Vereinfachte Zugriffsrichtlinie mit ODBC und ISE DB (benutzerdefiniertes Attribut) für großes Campus-Netzwerk

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Technologietrends
Problem
Vorgeschlagene Lösung
Konfiguration mit externer DB
ODBC-Beispielkonfigurationen
Lösungs-Workflow (ISE 2.7 und früher)
Vorteile
Nachteile
Externe DB - Beispielkonfigurationen
Lösungs-Workflow (nach ISE 2.7)
Externe DB - Beispielkonfigurationen
Interne Datenbank verwenden
Lösungs-Workflow
Vorteile
Nachteile
Interne DB-Beispielkonfigurationen
Schlussfolgerung
Zugehörige Informationen
Glossar

Einleitung

In diesem Dokument wird eine umfangreiche Campus-Bereitstellung ohne Kompromisse bei den Funktionen und der Durchsetzung von Sicherheitsrichtlinien beschrieben. Die Identity Services Engine (ISE), die Sicherheitslösung von Cisco für Endgeräte, erfüllt diese Anforderung durch die Integration in eine externe Identitätsquelle.

Bei großen Netzwerken mit mehr als 50 geografischen Standorten, mehr als 4.000 unterschiedlichen Benutzerprofilen und mehr als 600.000 Endpunkten müssen herkömmliche IBN-Lösungen aus einem anderen Blickwinkel betrachtet werden - mehr als nur Funktionen, unabhängig davon, ob sie mit allen Funktionen skalierbar sind. Die IBN-Lösung (Intent-Based Network) in herkömmlichen großen Netzwerken erfordert neben den Funktionen einen zusätzlichen Fokus auf Skalierbarkeit und einfaches Management.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 802.1x/MAB-Authentifizierung
- Cisco Identity Service Engine (Cisco ISE)
- Cisco TrustSec (CTS)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

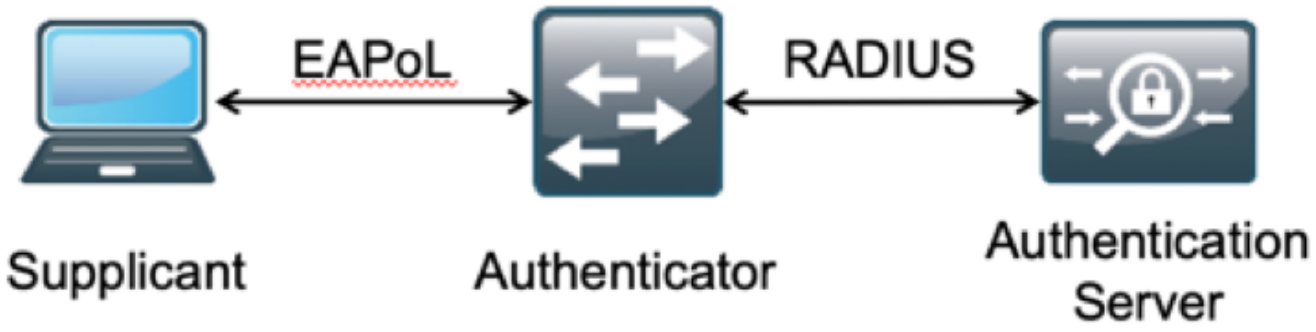
- Cisco Identity Services Engine (ISE) Version 2.6 Patch 2 und Version 3.0
- Windows Active Directory (AD) Server 2008 Version 2
- Microsoft SQL Server 2012

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn das Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen jeder Konfiguration kennen.

Hintergrundinformationen

Die grundlegenden Elemente einer Identity Based Network (IBN)-Lösung sind Supplicant, Authenticator und Authentication (AAA) Server. Der Supplicant ist ein Agent auf dem Endpunkt, der die Anmeldeinformationen bereitstellt, wenn der Netzwerkzugriff angefordert wird. Authenticator oder NAS (Network Access Server) ist die Zugriffsebene, die Netzwerk-Switches und WLCs umfasst, die die Anmeldeinformationen für den AAA-Server übertragen. Der Authentifizierungsserver validiert die Benutzerauthentifizierungsanforderung anhand eines ID-Speichers und autorisiert sie entweder durch Akzeptieren oder Ablehnen des Zugriffs. Der ID-Speicher kann sich im AAA-Server oder auf einem externen dedizierten Server befinden.

Dieses Bild zeigt die grundlegenden IBN-Elemente.



RADIUS ist ein UDP-basiertes Protokoll (User Datagram Protocol), bei dem Authentifizierung und Autorisierung miteinander verbunden sind. In der Cisco IBN-Lösung für Campus-Unternehmen

fungiert der Policy Service Node (PSN) der ISE als AAA-Server, der die Endpunkte anhand des Unternehmens-ID-Speichers authentifiziert und unter bestimmten Bedingungen autorisiert.

In der Cisco ISE werden Authentifizierungs- und Autorisierungsrichtlinien konfiguriert, um diese Anforderungen zu erfüllen. Die Authentifizierungsrichtlinien umfassen den Medientyp (kabelgebunden oder drahtlos) sowie die EAP-Protokolle für die Benutzervalidierung. Autorisierungsrichtlinien bestehen aus Bedingungen, die die Kriterien für die Übereinstimmung der verschiedenen Endpunkte und das Netzwerkzugriffsergebnis definieren. Dabei kann es sich um ein VLAN, eine herunterladbare ACL oder ein Secure Group Tag (SGT) handeln. Dies sind die maximalen Skalierungszahlen für Richtlinien, mit denen die ISE konfiguriert werden kann.

Diese Tabelle zeigt die Skalierung der Cisco ISE-Richtlinien.

Attribut	Skalierungszahl
Maximale Anzahl von Authentifizierungsregeln	1000 (Policy Set Mode)
Maximale Anzahl von Autorisierungsregeln	3.000 (Richtliniensatzmodus) mit 3200 Autz-Profilen

Technologietrends

Die Segmentierung hat sich zu einem der wichtigsten Sicherheitselemente für moderne Unternehmensnetzwerke entwickelt, ohne dass ein tatsächliches Edge-Netzwerk erforderlich ist. Die Endpunkte können zwischen internen und externen Netzwerken wechseln. Die Segmentierung hilft, alle Sicherheitsangriffe auf ein bestimmtes Segment einzudämmen, um das Netzwerk zu durchdringen. Die SDA-Lösung (Software-Defined Access) von heute bietet mithilfe von Cisco ISE TrustSec eine Möglichkeit zur Segmentierung auf Grundlage des Geschäftsmodells des Kunden, um Abhängigkeiten von Netzwerkelementen wie VLANs oder IP-Subnetzen zu vermeiden.

Problem

ISE-Richtlinienkonfiguration für große Unternehmensnetzwerke mit mehr als 500 unterschiedlichen Endgeräteprofilen - die Anzahl der Autorisierungsrichtlinien kann bis zu einem nicht zu verwaltenden Punkt ansteigen. Selbst wenn die Cisco ISE dedizierte Autorisierungsbedingungen unterstützt, um so viele Benutzerprofile zu verwalten, besteht die Herausforderung darin, diese Vielzahl an Richtlinien durch Administratoren zu verwalten.

Darüber hinaus benötigen Kunden ggf. gemeinsame Autorisierungsrichtlinien anstelle dedizierter Richtlinien, um Managementkosten zu vermeiden, und verfügen auf der Grundlage ihrer Kriterien über differenzierten Netzwerkzugriff für Endgeräte.

Betrachten Sie beispielsweise ein Unternehmensnetzwerk mit Active Directory (AD) als **Quelle der Wahrheit,** und das einzigartige Differenzierungsmerkmal des Endpunkts ist eines der Attribute in AD. In diesem Fall umfasst die herkömmliche Richtlinienkonfiguration mehr Autorisierungsrichtlinien für jedes einzelne Endgeräteprofil.

