Simplified Access Policy using ODBC & ISE DB (Custom Attribute) for Large Scale Campus Network

Contents

Introduction

This document describes large scale campus deployment with no compromise to its features and security enforcement. Cisco's endpoint security solution, Identity Services Engine (ISE) addresses this requirement with integration to an External Identity Source.

For large-scale networks with 50+ geo-locations, 4000+ different user-profiles, and 600,000 endpoints or more, traditional IBN solutions need to be looked at from a different perspective – more than just features, whether it scales with all the features. Intent-Based Network (IBN) solution in today's traditional large scale networks requires additional focus on scalability and ease of management and not just its features.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Dot1x/MAB Authentication
- Cisco Identity Service Engine (CiscoISE)
- Cisco TrustSec (CTS)

Components Used

The information in this document is based on these software and hardware versions:

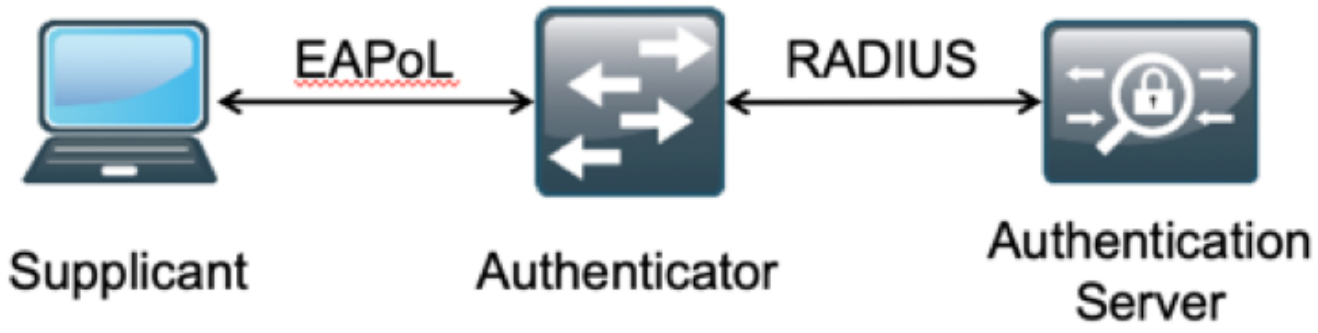
- Cisco Identity Services Engine (ISE) Version 2.6 Patch 2 and Version 3.0
- Windows Active Directory (AD) Server 2008 Release 2
- Microsoft SQL Server 2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If the network is live, make sure to understand the potential impact of any configuration.

Background Information

In an Identity Based Network (IBN) solution, the basic elements are Supplicant, Authenticator and Authentication (AAA) Server. The Supplicant is an agent on the endpoint that supplies the credentials when challenged for network access. Authenticator or NAS (Network Access Server) is the access layer, which comprises network switches & WLCs that carry the credentials to the AAA server. Authentication Server validates the user authentication request against an ID store and authorizes either with an access-accept or access-reject. The ID store can be within the AAA server or on an external dedicated server.

This image shows the Basic IBN Elements.



RADIUS is a User Datagram Protocol (UDP) based protocol with authentication and authorization coupled together. In Cisco’s IBN solution for enterprise campus, the ISE's Policy Service Node (PSN) persona acts as the AAA server which authenticates the endpoints against the enterprise ID Store and authorizes based on a condition.

In Cisco ISE, authentication and authorization policies are configured to meet these requirements. Authentication policies consist of the type of media, either wired or wireless, and the EAP protocols for user validation. Authorization policies consist of conditions that define the criteria for the various endpoints to match and network access result which can be a VLAN or a downloadable ACL or a Secure Group Tag (SGT). These are maximum scale numbers for policies that ISE can be configured with.

This table shows the Cisco ISE Policies Scale.

Attribute	**Scale number**
Maximum number of Authentication Rules	1000 (Policy Set Mode)
Maximum number of Authorization Rules	3,000 (Policy Set Mode) with 3200 Authz profiles

Technology Trends

Segmentation has become one of the key security elements for today's enterprise networks with no necessity for an actual edge network. The endpoints are allowed to roam between internal and external networks. Segmentation helps to contain any security attack on a particular segment to extend across the network. Today’s Software-Defined Access (SDA) solution with the help of Cisco ISE’s TrustSec provides a way to segment based on customer’s business model to avoid dependencies on network elements such as VLANs or IP Subnets.

Problem

ISE policy configuration for large-scale enterprise networks with more than 500 different endpoint profiles, the number of authorization policies can increase to an unmanageable point. Even if Cisco ISE supports dedicated authorization conditions to cater to such a volume of user-profiles, there lies a challenge to manage those many numbers of policies by administrators.

Additionally, customers may require common authorization policies instead of dedicated policies to avoid management overheads and also have differentiated network access for endpoints based on their criteria.

For example, consider an enterprise network with Active Directory (AD) as the **source of truth** and the endpoint’s unique differentiator is one of the attributes in AD. In such a case, the traditional way of policy configuration has more authorization policies for each unique endpoint profile.

In this method, each endpoint profile is distinguished with an AD attribute under domain.com. Hence,a dedicated authorization policy needs to be configured.

This table shows the Traditional AuthZ Policies.

ABC-Policy	If AnyConnect EQUALS User-AND-Machine-Both-Passed AND If AD-Group EQUALS domain.com/groups/ABC THEN SGT:C2S-ABC AND VLAN:1021
DEF-	If AnyConnect EQUALS User-AND-Machine-Both-Passed

Policy	AND If AD-Group EQUALS domain.com/groups/DEF THEN SGT:C2S-DEF AND VLAN:1022 If AnyConnect EQUALS User-AND-Machine-Both-Passed
GHI-Policy	AND If AD-Group EQUALS domain.com/groups/GHI THEN SGT:C2S-GHI AND VLAN:1023 If AnyConnect EQUALS User-AND-Machine-Both-Passed
XYZ-Policy	AND If AD-Group EQUALS domain.com/groups/XYZ THEN SGT:C2S-XYZ AND VLAN:1024

Proposed Solution

To circumvent the breach on the maximum scalable number of supported authorization policies on Cisco ISE, the proposed solution is to use an external DB that authorizes each endpoint with the authorization result fetched from its attributes. For example, if AD is used as an external DB for authorization, any unused user attributes (like Department or Pin code) can be referred to provide authorized results mapped with SGT or VLAN.

This is achieved with the integration of Cisco ISE with an external DB or within ISE's internal DB configured with custom attributes. This section explains the deployment of these 2 scenarios:

> **Note**: In both options, the DB contains the **user-id** but not the **password** of the DOT1X endpoints. The DB is used as the **authorization** point only. Authentication can still continue to be the customer's ID store which in most cases resides on the Active Directory (AD) server.

Configuration with External DB

Cisco ISE is integrated with an external DB for endpoint credential validation:

This table shows the Validated External Identity Sources.

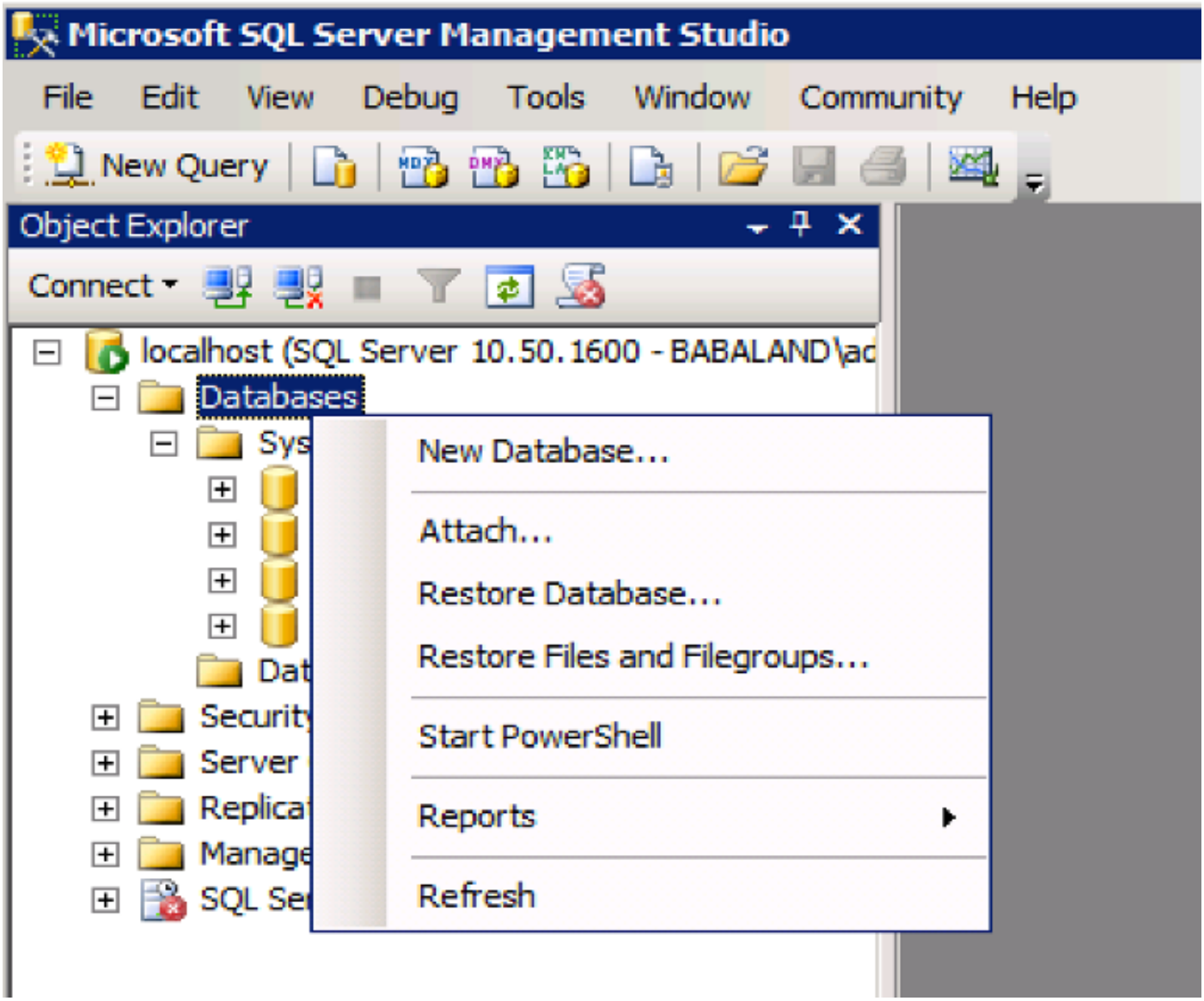
External Identity Source	OS/Version
Active Directory	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—
LDAP Servers	
SunONE LDAP Directory Server	Version 5.2
OpenLDAP Directory Server	Version 2.4.23
Any LDAP v3 compliant server	—
Token Servers	

RSA ACE/Server	6.x series
RSA Authentication Manager	7.x and 8.x series
Any RADIUS RFC 2865-compliant token server	—
Security Assertion Markup Language (SAML) Single Sign-On (SSO)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate Server	Version 6.10.0.4
PingOne Cloud	—
Secure Auth	8.1.1
Any SAMLv2-compliant Identity Provider	—
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition Release 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Social Login (for Guest User Accounts)	
Facebook	—

