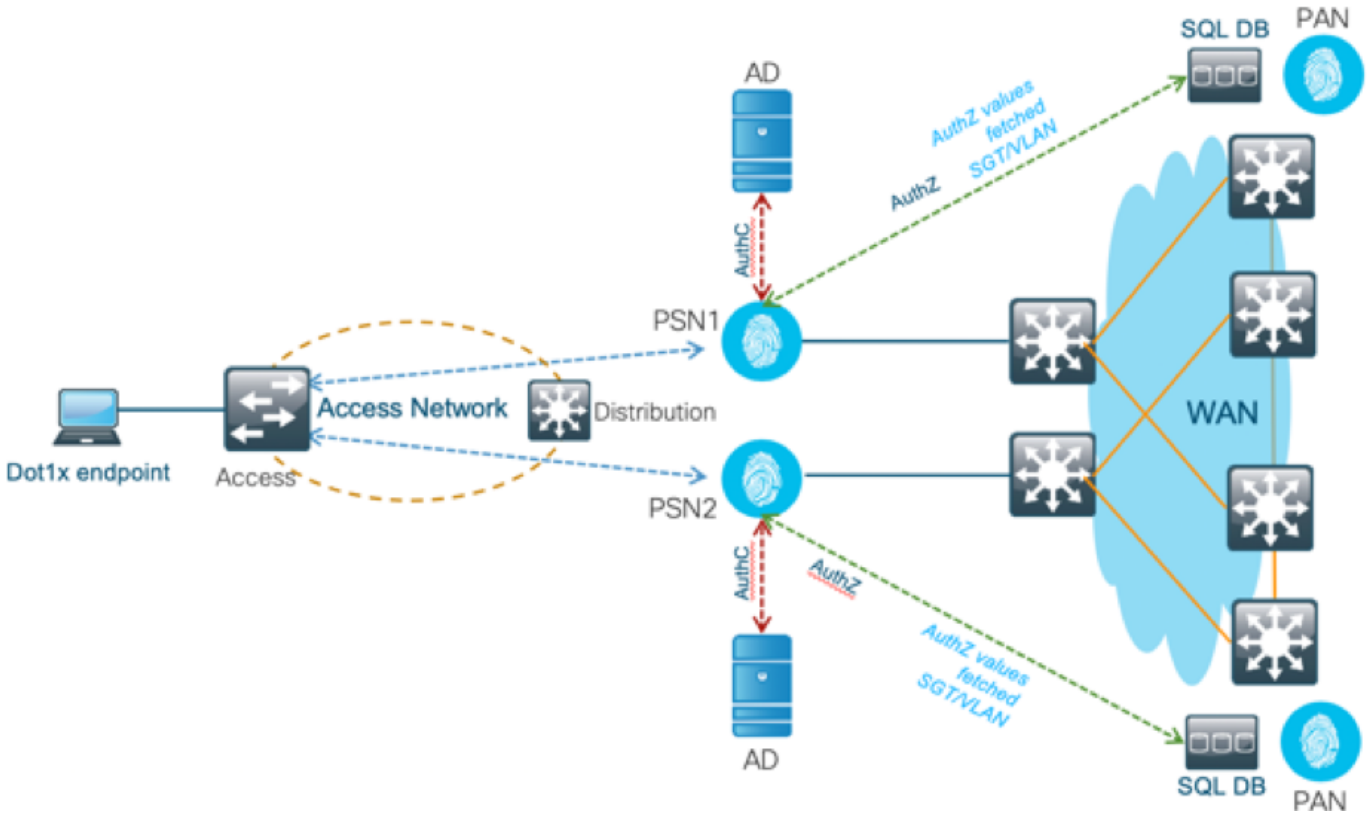


이 문서에서는 Cisco ISE를 Microsoft SQL 솔루션과 통합하여 대기업 네트워크의 인증 범위 요구 사항을 충족합니다.

솔루션 워크플로(ISE 2.7 이하)

이 솔루션에서 Cisco ISE는 AD(Active Directory) 및 Microsoft SQL과 통합됩니다. AD는 권한 부여를 위해 인증 ID 저장소 및 MS SQL로 사용됩니다. 인증 프로세스 중에 NAD(Network Access Device)는 사용자 자격 증명을 IBN 솔루션의 AAA 서버인 PSN에 전달합니다. PSN은 Active Directory ID 저장소로 엔드포인트 자격 증명을 검증하고 사용자를 인증합니다. 권한 부여 정책은 MS SQL DB를 참조하여 **사용자 ID**가 참조로 사용되는 SGT/VLAN**과** 같은 권한 부여된 결과를 가져옵니다.





장점

이 솔루션은 다음과 같은 장점이 있어 유연합니다.

- Cisco ISE는 외부 DB가 제공하는 모든 가능한 추가 기능을 활용할 수 있습니다.
- 이 솔루션은 Cisco ISE 확장 제한에 의존하지 않습니다.

단점

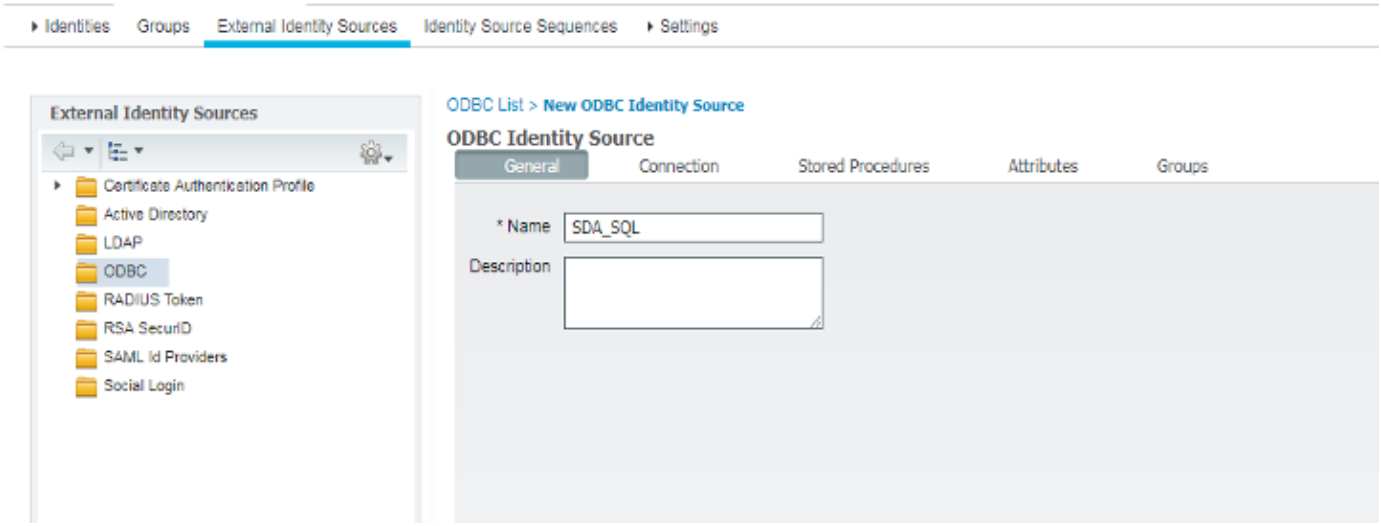
이 솔루션의 단점은 다음과 같습니다.

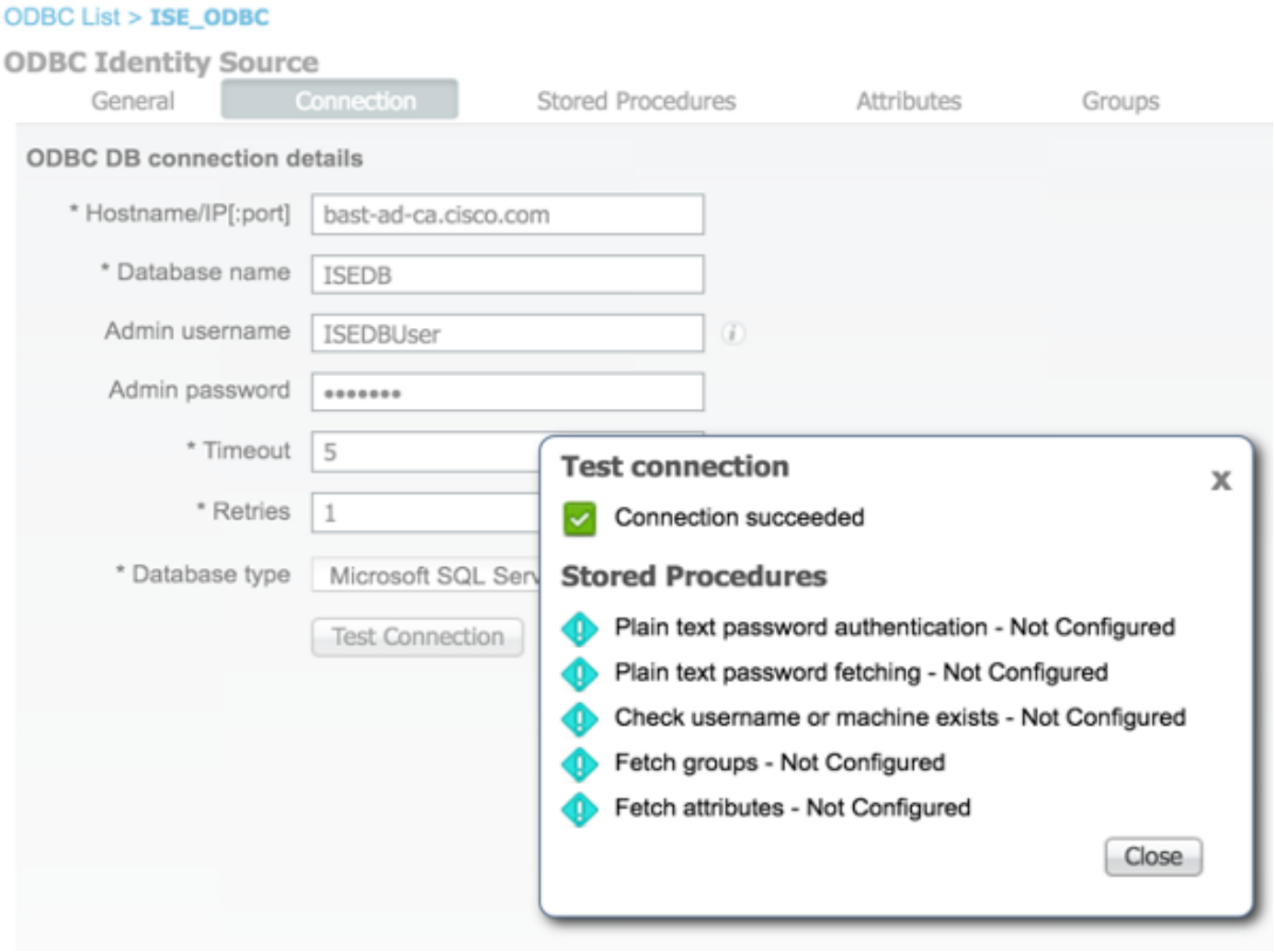
- 외부 DB를 엔드포인트 자격 증명으로 채우려면 추가 프로그래밍이 필요합니다.
- 외부 DB가 PSN처럼 로컬에 없는 경우 이 솔루션은 WAN에 따라 엔드포인트 AAA 데이터 흐름에서 3번째 실패 지점이 됩니다.
- 외부 DB 프로세스 및 절차를 유지 관리하기 위한 추가 지식이 필요합니다.
- DB에 대한 user-id의 수동 컨피그레이션으로 인한 오류를 고려해야 합니다.

