Política de acceso simplificada mediante ODBC e ISE DB (atributo personalizado) para la red de instalaciones a gran escala

Contenido

Introducción

En este documento se describe la implementación a gran escala en instalaciones sin poner en peligro sus funciones y la aplicación de la seguridad. La solución de seguridad para terminales de Cisco, Identity Services Engine (ISE), cumple este requisito mediante la integración con una fuente de identidad externa.

En el caso de redes a gran escala con más de 50 ubicaciones geográficas, más de 4000 perfiles de usuario diferentes y 600 000 terminales o más, las soluciones IBN tradicionales deben considerarse desde una perspectiva diferente, más que solo características, independientemente de si se amplían con todas ellas. La solución de red basada en intención (IBN) de las redes tradicionales a gran escala de hoy en día requiere centrarse más en la escalabilidad y la facilidad de gestión, y no solo en sus funciones.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

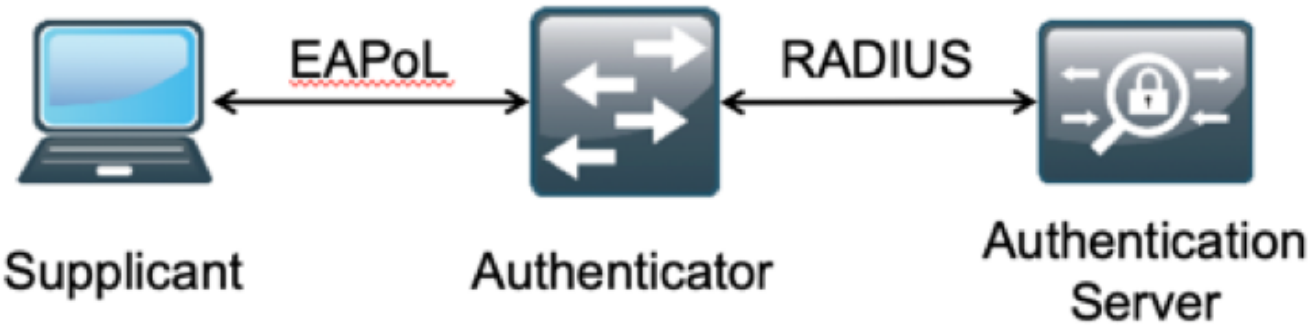
- Cisco Identity Services Engine (ISE) versión 2.6, parche 2 y versión 3.0
- Windows Active Directory (AD) Server 2008 Versión 2
- Microsoft SQL Server 2012

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. Si la red está activa, asegúrese de comprender el impacto potencial de cualquier configuración.

Antecedentes

En una solución de red basada en identidad (IBN), los elementos básicos son el suplicante, el autenticador y el servidor de autenticación (AAA). El Suplicante es un agente del terminal que proporciona las credenciales cuando se le solicita acceso a la red. El autenticador o NAS (Network Access Server) es la capa de acceso, que comprende los switches de red y los WLC que llevan las credenciales al servidor AAA. El Servidor de autenticación valida la solicitud de autenticación de usuario contra un almacén de ID y autoriza con un access-accept o access-reject. El almacén de ID puede estar dentro del servidor AAA o en un servidor dedicado externo.

Esta imagen muestra los elementos básicos de IBN.



RADIUS es un protocolo basado en protocolo de datagramas de usuario (UDP) con autenticación y autorización acopladas. En la solución IBN de Cisco para instalaciones empresariales, el personaje del nodo de servicios de políticas (PSN) de ISE actúa como el servidor AAA que autentica los terminales frente al almacén de ID de empresa y autoriza en función de una

condición.

En Cisco ISE, las políticas de autenticación y autorización se configuran para cumplir estos requisitos. Las políticas de autenticación están formadas por el tipo de medio, ya sea por cable o inalámbrico, y los protocolos EAP para la validación de usuarios. Las políticas de autorización constan de condiciones que definen los criterios con los que deben coincidir los distintos terminales y el resultado del acceso a la red, que puede ser una VLAN, una ACL descargable o una etiqueta de grupo seguro (SGT). Se trata de los números de escala máxima para las políticas con las que se puede configurar ISE.

Esta tabla muestra la Escala de políticas de Cisco ISE.

Atributo	Número de escala
Número máximo de reglas de autenticación	1000 (modo de conjunto de políticas)
Número máximo de reglas de autorización	3000 (modo de conjunto de políticas) con perfiles Authz 3200

Tendencias de tecnología

La segmentación se ha convertido en uno de los elementos de seguridad clave para las redes empresariales actuales, sin necesidad de una red periférica real. Los terminales pueden desplazarse entre las redes internas y externas. La segmentación ayuda a contener cualquier ataque de seguridad en un segmento concreto para que se extienda por la red. La solución actual de acceso definido por software (SDA) con la ayuda de TrustSec de Cisco ISE ofrece una forma de segmentar en función del modelo empresarial del cliente para evitar dependencias de elementos de red como VLAN o subredes IP.

Problema

Configuración de políticas de ISE para redes empresariales a gran escala con más de 500 perfiles de terminales diferentes; el número de políticas de autorización puede aumentar hasta un punto inmanejable. Incluso si Cisco ISE admite condiciones de autorización dedicadas para hacer frente a un volumen de perfiles de usuario de este tipo, existe el reto de que los administradores administren estas numerosas políticas.

Además, es posible que los clientes necesiten políticas de autorización comunes en lugar de políticas específicas para evitar gastos generales de gestión y que también tengan un acceso a la red diferenciado para los terminales en función de sus criterios.

Por ejemplo, piense en una red empresarial con Active Directory (AD) como **fuente fidedigna** y el diferenciador único del terminal es uno de los atributos de AD. En tal caso, la forma tradicional de configuración de políticas tiene más políticas de autorización para cada perfil de terminal único.

En este método, cada perfil de extremo se distingue con un atributo AD en domain.com. Por lo tanto, es necesario configurar una política de autorización dedicada.

Esta tabla muestra las Políticas de AuthZ Tradicionales.

Política	Si AnyConnect EQUIVALE a User-AND-Machine-Both-Passed

ABC	Y Si AD-Group ES IGUAL A domain.com/groups/ABC LUEGO SGT:C2S-ABC Y VLAN:1021 Si AnyConnect EQUIVALE a User-AND-Machine-Both-Passed
DEF-Policy	Y Si AD-Group ES IGUAL A domain.com/groups/DEF LUEGO SGT:C2S-DEF Y VLAN:1022 Si AnyConnect EQUIVALE a User-AND-Machine-Both-Passed
Política de GHI	Y Si AD-Group ES IGUAL A domain.com/groups/GHI LUEGO SGT:C2S-GHI Y VLAN:1023 Si AnyConnect EQUIVALE a User-AND-Machine-Both-Passed
Política XYZ	Y Si AD-Group ES IGUAL A domain.com/groups/XYZ LUEGO SGT:C2S-XYZ Y VLAN:1024

Solución propuesta

Para evitar la brecha en el número máximo escalable de políticas de autorización admitidas en Cisco ISE, la solución propuesta consiste en utilizar una base de datos externa que autorice cada terminal con el resultado de autorización obtenido a partir de sus atributos. Por ejemplo, si AD se utiliza como una base de datos externa para la autorización, se puede hacer referencia a cualquier atributo de usuario no utilizado (como el código de departamento o PIN) para proporcionar resultados autorizados asignados con SGT o VLAN.

Esto se consigue mediante la integración de Cisco ISE con una base de datos externa o con la base de datos interna de ISE configurada con atributos personalizados. Esta sección explica la implementación de estos 2 escenarios:

> **Nota:** En ambas opciones, la BD contiene el **user-id** pero no la **contraseña** de los puntos finales DOT1X. DB se utiliza solamente como punto de **autorización**. La autenticación puede seguir siendo el almacén de ID del cliente que, en la mayoría de los casos, reside en el servidor de Active Directory (AD).

Configuración con BD externa

Cisco ISE se integra con una base de datos externa para la validación de credenciales de terminales:

Esta tabla muestra los orígenes de identidad externos validados.

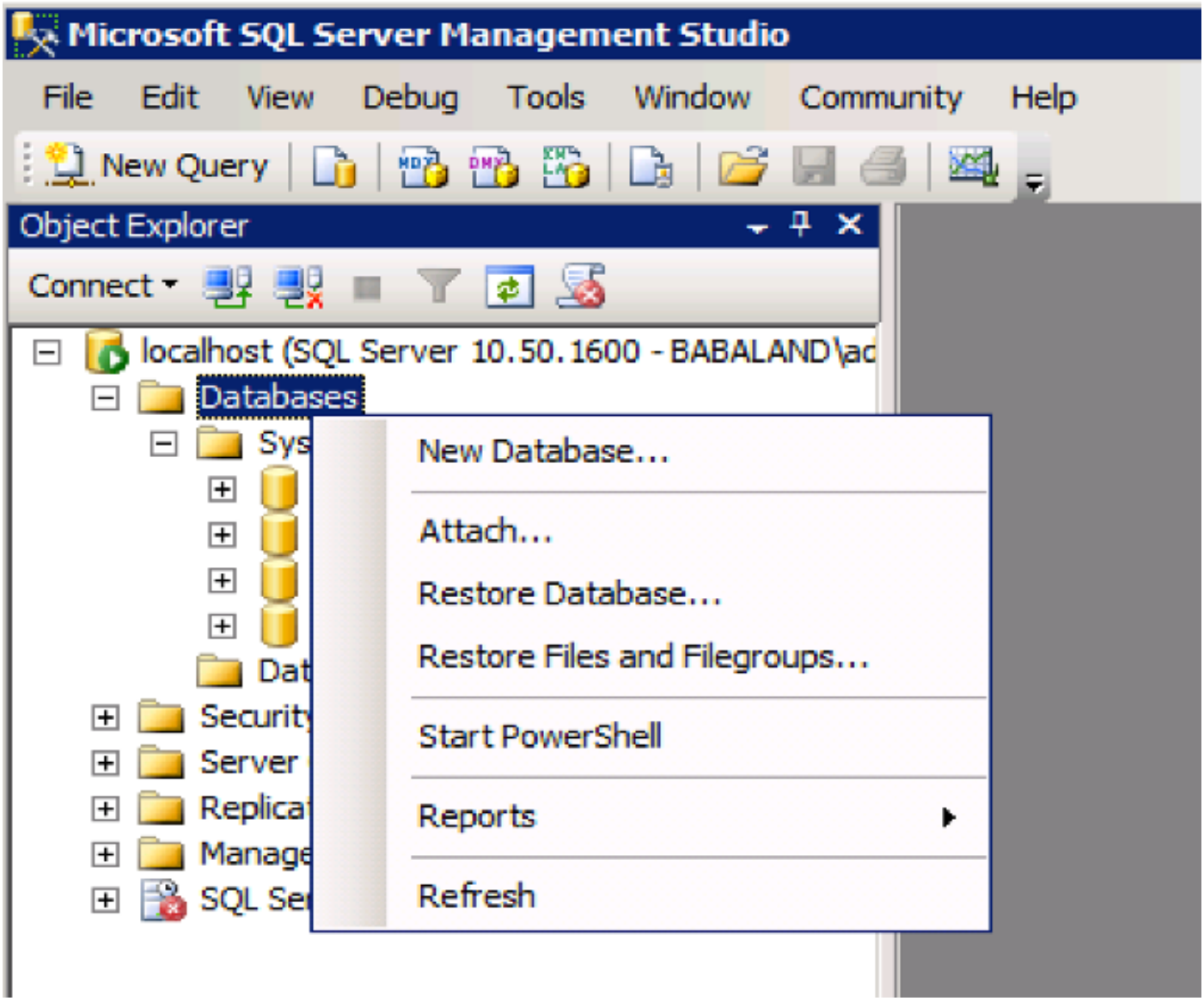
Origen de identidad externa	SO/Versión
Directorio activo	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—

Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—
Servidores LDAP	
Servidor de directorio LDAP SunONE	Versión 5.2
Servidor de directorio OpenLDAP	Versión 2.4.23
Cualquier servidor compatible con LDAP v3	—
Servidores Token	
RSA ACE/Server	Serie 6.x
Administrador de autenticación RSA	Series 7.x y 8.x
Cualquier servidor de tokens compatible con RADIUS RFC 2865	—
Inicio de sesión único (SSO) mediante el lenguaje de marcado de aserción de seguridad (SAML)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Versión 11.1.2.2.0
Oracle Identity Federation (OIF)	Versión 11.1.1.2.0
Servidor PingFederate	Versión 6.10.0.4
Nube de PingOne	—
Autenticación segura	8.1.1
Cualquier proveedor de identidad compatible con SAMLv2	—
Origen de identidad de conectividad abierta de bases de datos (ODBC)	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition versión 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Inicio de sesión en redes sociales (para cuentas de usuarios invitados)	
Facebook	—