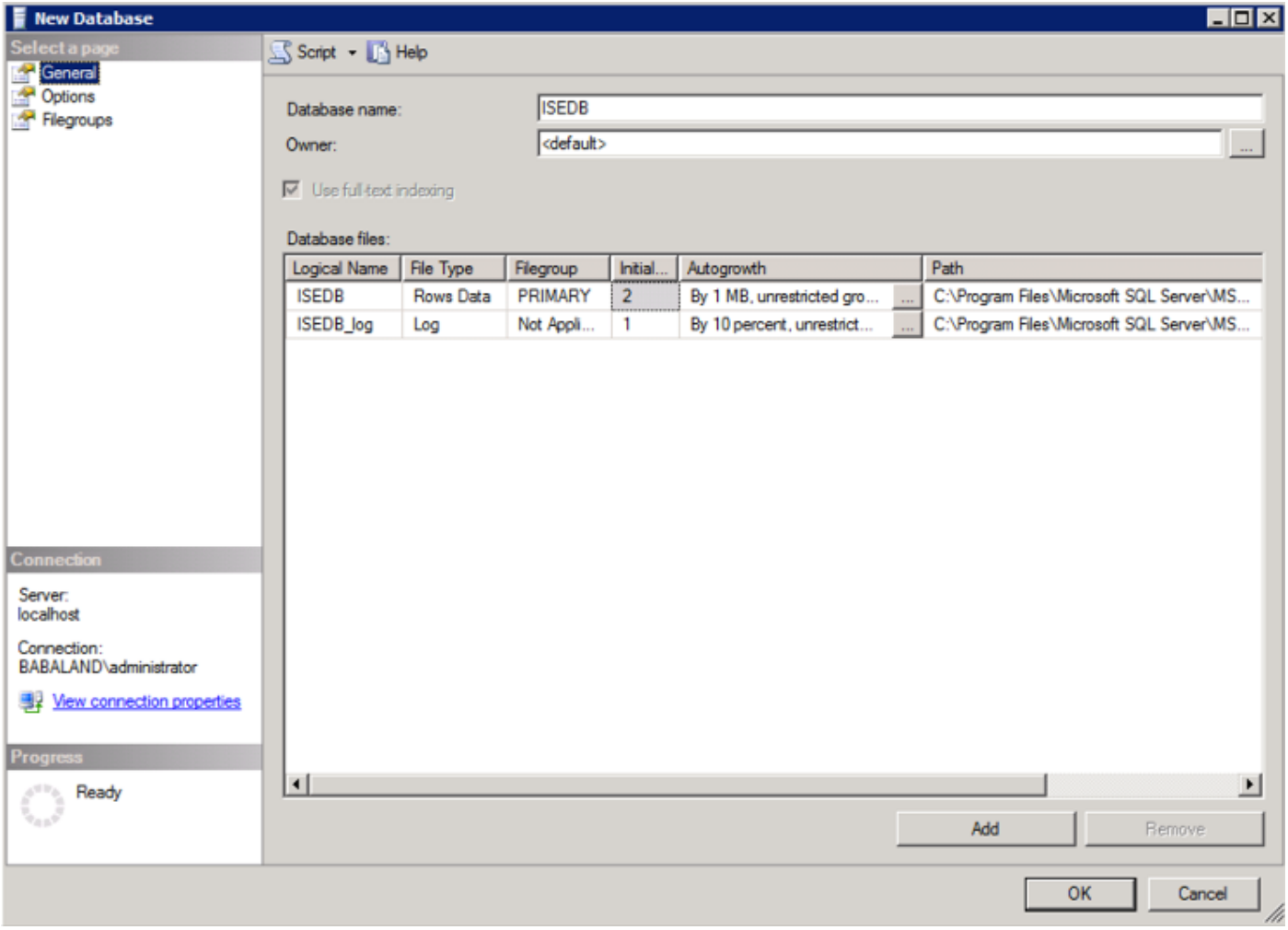
ODBC Sample Configurations

This configuration is done on Microsoft SQL to build the solution:

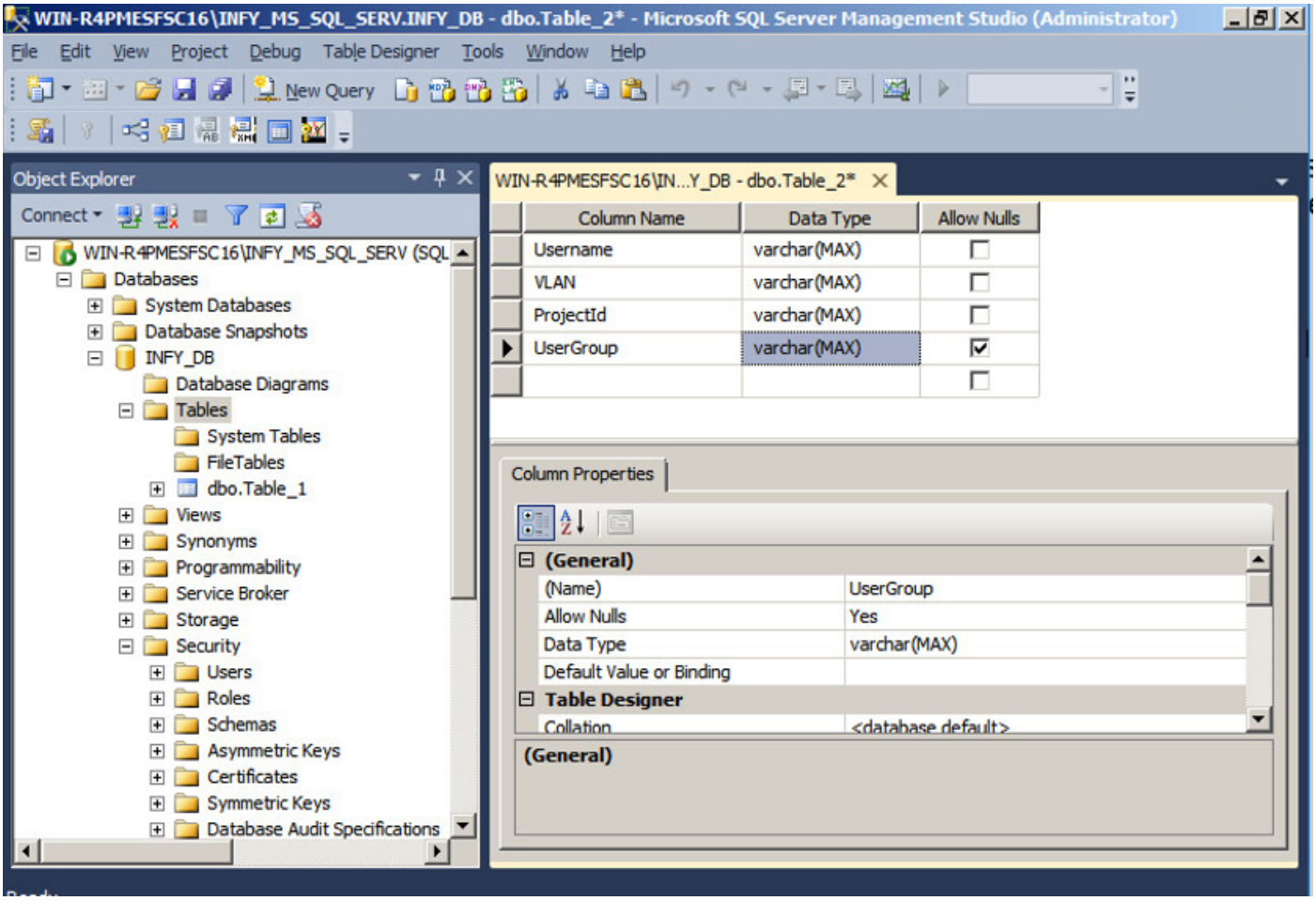
Step 1. Open SQL Server Management Studio (**Start menu > Microsoft SQL Server**) to create a database:



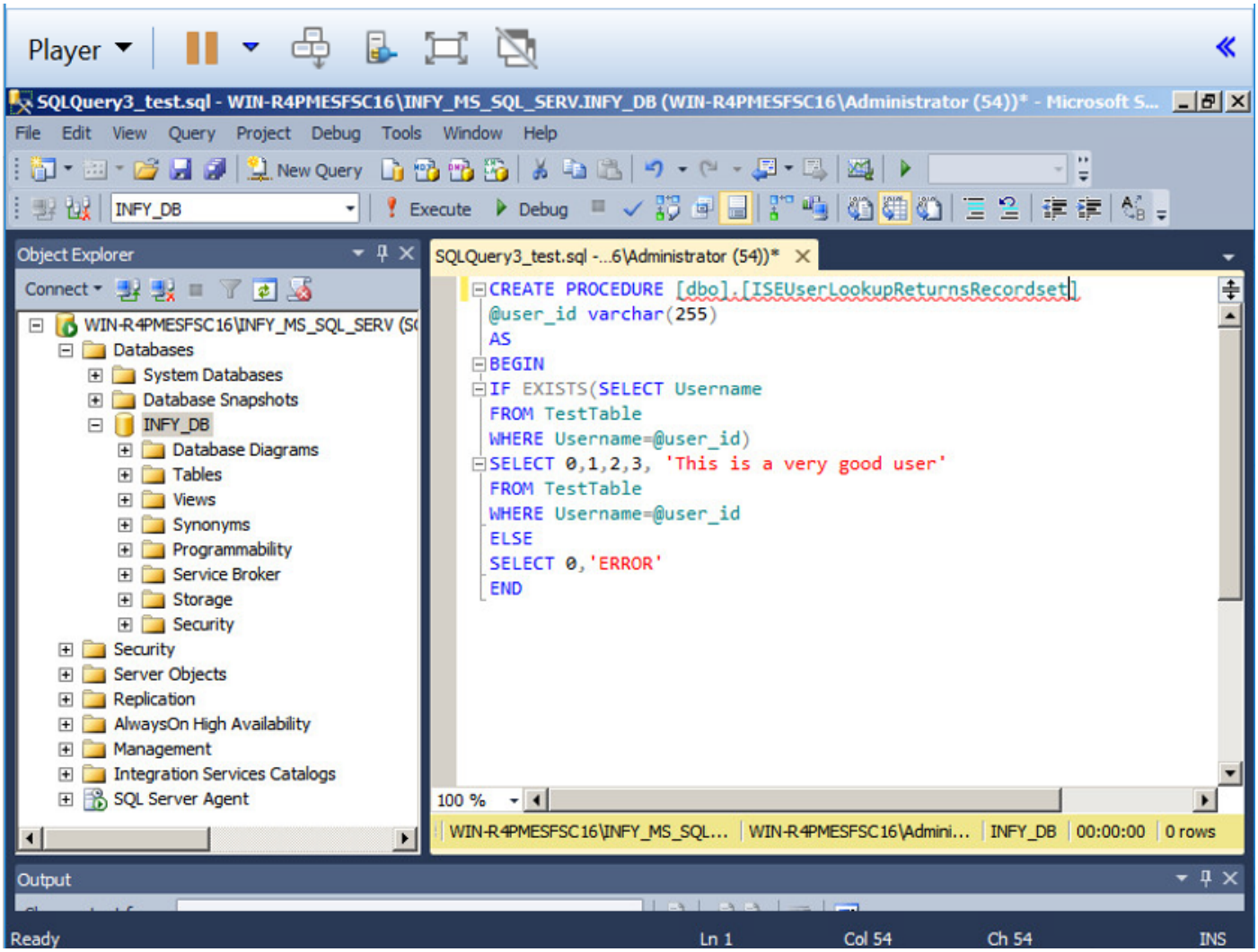
Step 2. Provide a name and create the database.



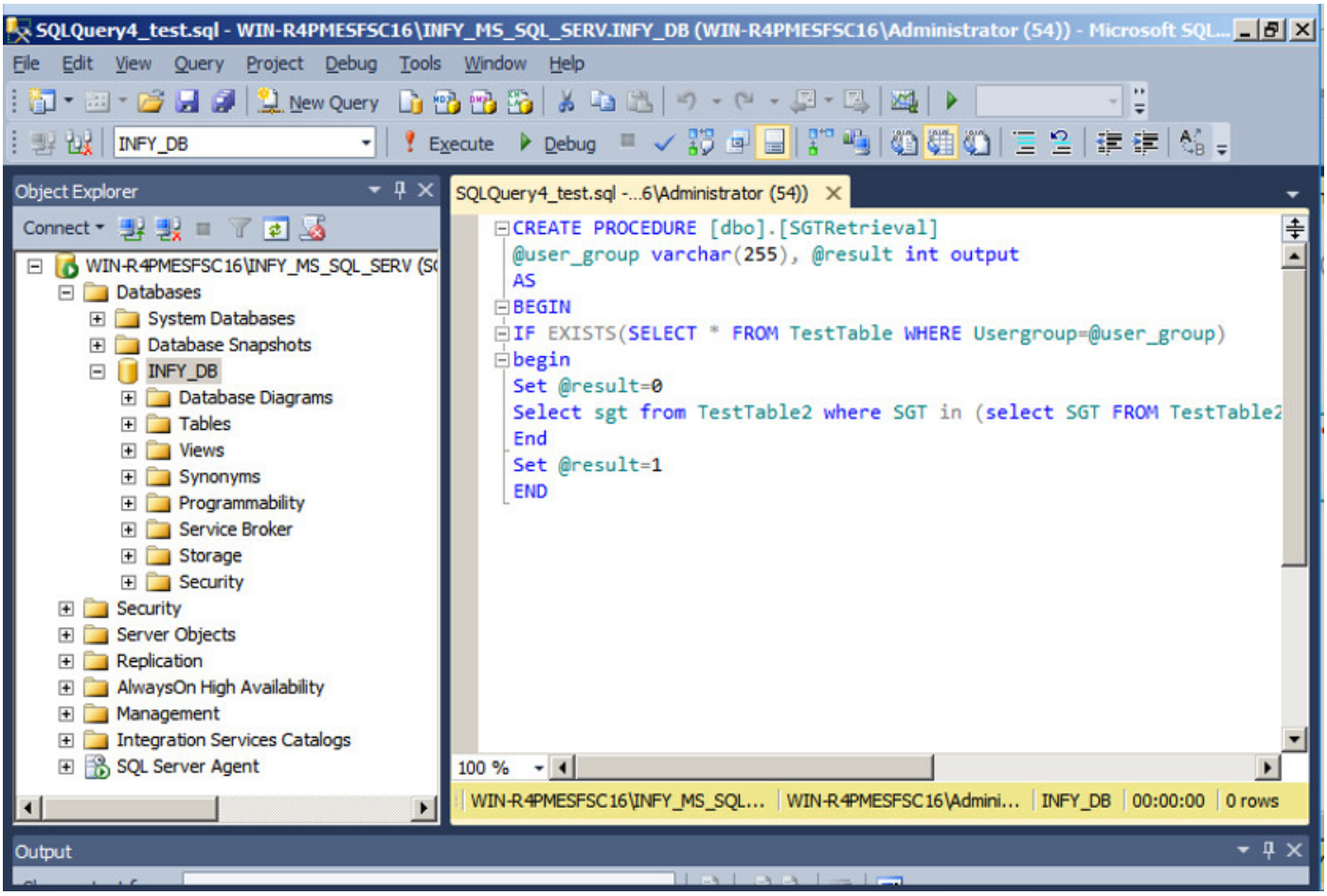
Step 3. Create a new table with the required columns as parameters for endpoints to get authorized.