외부 DB 샘플 컨피그레이션

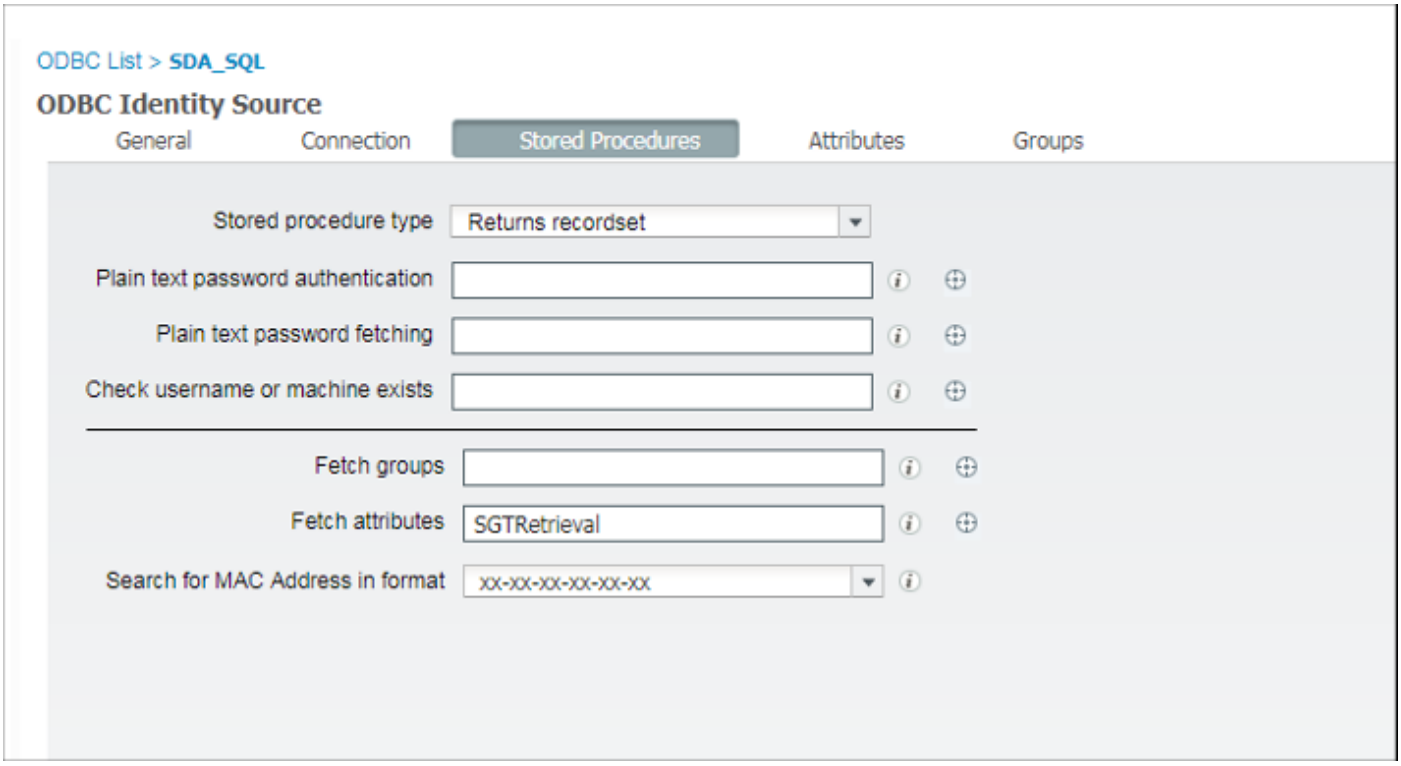
이 문서에서는 Microsoft SQL이 인증 지점으로 사용되는 외부 DB로 표시됩니다.

1단계. Administration(관리) > External Identity Source(외부 ID **소스) > ODBC 메뉴**에서 Cisco ISE의 ODBC Identity **Store(ODBC ID 저장소)**를 생성하고 연결을 테스트합니다.