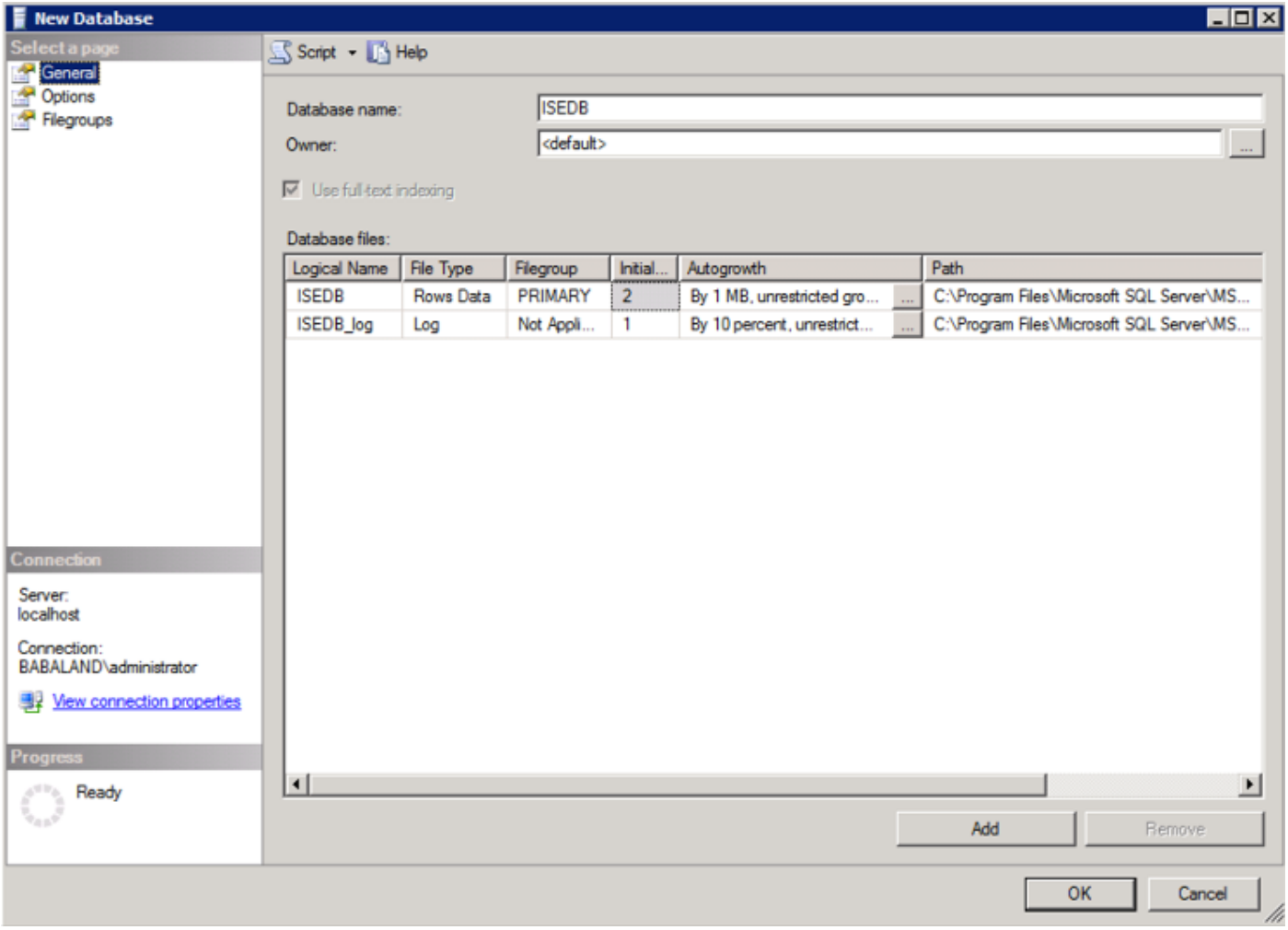
Configuraciones de ejemplo de ODBC

Esta configuración se realiza en Microsoft SQL para generar la solución:

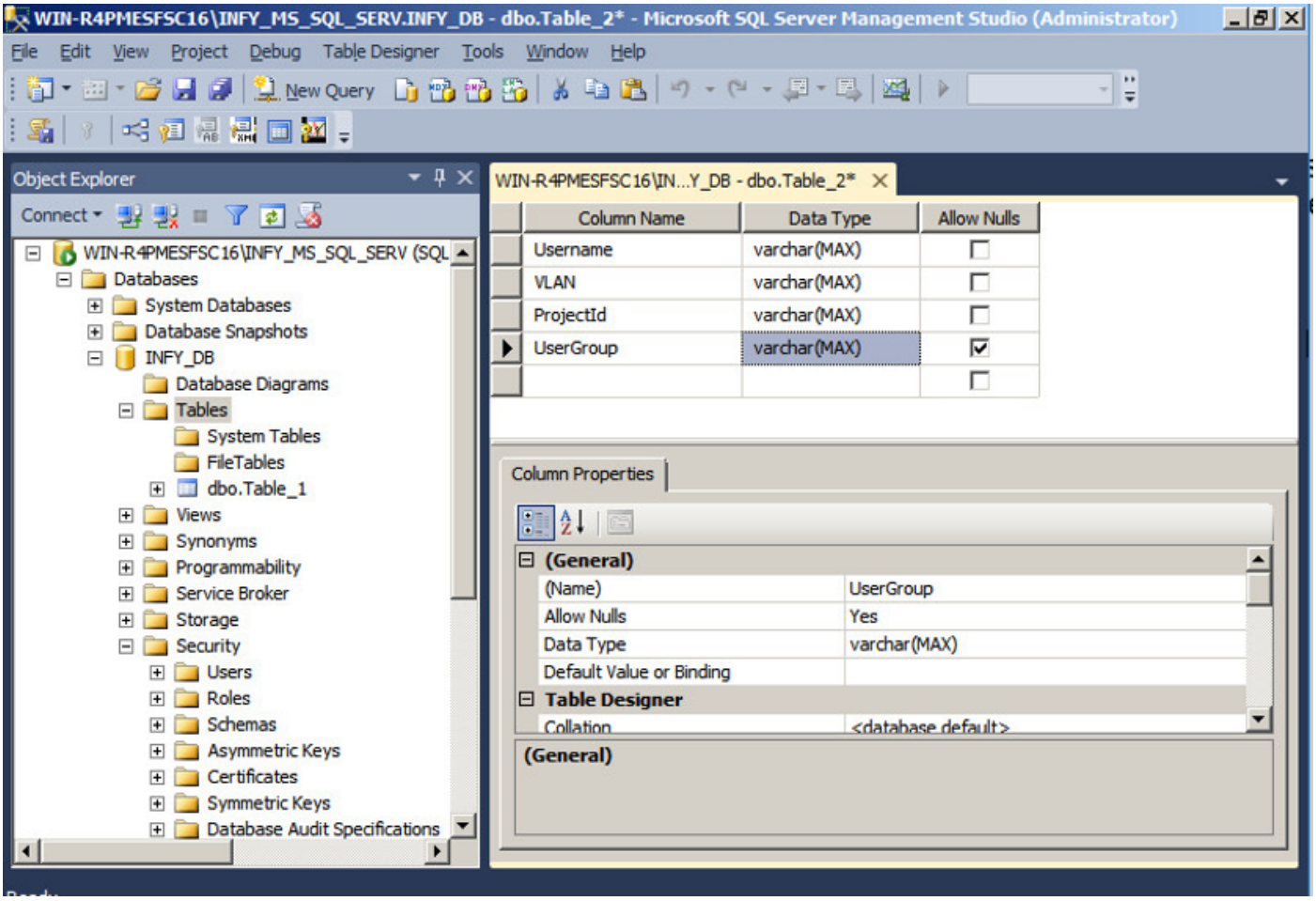
Paso 1. Abra SQL Server Management Studio (**menú Inicio > Microsoft SQL Server**) para crear una base de datos:



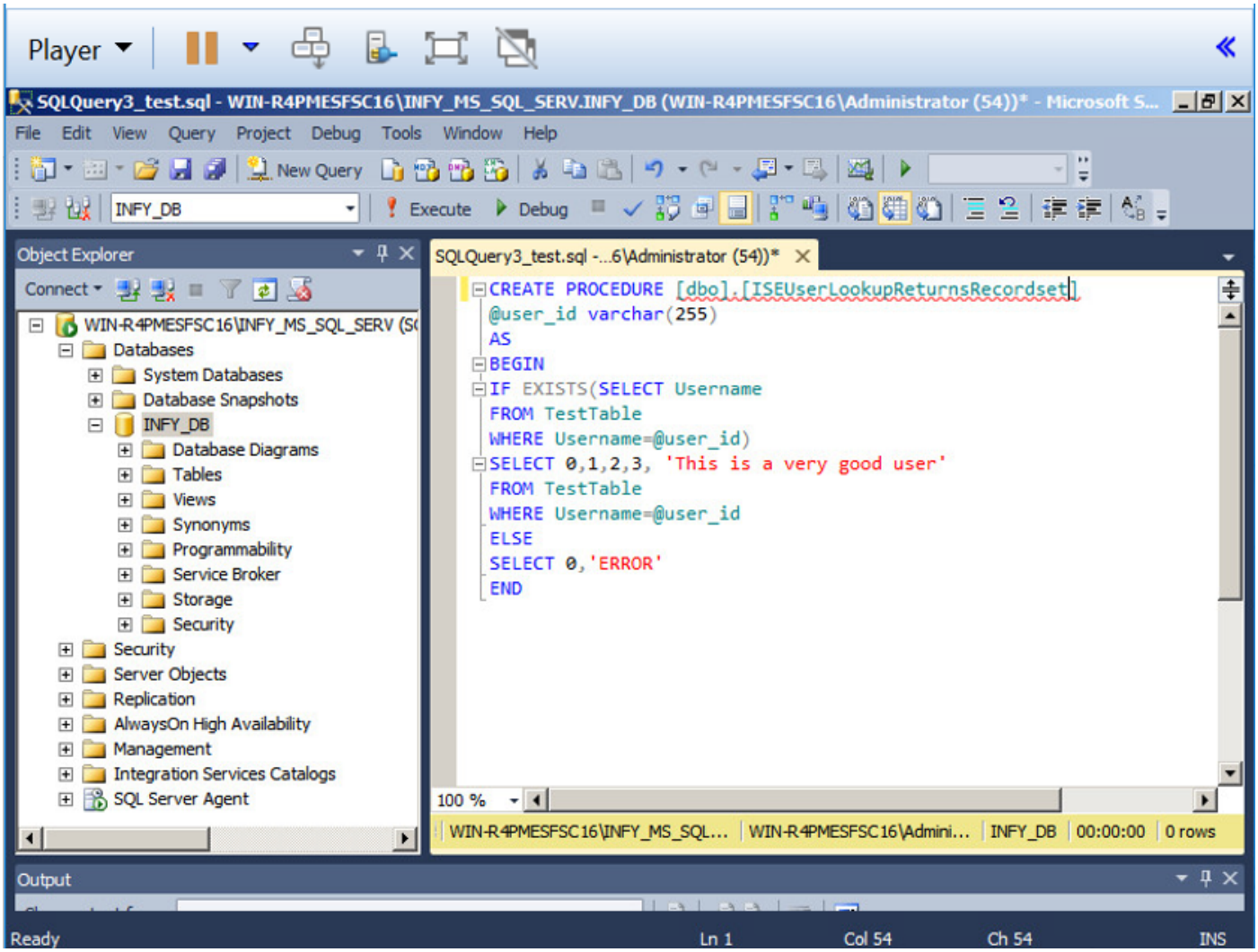
Paso 2. Proporcione un nombre y cree la base de datos.



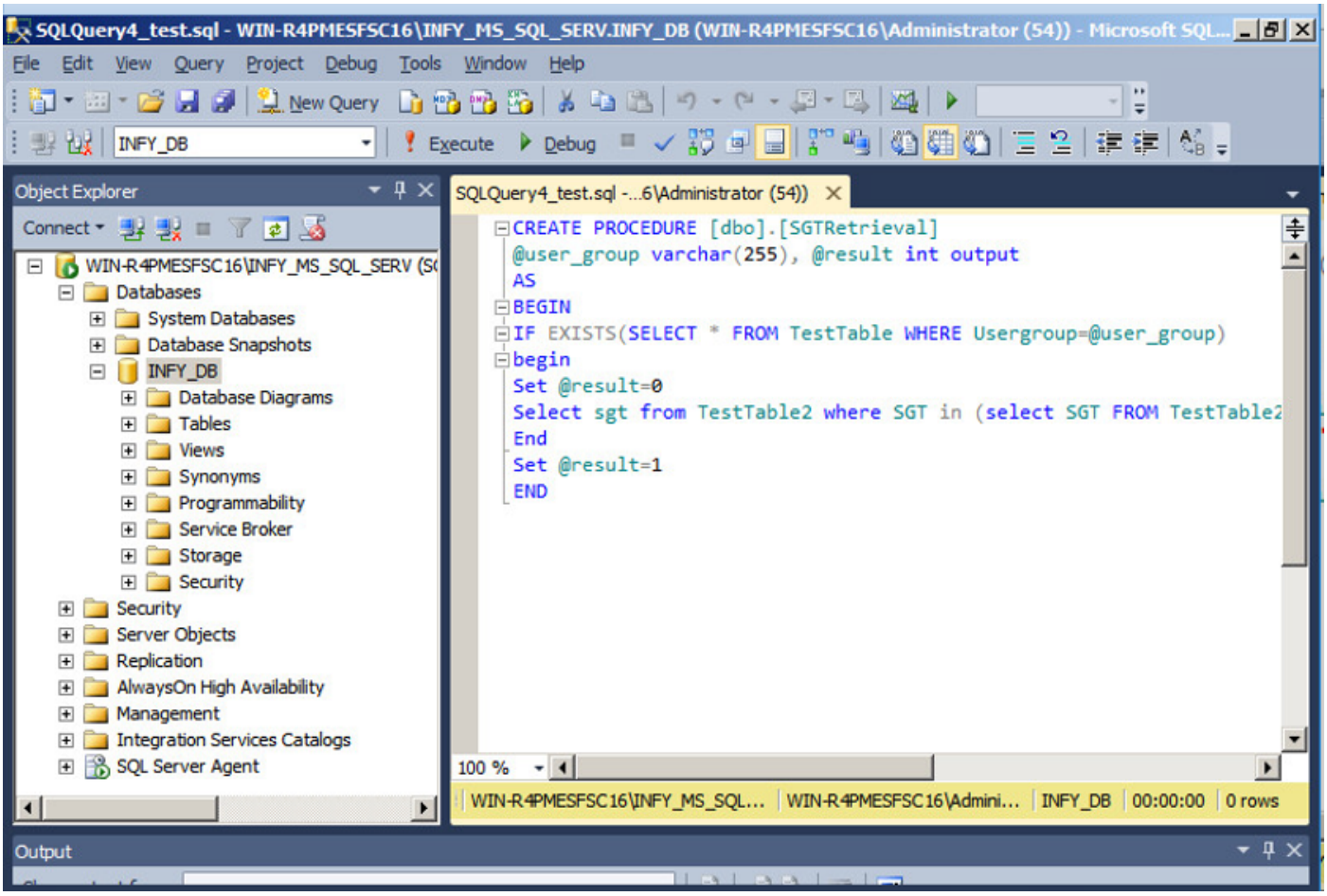
Paso 3. Cree una nueva tabla con las columnas requeridas como parámetros para que los terminales se autoricen.