Bei dieser Methode wird jedes Endpunktprofil mit einem AD-Attribut unter domain.com unterschieden. Daher muss eine dedizierte Autorisierungsrichtlinie konfiguriert werden.

Diese Tabelle zeigt die traditionellen AuthZ-Richtlinien.

ABC-Richtlinie	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND Wenn AD-Gruppe GLEICH domain.com/groups/ABC DANN SGT:C2S-ABC UND VLAN:1021
DEF-Richtlinie	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND Wenn AD-Gruppe GLEICH domain.com/groups/DEF DANN SGT:C2S-DEF UND VLAN:1022
GHI-Richtlinie	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND Wenn AD-Gruppe GLEICH domain.com/groups/GHI DANN SGT:C2S-GHI UND VLAN:1023
XYZ-Richtlinie	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND Wenn AD-Gruppe GLEICH domain.com/groups/XYZ DANN SGT:C2S-XYZ UND VLAN:1024

Vorgeschlagene Lösung

Um die Verletzung der maximal skalierbaren Anzahl unterstützter Autorisierungsrichtlinien auf der Cisco ISE zu umgehen, wird eine externe Datenbank vorgeschlagen, die die Autorisierung jedes Endpunkts mit dem aus den Attributen abgerufenen Autorisierungsergebnis vornimmt. Wenn AD beispielsweise als externe Datenbank für die Autorisierung verwendet wird, können alle nicht verwendeten Benutzerattribute (wie Abteilungs- oder Pin-Code) referenziert werden, um autorisierte Ergebnisse bereitzustellen, die mit SGT oder VLAN verknüpft sind.

Dies wird durch die Integration der Cisco ISE in eine externe Datenbank oder in die interne ISE-Datenbank erreicht, die mit benutzerdefinierten Attributen konfiguriert ist. In diesem Abschnitt wird die Bereitstellung dieser beiden Szenarien erläutert:

> **Anmerkung:** In beiden Optionen enthält die DB die **Benutzer-ID,** aber nicht das **Kennwort** der DOT1X-Endpunkte. Die DB dient nur als **Autorisierungspunkt**. Die Authentifizierung kann weiterhin der ID-Speicher des Kunden sein, der sich in den meisten Fällen auf dem Active Directory (AD)-Server befindet.

Konfiguration mit externer DB

Die Cisco ISE ist zur Validierung der Endgeräteanmeldeinformationen in eine externe Datenbank integriert:

Diese Tabelle zeigt die validierten externen Identitätsquellen.

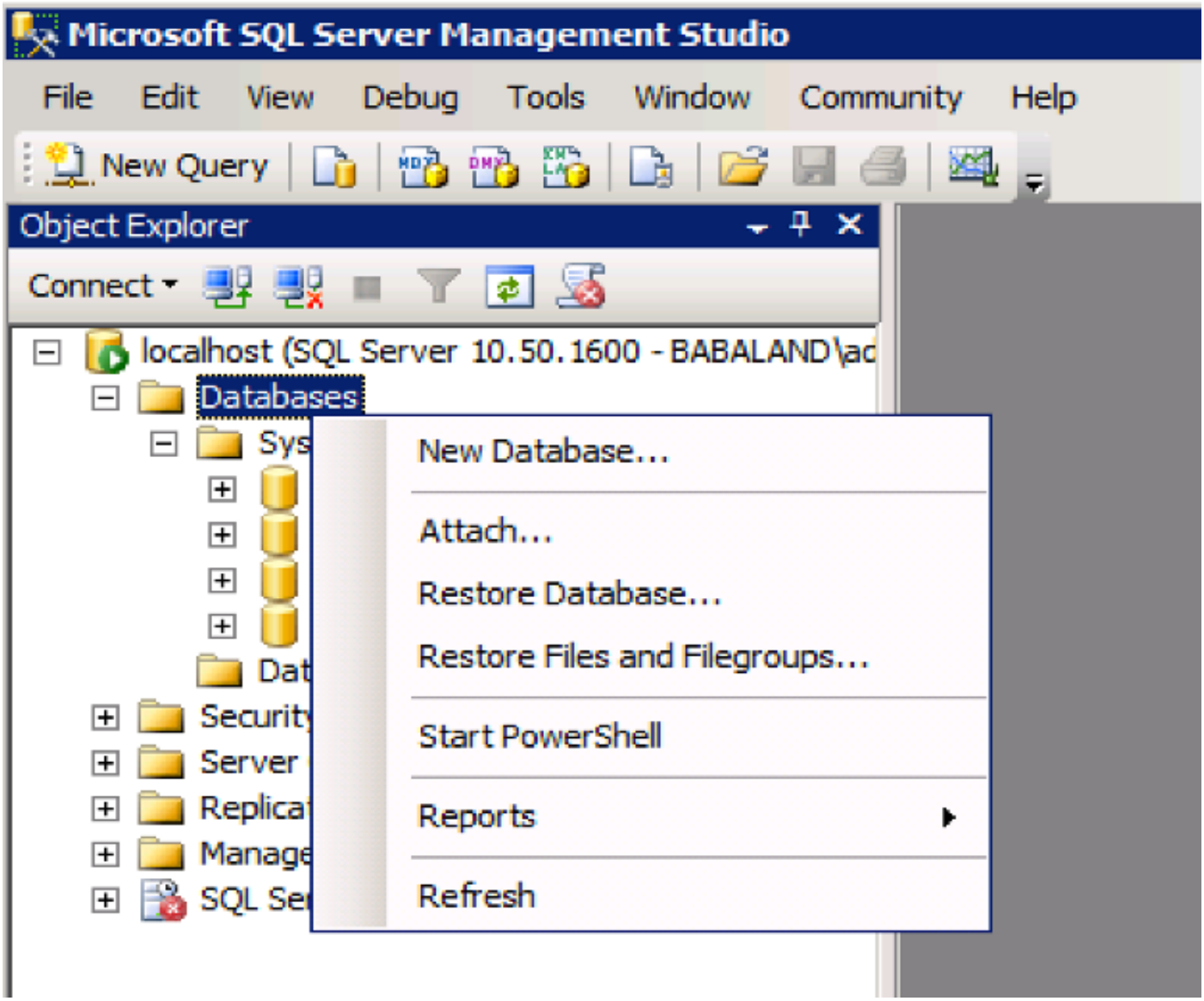
Externe Identitätsquelle	Betriebssystem/Version
Active Directory	
Microsoft Windows Active Directory 2003	—

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-Server	
SunONE LDAP-Verzeichnisserver	Version 5.2
OpenLDAP-Verzeichnisserver	Version 2.4.23
Jeder LDAP v3-kompatible Server	—
Token-Server	
RSA ACE/Server	Serie 6.x
RSA-Authentifizierungs-Manager	Serien 7.x und 8.x
Jeder RADIUS RFC 2865-kompatible Tokenserver	—
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	—
Sichere Authentifizierung	8.1.1
Jeder SAMLv2-konforme Identitätsanbieter	—
Open Database Connectivity (ODBC) Identity Source	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition Version 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Social Login (für Gastbenutzerkonten)	
Facebook	—