Step 4. Create a **procedure** to check if the username exists.



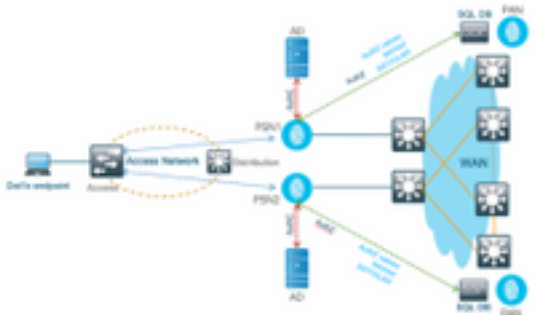
Step 5. Create a procedure to fetch attributes (SGT) from the table.

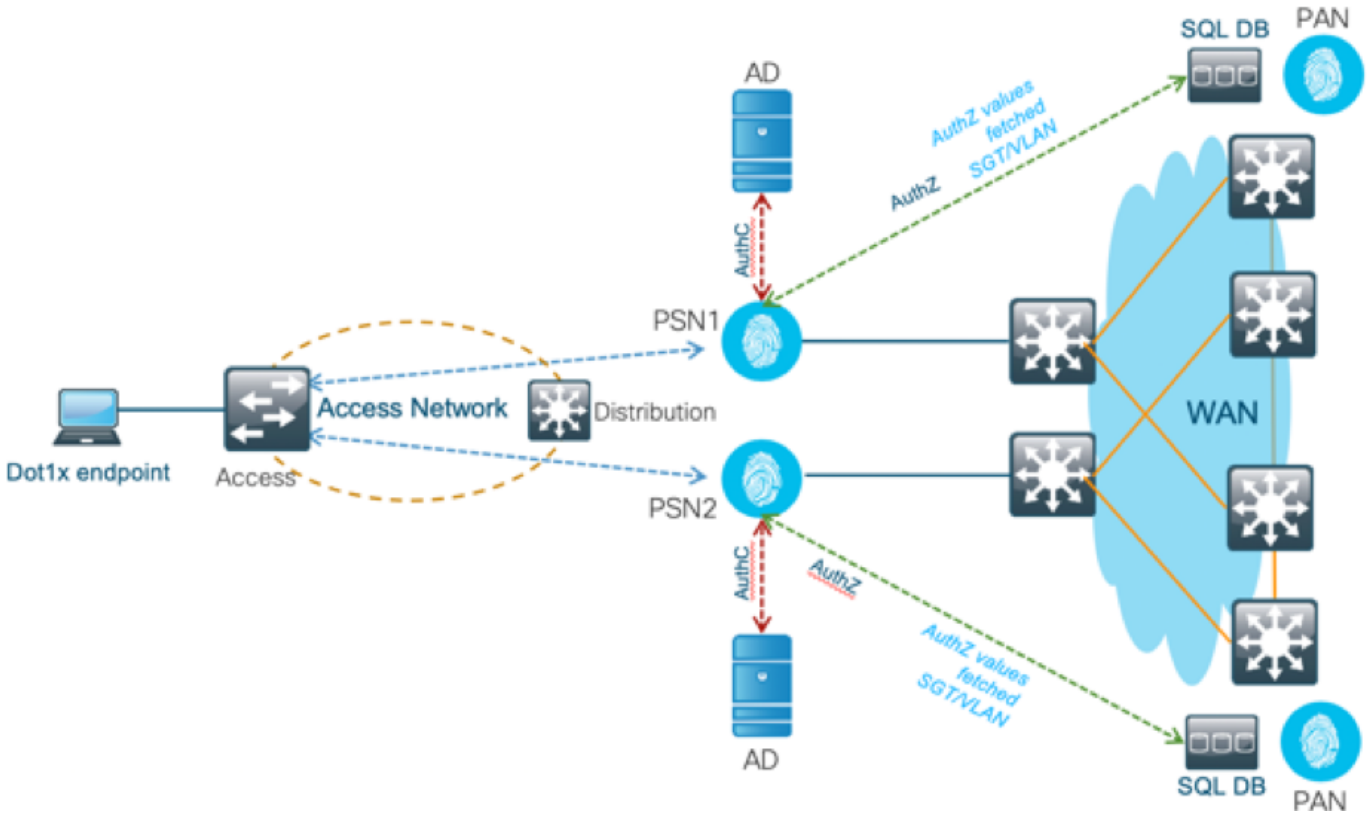


In this document, Cisco ISE is integrated with Microsoft SQL solution to meet the authorization scale requirements on large enterprise networks.

Solution Workflow (ISE 2.7 & earlier)

In this solution, Cisco ISE is integrated with an Active Directory (AD) and Microsoft SQL. AD is used as an Authentication ID store and MS SQL for authorization. During the authentication process, the Network Access Device (NAD) forwards the user credentials to the PSN – the AAA server in the IBN solution. PSN validates the endpoint credentials with the Active Directory ID store and authenticates the user. The authorization policy refers to the MS SQL DB to fetch the authorized results like SGT / VLAN for which **user-id** is used as the reference.





Advantages

This solution has these advantages, which makes it flexible:

- Cisco ISE can leverage all possible additional features that the external DB offers.
- This solution doesn't depend on any Cisco ISE scale limits.

Disadvantages

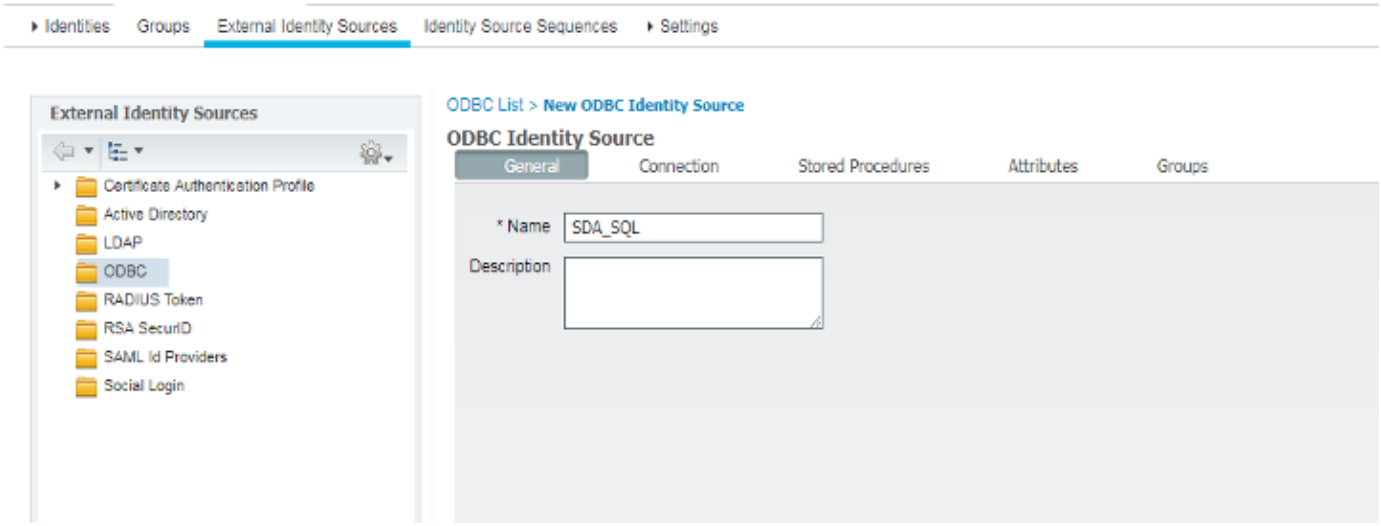
This solution has these disadvantages:

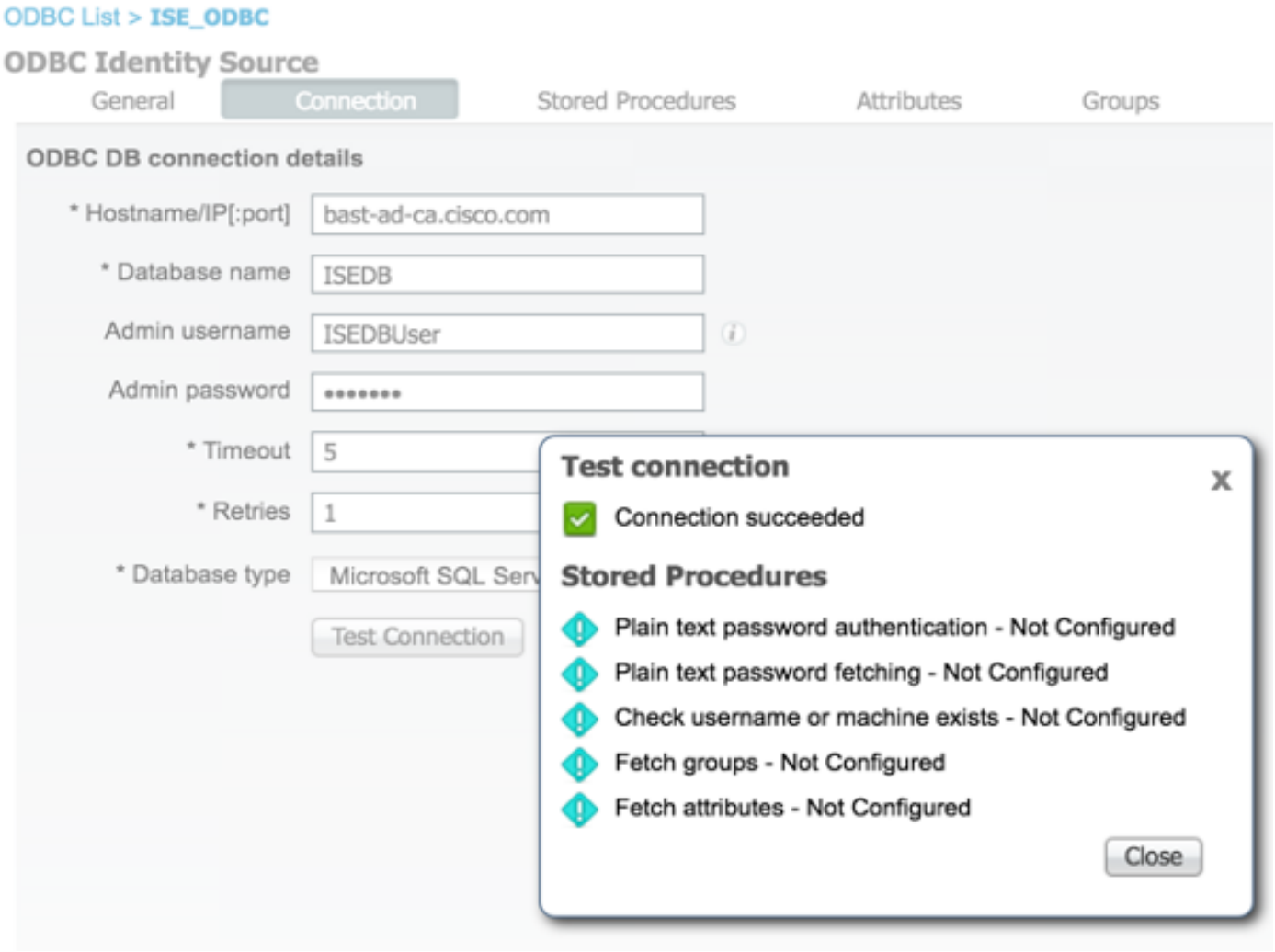
- Requires additional programming to populate the external DB with endpoint credentials.
- If the external DB is not locally present like PSNs, this solution depends on WAN which makes it the 3rd point of failure in the endpoint AAA data flow.
- Requires additional knowledge to maintain external DB processes and procedures.
- Errors caused by manual configuration of user-id to DB must be considered.