Paso 4. Cree un **procedimiento** para verificar si existe el nombre de usuario.



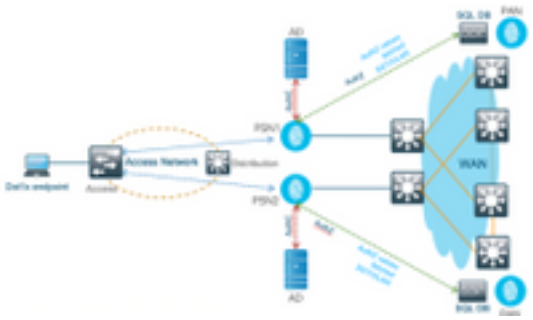
Paso 5. Cree un procedimiento para recuperar atributos (SGT) de la tabla.

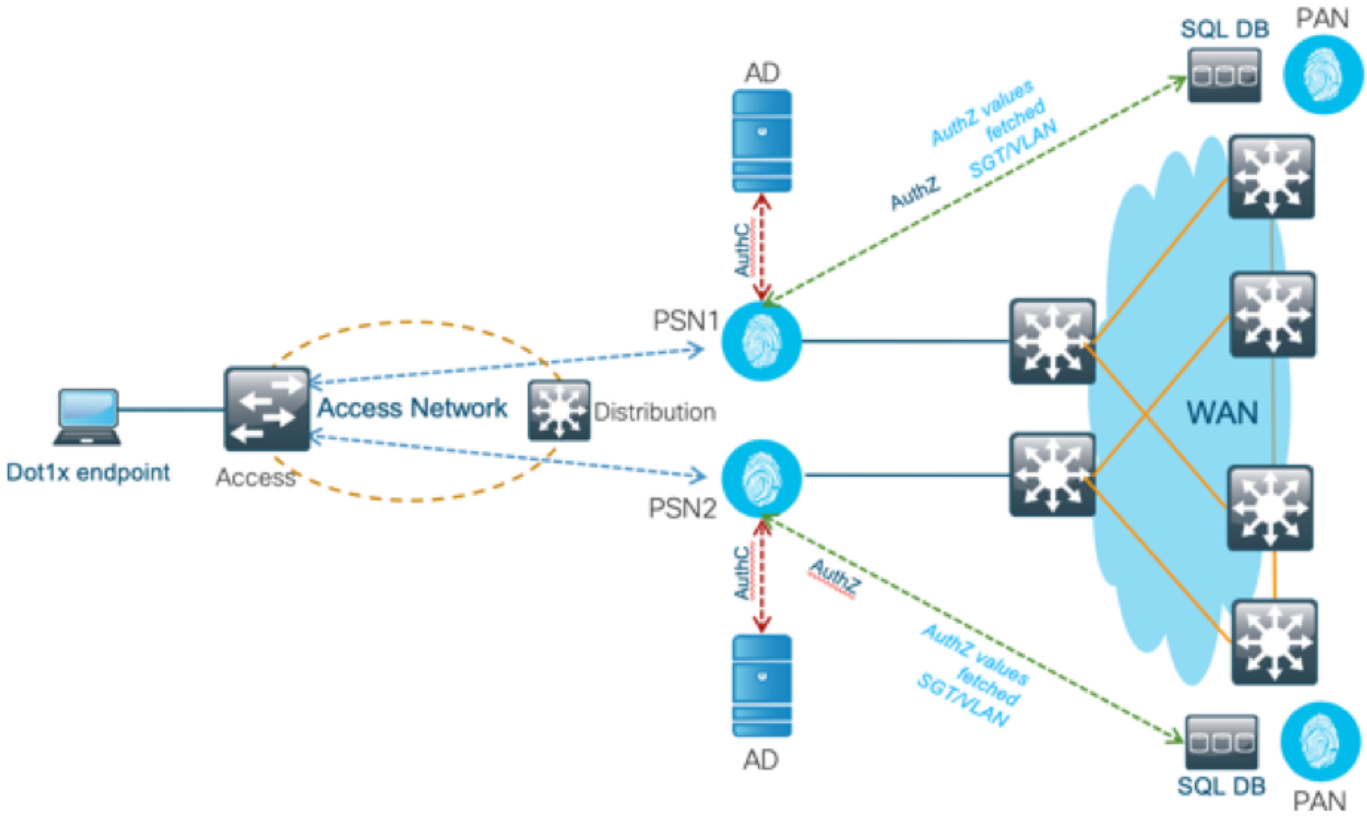


En este documento, Cisco ISE se integra con la solución Microsoft SQL para cumplir los requisitos de ampliación de autorización en redes de grandes empresas.

Flujo de trabajo de la solución (ISE 2.7 y versiones anteriores)

En esta solución, Cisco ISE se integra con Active Directory (AD) y Microsoft SQL. AD se utiliza como almacén de Id. de autenticación y MS SQL para la autorización. Durante el proceso de autenticación, el dispositivo de acceso a la red (NAD) reenvía las credenciales del usuario a PSN, el servidor AAA de la solución IBN. PSN valida las credenciales del extremo con el almacén de ID de Active Directory y autentica al usuario. La política de autorización se refiere a la base de datos MS SQL para obtener los resultados autorizados, como SGT/VLAN, para los cuales se utiliza **user-id** como referencia.





Ventajas

Esta solución tiene estas ventajas, que la hacen flexible:

- Cisco ISE puede aprovechar todas las funciones adicionales posibles que ofrece la base de datos externa.
- Esta solución no depende de los límites de escalabilidad de Cisco ISE.

Desventajas

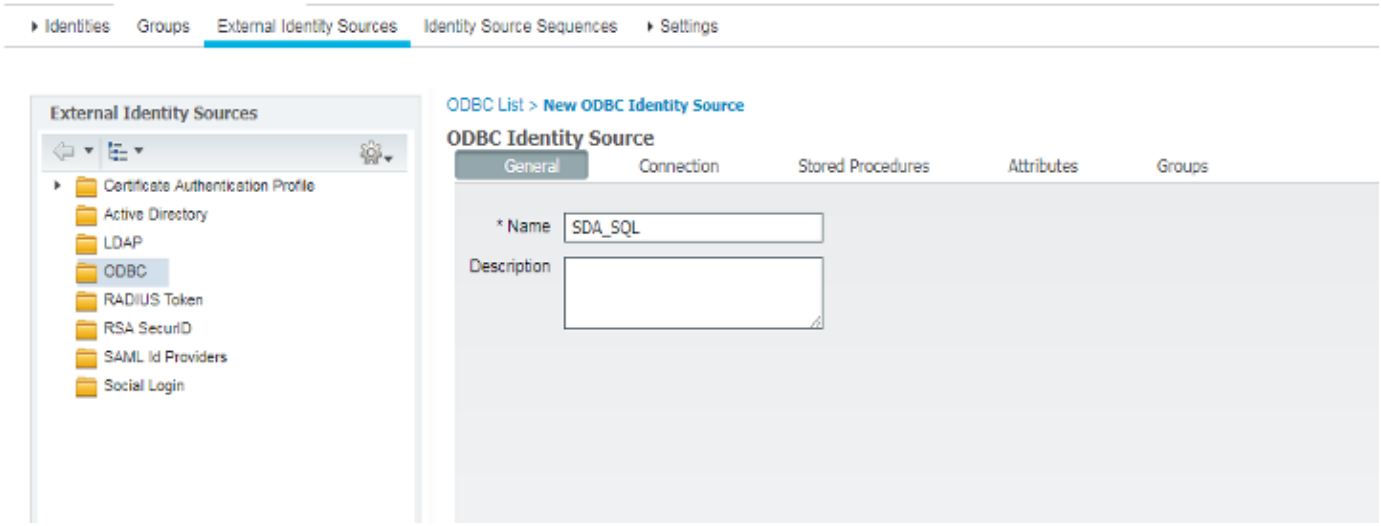
Esta solución tiene estas desventajas:

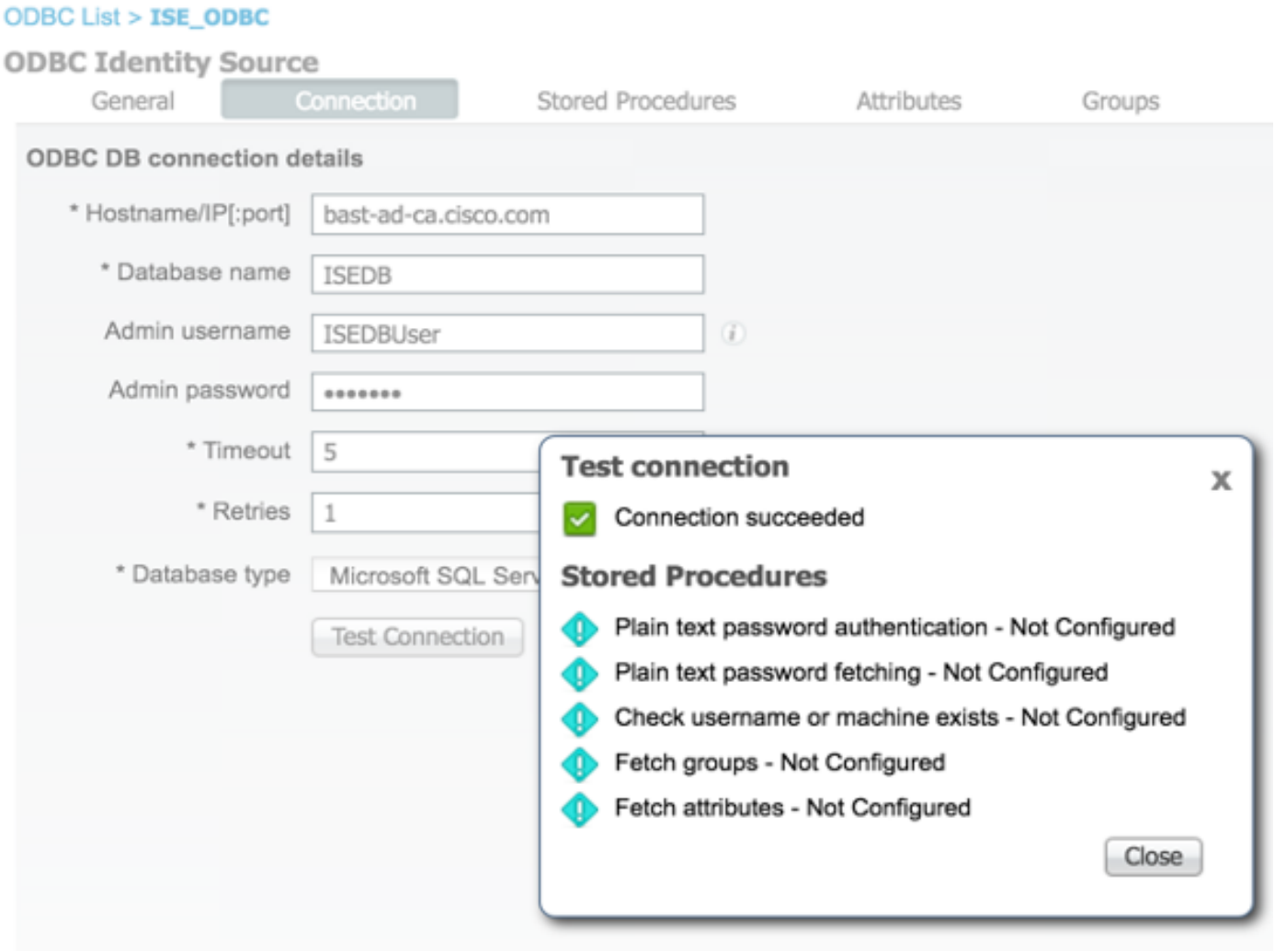
- Requiere programación adicional para llenar la base de datos externa con credenciales de terminal.
- Si la base de datos externa no está localmente presente como los PSN, esta solución depende de la WAN, lo que la convierte en el tercer ^{tercer} punto de fallo en el flujo de datos AAA del terminal.
- Requiere conocimientos adicionales para mantener los procesos y procedimientos externos de la base de datos.
- Se deben considerar los errores causados por la configuración manual de user-id a DB.