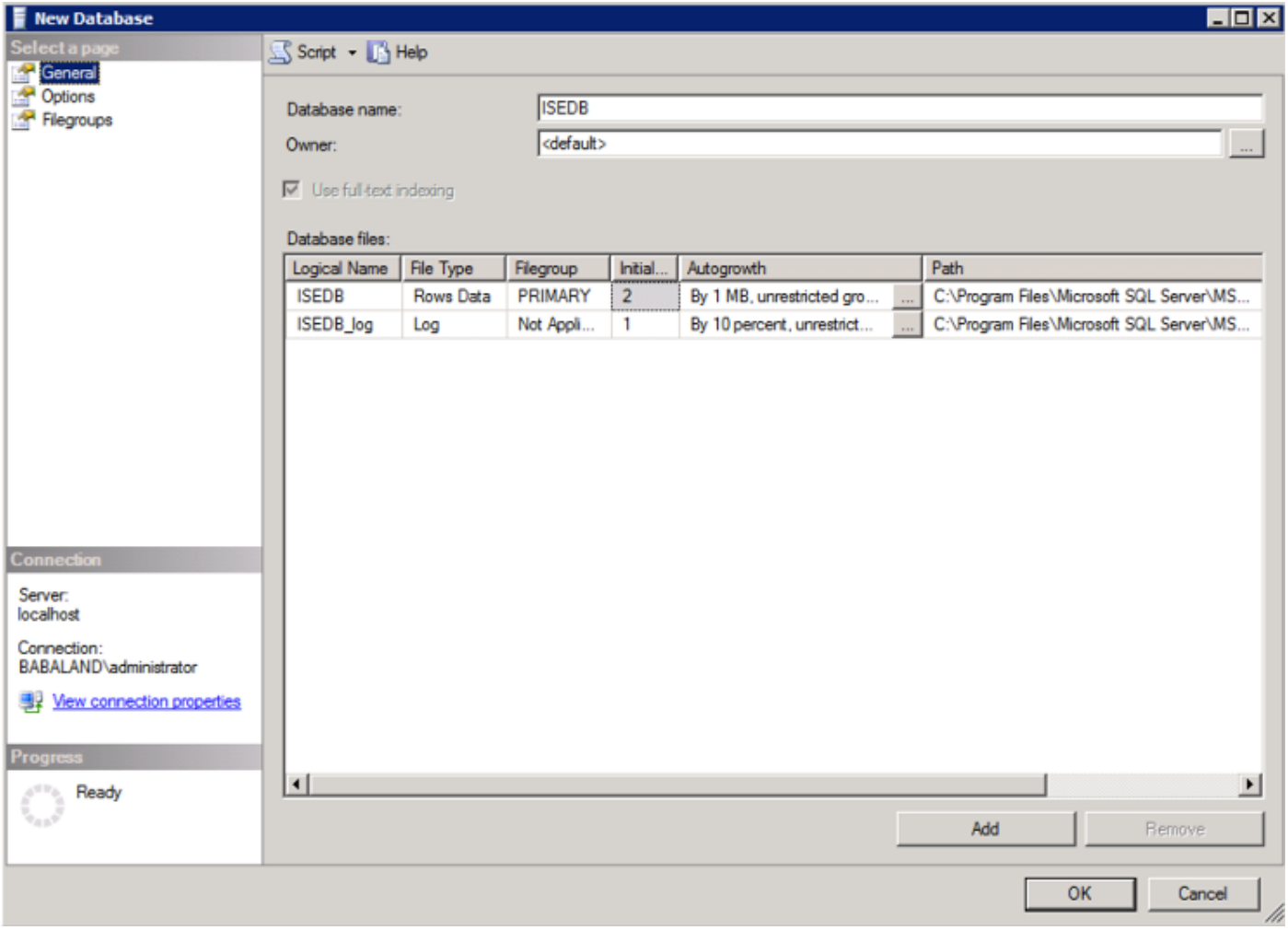
ODBC-Beispielkonfigurationen

Diese Konfiguration wird in Microsoft SQL durchgeführt, um die Lösung zu erstellen:

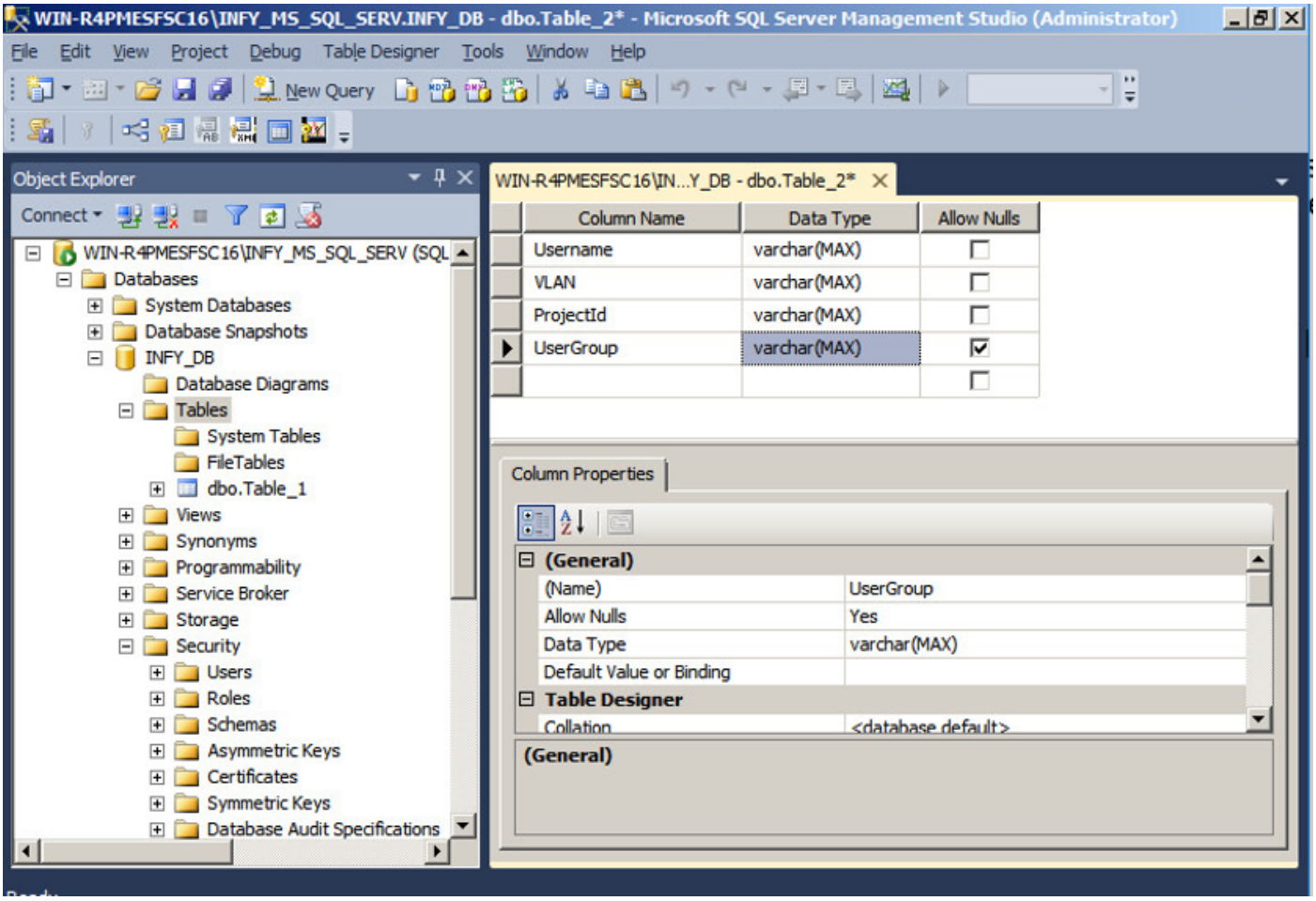
Schritt 1: Öffnen Sie SQL Server Management Studio (**Startmenü > Microsoft SQL Server**), um eine Datenbank zu erstellen:



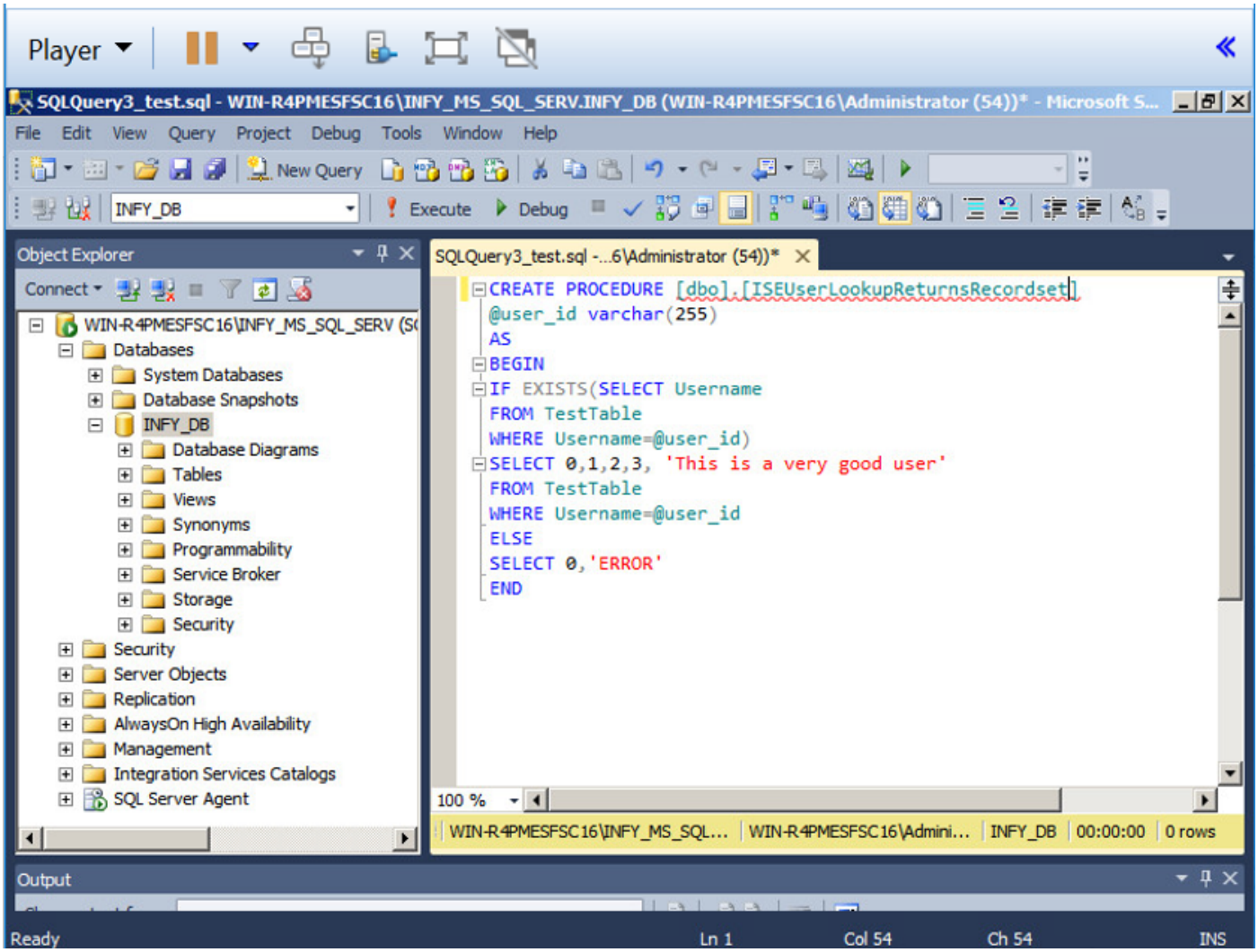
Schritt 2: Geben Sie einen Namen an, und erstellen Sie die Datenbank.



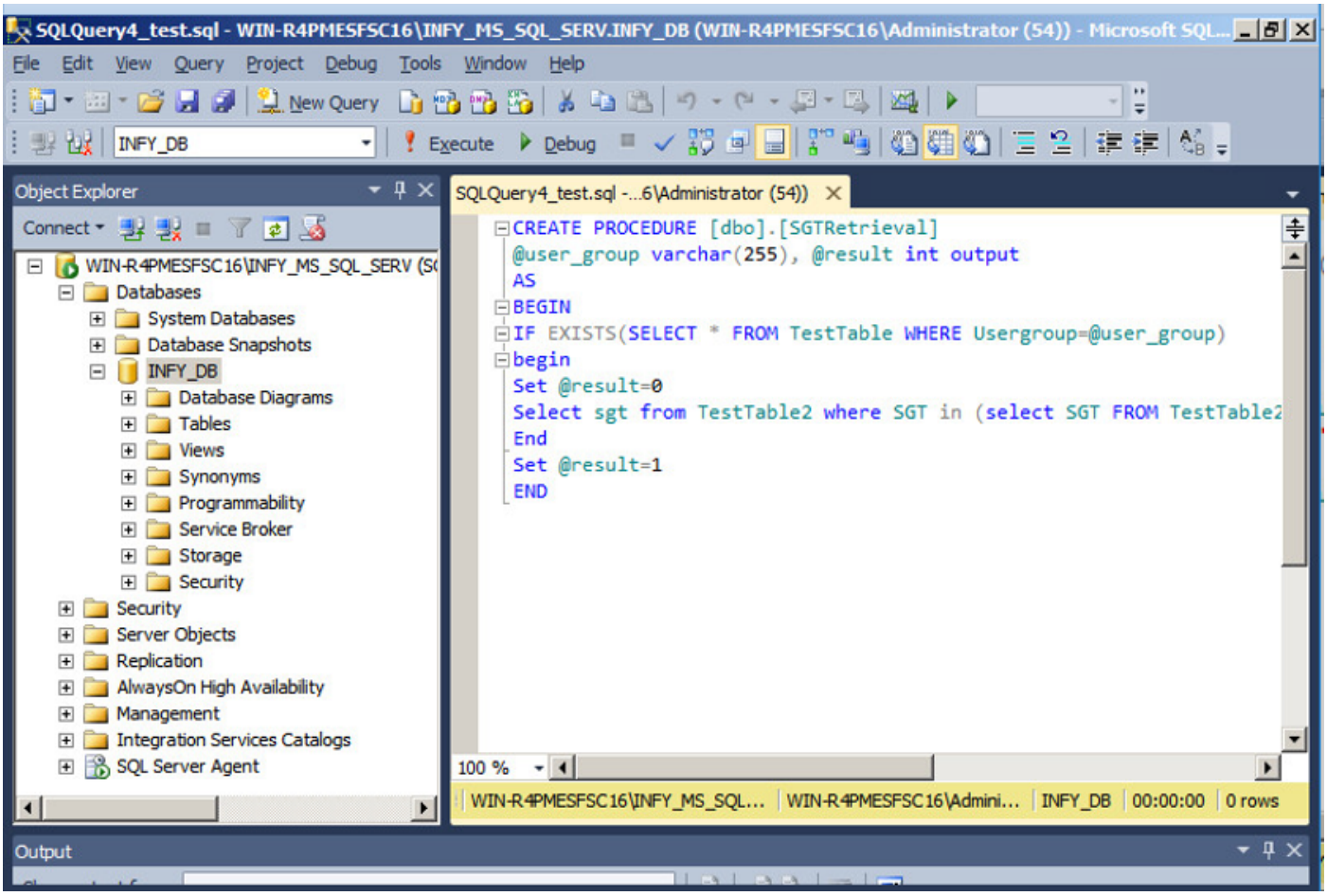
Schritt 3: Erstellen Sie eine neue Tabelle mit den erforderlichen Spalten als Parameter für Endpunkte, um autorisiert zu werden.



Schritt 4: Erstellen Sie eine **Prozedur**, um zu überprüfen, ob der Benutzername vorhanden ist.