External DB Sample Configurations

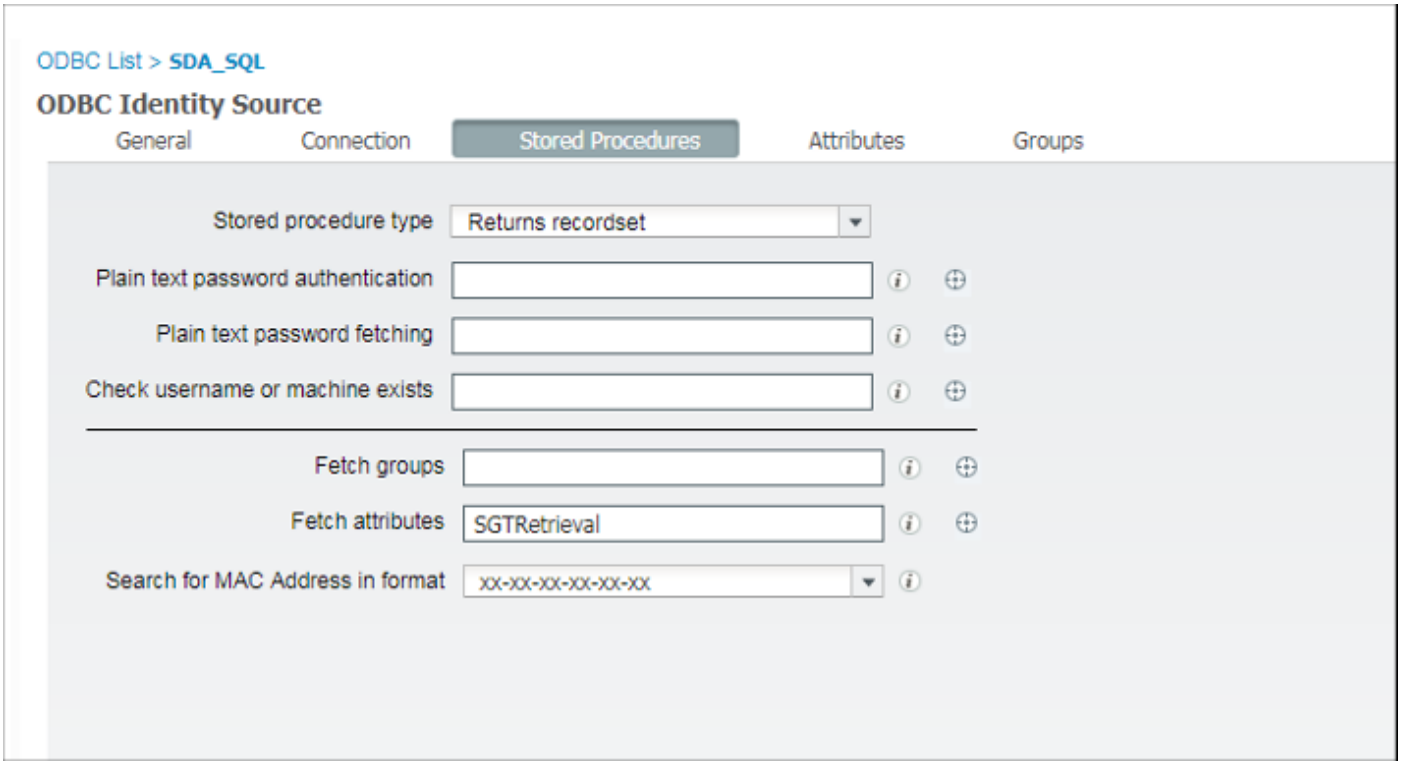
In this document, Microsoft SQL is shown as the external DB used as an authorization point.

Step 1. Create ODBC Identity store in Cisco ISE from the menu **Administration > External Identity Source > ODBC** and test the connections.

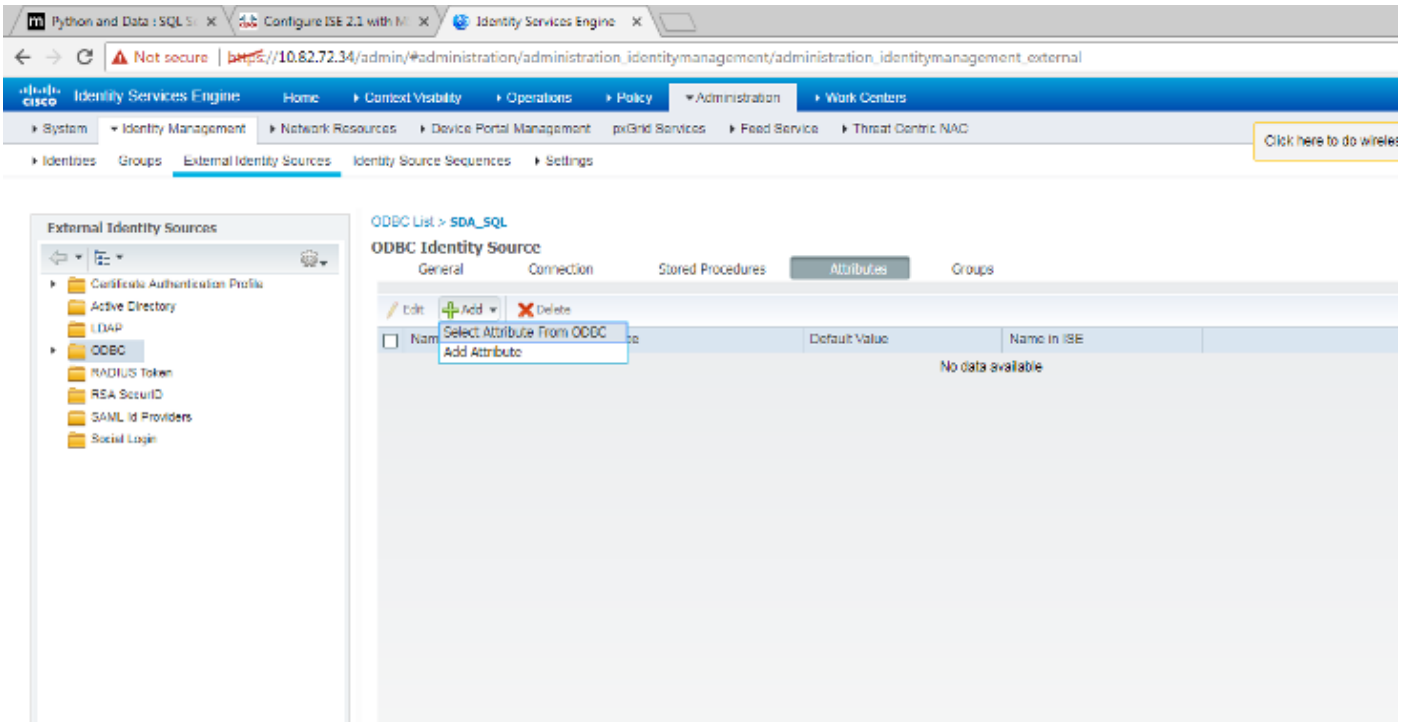


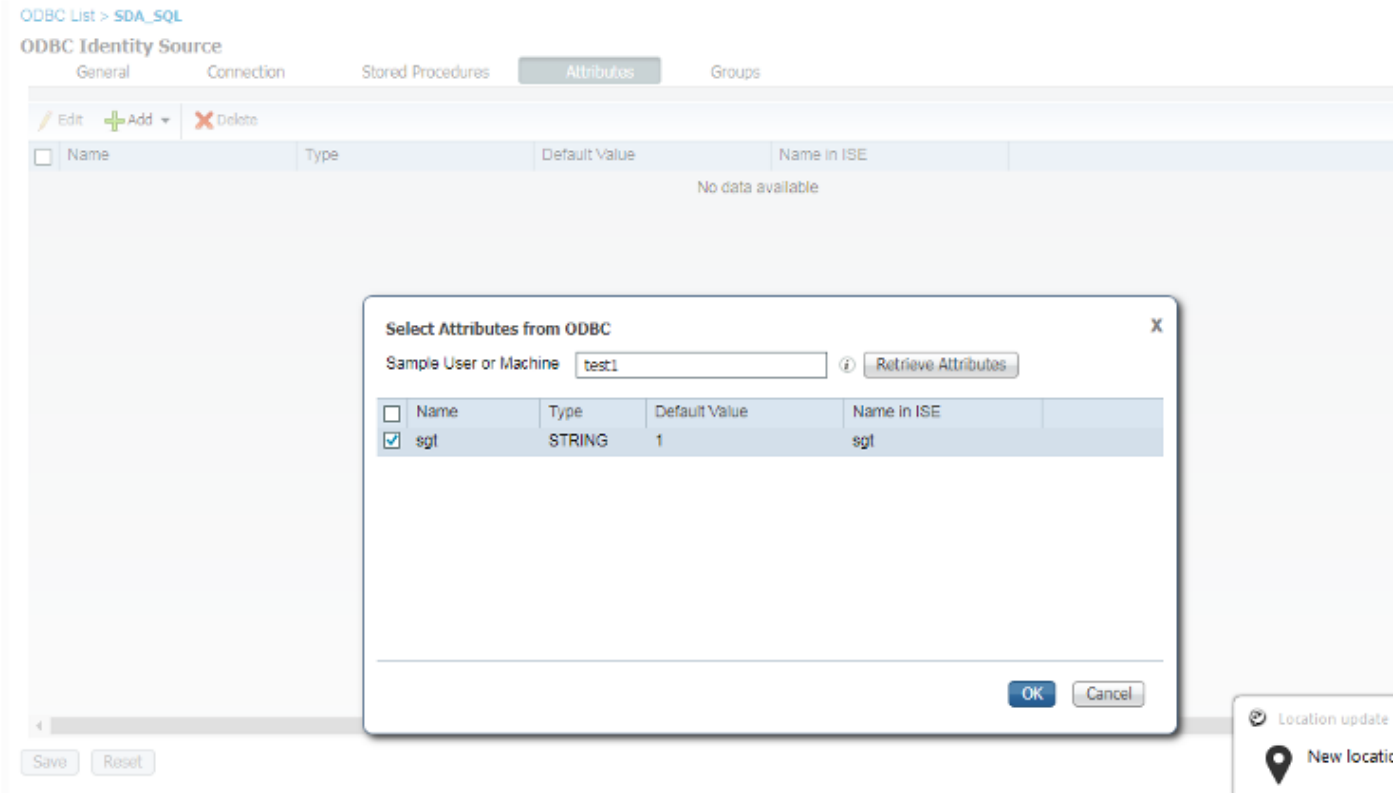


Step 2. Navigate to the Stored Procedures tab on the ODBC page to configure the created procedures in Cisco ISE.