Configuraciones de ejemplo de BD externa

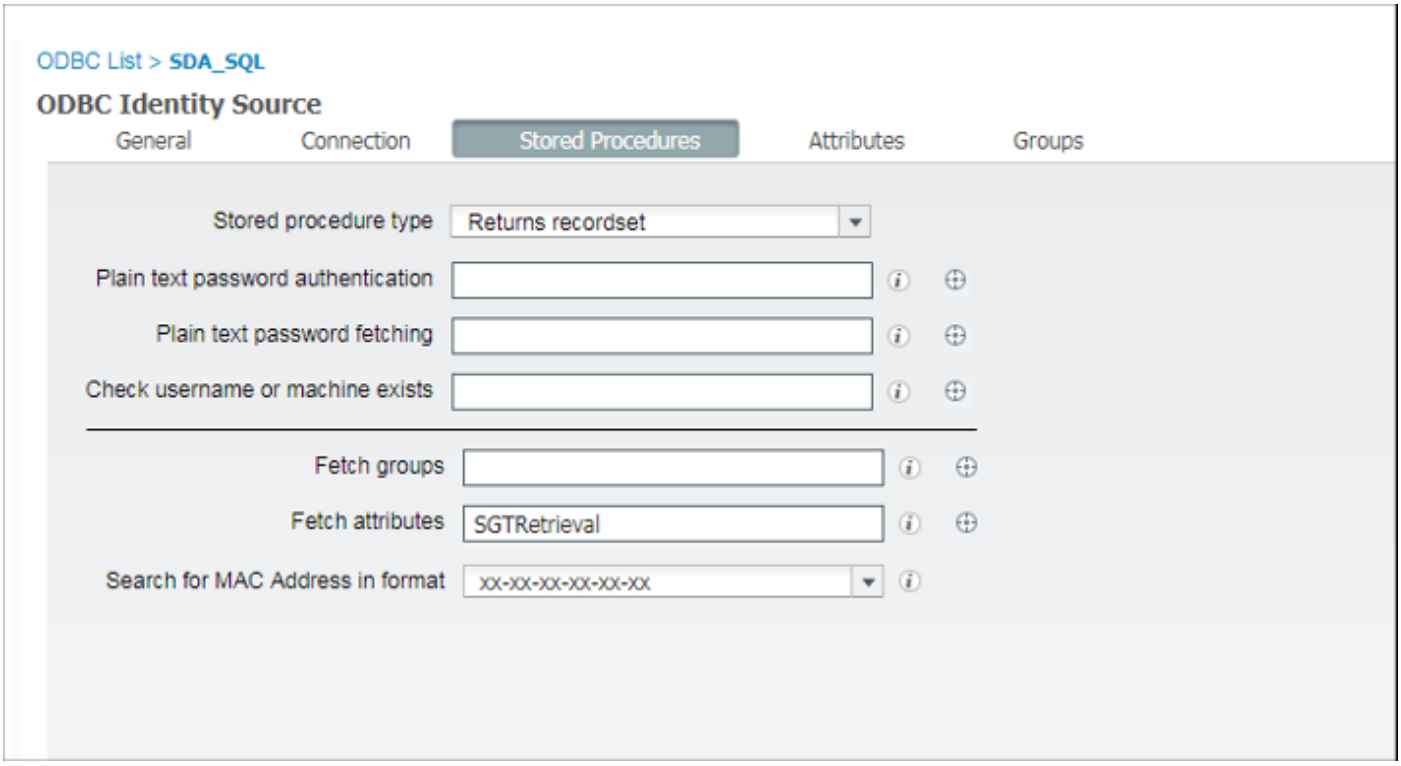
En este documento, Microsoft SQL se muestra como la base de datos externa utilizada como punto de autorización.

Paso 1. Cree el almacén de identidad ODBC en Cisco ISE desde el menú **Administration > External Identity Source > ODBC** y pruebe las conexiones.

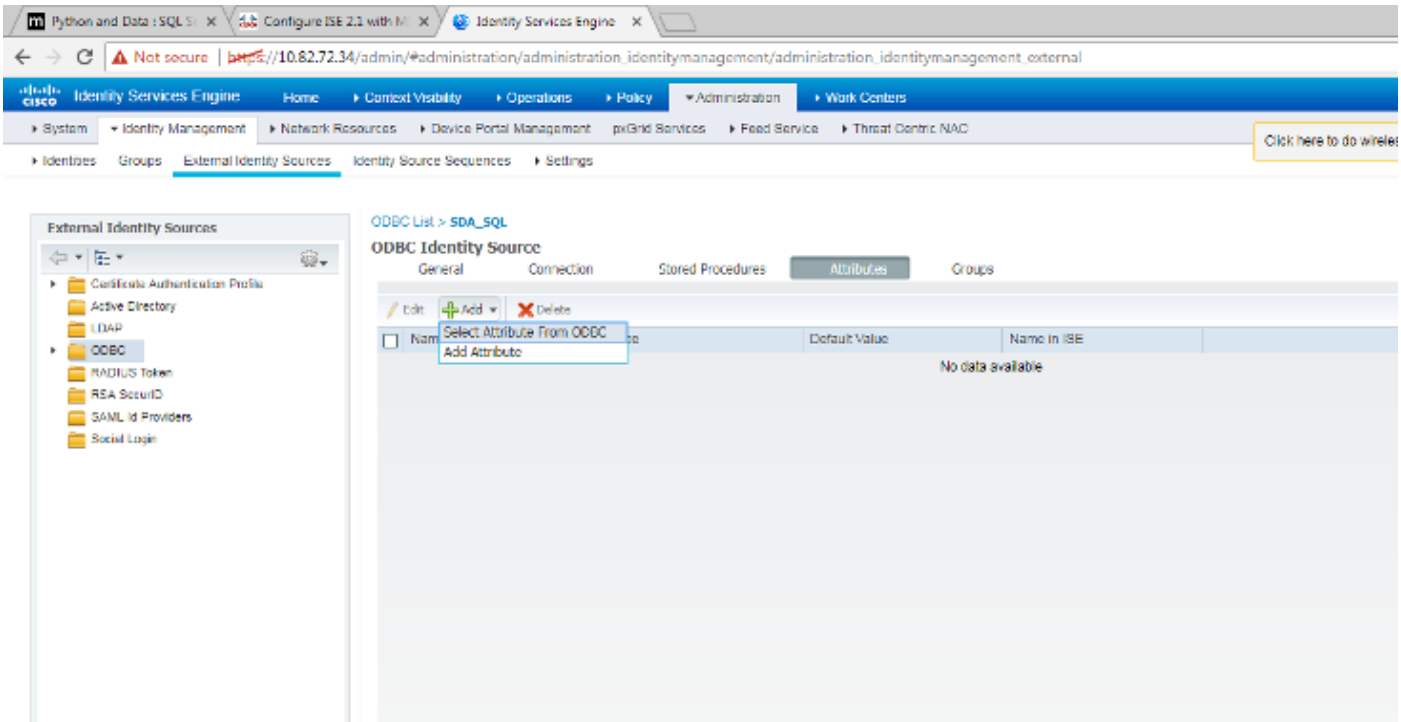


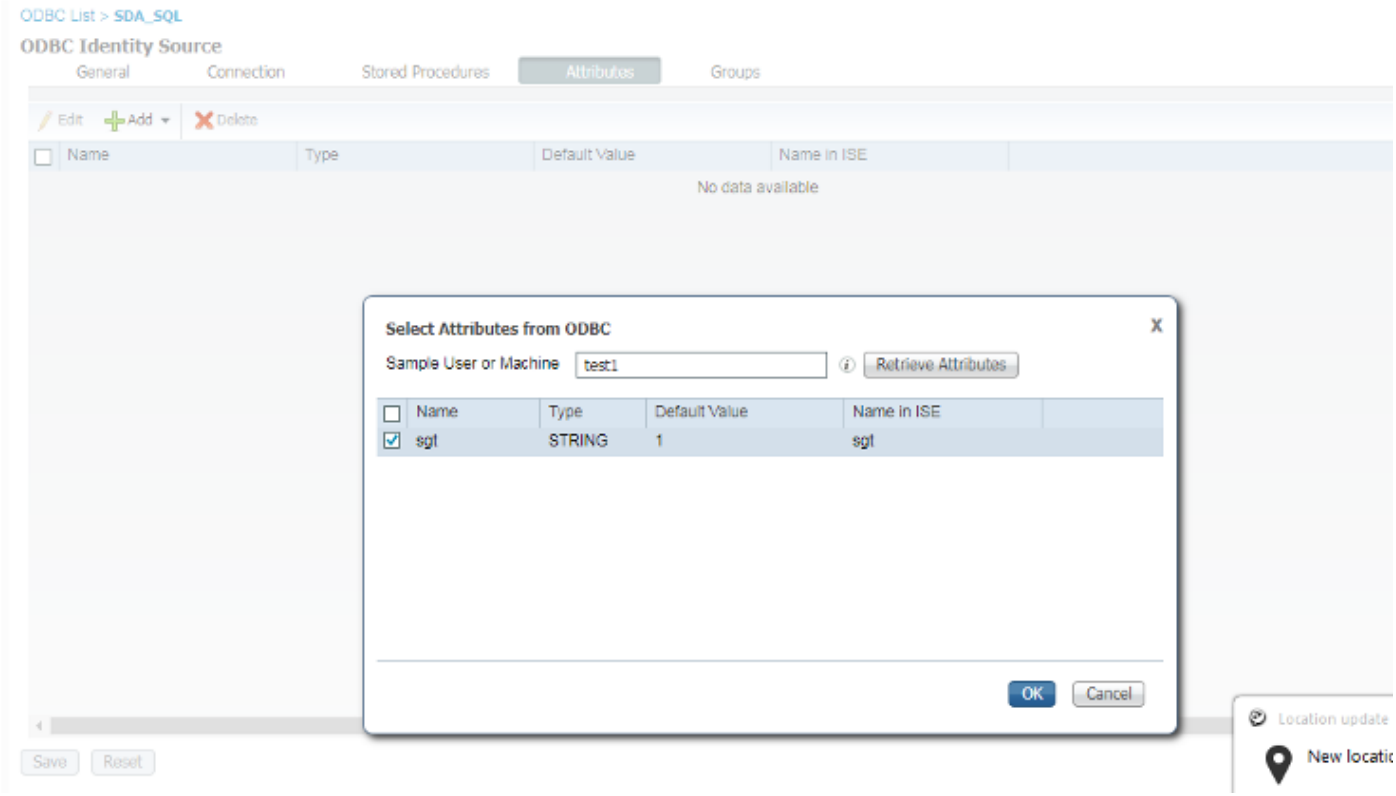


Paso 2. Vaya a la pestaña Procedimientos almacenados en la página ODBC para configurar los procedimientos creados en Cisco ISE.