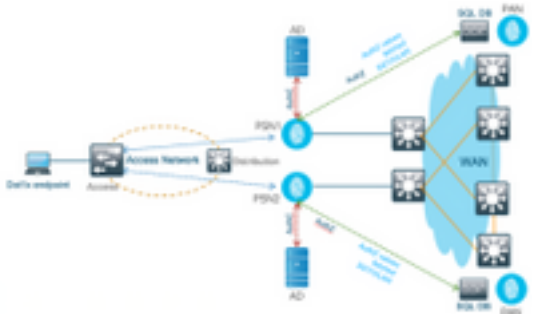
Schritt 5: Erstellen Sie eine Prozedur, um Attribute (SGT) aus der Tabelle abzurufen.

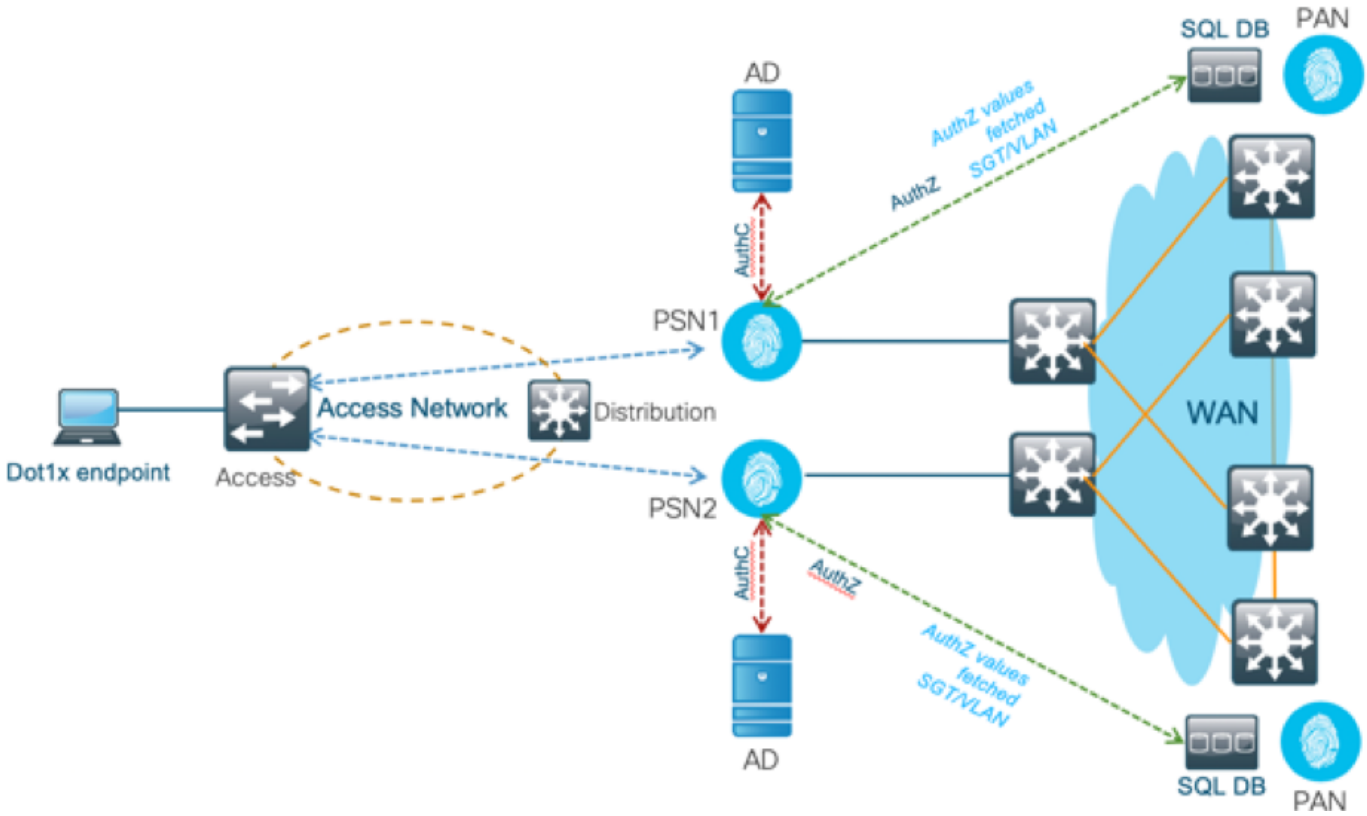


In diesem Dokument wird die Cisco ISE in die Microsoft SQL-Lösung integriert, um die Anforderungen für die Autorisierungsskalierung in großen Unternehmensnetzwerken zu erfüllen.

Lösungs-Workflow (ISE 2.7 und früher)

Bei dieser Lösung ist die Cisco ISE in ein Active Directory (AD) und Microsoft SQL integriert. AD wird als Authentifizierungs-ID-Speicher und MS SQL für die Autorisierung verwendet. Während des Authentifizierungsprozesses leitet das Netzwerkzugriffsgerät (Network Access Device, NAD) die Benutzeranmeldeinformationen an das PSN weiter - den AAA-Server in der IBN-Lösung. PSN überprüft die Anmeldeinformationen des Endpunkts im Active Directory-ID-Speicher und authentifiziert den Benutzer. Die Autorisierungsrichtlinie bezieht sich auf die MS SQL-Datenbank, um autorisierte Ergebnisse wie SGT/VLAN abzurufen, für die die **Benutzer-ID** als Referenz verwendet wird.





Vorteile

Diese Lösung bietet die folgenden Vorteile, die sie flexibel macht:

- Die Cisco ISE kann alle möglichen zusätzlichen Funktionen nutzen, die die externe DB bietet.
- Für diese Lösung gelten keine Größenbeschränkungen der Cisco ISE.

Nachteile

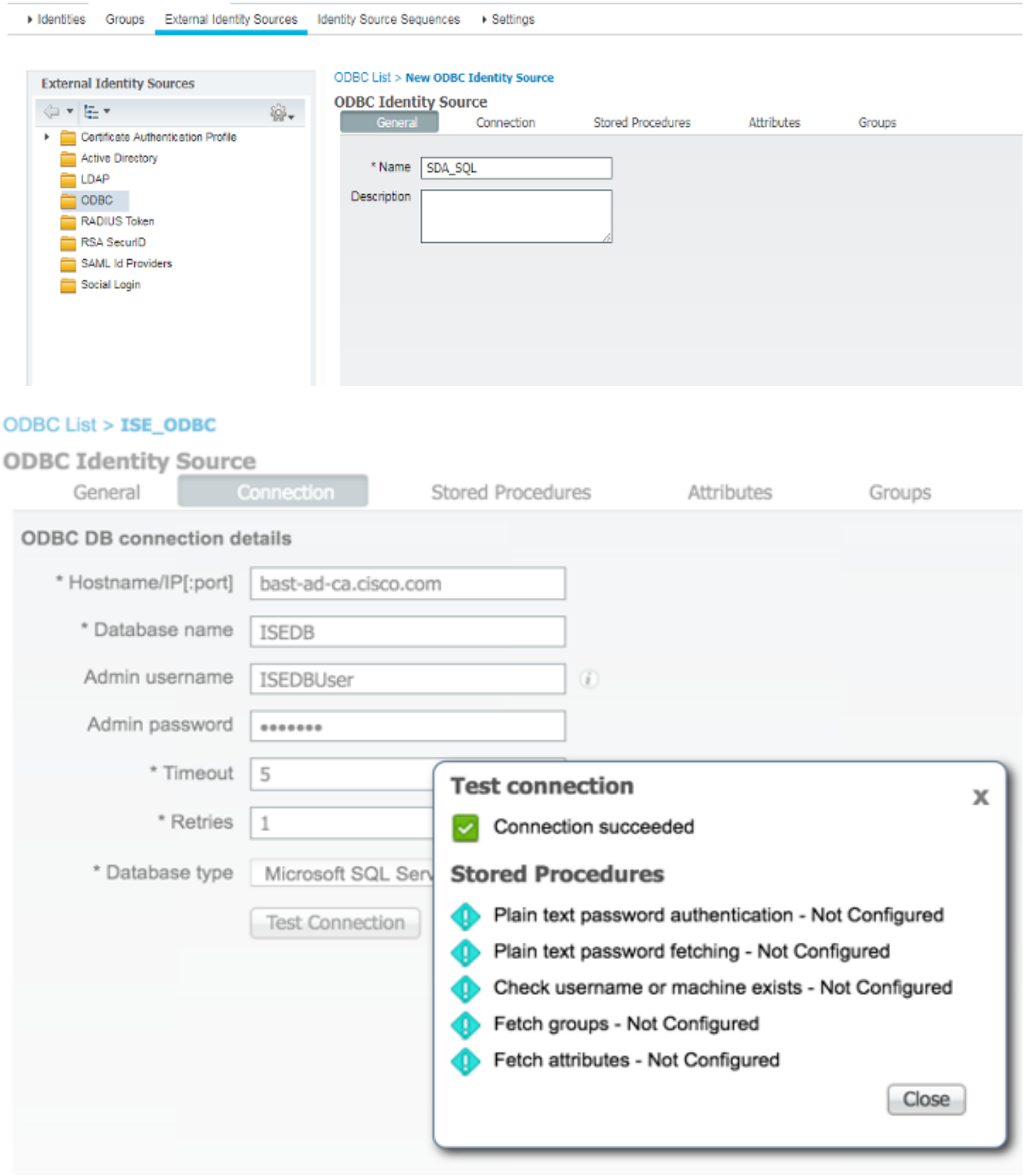
Diese Lösung hat folgende Nachteile:

- Zusätzliche Programmierung erforderlich, um die Anmeldeinformationen für den Endpunkt in die externe DB einzutragen.
- Wenn die externe DB nicht lokal wie PSNs vorhanden ist, ist diese Lösung vom WAN abhängig, das sie zum dritten Fehlerpunkt im AAA-Datenfluss des Endpunkts macht.
- Erfordert zusätzliches Wissen zur Verwaltung externer DB-Prozesse und -Verfahren.
- Fehler, die durch die manuelle Konfiguration der Benutzer-ID für DB verursacht wurden, müssen berücksichtigt werden.

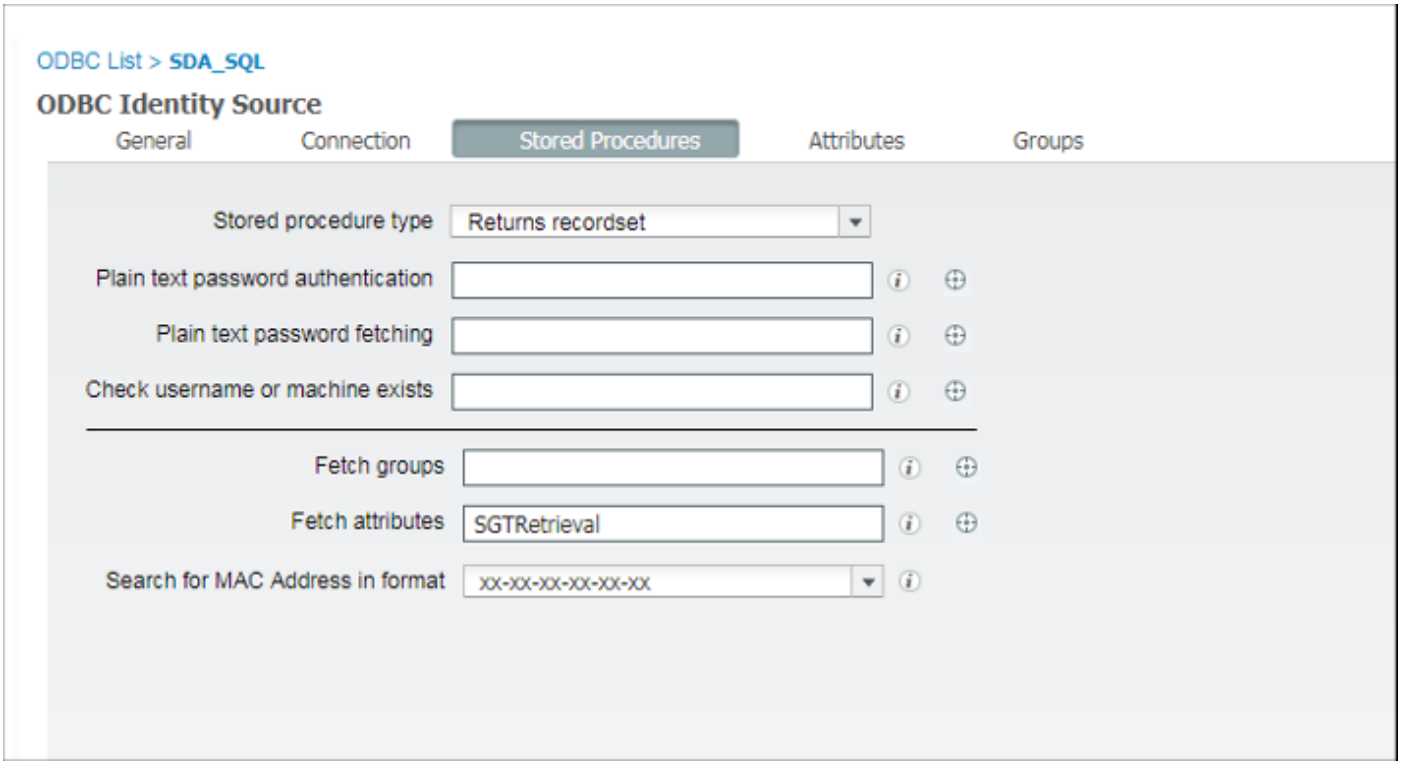
Externe DB - Beispielkonfigurationen

In diesem Dokument wird Microsoft SQL als externe Datenbank dargestellt, die als Autorisierungspunkt verwendet wird.

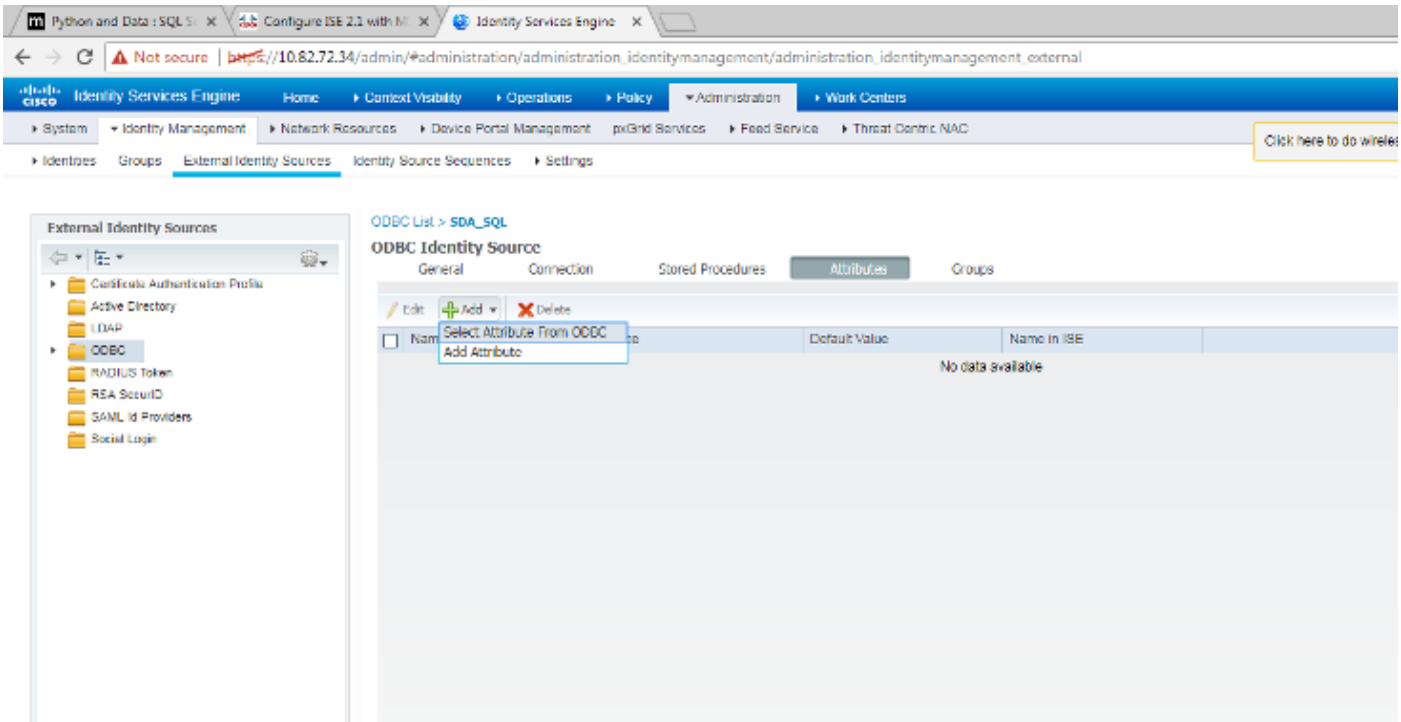
Schritt 1: Erstellen Sie den ODBC Identity Store in Cisco ISE aus dem Menü **Administration > External Identity Source > ODBC** und testen Sie die Verbindungen.