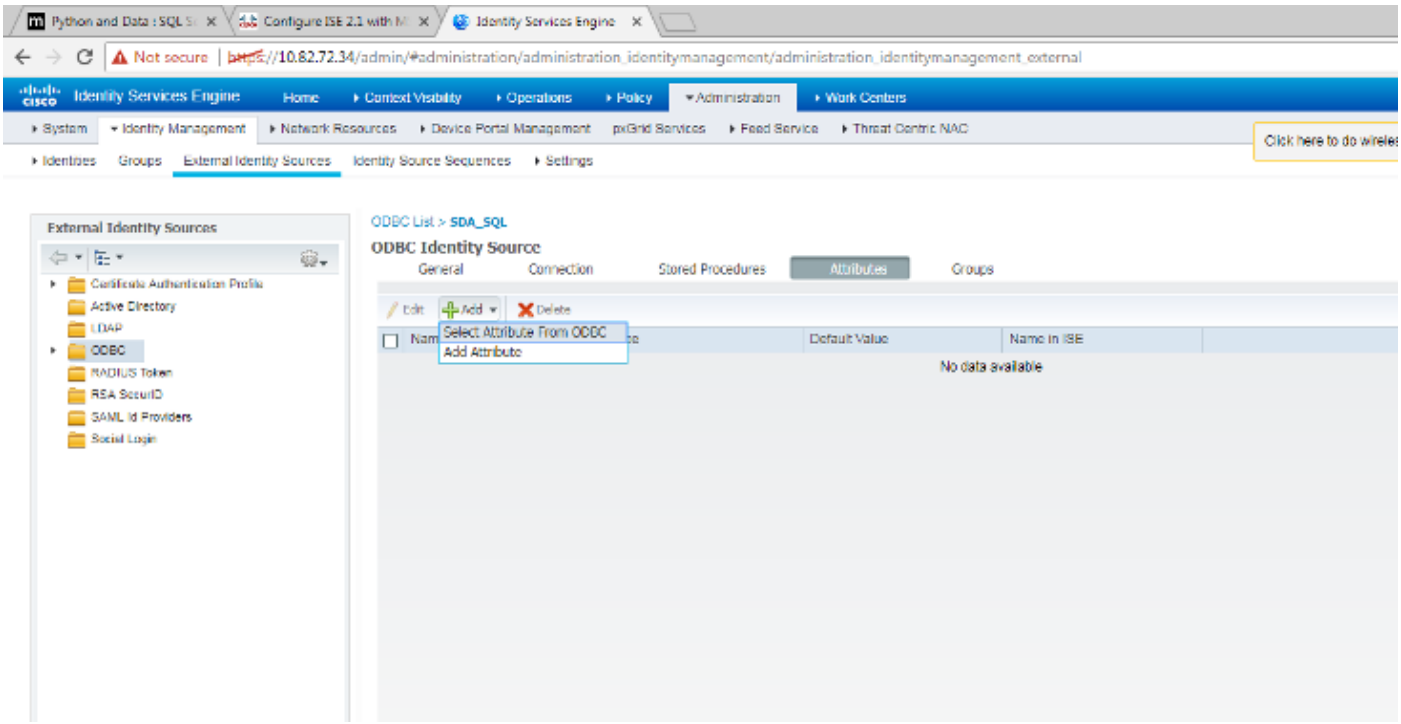


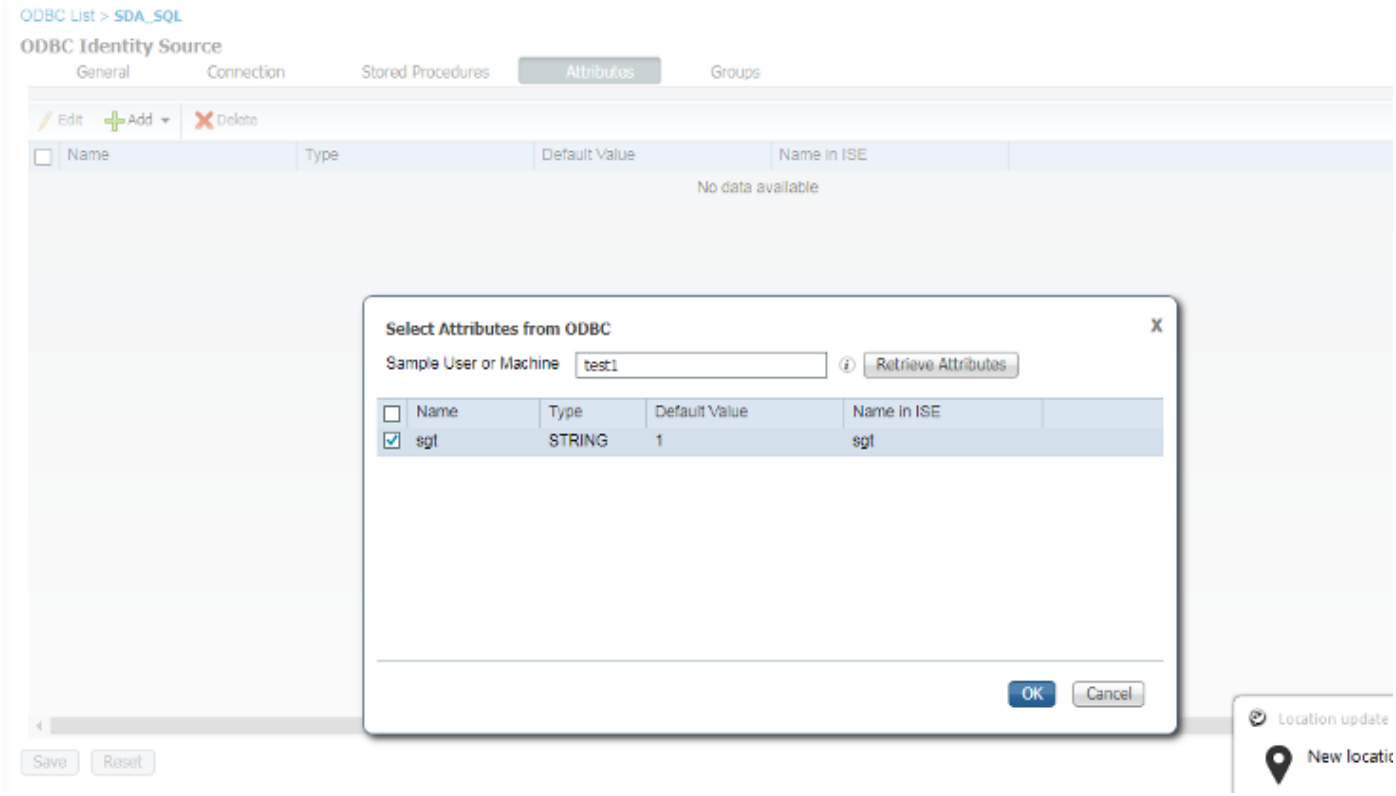


2단계. ODBC 페이지의 Stored Procedures(저장 프로시저) 탭으로 이동하여 Cisco ISE에서 생성된 프로시저를 구성합니다.

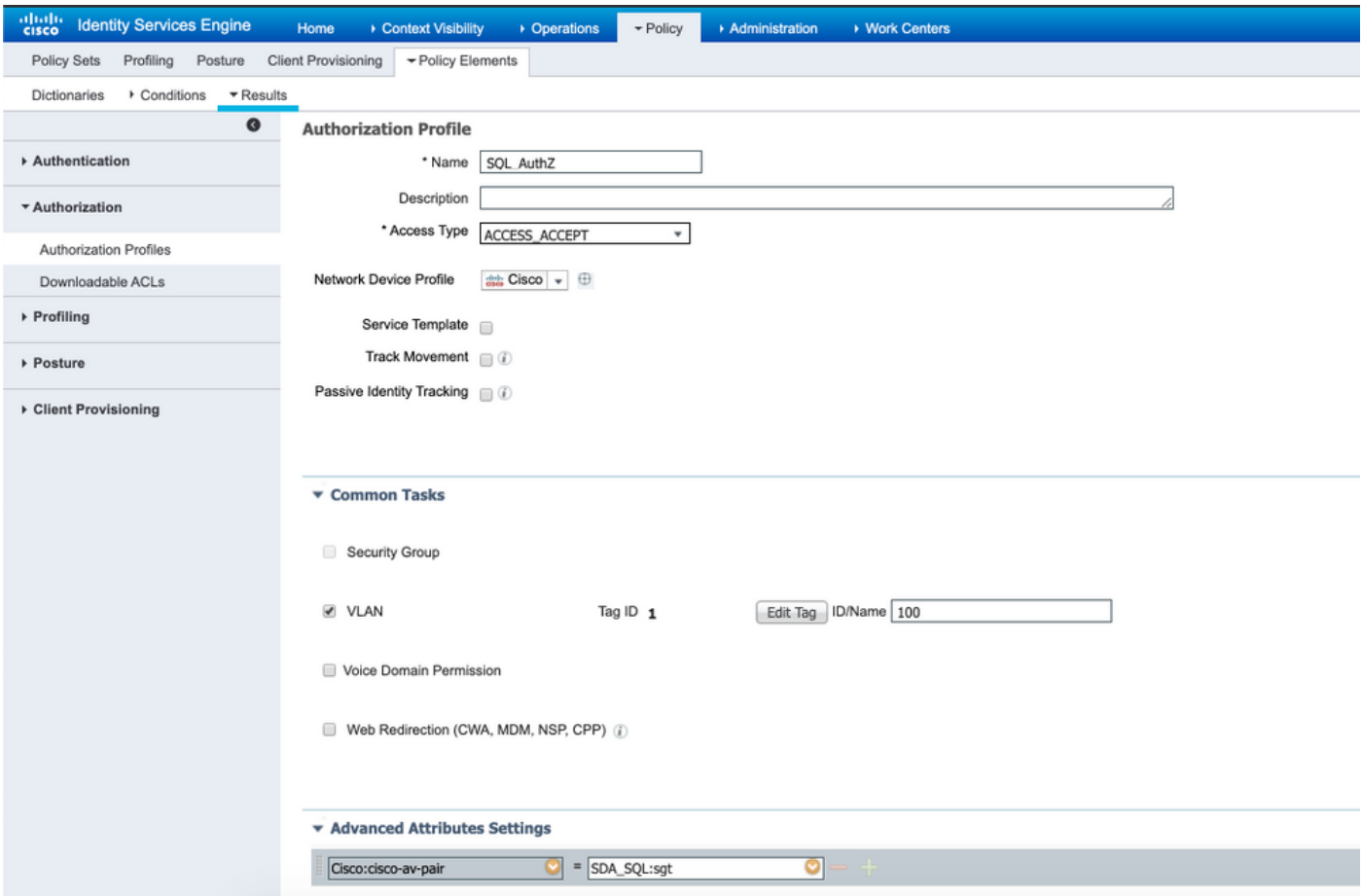


3단계. 확인을 위해 ODBC ID 소스에서 사용자 ID의 특성을 가져옵니다.



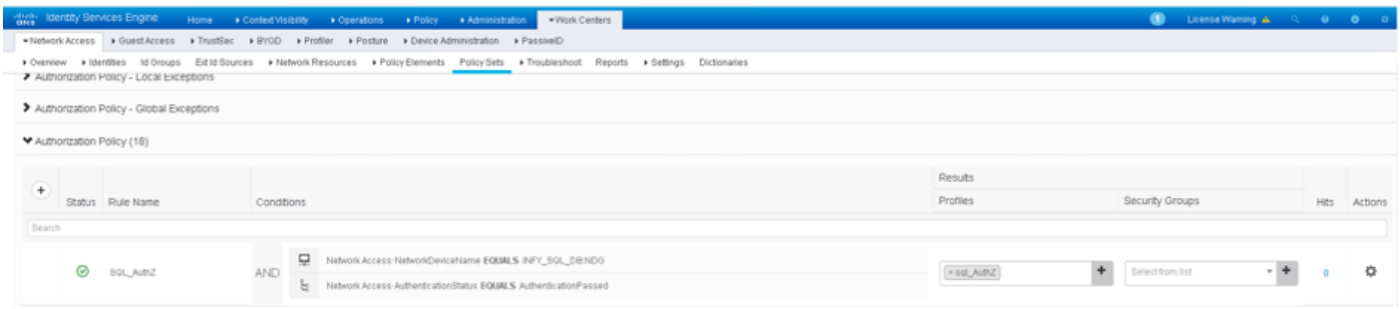


4단계. **권한 부여 프로파일**을 생성하고 구성합니다. Cisco ISE에서 **Policy(정책) > Results(결과) > Authorization profile(권한 부여 프로파일) > Advance Attributes Settings(고급 특성 설정)**로 이동하여 특성을 **Cisco:cisco-av-pair**로 선택합니다**. 값을** <name of ODBC database>:sgt로 선택한 다음 저장합니다.

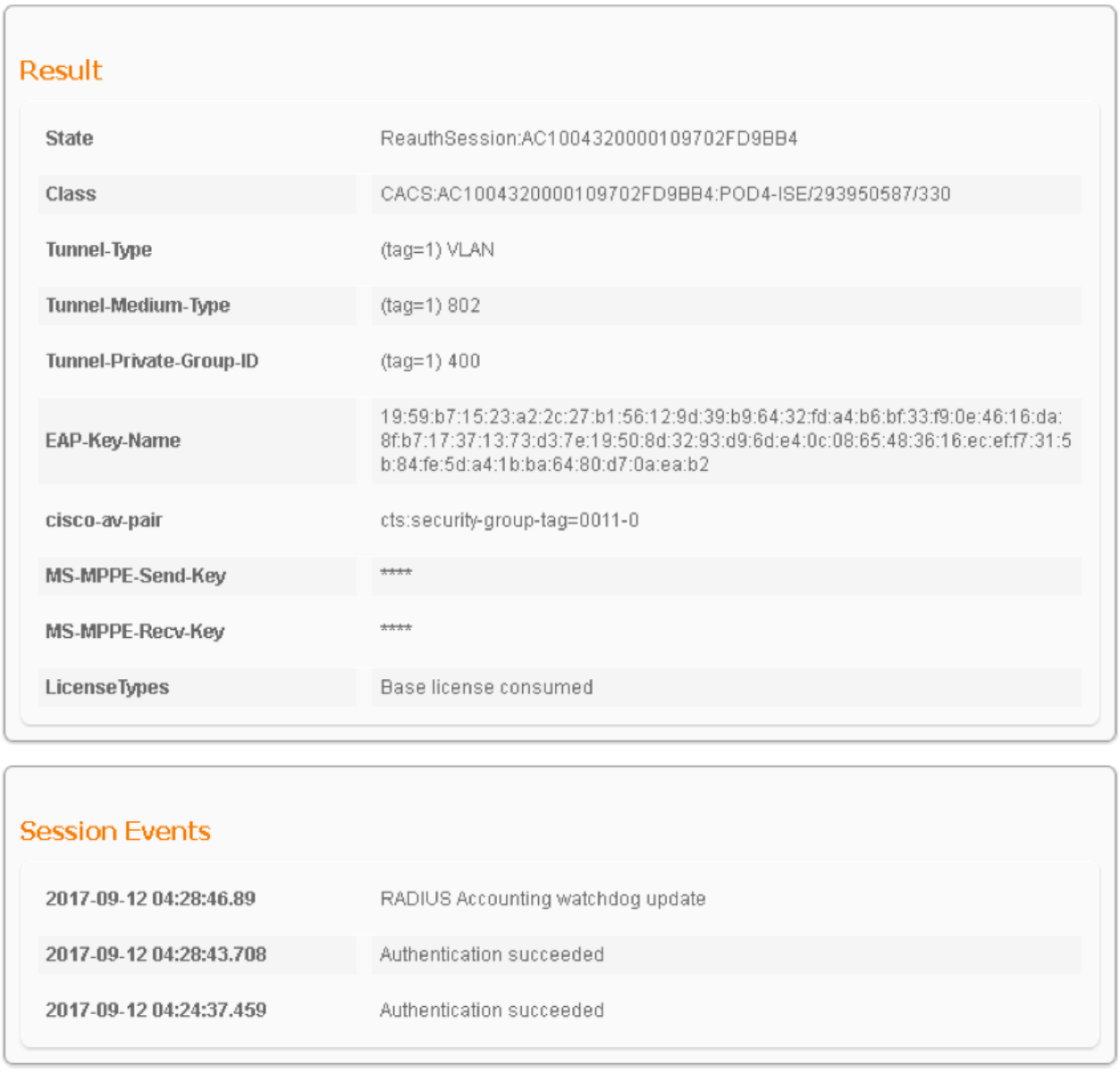


5단계. 권한 부여 **정책**을 생성하고 구성합니다. Cisco ISE에서 **Policy(정책) > Policy sets(정책 집합) > Authorization Policy(권한 부여 정책) > Add(추가)로 이동합니다.** ID 소스가 SQL 서버인 경우 조

건을 입력합니다. Result(결과) 프로파일을 이전에 생성한 Authorization(권한 부여) 프로파일로 선택합니다.