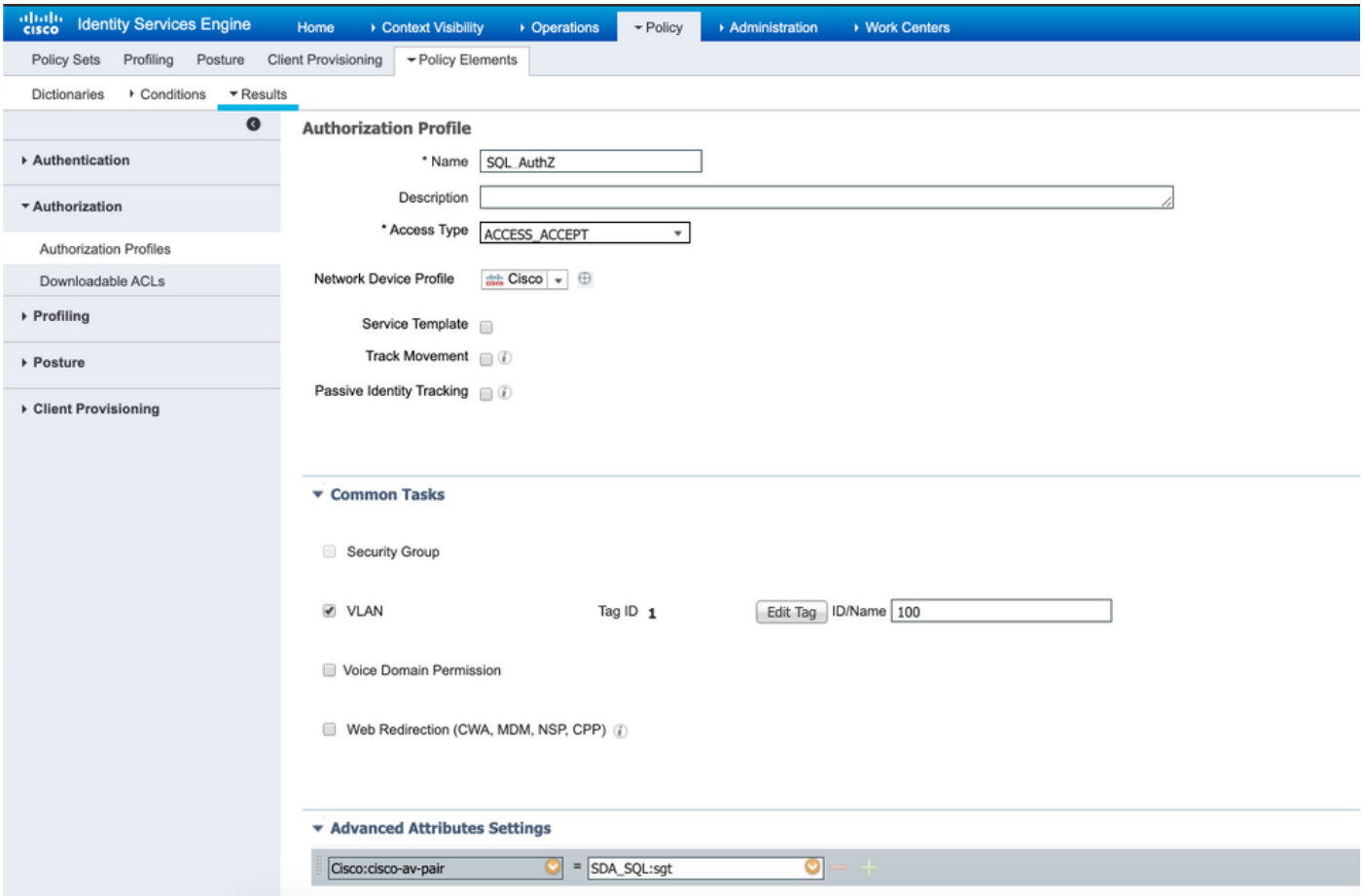


Paso 3. Obtenga los atributos para el id de usuario del origen de ID de ODBC para verificarlos.



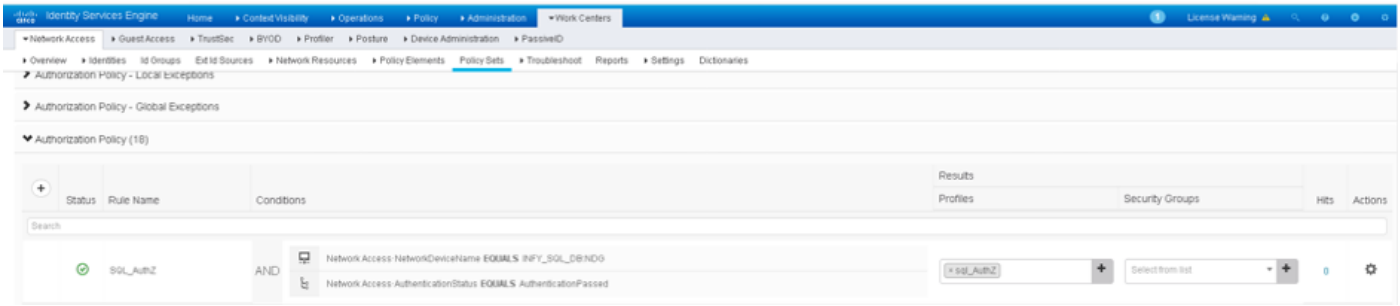


Paso 4. Crear un **perfil de autorización** y configurarlo. En Cisco ISE, vaya a **Policy > Results > Authorization profile > Advance Attributes Settings** y seleccione el atributo como **Cisco:cisco-av-pair.** Seleccione los valores como <name of ODBC database>:sgt y, a continuación, guárdelo.



Paso 5. Cree una **política de autorización** y configúrela. En Cisco ISE, navegue hasta **Policy > Policy sets > Authorization Policy > Add.** Coloque la condición como Origen de identidad es el servidor SQL. Seleccione el perfil de resultados como el perfil de autorización creado

anteriormente.



Paso 6. Una vez autenticado y autorizado el usuario, los registros contendrán el sgt asignado al usuario, para su verificación.

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

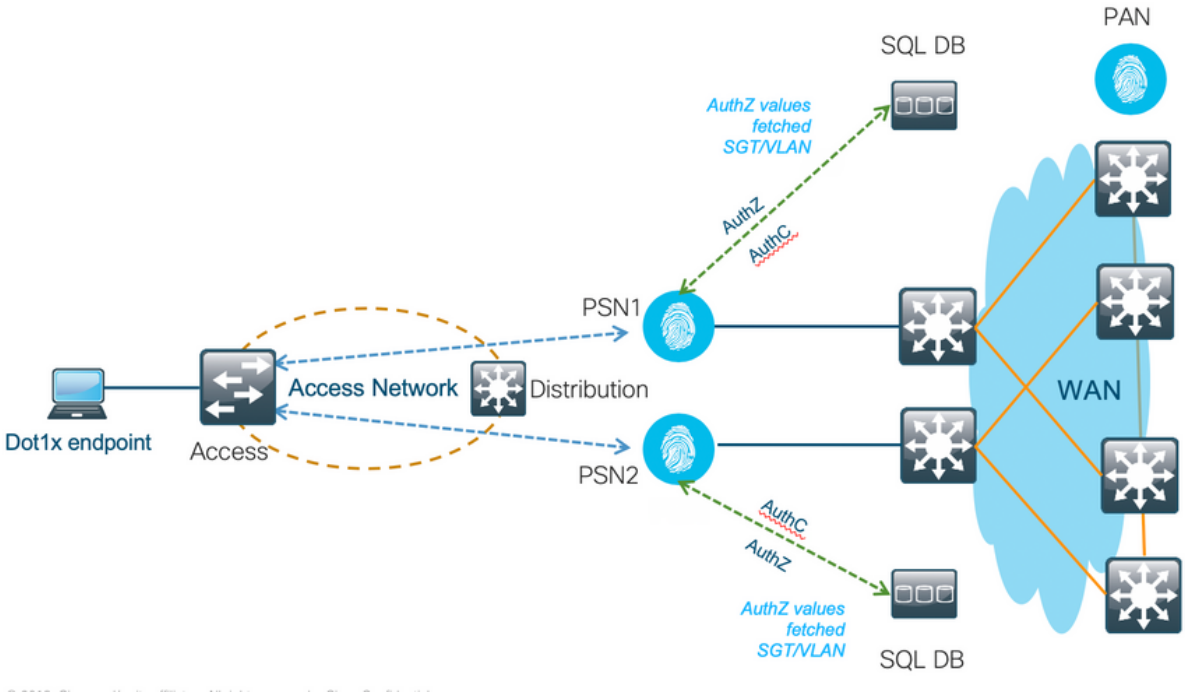
2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

Flujo de trabajo de la solución (posterior a ISE 2.7)

Después de ISE 2.7, los atributos de autorización se pueden obtener de ODBC, como Vlan, SGT y ACL, y estos atributos se pueden consumir en políticas.

En esta solución, Cisco ISE se integra con Microsoft SQL. MS SQL se utiliza como almacén de ID

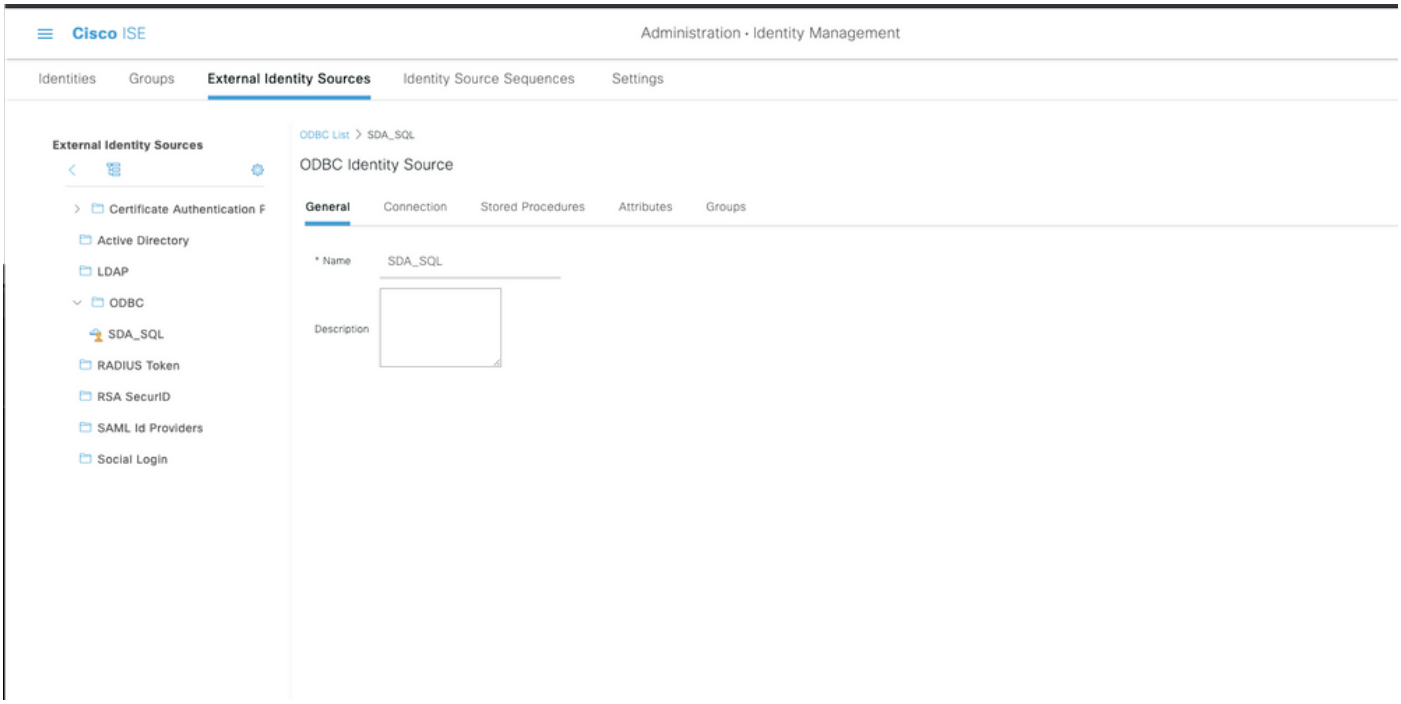
para la autenticación y la autorización. Cuando se proporcionan las credenciales de los terminales a PSN, se validan las credenciales con la base de datos de MS SQL. La política de autorización hace referencia a la base de datos MS SQL para obtener los resultados autorizados, como SGT/VLAN, para los que se utiliza **user-id** como referencia.



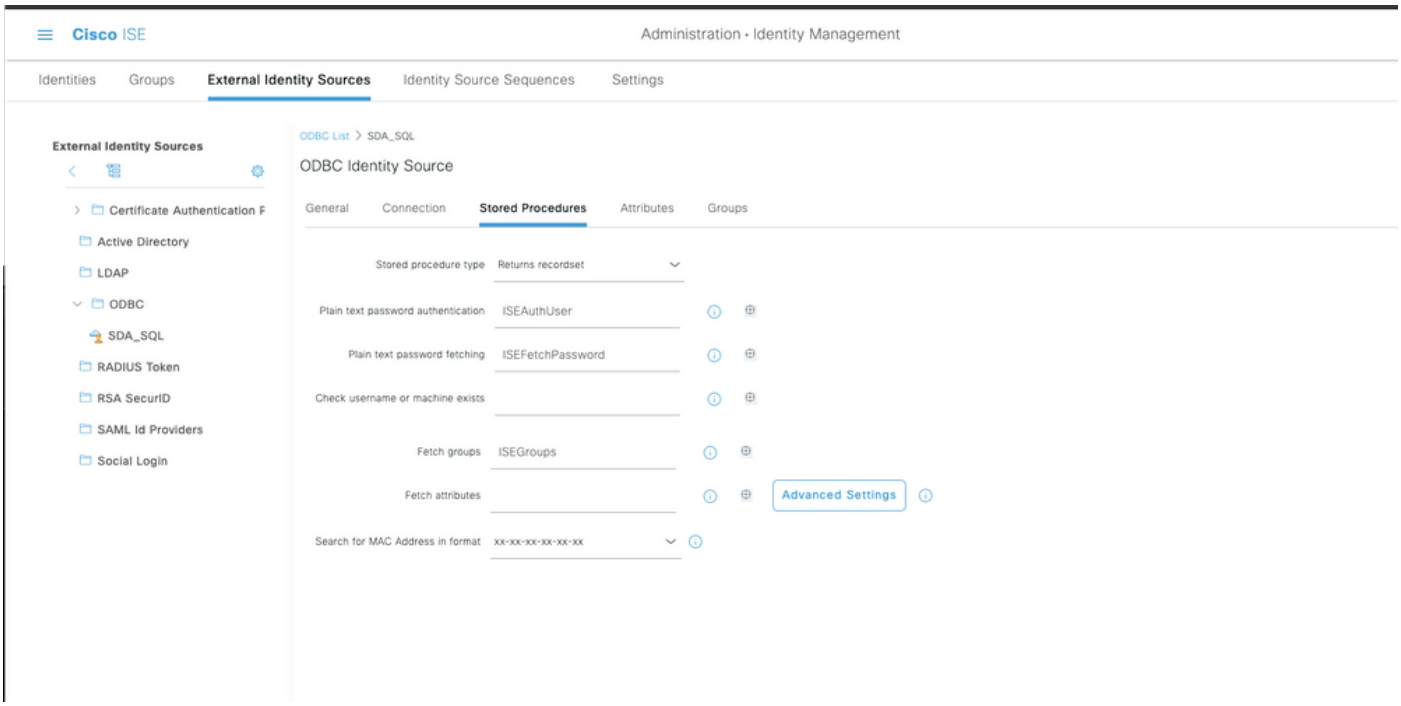
Configuraciones de ejemplo de BD externa

Siga el procedimiento proporcionado anteriormente en este documento para crear MS SQL DB junto con el nombre de usuario, la contraseña, el ID de VLAN y SGT.