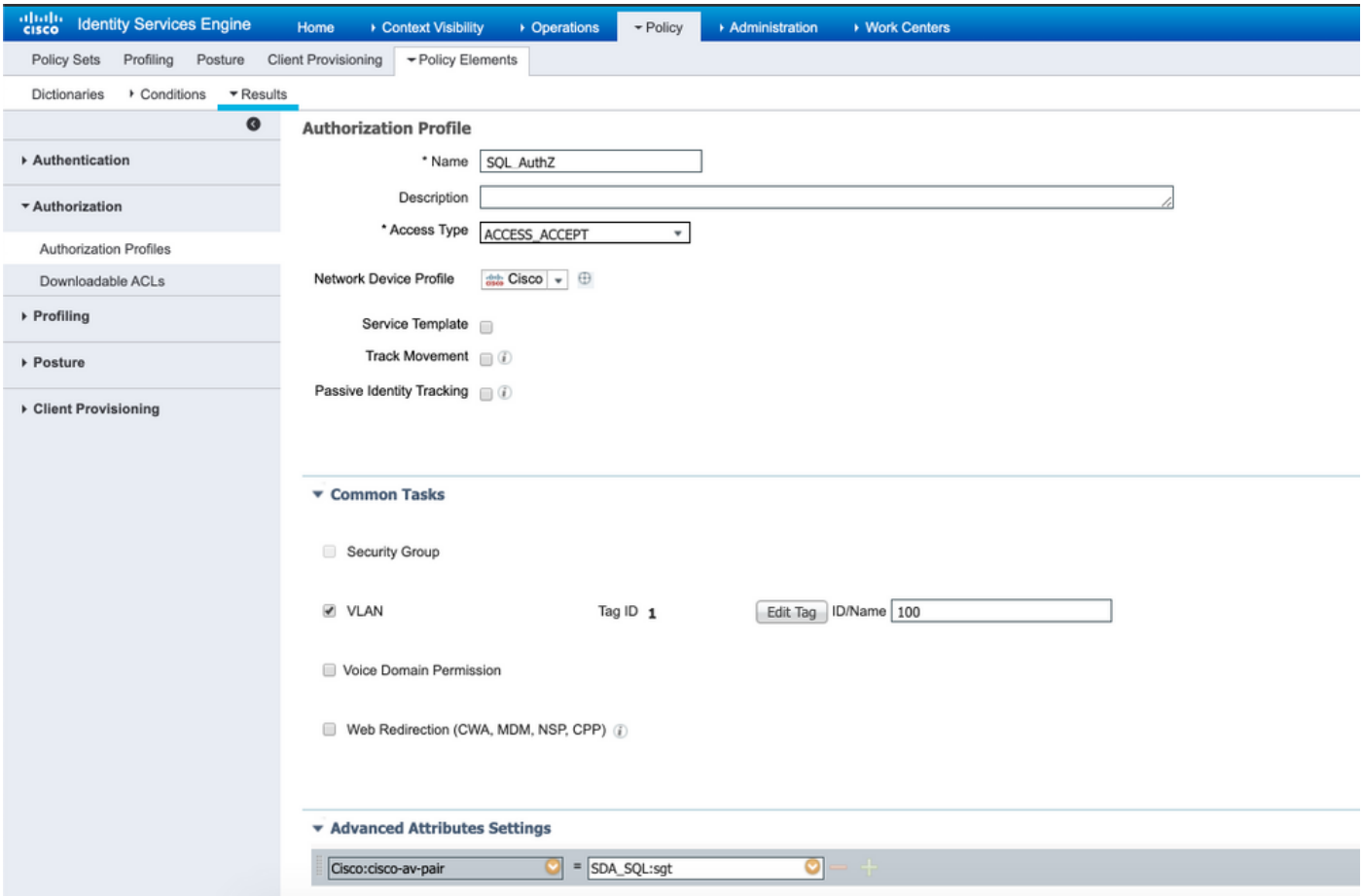


Step 3. Fetch the attributes for user id from the ODBC ID source for verification.

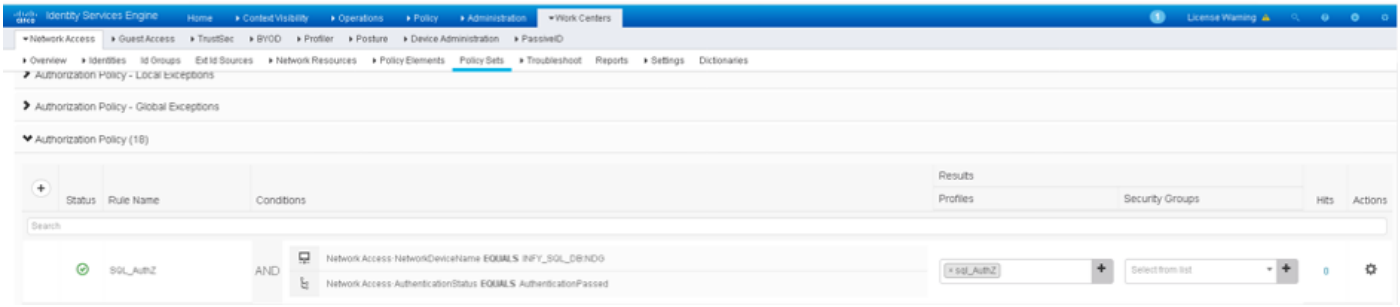




Step 4. Create an **authorization profile** and configure it. In Cisco ISE, go to **Policy > Results > Authorization profile > Advance Attributes Settings** and select the attribute as **Cisco:cisco-av-pair.** Select the values as <name of ODBC database>:sgt and then save it.



Step 5. Create an **authorization policy** and configure it. In Cisco ISE, navigate to **Policy > Policy sets > Authorization Policy > Add.** Put the condition as Identity Source is the SQL server. Select the Result profile as the Authorization profile created previously.



Step 6. Once the user is authenticated and authorized, the logs shall contain the sgt assigned to the user, for verification.

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

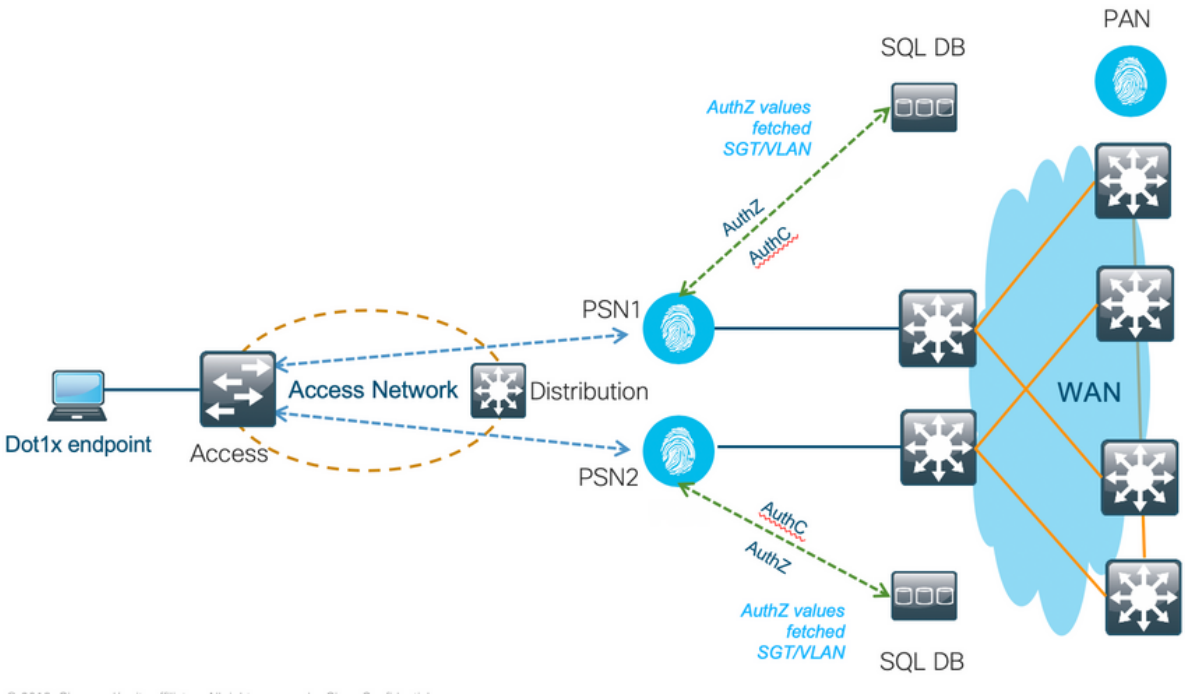
2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

Solution Workflow (Post ISE 2.7)

Post ISE 2.7, Attributes of authorization can be fetched from ODBC such as Vlan, SGT, ACL and these attributes can be consumed in Policies.

In this solution, Cisco ISE is integrated with Microsoft SQL. MS SQL is used as an ID store for authentication as well as for authorization. When the credentials from endpoints are provided to PSN, it validates the credentials against the MS SQL DB. The authorization policy refers to the MS

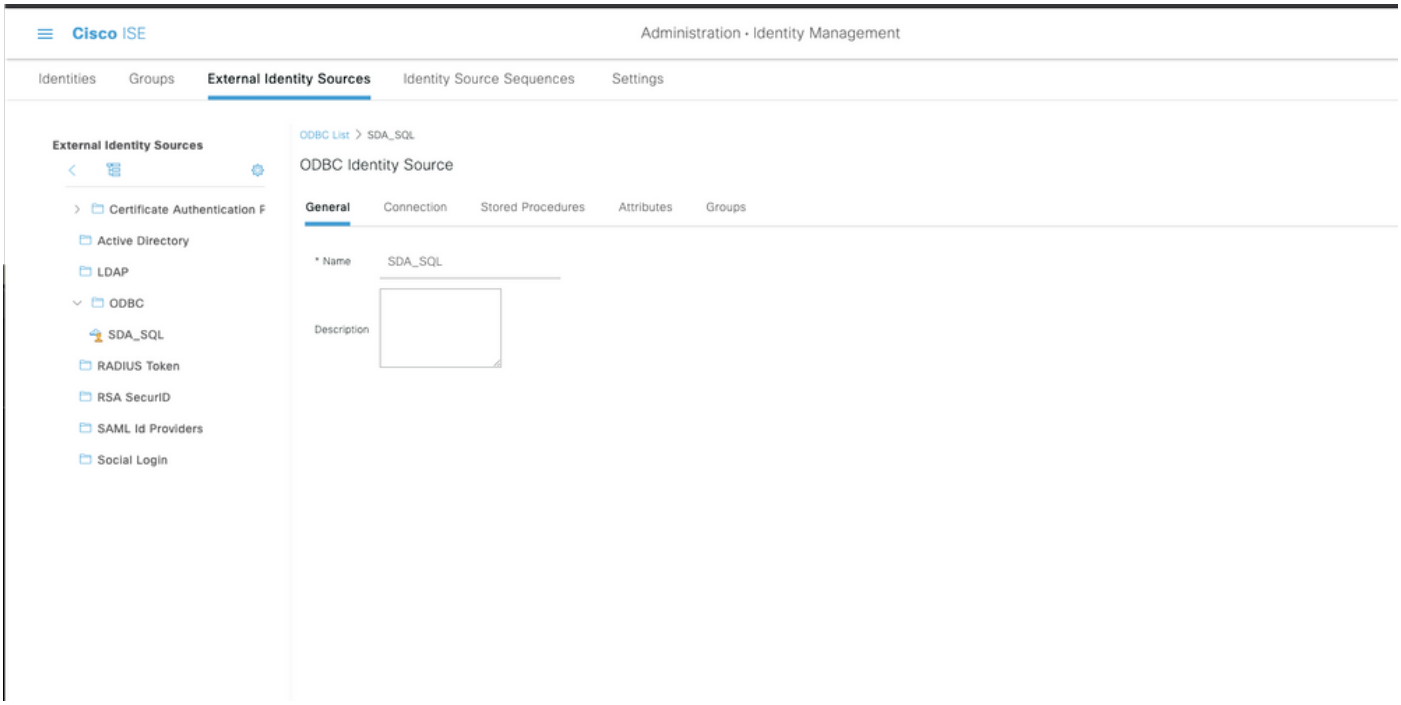
SQL DB to fetch the authorized results such as SGT / VLAN for which **user-id** is used as the reference.



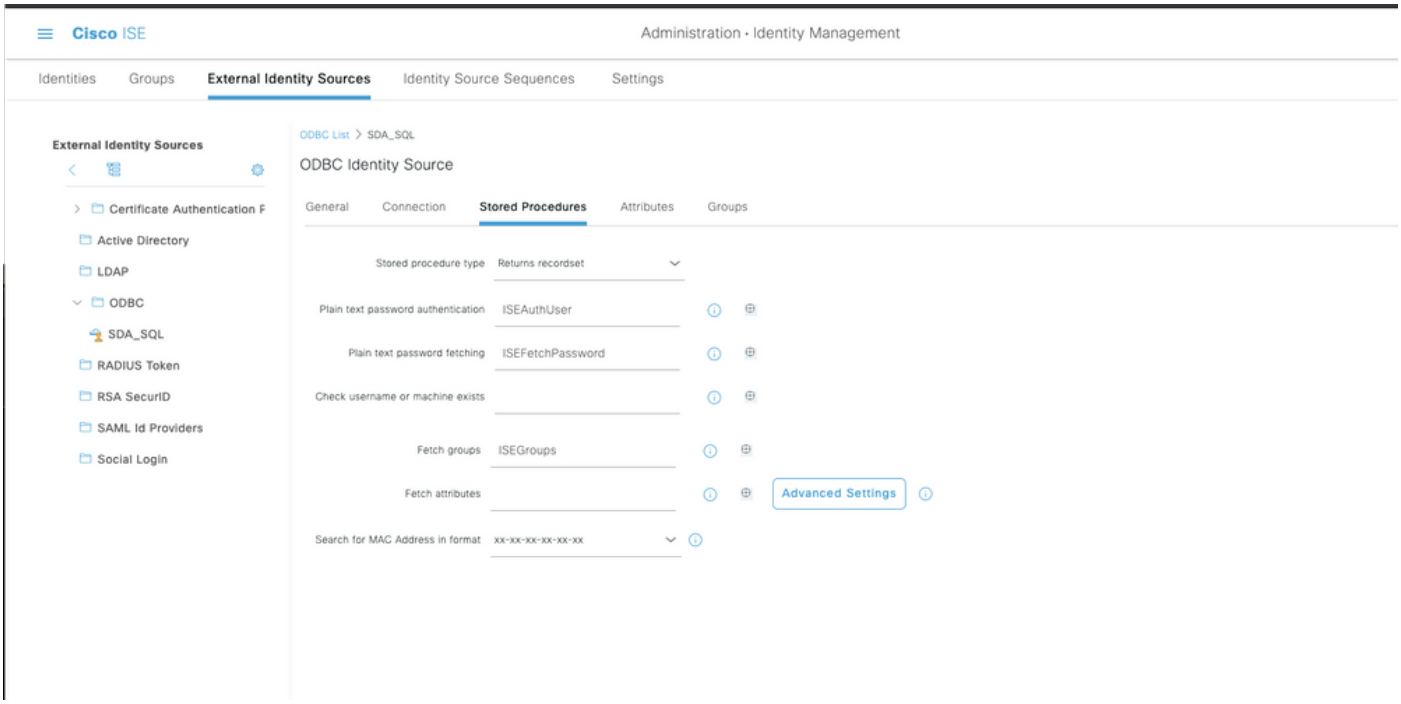
External DB Sample Configurations

Follow the procedure provided earlier in this document to create MS SQL DB along with Username, Password, VLAN id, and SGT.