6단계. 사용자를 인증하고 권한을 부여하면 확인을 위해 로그에 사용자에게 할당된 sgt가 포함됩니다.



Result

State	ReauthSession:AC1004320000109702FD9BB4
Class	CACS:AC1004320000109702FD9BB4:POD4-ISE/293950587/330
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 400
EAP-Key-Name	19:59:b7:15:23:a2:2c:27:b1:56:12:9d:39:b9:64:32:fd:a4:b6:bf:33:f9:0e:46:16:da:8f:b7:17:37:13:73:d3:7e:19:50:8d:32:93:d9:6d:e4:0c:08:65:48:36:16:ec:ef:f7:31:5b:84:fe:5d:a4:1b:ba:64:80:d7:0a:ea:b2
cisco-av-pair	cts:security-group-tag=0011-0
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

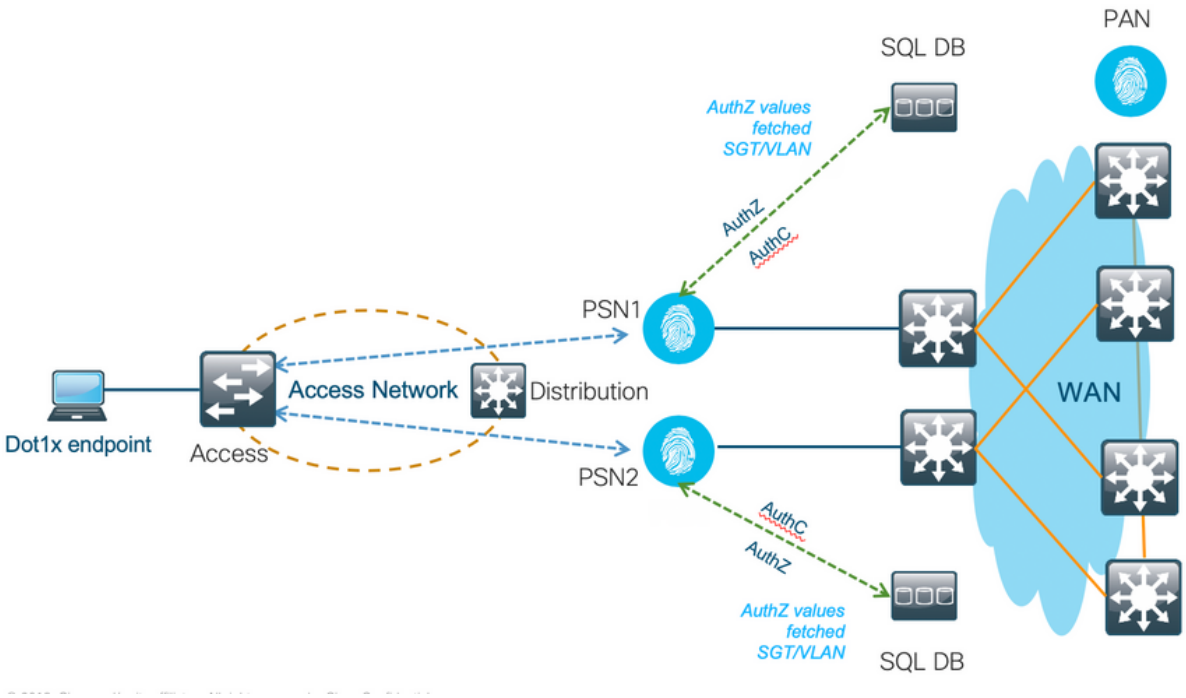
Session Events

2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

솔루션 워크플로(Post ISE 2.7)

ISE 2.7 이후의 권한 부여 특성은 ODBC에서 가져올 수 있으며(예: Vlan, SGT, ACL) 이러한 특성은 정책에서 사용할 수 있습니다.

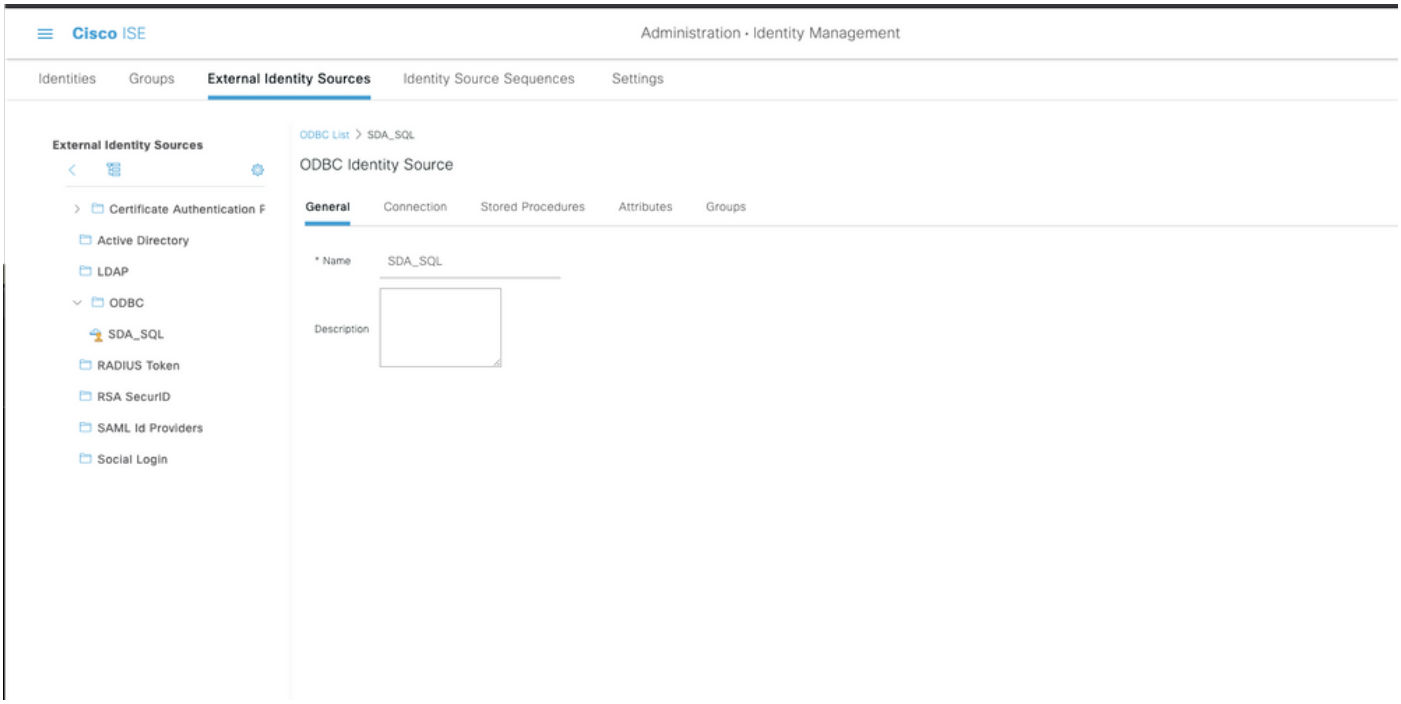
이 솔루션에서 Cisco ISE는 Microsoft SQL과 통합됩니다. MS SQL은 인증과 권한 부여를 위한 ID 저장소로 사용됩니다. 엔드포인트의 자격 증명이 PSN에 제공되면 MS SQL DB에 대해 자격 증명을 검증합니다. 권한 부여 정책은 MS SQL DB를 참조하여 **사용자 ID**가 참조로 사용되는 SGT/VLAN**과** 같은 **권한** 있는 결과를 가져옵니다.