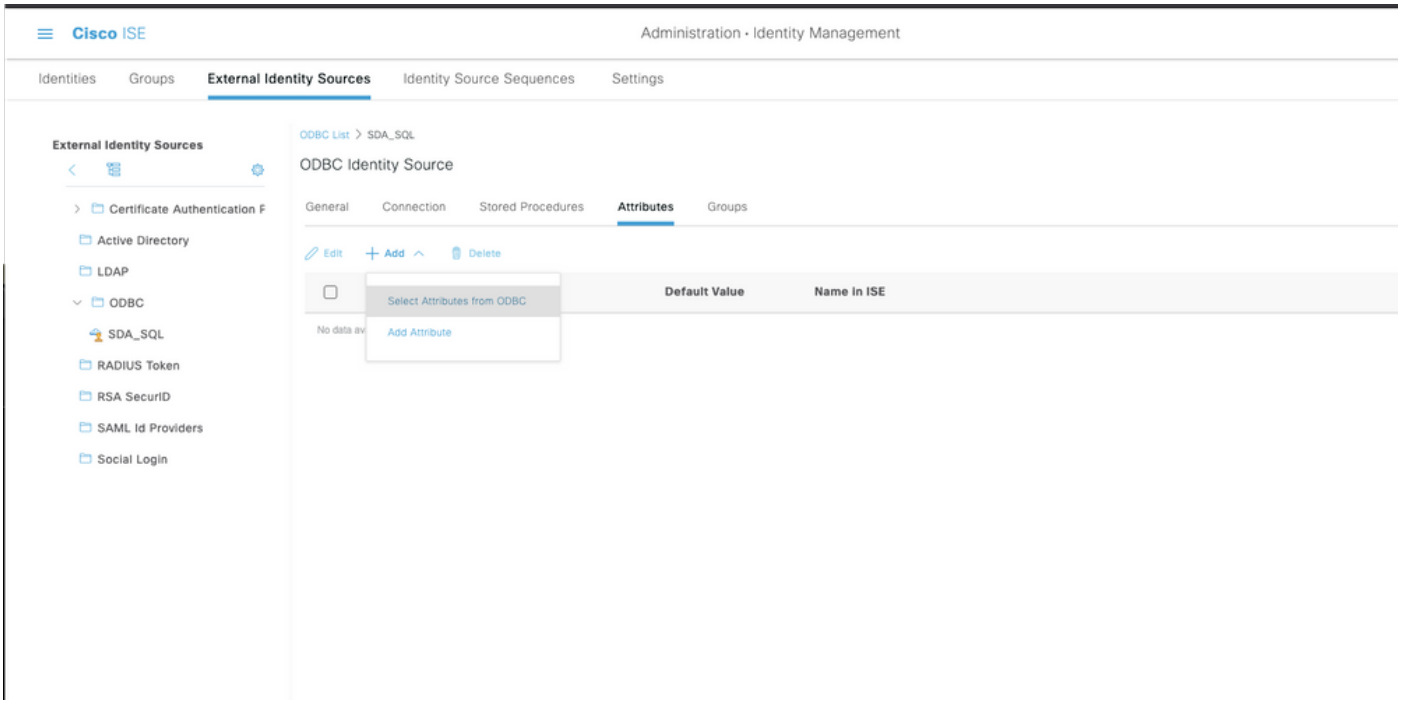
Paso 1. Cree un almacén de identidad ODBC en Cisco ISE desde el menú **Administration > External Identity Source > ODBC** y pruebe las conexiones.

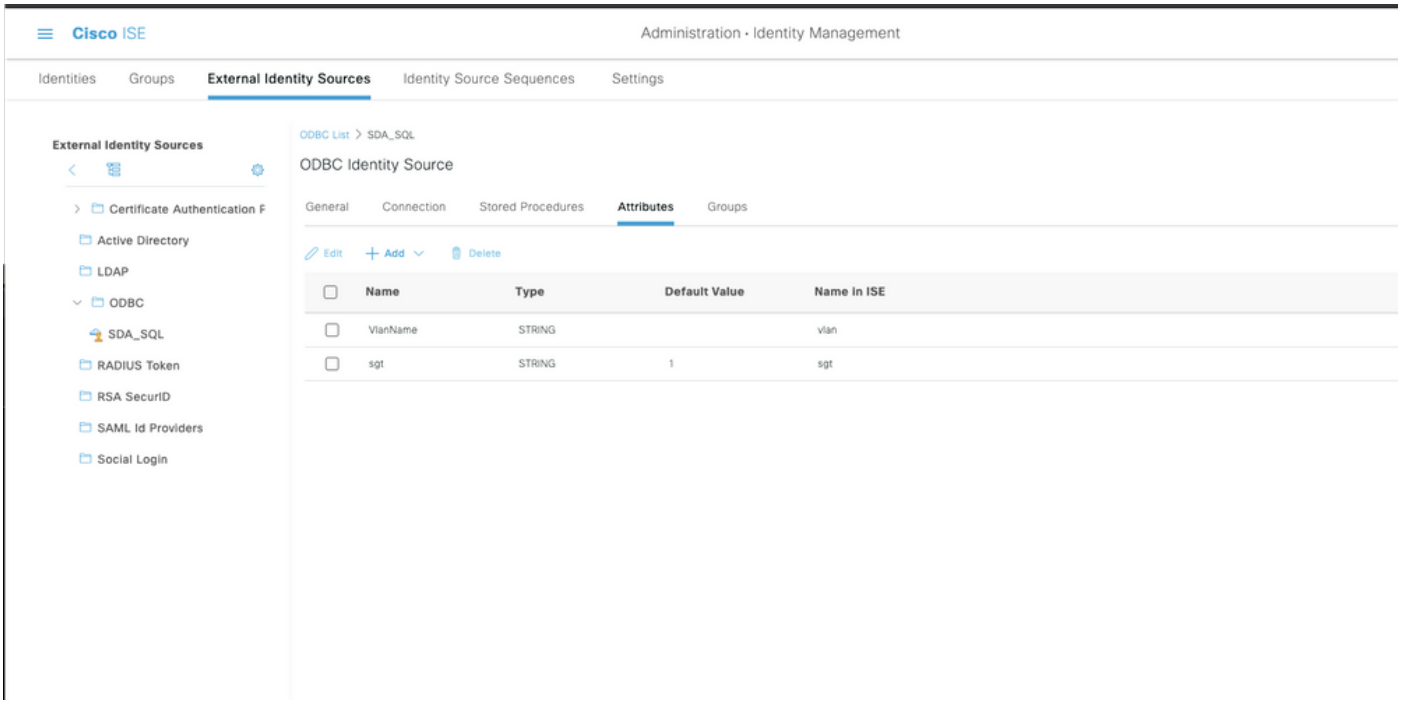


Paso 2. Vaya a la pestaña Procedimientos almacenados en la página ODBC para configurar los procedimientos creados en Cisco ISE.

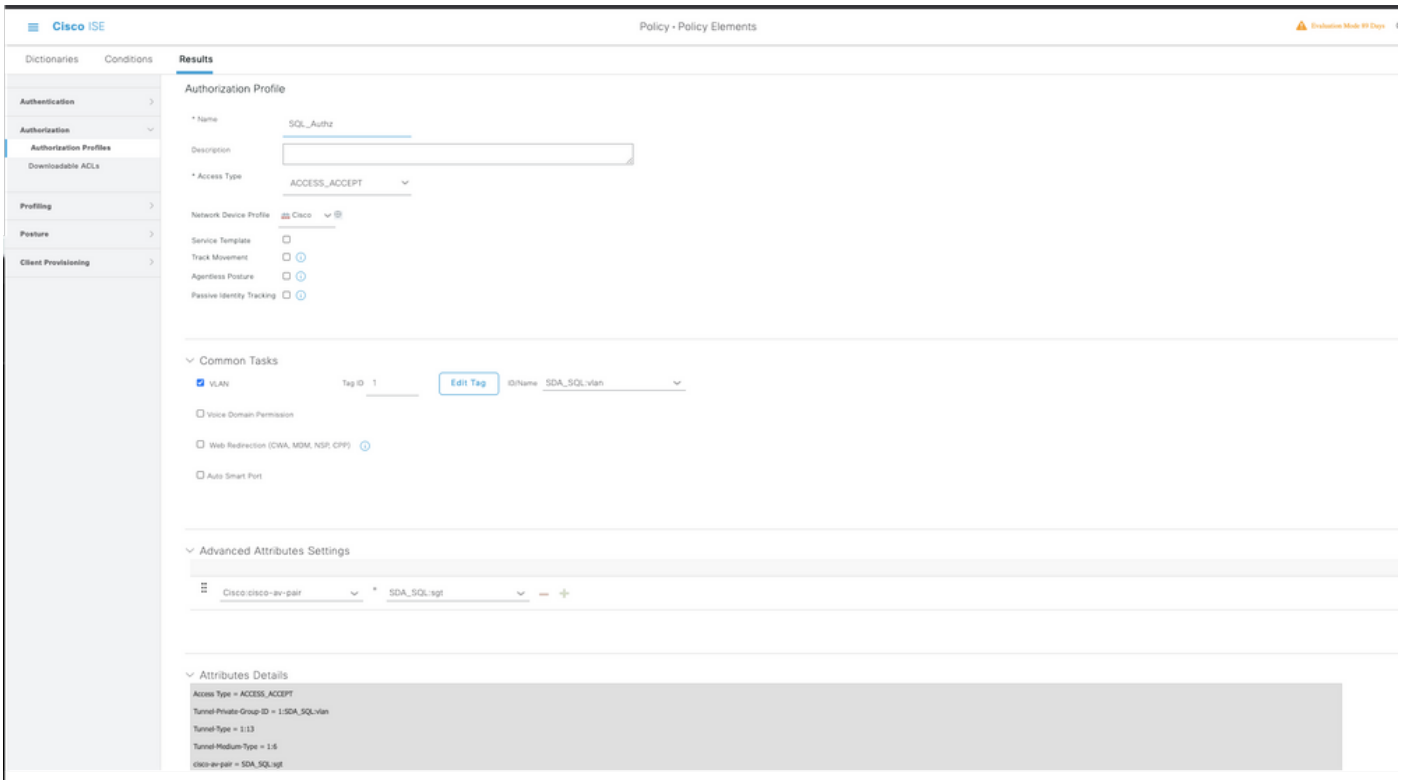


Paso 3. Obtenga los atributos para el id de usuario del origen de ID de ODBC para verificarlos.

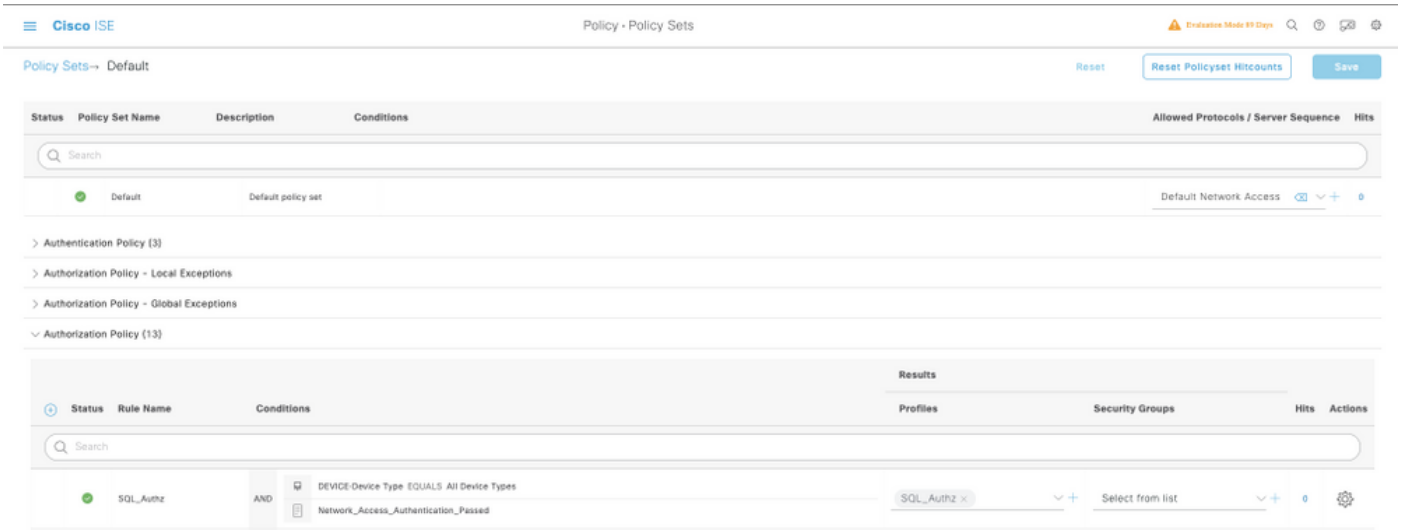




Paso 4. Crear un **perfil de autorización** y configurarlo. En Cisco ISE, vaya a **Policy > Results > Authorization profile > Advance Attributes Settings** y seleccione el atributo como **Cisco:cisco-av-pair.** Seleccione los valores como <name of ODBC database>:sgt. En Common Tasks, Select **VLAN** with ID/Name as <name of ODBC database>:vlan y guárdelo



Paso 5. Cree una **política de autorización** y configúrela. En Cisco ISE, navegue hasta **Policy > Policy sets > Authorization Policy > Add.** Coloque la condición como Origen de identidad es el servidor SQL. Seleccione el perfil de resultados como el perfil de autorización creado anteriormente.