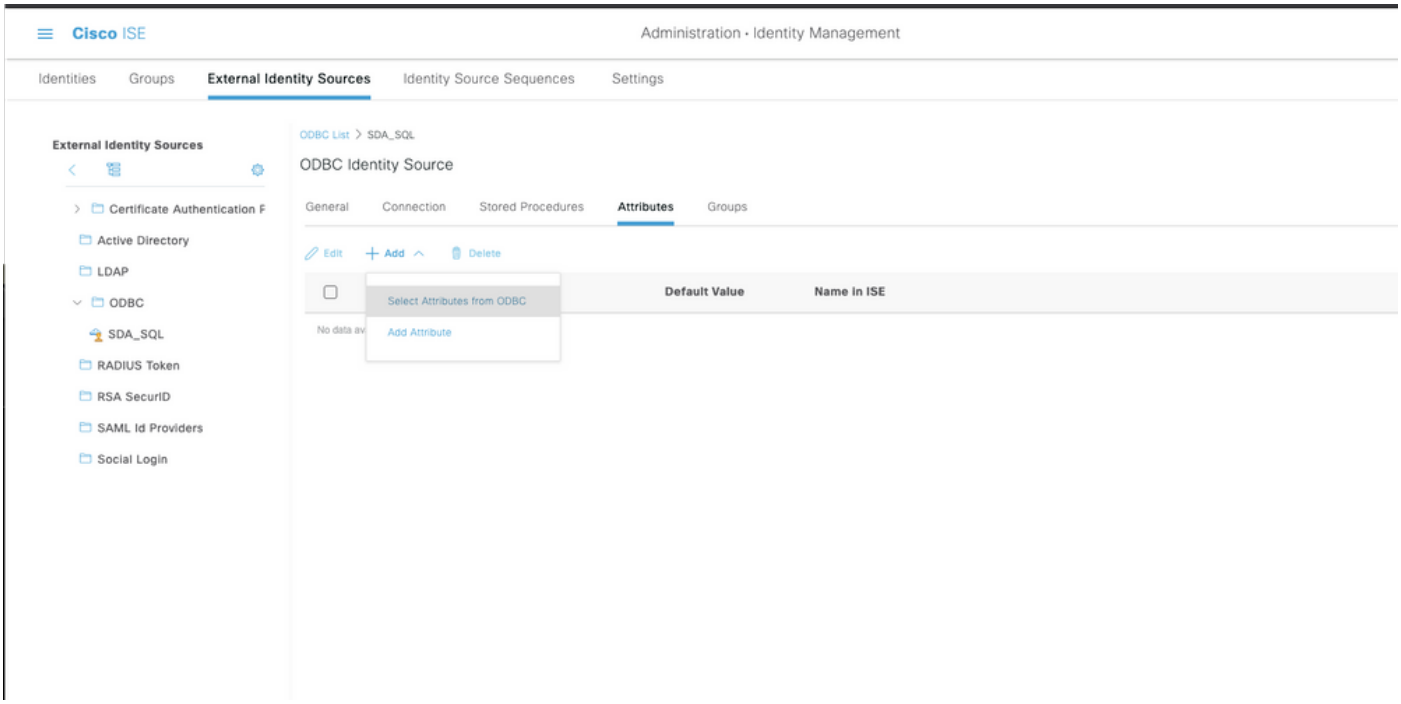
Step 1. Create an ODBC Identity store in Cisco ISE from the menu **Administration > External Identity Source > ODBC** and test the connections.

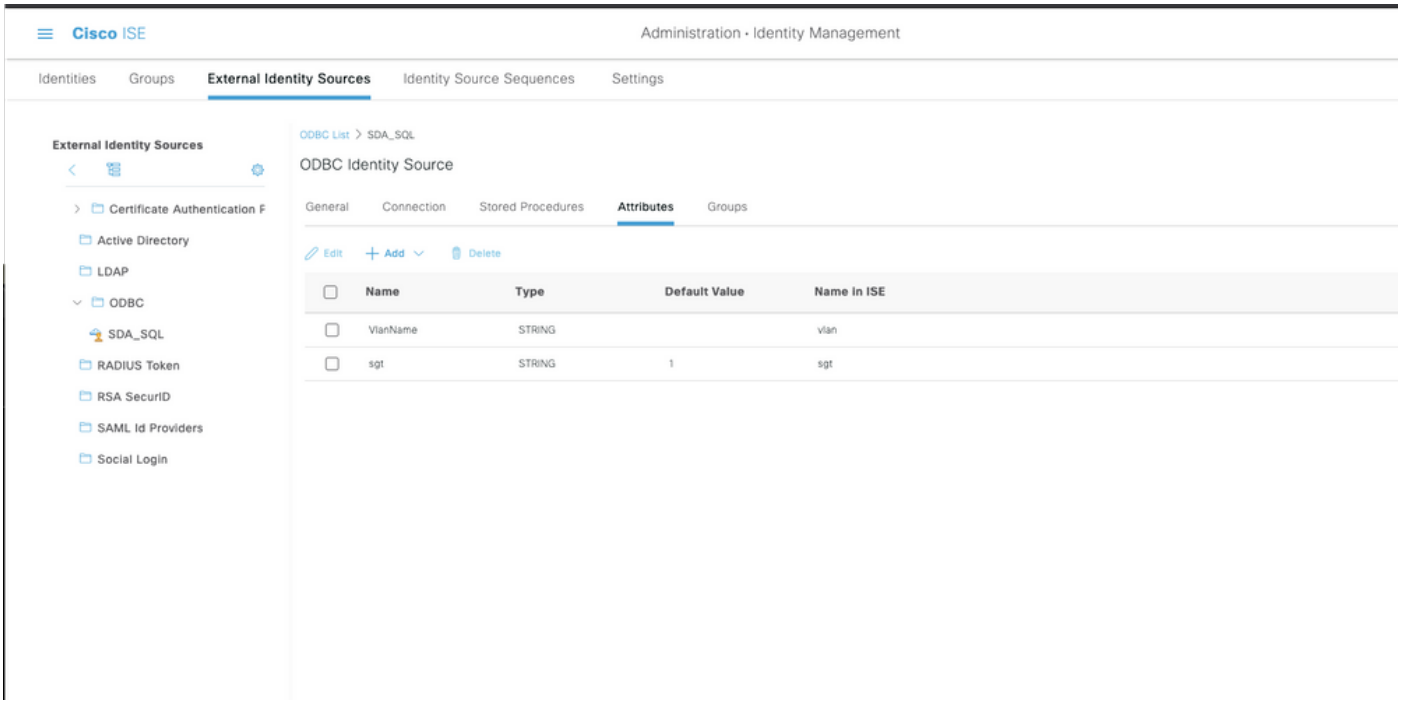


Step 2. Navigate to the Stored Procedures tab on the ODBC page to configure the created procedures in Cisco ISE.

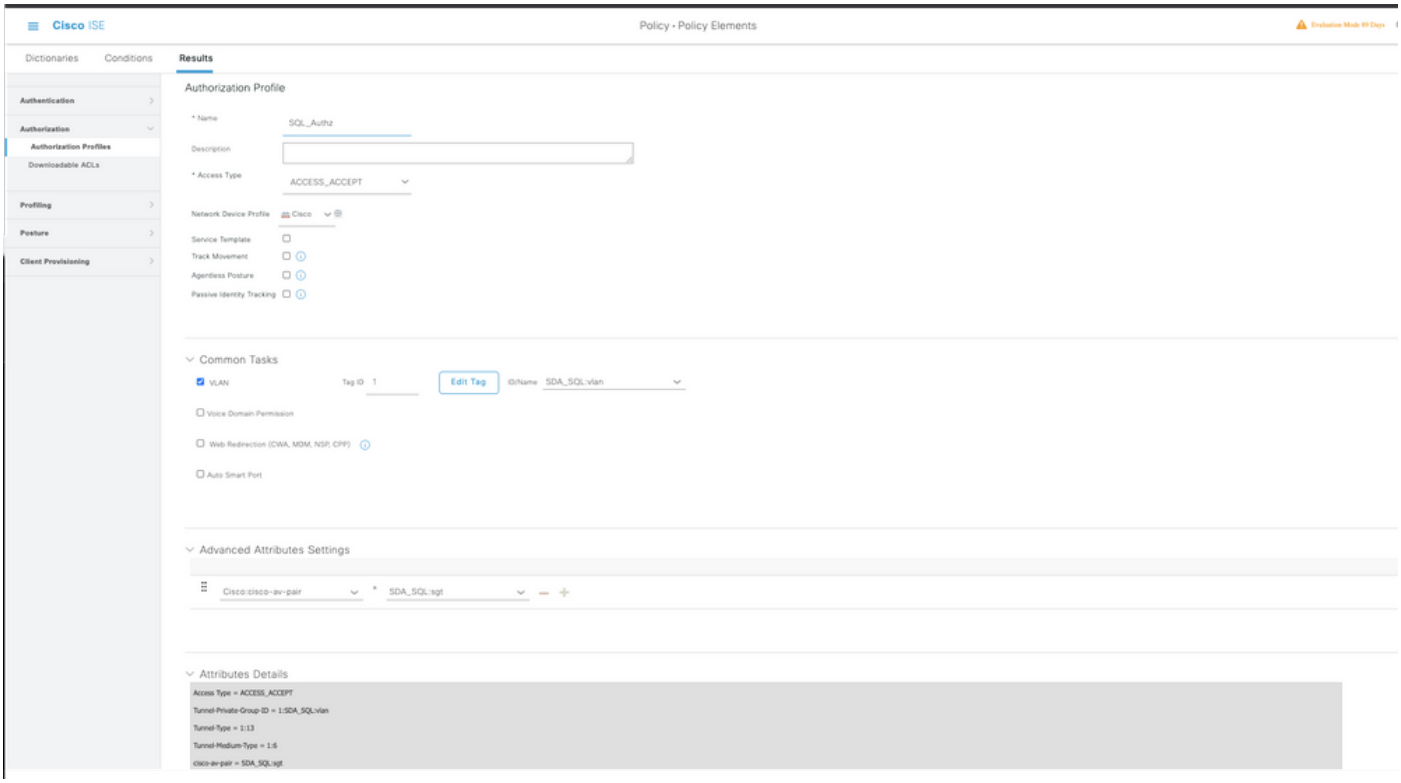


Step 3. Fetch the attributes for user id from the ODBC ID source for verification.