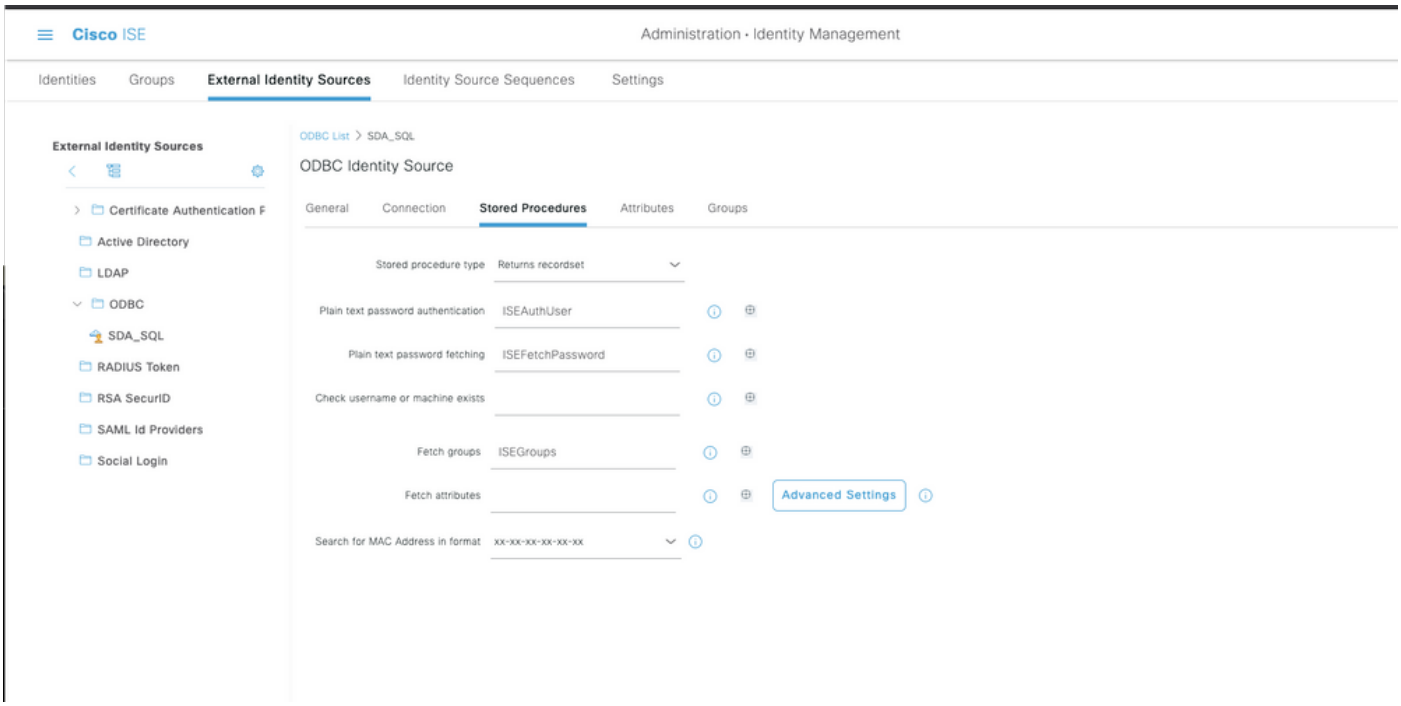
외부 DB 샘플 컨피그레이션

사용자 이름, 비밀번호, VLAN ID 및 SGT와 함께 MS SQL DB를 생성하려면 이 문서의 앞부분에 제공된 절차를 수행합니다.

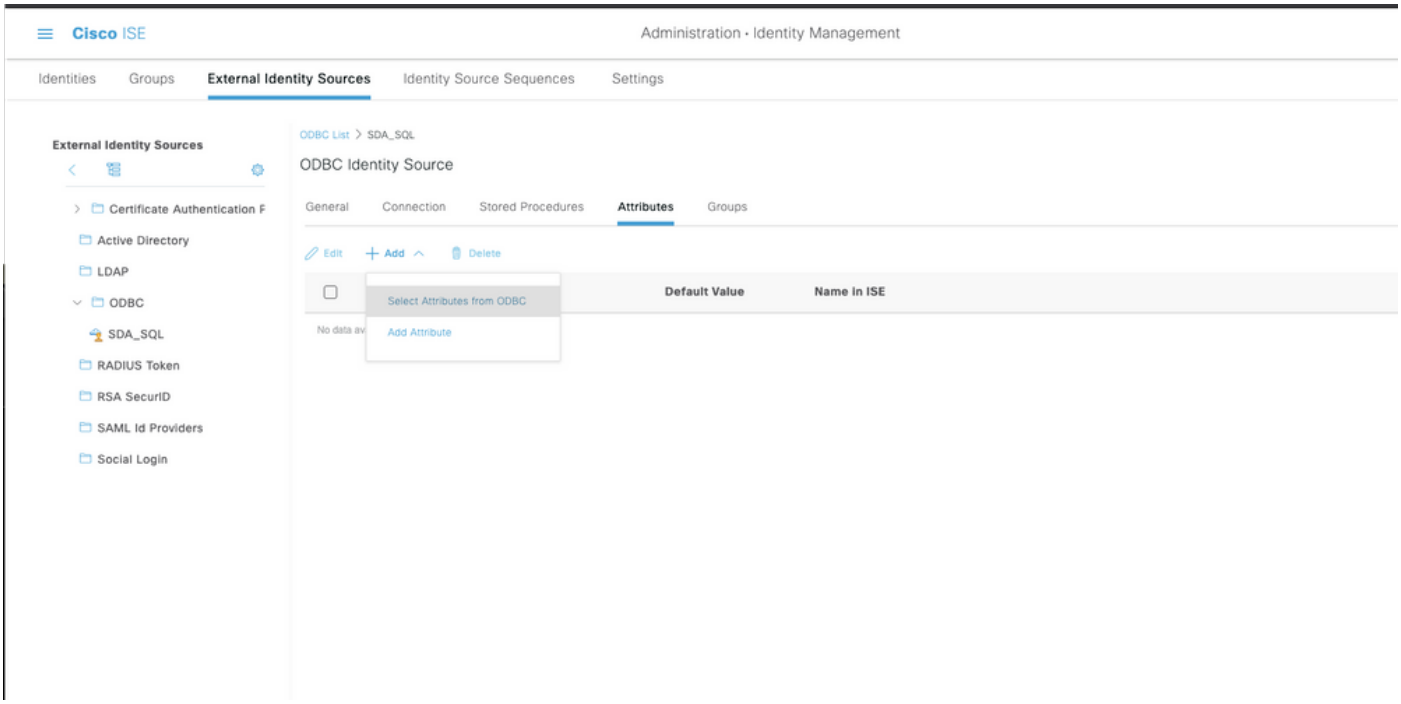
1단계. Administration(관리) > External Identity Source(외부 ID 소스) > ODBC 메뉴에서 Cisco ISE**에 ODBC ID 저장소**를 생성하고 연결을 테스트합니다.

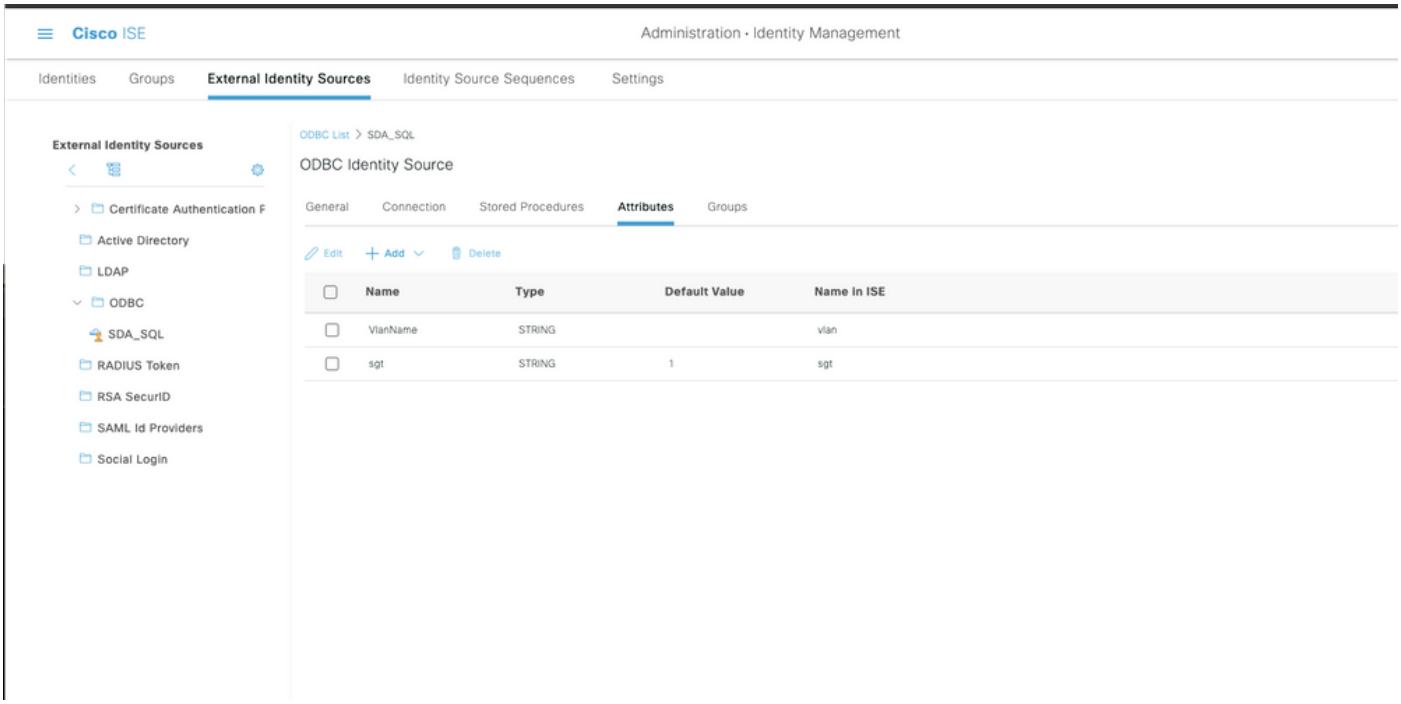


2단계. ODBC 페이지의 Stored Procedures(저장 프로시저) 탭으로 이동하여 Cisco ISE에서 생성된 프로시저를 구성합니다.