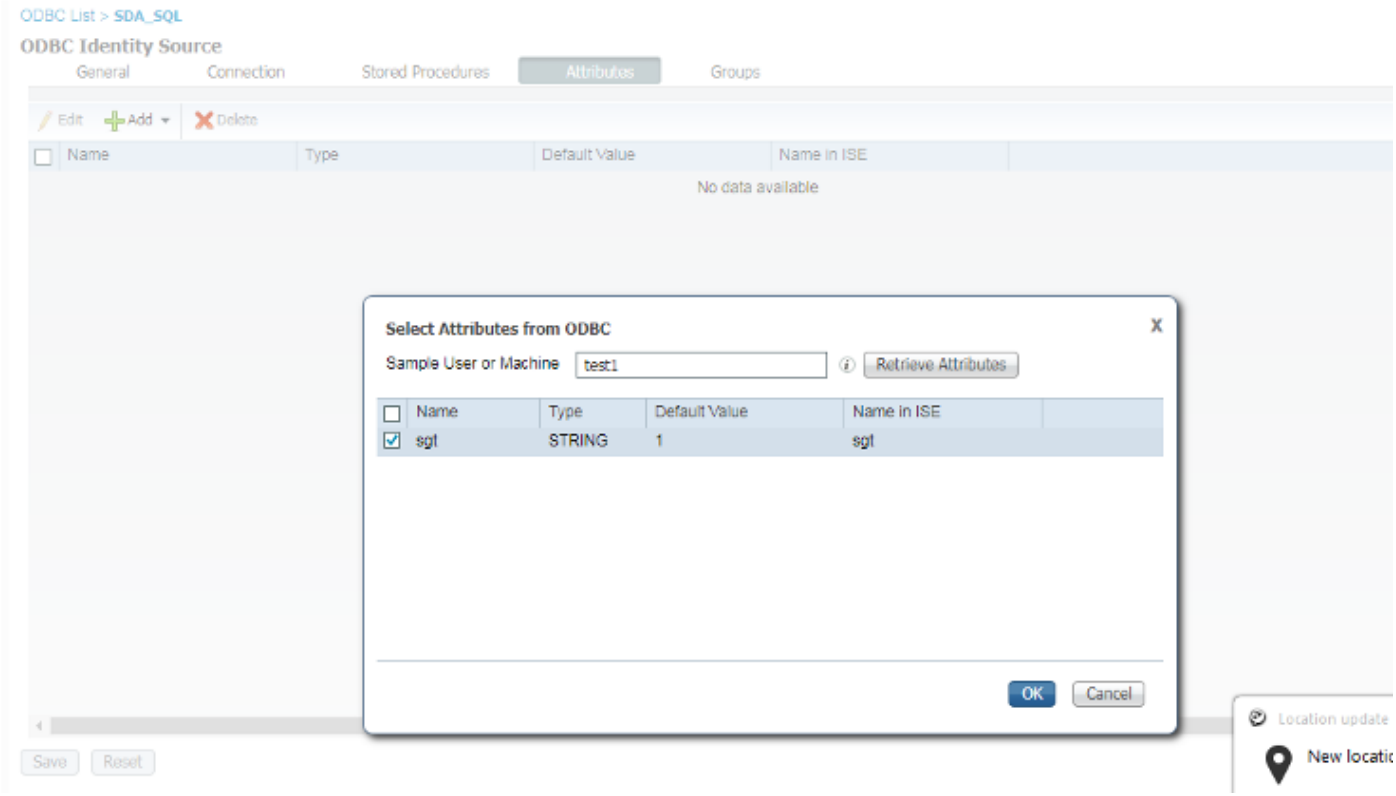


Schritt 2: Navigieren Sie auf der Seite ODBC zur Registerkarte Gespeicherte Prozeduren, um die in Cisco ISE erstellten Prozeduren zu konfigurieren.