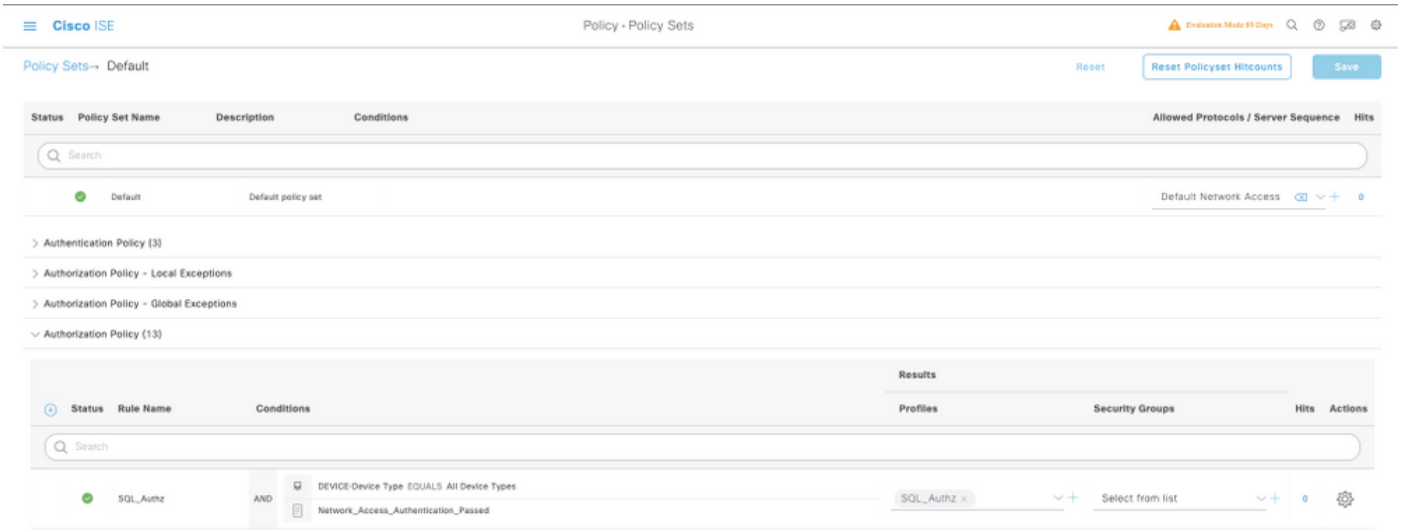




Step 4. Create an **authorization profile** and configure it. In Cisco ISE, go to **Policy > Results > Authorization profile > Advance Attributes Settings** and select the attribute as **Cisco:cisco-av-pair.** Select the values as <name of ODBC database>:sgt. Under Common Tasks, Select **VLAN** with ID/Name as <name of ODBC database>:vlan and save it



Step 5. Create an **authorization policy** and configure it. In Cisco ISE, navigate to **Policy > Policy sets > Authorization Policy > Add.** Put the condition as Identity Source is the SQL server. Select the Result profile as the Authorization profile created previously.

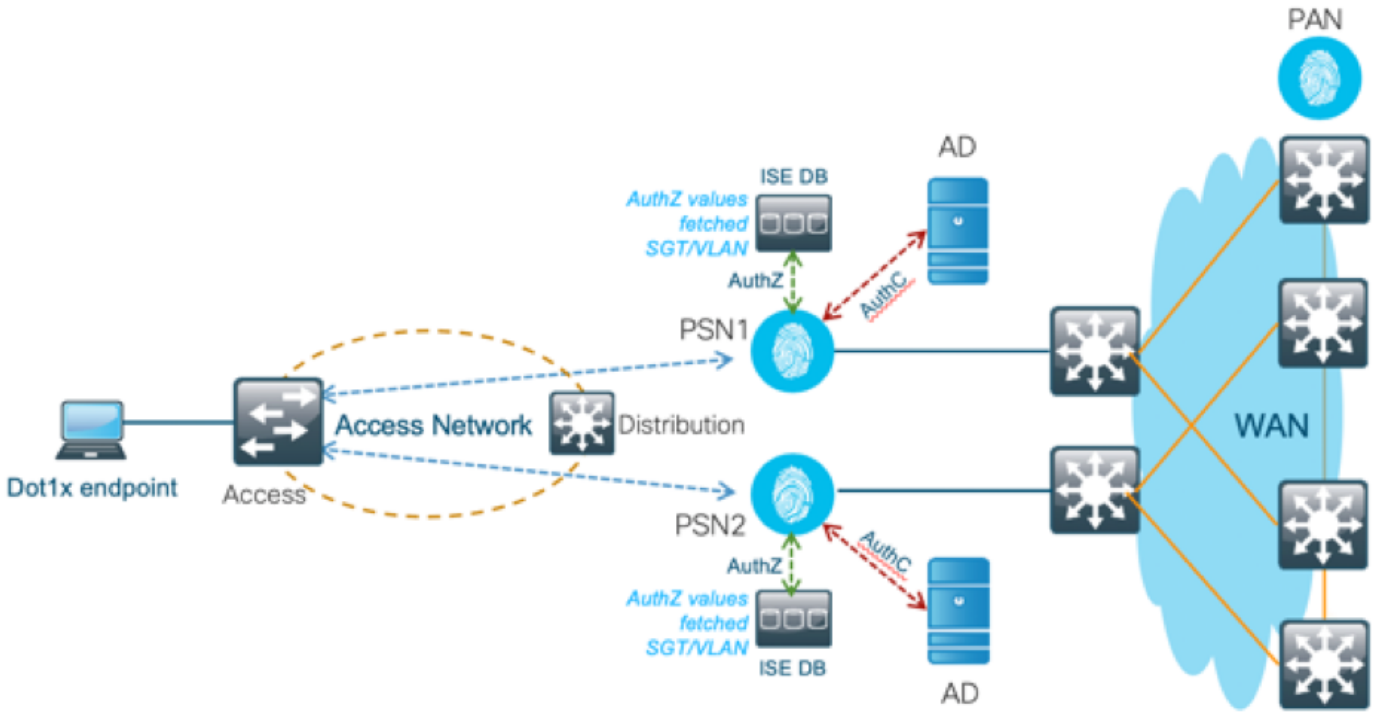


Use Internal DB

Cisco ISE itself has an inbuilt DB that can be utilized to have user-ids for authorization.

Solution Workflow

In this solution, Cisco ISE's internal DB is used as an authorization point while Active Directory (AD) continues to be the authentication source. User-ID of endpoints is included in Cisco ISE DB along with **custom attributes** that return the authorized results such as SGT or VLAN. When the credentials from endpoints are provided to PSN, it checks the validity of the endpoints' credentials with the Active Directory ID store and authenticates the endpoint. The authorization policy refers to the ISE DB to fetch the authorized results such as SGT / VLAN for which user-id is used as the reference.



Advantages

This solution has these advantages, which makes it a flexible solution:

- Cisco ISE DB is an inbuilt solution and therefore it has no 3rd point of failure, unlike the external DB solution.
- As the Cisco ISE cluster ensures real-time synchronization between all personas, there is no WAN dependency as the PSN has all the user-ids and custom attributes pushed from PAN in real-time.
- Cisco ISE can leverage all possible additional features that the external DB offers.
- This solution doesn’t depend on any Cisco ISE scale limits.

Disadvantages

This solution has these disadvantages:

- The maximum number of user-ids Cisco ISE DB can withhold is 300,000.
- Errors caused by manual configuration of user-id to DB must be considered.

Internal DB Sample Configurations

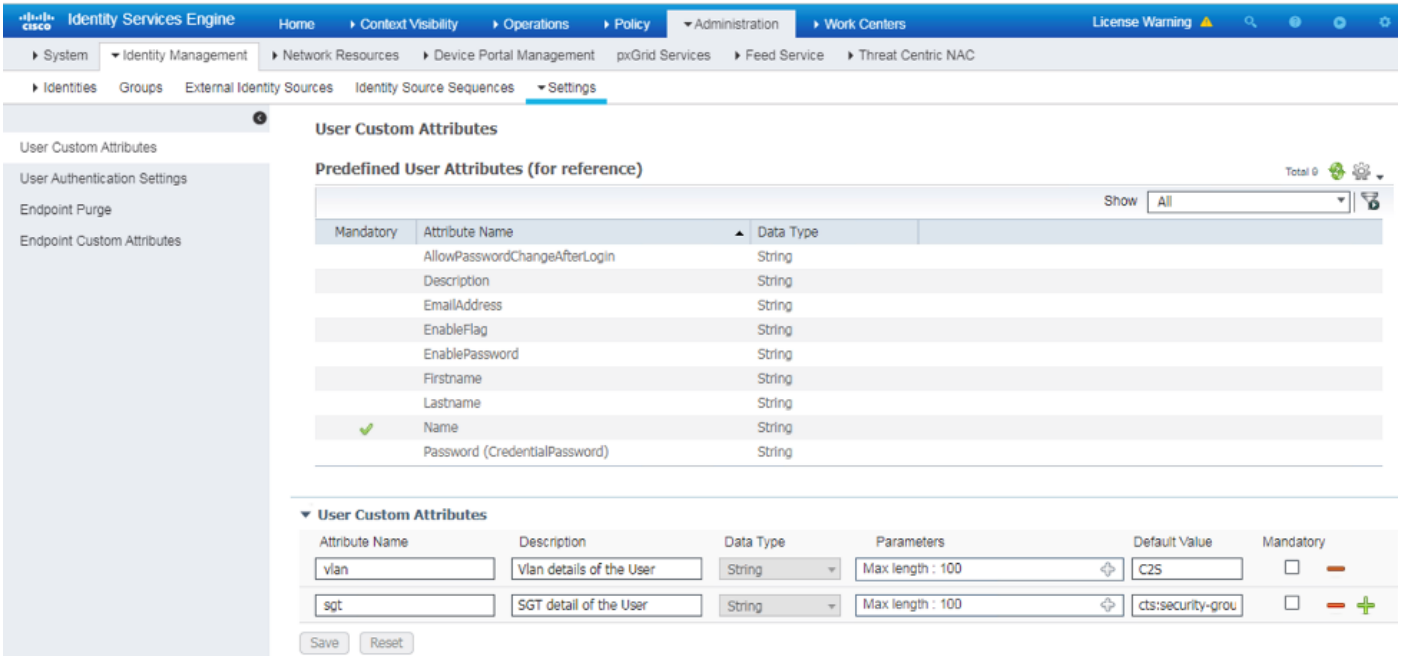
Per-user VLAN & SGT can be configured for any user in the internal ID store with a custom user attribute.

Step 1. Create new user custom attributes to represent the VLAN & SGT value of the respective users. Navigate to **Administration > Identity Management > Settings > User Custom Attributes.** Create new User custom attributes as shown in this table.

Here the ISE DB Table is shown with Custom attributes.

Attribute Name	Data Type	Parameters(Length)	Default Value
vlan	String	100	C2S (Default Vlan Name)
sgt	String	100	cts:security-group-tag=0003-0 (Default SGT value)

- In this scenario, VLAN value represents the vlan name & sgt value represents cisco-av-pair attribute of SGT in Hex.

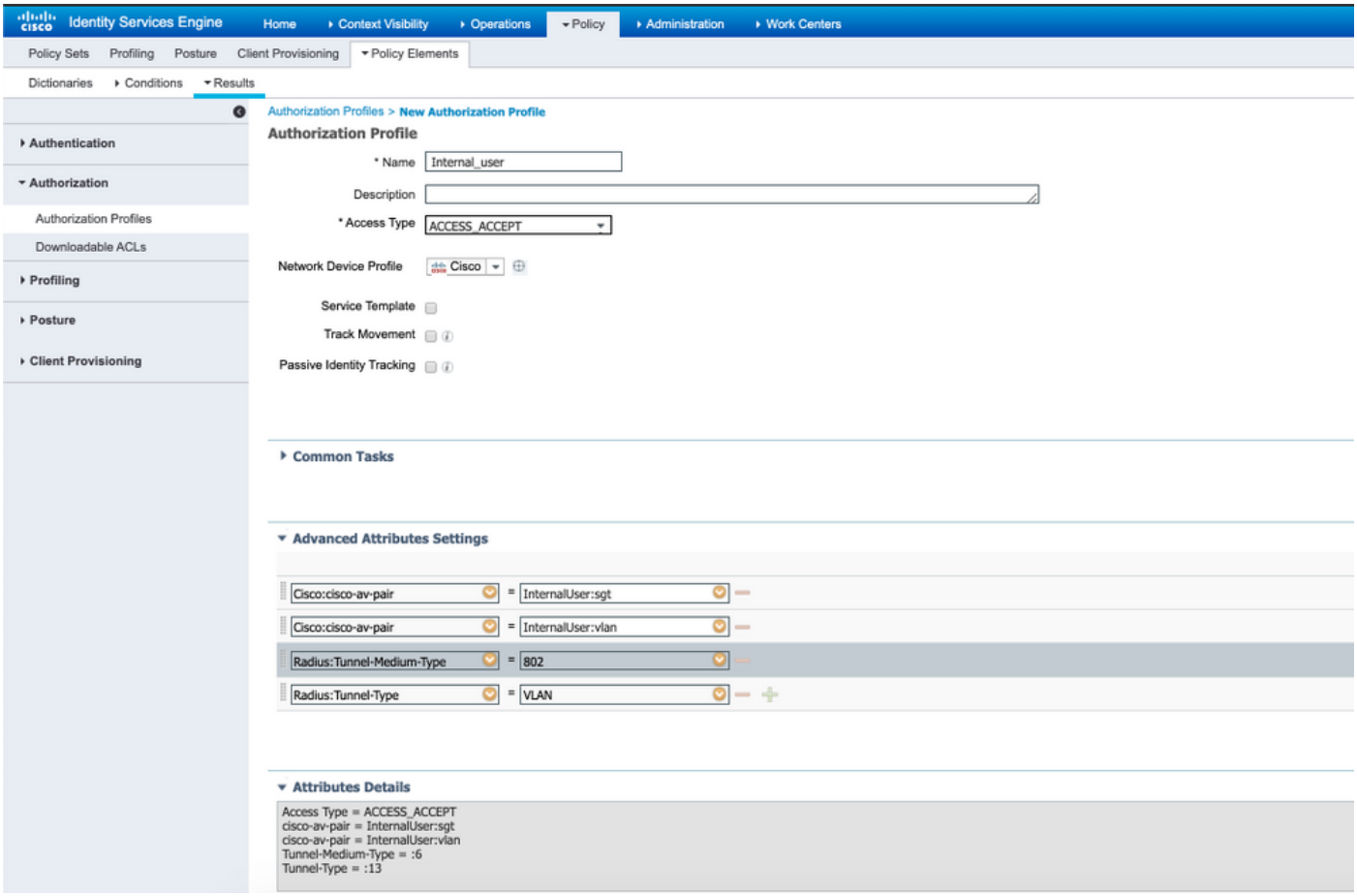


Step 2. Create an authorization Profile with user custom attributes to imply the vlan & sgt values of respective users. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.** Add the below-mentioned attributes under Advanced Attributes Settings.