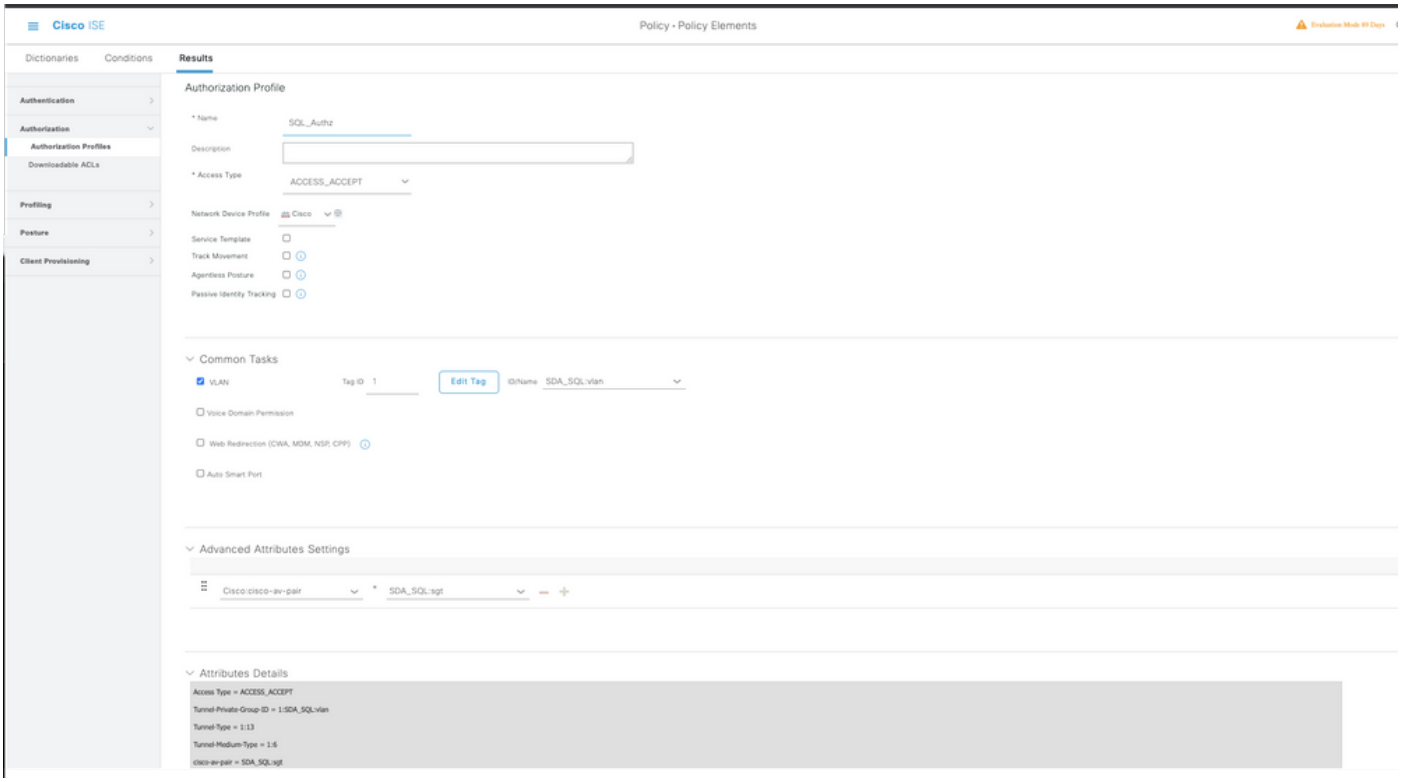


3단계. 확인을 위해 ODBC ID 소스에서 사용자 ID의 특성을 가져옵니다.

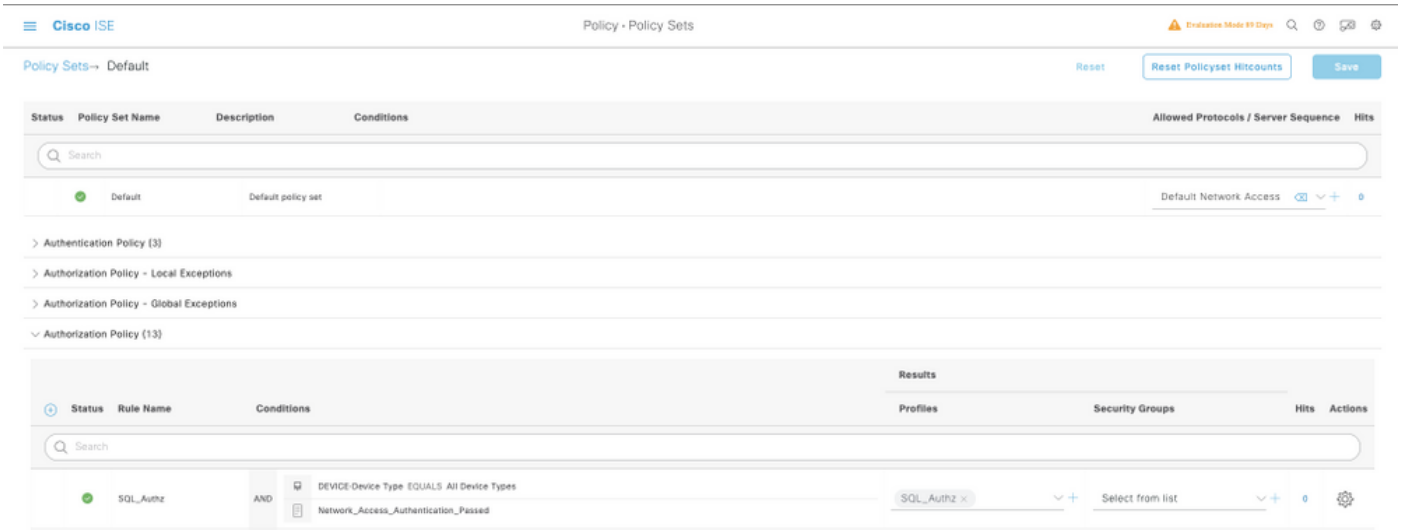




4단계. **권한 부여 프로파일**을 생성하고 구성합니다. Cisco ISE에서 **Policy(정책) > Results(결과) > Authorization profile(권한 부여 프로파일) > Advance Attributes Settings(고급 특성 설정)**로 이동하여 특성을 **Cisco:cisco-av-pair**로 선택합니다**. 값**을 <name of ODBC database>:sgt로 선택합니다. Common Tasks(일반 작업) 아래에서 **VLAN** with ID/Name as <name of ODBC database>:vlan을 선택하고 저장합니다



5단계. 권한 부여 **정책**을 생성하고 구성합니다. Cisco ISE에서 **Policy(정책) > Policy sets(정책 집합) > Authorization Policy(권한 부여 정책) > Add(추가)로 이동합니다.** ID 소스가 SQL 서버인 경우 조건을 입력합니다. Result(결과) 프로파일을 이전에 생성한 Authorization(권한 부여) 프로파일로 선택합니다.

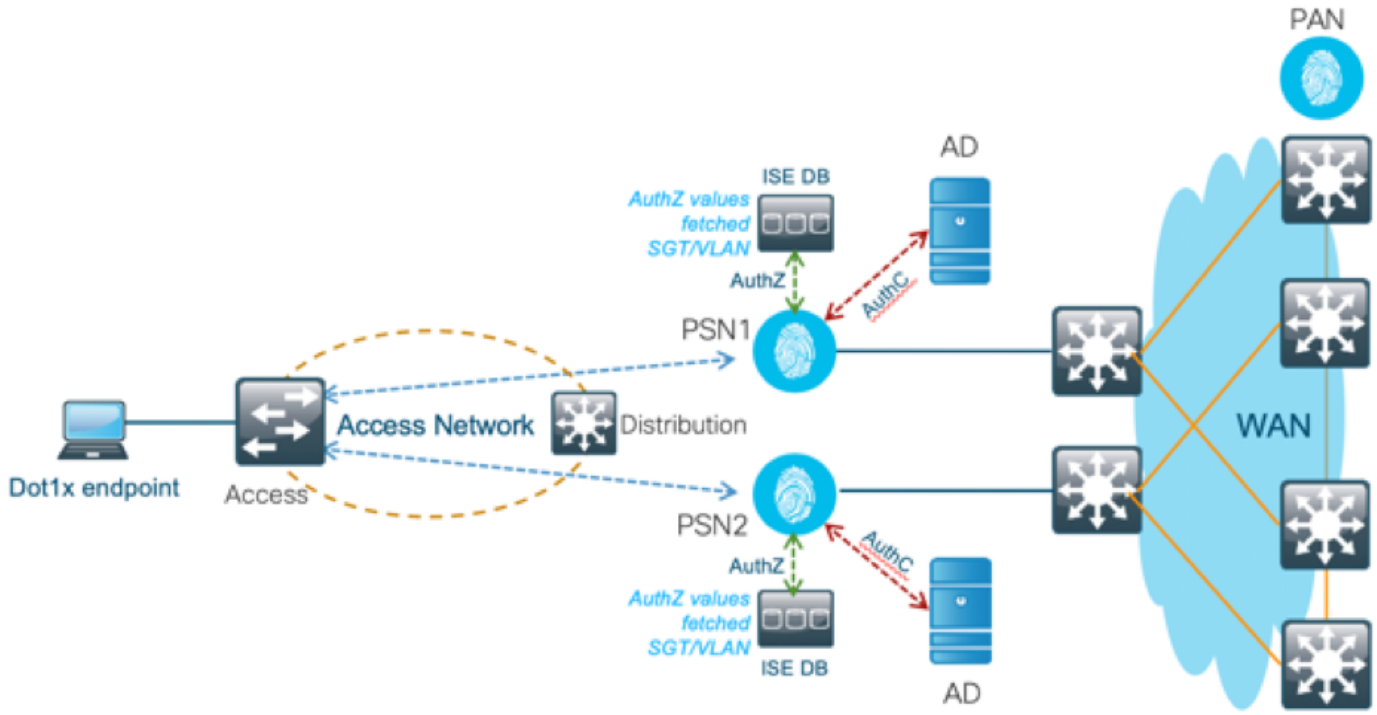


내부 DB 사용

Cisco ISE 자체에는 권한 부여를 위한 사용자 ID를 갖는 데 사용할 수 있는 내장 DB가 있습니다.

솔루션 워크플로

이 솔루션에서는 Cisco ISE의 내부 DB가 권한 부여 지점으로 사용되지만 AD(Active Directory)는 인증 소스로 계속 사용됩니다. 엔드포인트의 사용자 ID는 SGT 또는 VLAN과 같은 인증된 결과를 반환하는 **사용자 지정 특성과** 함께 Cisco ISE DB에 포함됩니다. 엔드포인트의 자격 증명이 PSN에 제공되면 Active Directory ID 저장소로 엔드포인트의 자격 증명의 유효성을 확인하고 엔드포인트를 인증합니다. 권한 부여 정책은 ISE DB를 참조하여 사용자 ID가 참조로 사용되는 SGT/VLAN과 같은 인증된 결과를 가져옵니다.



장점

이 솔루션은 다음과 같은 장점이 있어 유연한 솔루션이 됩니다.

- Cisco ISE DB는 내장 솔루션 이므로 외부 DB 솔루션과 달리 3번째 장애 지점이 없습니다.
- Cisco ISE 클러스터는 모든 페르소나 간의 실시간 동기화를 보장하므로 PAN에서 실시간으로 푸시되는 모든 사용자 ID 및 사용자 지정 특성이 PSN에 있으므로 WAN 종속성이 없습니다.
- Cisco ISE는 외부 DB가 제공하는 모든 가능한 추가 기능을 활용할 수 있습니다.
- 이 솔루션은 Cisco ISE 확장 제한에 의존하지 않습니다.

단점

이 솔루션의 단점은 다음과 같습니다.

- Cisco ISE DB가 보류할 수 있는 최대 사용자 ID 수는 300,000입니다.
- DB에 대한 user-id의 수동 컨피그레이션으로 인한 오류를 고려해야 합니다.