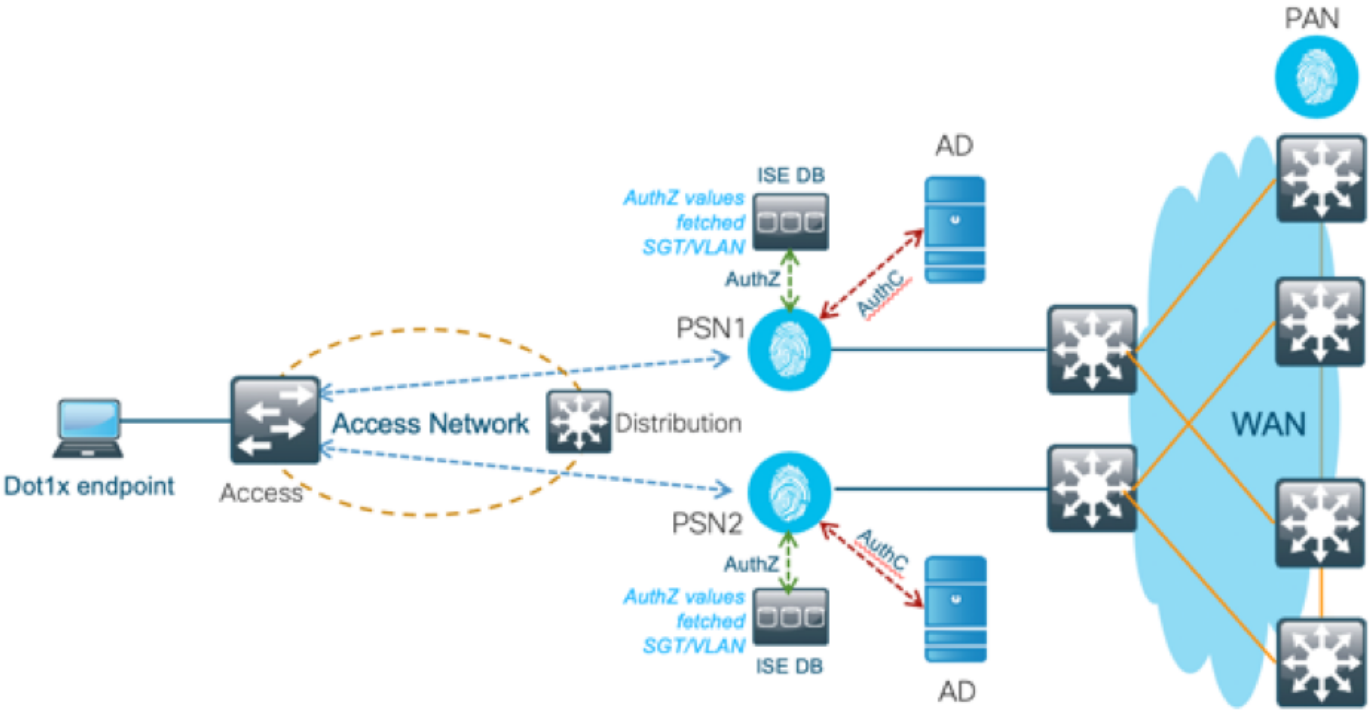


Utilizar base de datos interna

Cisco ISE cuenta con una base de datos incorporada que se puede utilizar para tener ID de usuario para la autorización.

Flujo de soluciones

En esta solución, la base de datos interna de Cisco ISE se utiliza como punto de autorización, mientras que Active Directory (AD) sigue siendo el origen de autenticación. La ID de usuario de los terminales se incluye en la base de datos de Cisco ISE junto con los **atributos personalizados** que devuelven los resultados autorizados, como SGT o VLAN. Cuando se proporcionan las credenciales de los terminales a PSN, se comprueba la validez de las credenciales de los terminales con el almacén de ID de Active Directory y se autentica el terminal. La política de autorización hace referencia a la base de datos de ISE para obtener los resultados autorizados, como SGT/VLAN, para los que se utiliza la ID de usuario como referencia.



Ventajas

Esta solución presenta estas ventajas, que la convierten en una solución flexible:

- Cisco ISE DB es una solución incorporada y, por lo tanto, no tiene ningún tercer punto de fallo, a diferencia de la solución de base de datos externa.
- Dado que el clúster de Cisco ISE garantiza la sincronización en tiempo real entre todas las personas, no existe dependencia de WAN, ya que PSN tiene todas las ID de usuario y atributos personalizados transferidos desde PAN en tiempo real.
- Cisco ISE puede aprovechar todas las funciones adicionales posibles que ofrece la base de datos externa.
- Esta solución no depende de los límites de escalabilidad de Cisco ISE.

Desventajas

Esta solución tiene estas desventajas:

- El número máximo de ID de usuario que Cisco ISE DB puede retener es de 300 000.
- Se deben considerar los errores causados por la configuración manual de user-id a DB.

Configuraciones de ejemplo de BD internas

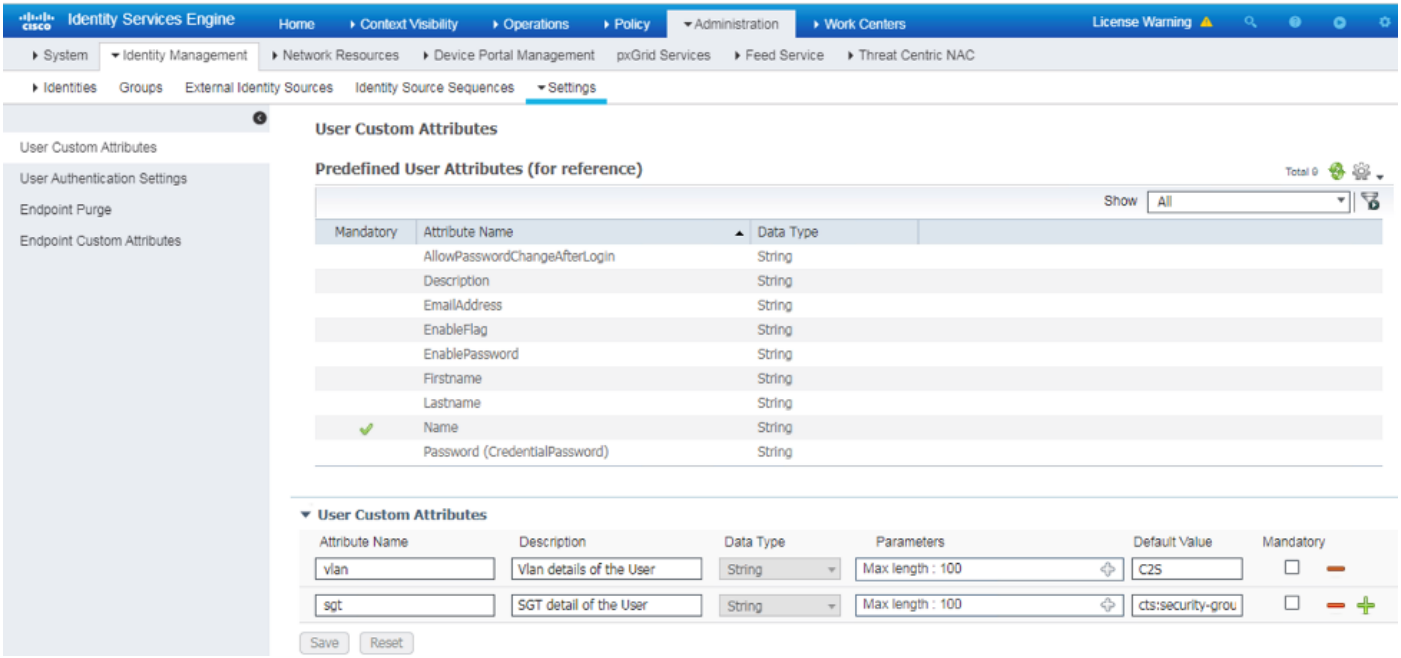
La VLAN y SGT por usuario se pueden configurar para cualquier usuario en el almacén de ID interno con un atributo de usuario personalizado.

Paso 1. Cree nuevos atributos personalizados de usuario para representar el valor de VLAN y SGT de los respectivos usuarios. Navegue hasta **Administración > Administración de identidades > Configuración > Atributos personalizados de usuario.** Cree nuevos atributos personalizados de usuario como se muestra en esta tabla.

Aquí se muestra la tabla de base de datos de ISE con atributos personalizados.

Nombre de atributo	Tipo de datos	Parámetros (longitud)	Valor Predeterminado
vlan	String (cadena)	100	C2S (nombre de VLAN predeterminado)
sgt	String (cadena)	100	cts:security-group-tag=0003-0 (valor SGT predeterminado)

- En este escenario, el valor de VLAN representa el nombre de VLAN y el valor sgt representa el atributo cisco-av-pair de SGT en hexadecimal.

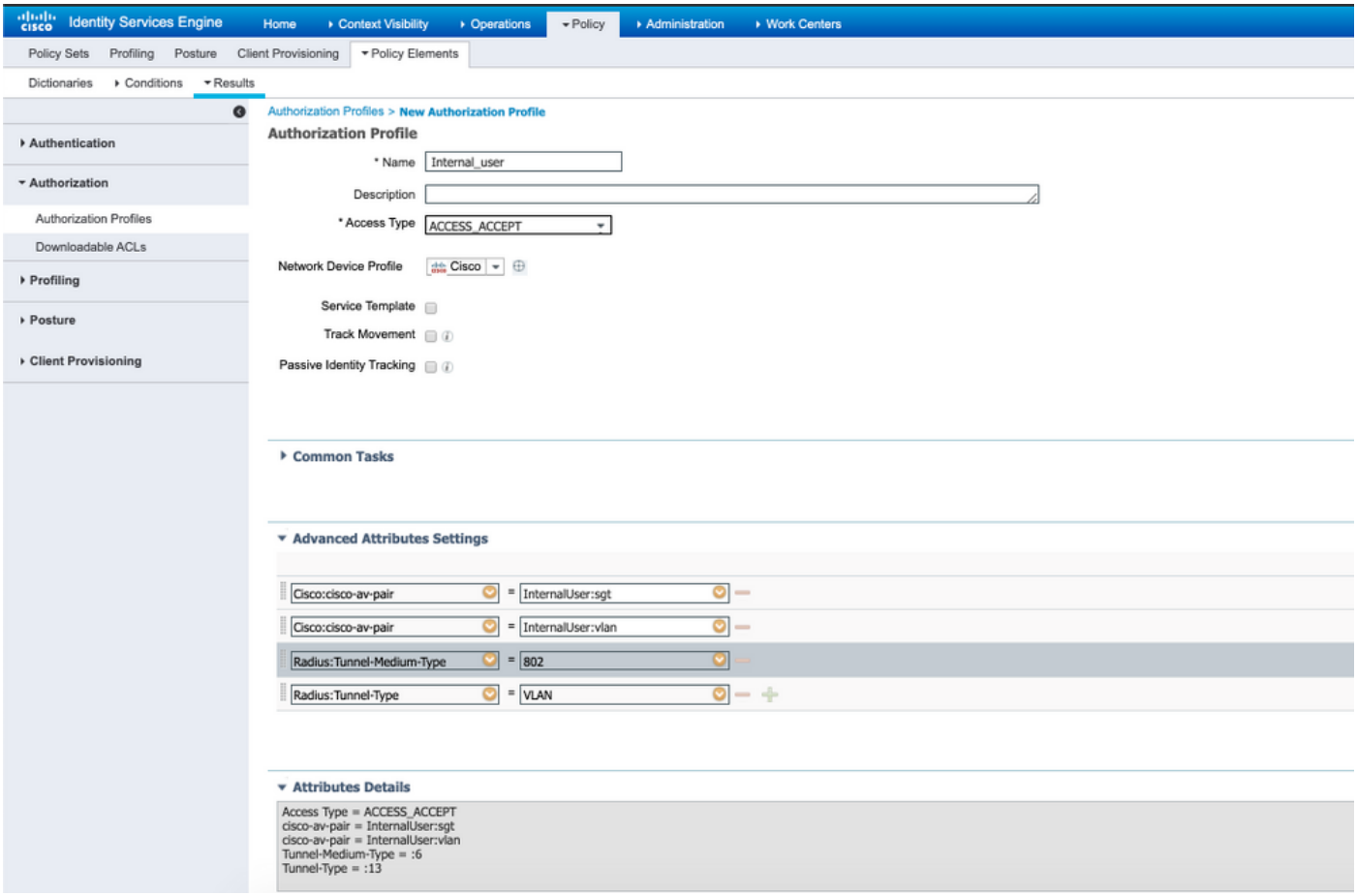


Paso 2. Cree un perfil de autorización con atributos personalizados de usuario para implicar los valores vlan y sgt de los usuarios respectivos. Navegue hasta **Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización > Agregar.** Agregue los atributos mencionados a continuación en Configuración de Atributos Avanzados.