This table shows the AuthZ Profile for Internal User.

Attribute	**Value**
Cisco:cisco-av-pair	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	InternalUser:vlan
Radius:Tunnel-Medium-Type	802
Radius:Tunnel-Type	VLAN

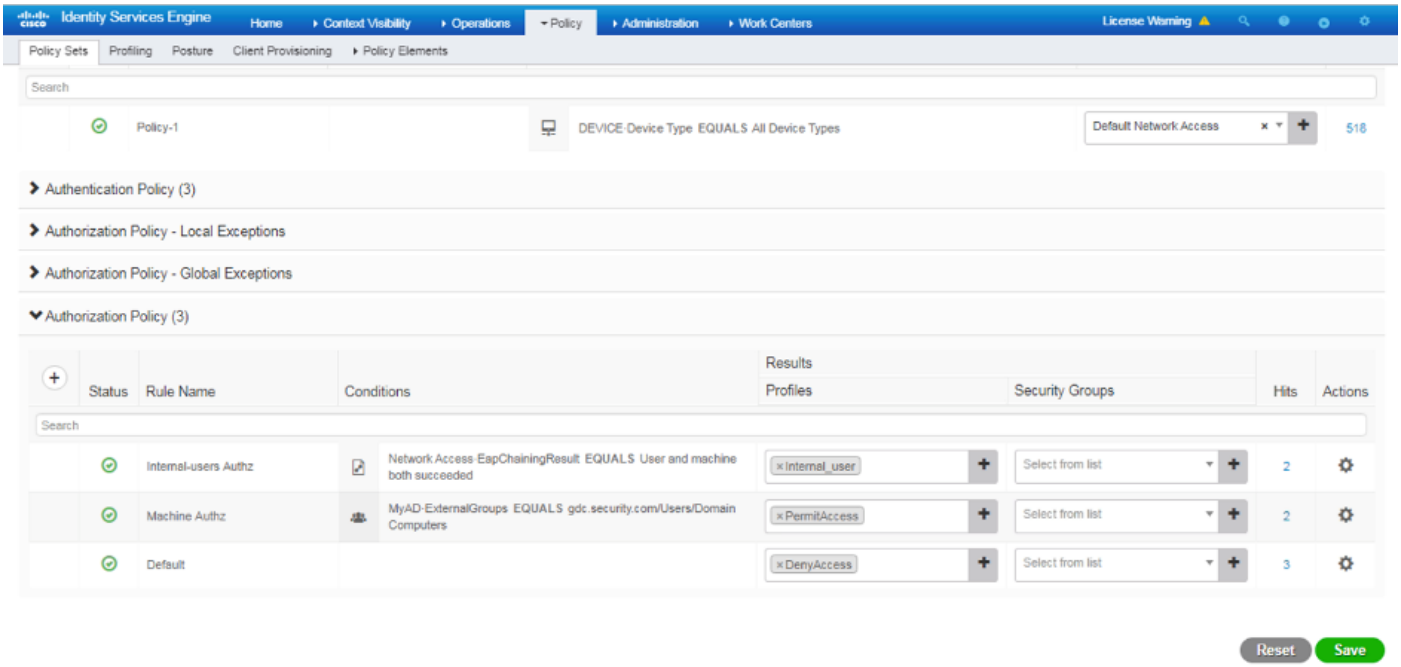
As shown in the image, for the internal users, the profile **Internal_user** is configured with the SGT & Vlan configured as **InternalUser:sgt** & **InternalUser:vlan** respectively.



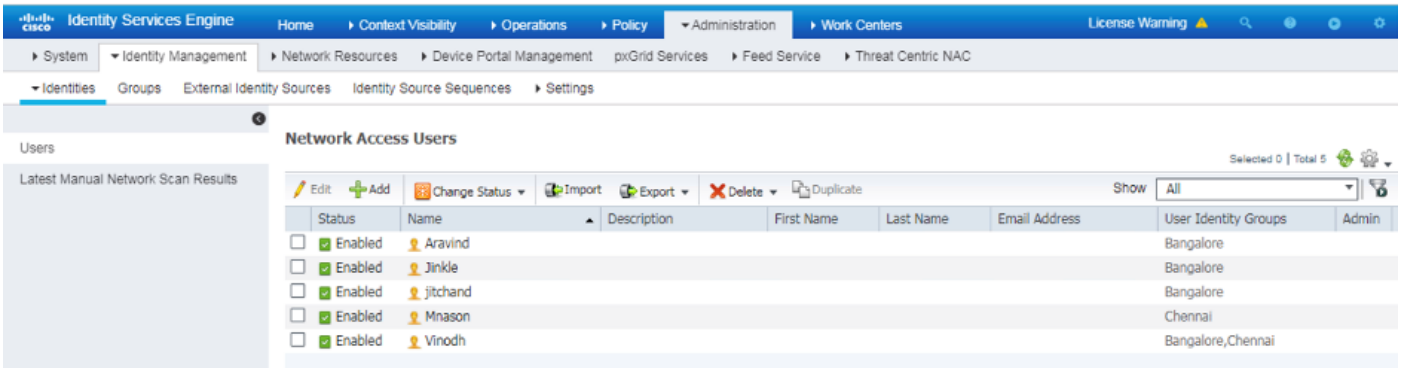
Step 3. Create authorization policy, Navigate to **Policy > Policy Sets > Policy-1 > Authorization.** Create authorization policies with the below-mentioned conditions & map it to respective Authorization profiles.

This table shows the AuthZ Policy for Internal User.

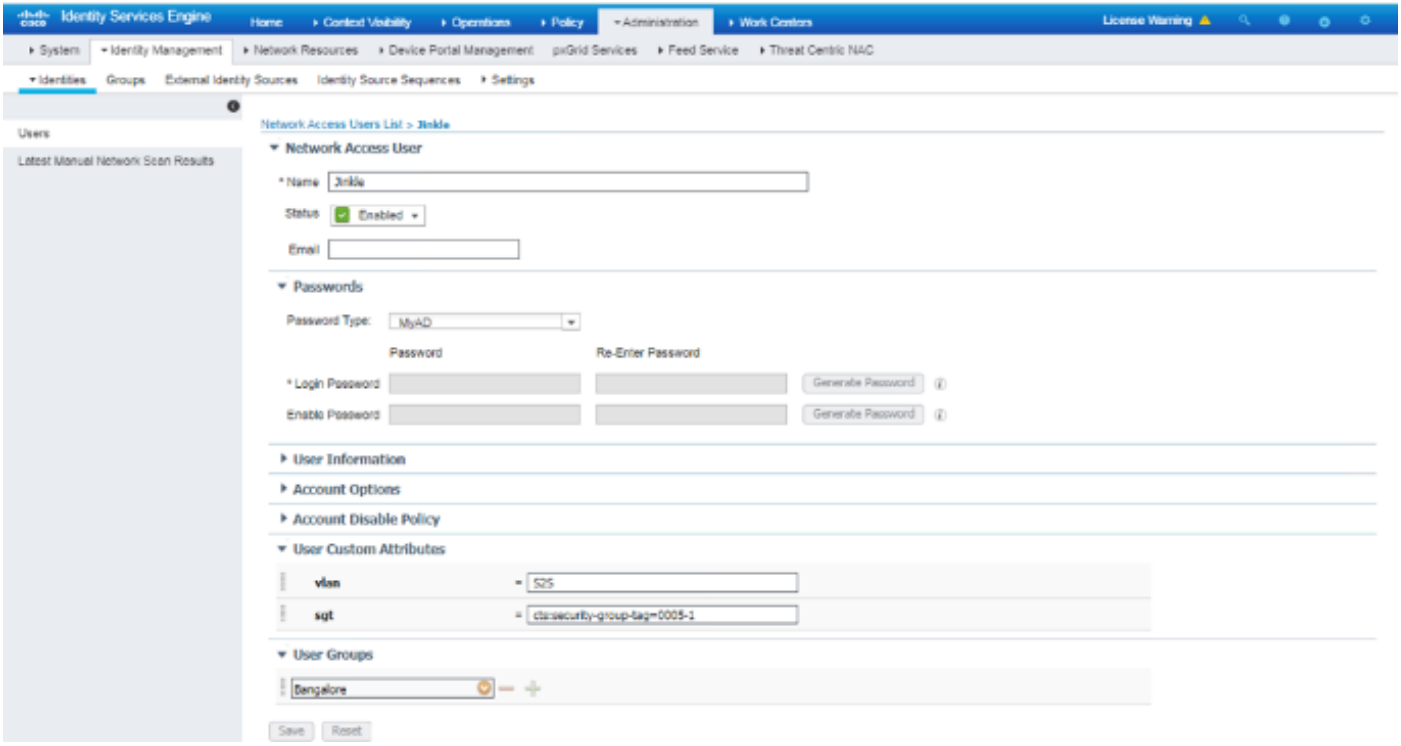
Rule Name	Condition	Result Authz Profile
Internal_User_Authz	If Network Access.EapChainingResults EQUALS User and machine both succeeded	Internal_user
Machine_Only_Authz	If MyAD.ExternalGroups EQUALS gdc.security.com/Users/Domain Computers	PermitAccess



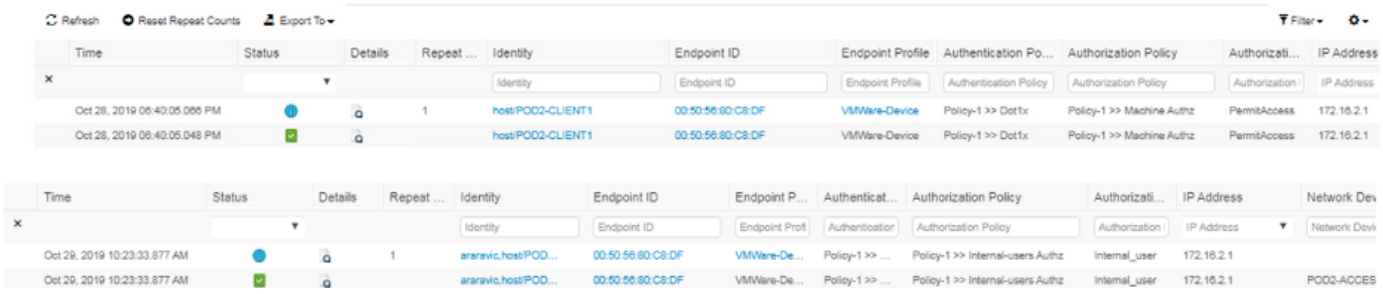
Step 4. Create bulk user identities with custom attributes with user details & their respective custom attributes in the csv template. Import the csv by Navigate to **Administration > Identity Management > Identities > Users > Import > Choose the file > Import.**



This picture shows a sample user with custom attribute details. Select the user & click on edit to view the custom attribute details mapped to the respective user.



Step 5: Verify the live logs:



Check the **Result** section to verify if the **Vlan** & **SGT** attribute is sent as a part of Access-Accept.

Conclusion

This solution allows some of the large enterprise customers to scale up to their requirements. Caution needs to be taken with the addition/deletion of user ids. Errors if triggered, can lead to unauthorized access for genuine users or vice versa.

Related Information

Configure Cisco ISE with MS SQL via ODBC:

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

Glossary

AAA	Authentication Authorization Accounting
AD	Active Directory
AuthC	Authentication
AuthZ	Authorization
DB	Data Base
DOT1X	802.1X
IBN	Identity Based Network
ID	Identity Database
ISE	Identity Services Engine
MnT	Monitoring and Troubleshooting
MsSQL	Microsoft SQL

ODBC	Open DataBase Connectivity
PAN	Policy Admin Node
PSN	Policy Services Node
SGT	Secure Group Tag
SQL	Structured Query Language
VLAN	Virtual LAN
WAN	Wide Area Network