내부 DB 샘플 컨피그레이션

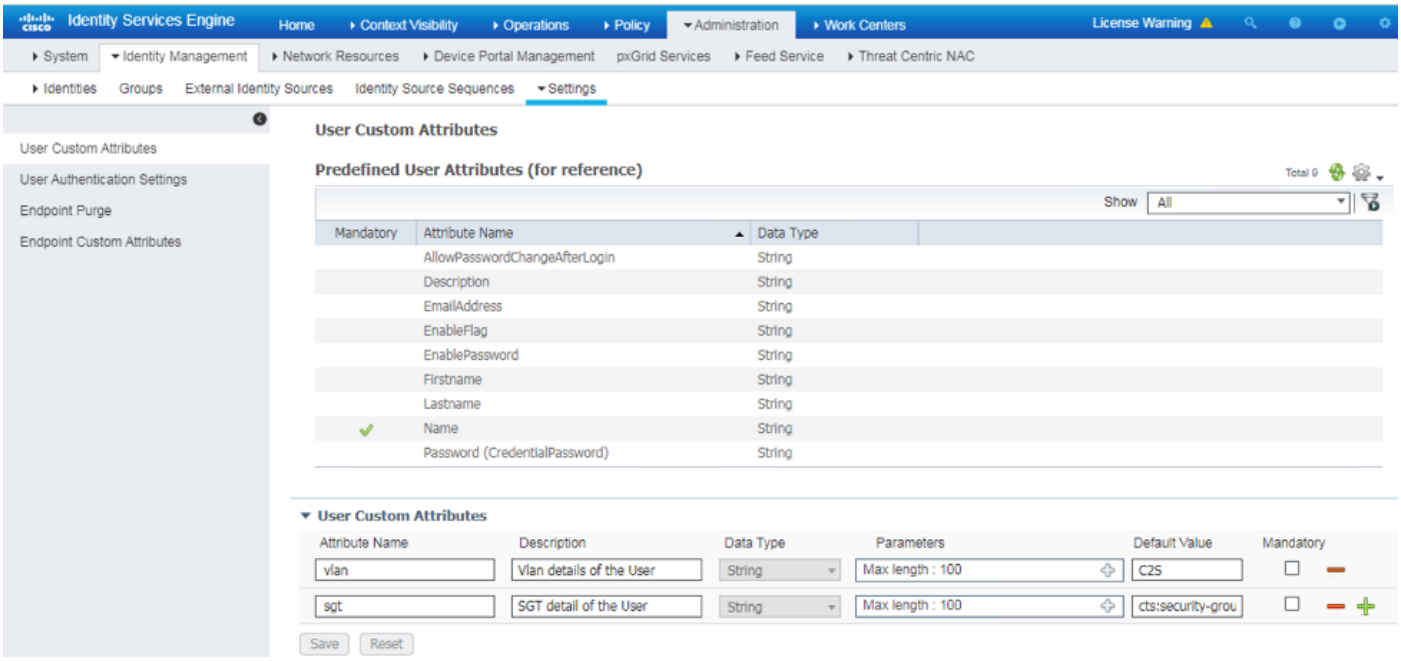
사용자별 VLAN 및 SGT는 사용자 지정 사용자 특성이 있는 내부 ID 저장소의 모든 사용자에 대해 구성할 수 있습니다.

1단계. 각 사용자의 VLAN 및 SGT 값을 나타내는 새 사용자 지정 특성을 만듭니다. **관리 > ID 관리 > 설정 > 사용자 지정 특성으로** 이동합니다. 이 표에 표시된 대로 새 사용자 지정 특성을 만듭니다.

여기에서는 ISE DB 테이블이 사용자 지정 특성과 함께 표시됩니다.

속성 이름	데이터 유형	매개변수(길이)	기본값
vlan	문자열	100	C2S(기본 Vlan 이름)
경사	문자열	100	cts:security-group-tag=0003-0(기본 SGT 값)

- 이 시나리오에서 VLAN 값은 vlan 이름을 나타내고 sgt 값은 SGT의 cisco av-pair 특성을 16진수로 나타냅니다.

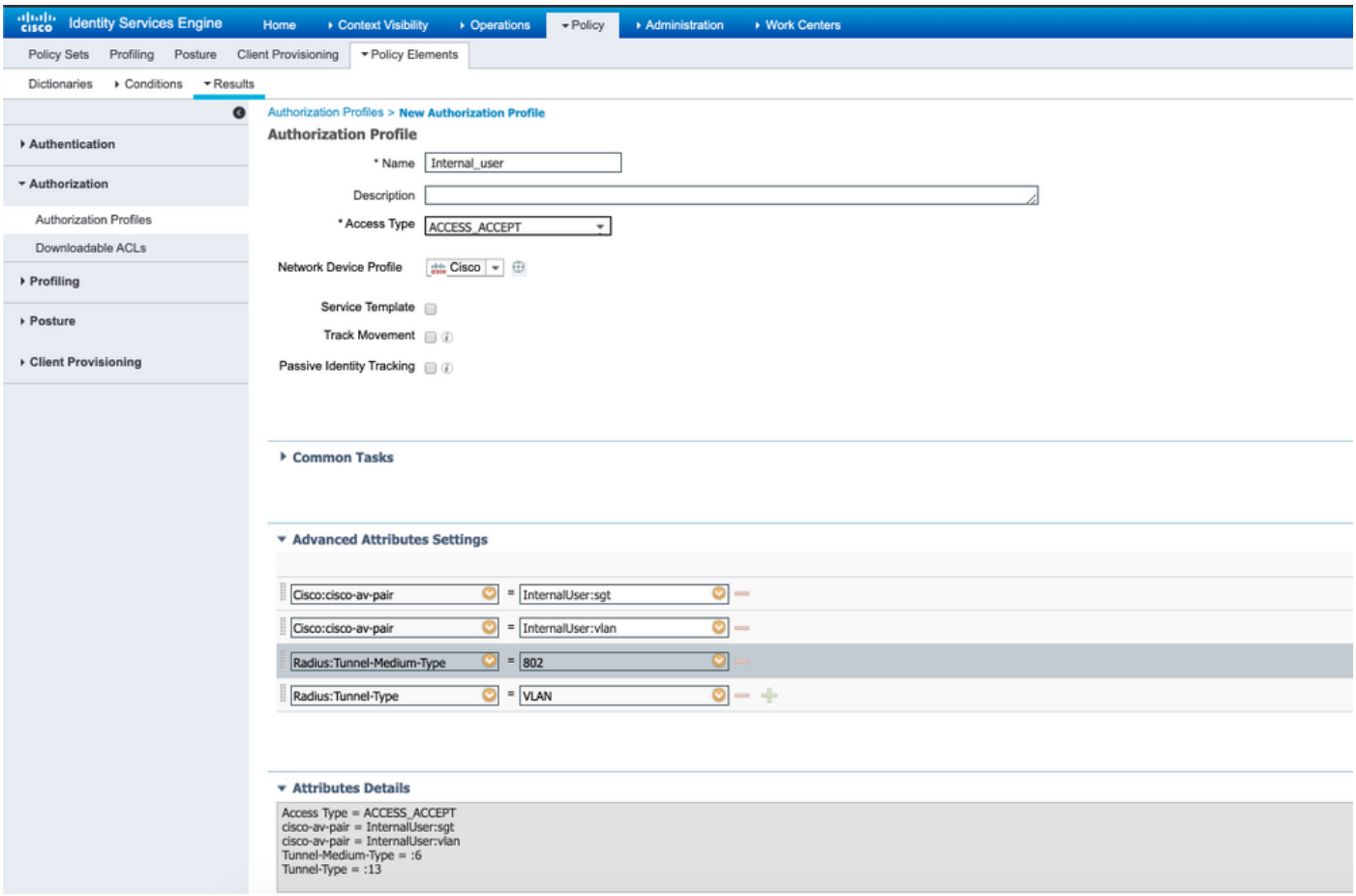


2단계. 사용자 지정 특성을 사용하여 권한 부여 프로파일을 생성하여 각 사용자의 vlan 및 sgt 값을 암시합니다. **Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add로** 이동합니다. Advanced Attributes Settings 아래에서 설명하는 특성을 추가합니다.

이 표에서는 내부 사용자에 대한 AuthZ 프로필을 보여줍니다.

속성	가치
Cisco:cisco av 쌍	내부 사용자:sgt
Radius: 터널 개인 그룹 ID	내부 사용자:vlan
Radius:Tunnel-Medium-Type	802
Radius:터널 유형	VLAN

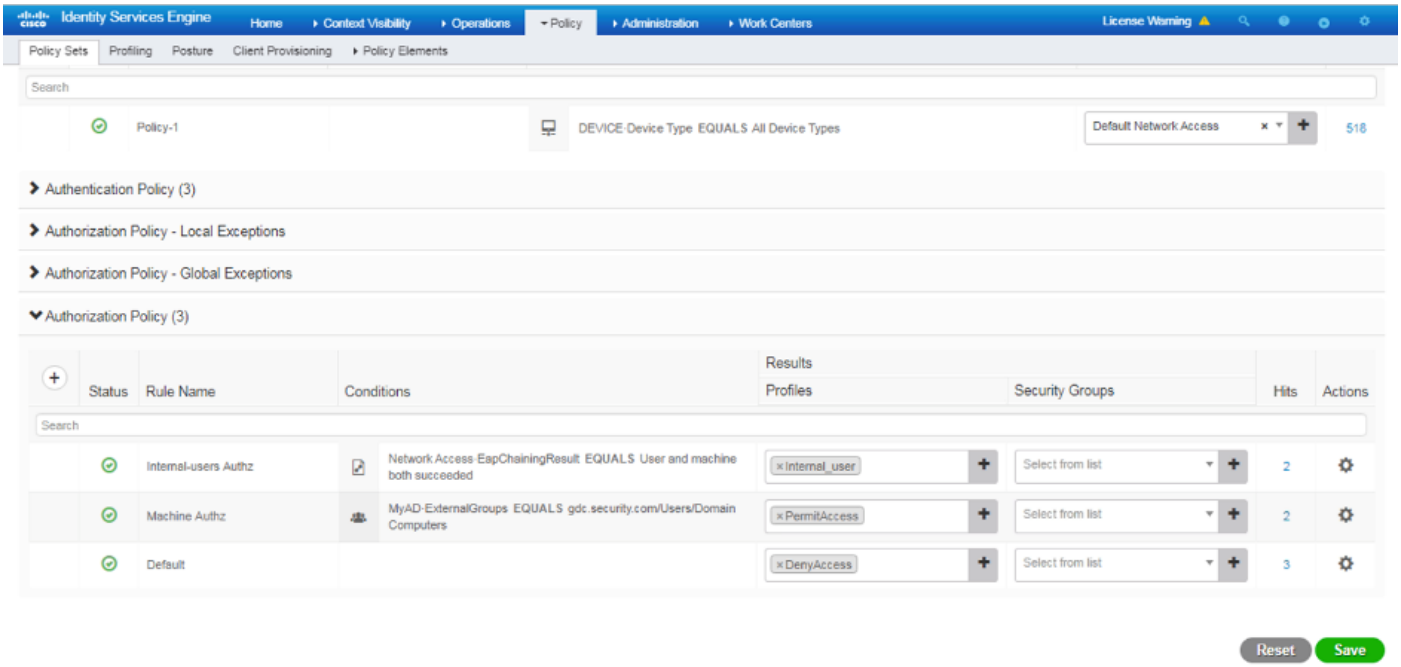
이미지에 표시된 것처럼 내부 사용자의 경우 프로파일 **Internal_user**는 SGT 및 Vlan이 InternalUser:sgt 및 InternalUser:**vlan**으로 **각각** 구성됩니다.