Esta tabla muestra el perfil de AuthZ para el usuario interno.

Atributo	Valor
Cisco:cisco-av-pair	Usuario interno:sgt
Radius:ID de grupo privado de túnel	Usuario interno:vlan
Radio:Tipo de túnel medio	802
Radio:Tipo de túnel	VLAN

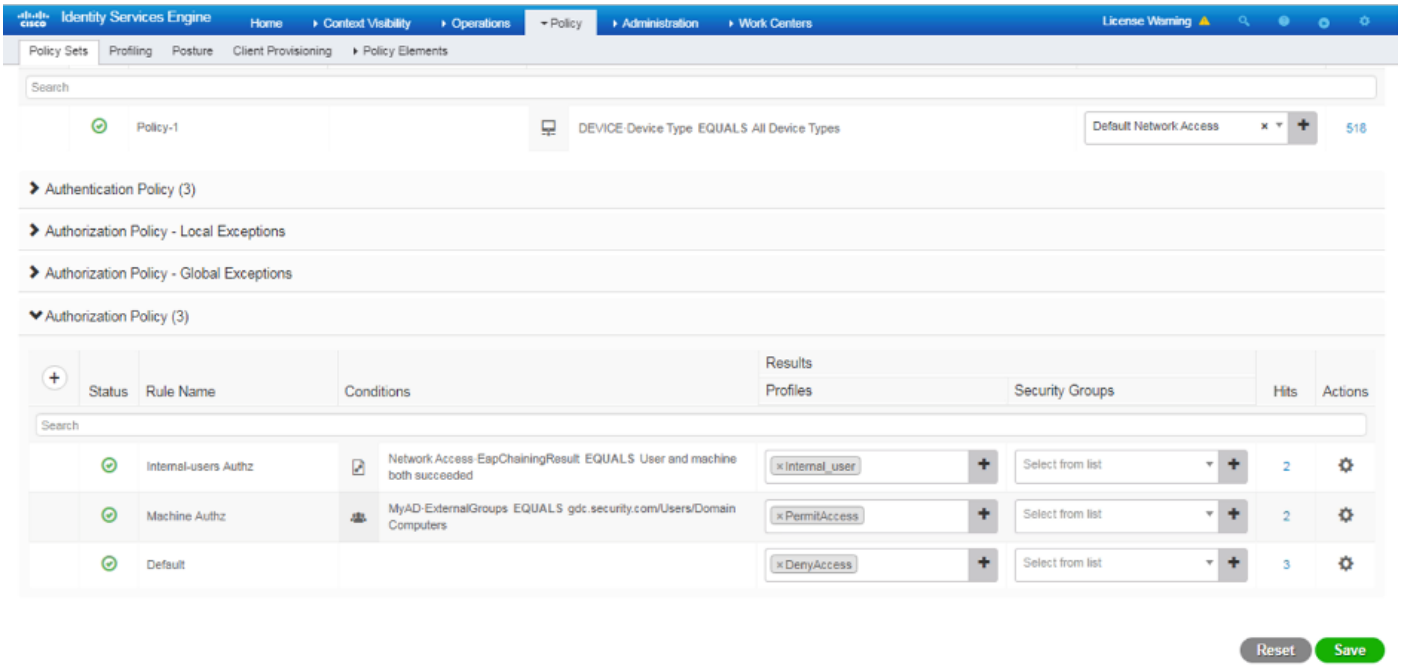
Como se muestra en la imagen, para los usuarios internos, el perfil **Internal_user** se configura con SGT y Vlan configuradas como **InternalUser:sgt** y **InternalUser:vlan** respectivamente.



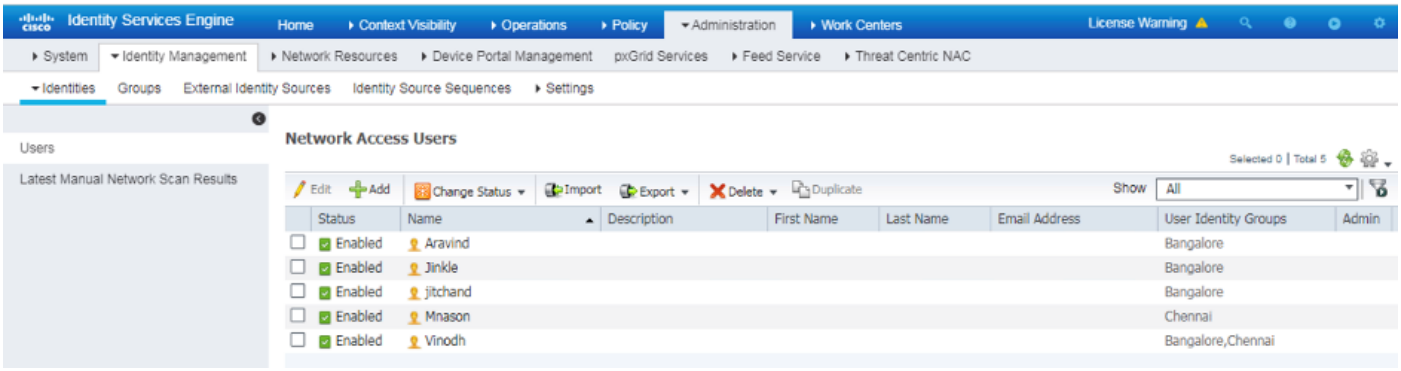
Paso 3. Cree una política de autorización, vaya a **Política > Juegos de Políticas > Política-1 > Autorización.** Cree políticas de autorización con las condiciones mencionadas a continuación y asígnelas a los perfiles de autorización respectivos.

Esta tabla muestra la política de AuthZ para el usuario interno.

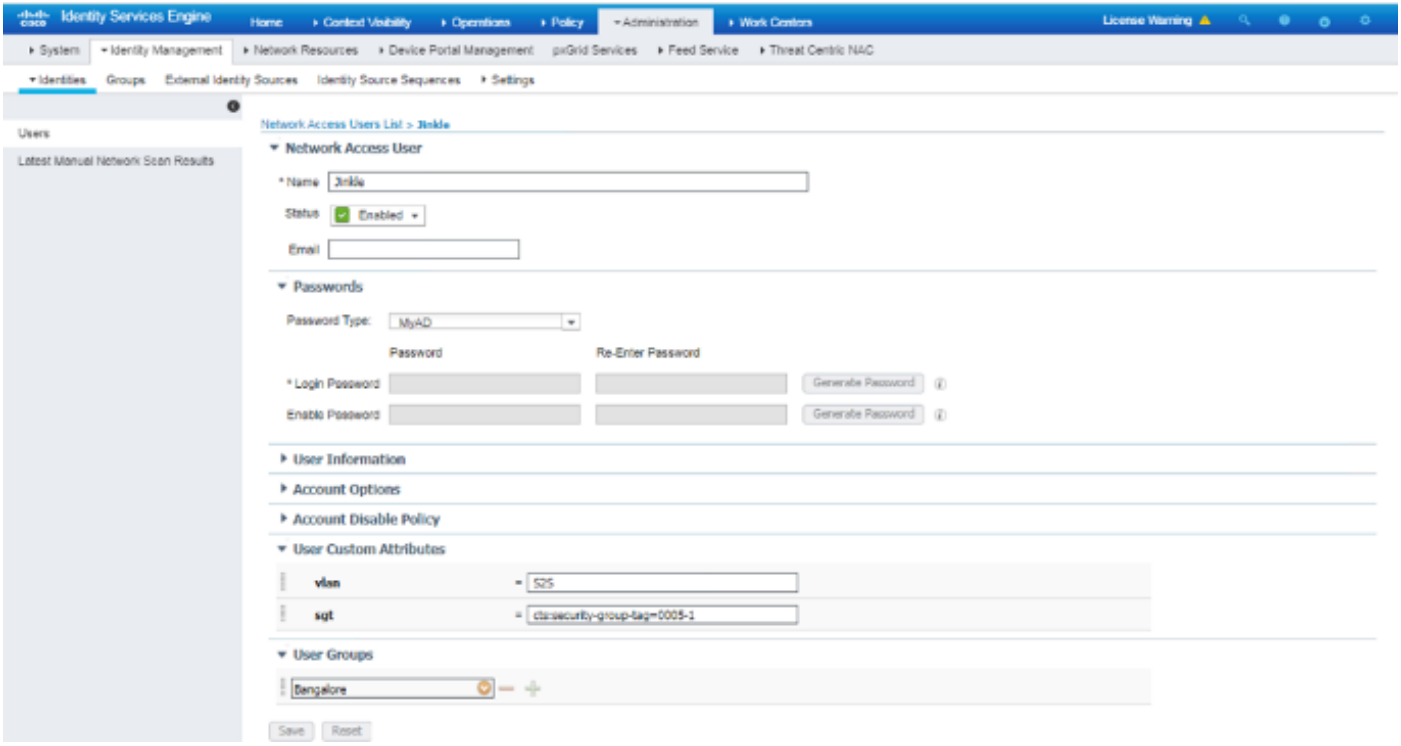
Nombre de regla	Condición	Perfil Authz de resultado
Internal_User_Authz	Si Network Access.EapChainingResults ES IGUAL a Usuario y equipo correctos	Internal_user
Machine_Only_Authz	Si MyAD.ExternalGroups ES IGUAL A gdc.security.com/Users/Domain Equipos	PermitirAcceso



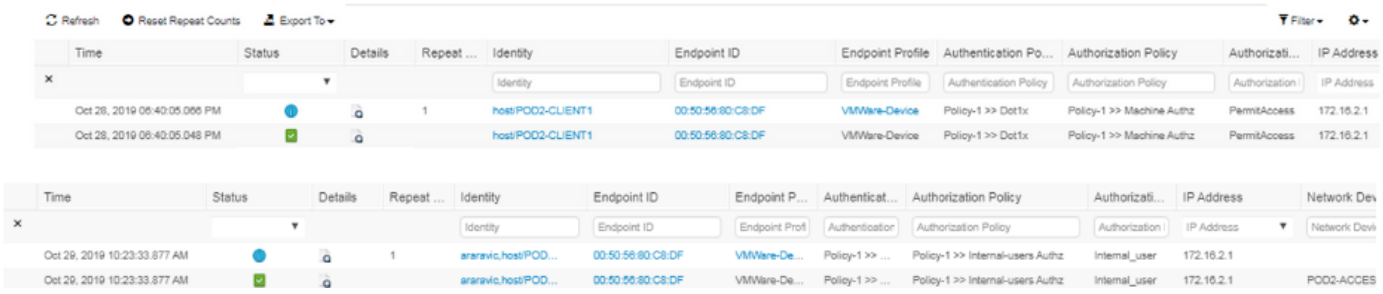
Paso 4. Crear identidades de usuario masivas con atributos personalizados con detalles de usuario y sus respectivos atributos personalizados en la plantilla csv. Importe el csv. Para ello, vaya a **Administration > Identity Management > Identities > Users > Import > Choose the file > Import.**



Esta imagen muestra un usuario de ejemplo con detalles de atributos personalizados. Seleccione el usuario y haga clic en editar para ver los detalles de atributos personalizados asignados al usuario correspondiente.



Paso 5: Verifique los registros activos:



Verifique la sección **Resultado** para verificar si el atributo **Vlan** & **SGT** se envía como parte de Access-Accept.

Conclusión

Esta solución permite a algunos de los clientes de grandes empresas ampliar la solución según sus requisitos. Se debe tener precaución al agregar/eliminar ID de usuario. Los errores, si se activan, pueden dar lugar a un acceso no autorizado para usuarios reales o viceversa.

Información Relacionada

Configuración de Cisco ISE con MS SQL mediante 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

Glosario

AAA	Autenticación Autorización Contabilización
AD	Directorio activo
AuthC	Autenticación
AuthZ	Autorización
DB	Base de datos
DOT1X	802.1x
IBN	Red basada en identidad
ID	Base de datos de identidad
ISE	Identity Services Engine
MnT	Supervisión y resolución de problemas
MsSQL	Microsoft SQL

ODBC	Conectividad abierta de DataBase
SARTÉN	Nodo de administración de políticas
PSN	Nodo de servicios de políticas
SGT	Etiqueta de grupo segura
SQL	Lenguaje de consulta estructurado
VLAN	LAN virtual
WAN	Red de área extensa

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).