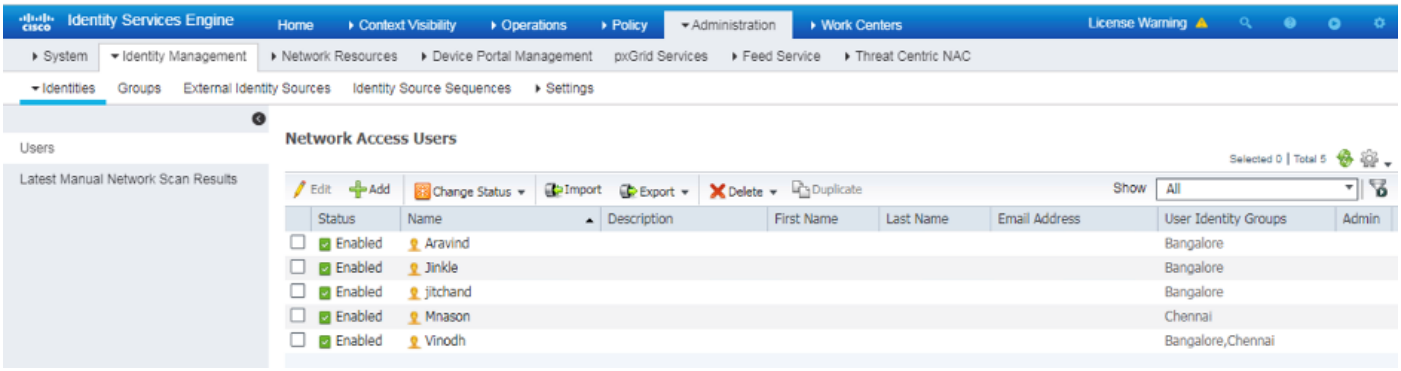
3단계. 권한 부여 정책을 생성하고 **Policy > Policy Sets > Policy-1 > Authorization으로 이동합니다. 아래**에서 언급한 조건으로 권한 부여 정책을 생성하고 각 권한 부여 프로파일에 매핑합니다.

이 표에서는 내부 사용자에 대한 AuthZ 정책을 보여줍니다.

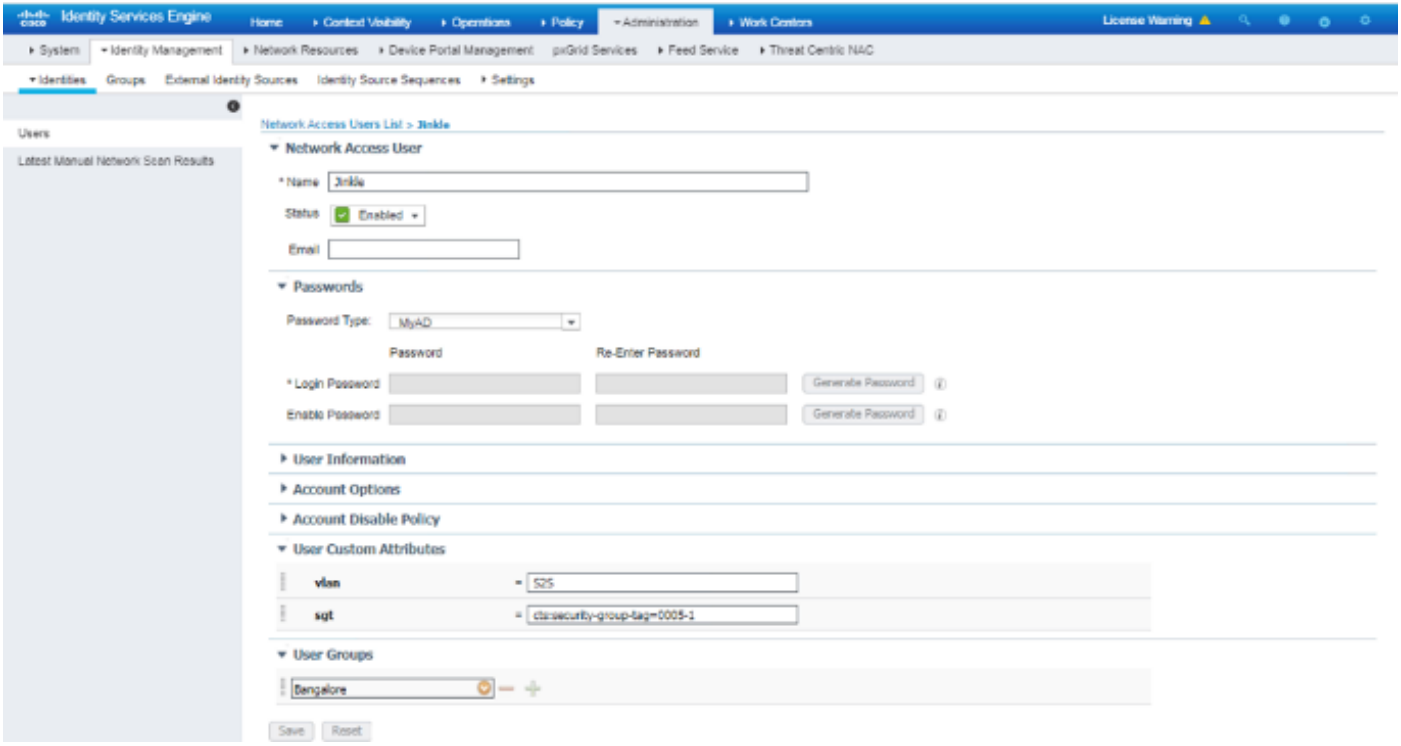
규칙 이름	조건	결과 인증 프로파일
내부 사용자 인증	네트워크 액세스가 성공하면 EapChainingResults는 사용자와 머신 모두 성공	내부 사용자
시스템 전용 인증	MyAD.ExternalGroups가 gdc.security.com/Users/Domain Computers와 같은 경우	액세스 허용



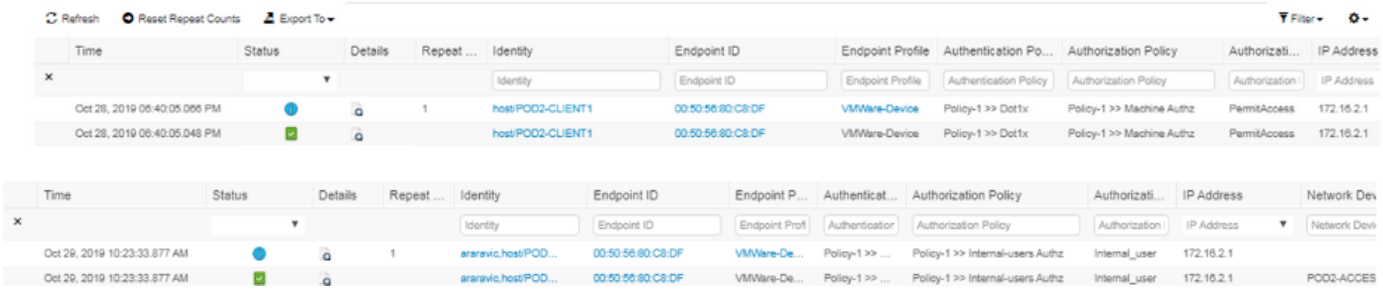
4단계. 사용자 세부사항 및 해당 사용자 지정 특성이 포함된 사용자 지정 특성이 포함된 대량 사용자 ID를 csv 템플릿에 생성합니다. Administration(관리) > Identity **Management(ID 관리) > Identities(ID) > Users(사용자) > Import(가져오기) > File(파일) > Import(가져오기)로 이동하여 csv를 가져옵니다.**



이 그림에서는 사용자 지정 특성 세부사항이 있는 샘플 사용자를 보여 줍니다. 사용자를 선택하고 edit(수정)를 클릭하여 각 사용자에 매핑된 사용자 지정 특성 세부사항을 확인합니다.



5단계: 라이브 로그를 확인합니다.



Vlan & **SGT** 특성이 Access-**Accept**의 일부로 전송되는지 확인하려면 Result 섹션을 확인합니다.

결론

이 솔루션을 통해 일부 대기업 고객은 요구 사항에 맞게 확장할 수 있습니다. 사용자 ID를 추가/삭제할 때는 주의해야 합니다. 오류가 트리거될 경우, 실제 사용자에 대한 무단 액세스가 발생하거나 그 반대의 상황이 발생할 수 있습니다.

관련 정보

ODBC를 통해 MS SQL로 Cisco ISE를 구성합니다.

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

용어집

AAA	인증 권한 부여 계정 관리
광고	액티브 디렉토리
인증	인증
인증	Ahthorization(권한 부여)
DB	데이터베이스
DOT1X	802.1X
IBN	ID 기반 네트워크
ID	ID 데이터베이스
ISE	Identity Services Engine
MnT	모니터링 및 문제 해결
MsSQL	Microsoft SQL

ODBC	개방형 DataBase 연결
팬	정책 관리 노드
PSN	정책 서비스 노드
SGT	보안 그룹 태그
SQL	구조적 쿼리 언어
VLAN	가상 LAN
WAN	광역 네트워크

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.