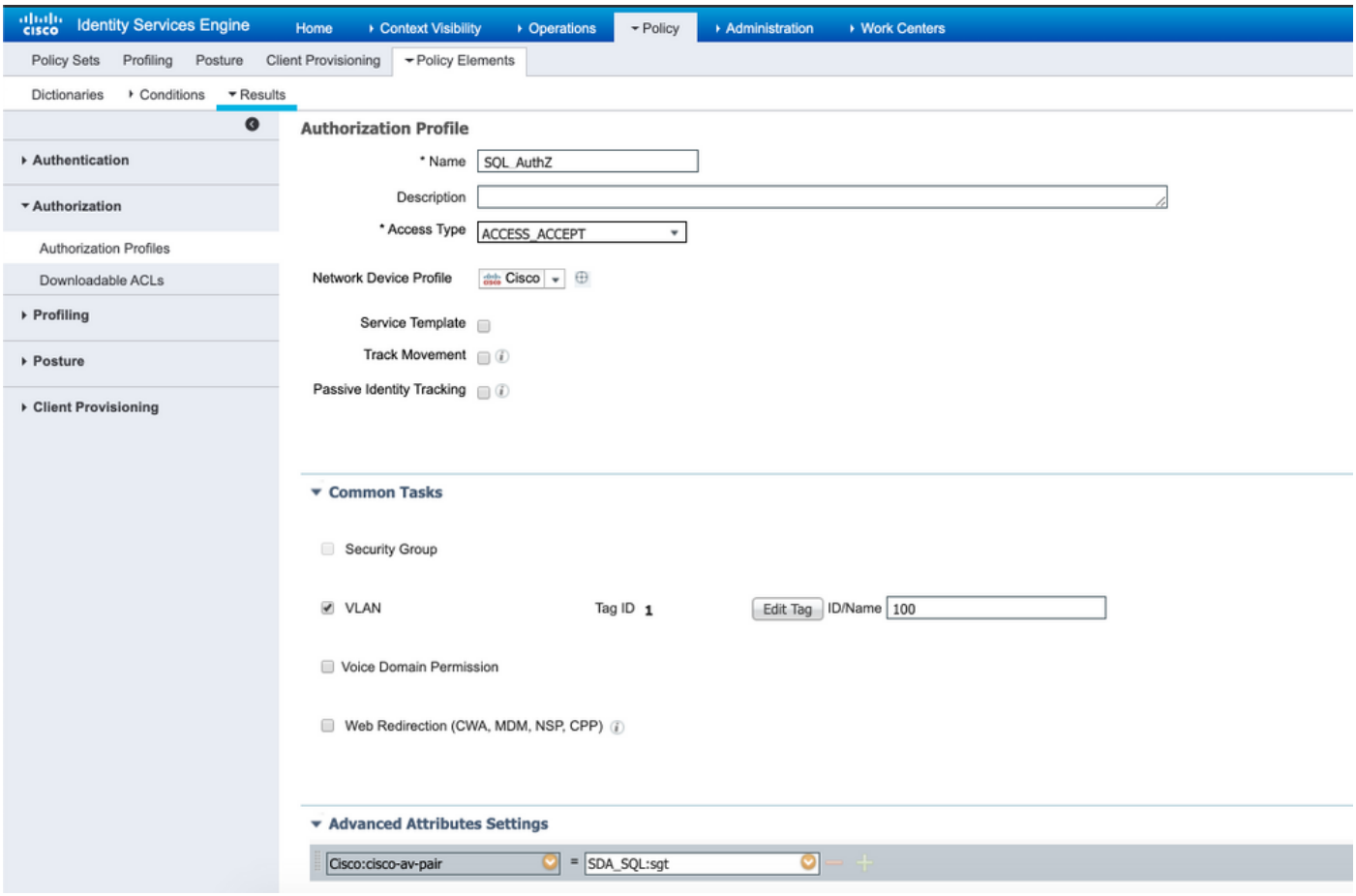


Schritt 3: Holen Sie die Attribute für die Benutzer-ID aus der ODBC-ID-Quelle zur Überprüfung.



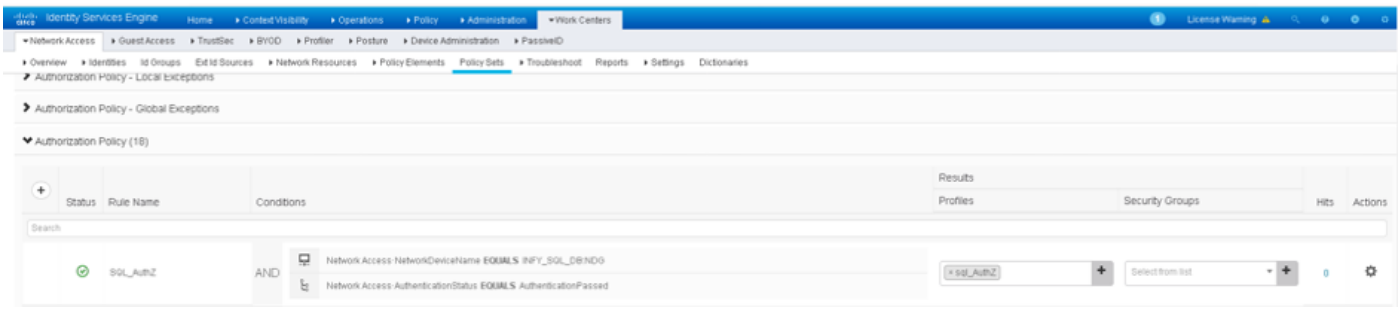


Schritt 4: Erstellen Sie ein **Autorisierungsprofil** und konfigurieren Sie es. Gehen Sie in Cisco ISE zu **Richtlinie > Ergebnisse > Autorisierungsprofil > Erweiterte Attributeinstellungen,** und wählen Sie das Attribut als **Cisco:cisco-av-pair.** Wählen Sie die Werte als <Name der ODBC-Datenbank>:sgt aus, und speichern Sie sie.

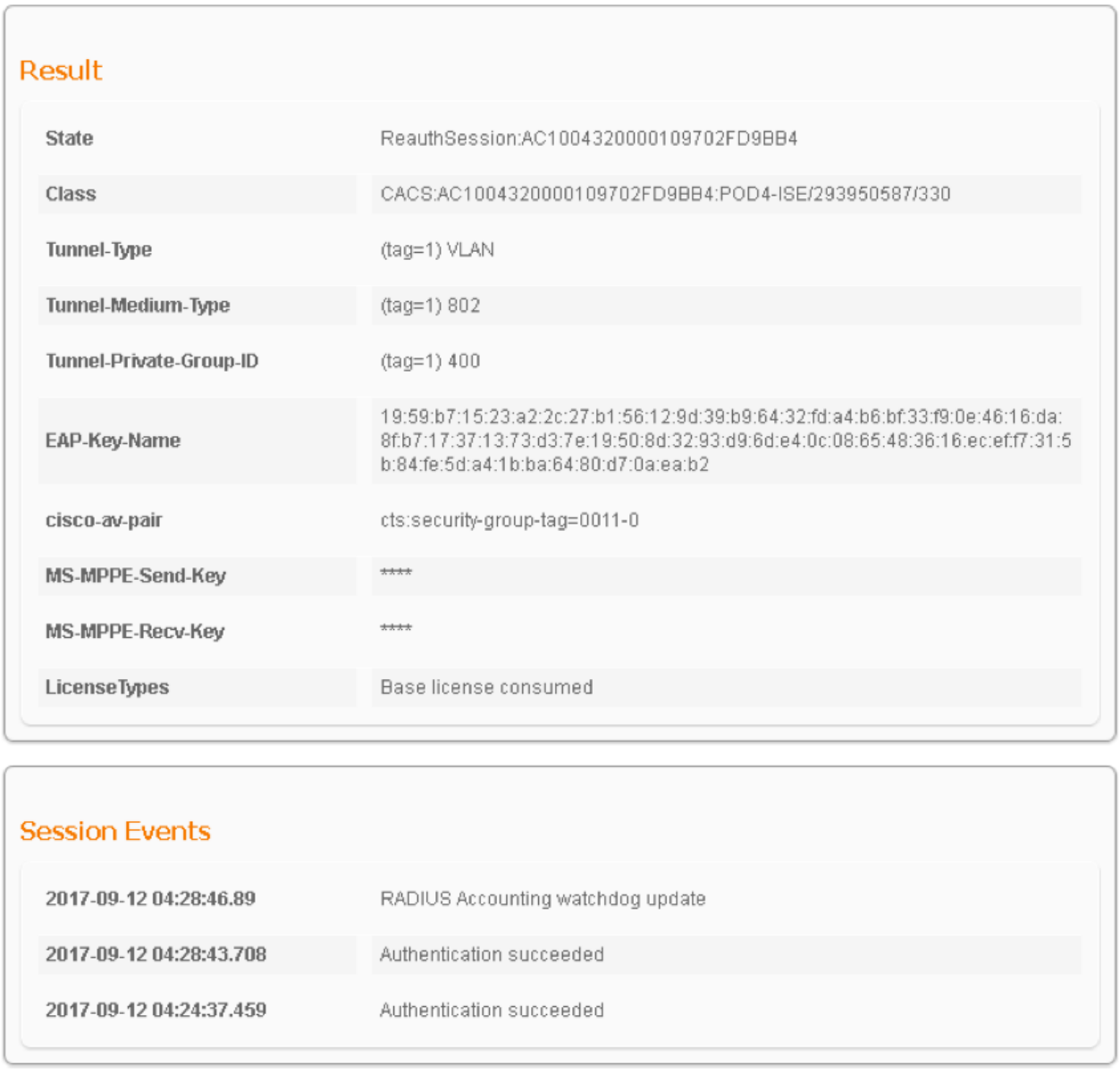


Schritt 5: Erstellen Sie eine **Autorisierungsrichtlinie,** und konfigurieren Sie sie. Navigieren Sie in der Cisco ISE zu **Policy > Policy Sets > Authorization Policy > Add.** Setzen Sie die Bedingung als

Identity Source auf den SQL-Server. Wählen Sie das Ergebnisprofil als Autorisierungsprofil aus, das zuvor erstellt wurde.



Schritt 6: Sobald der Benutzer authentifiziert und autorisiert ist, müssen die Protokolle die dem Benutzer zugewiesene sgt zur Überprüfung enthalten.



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

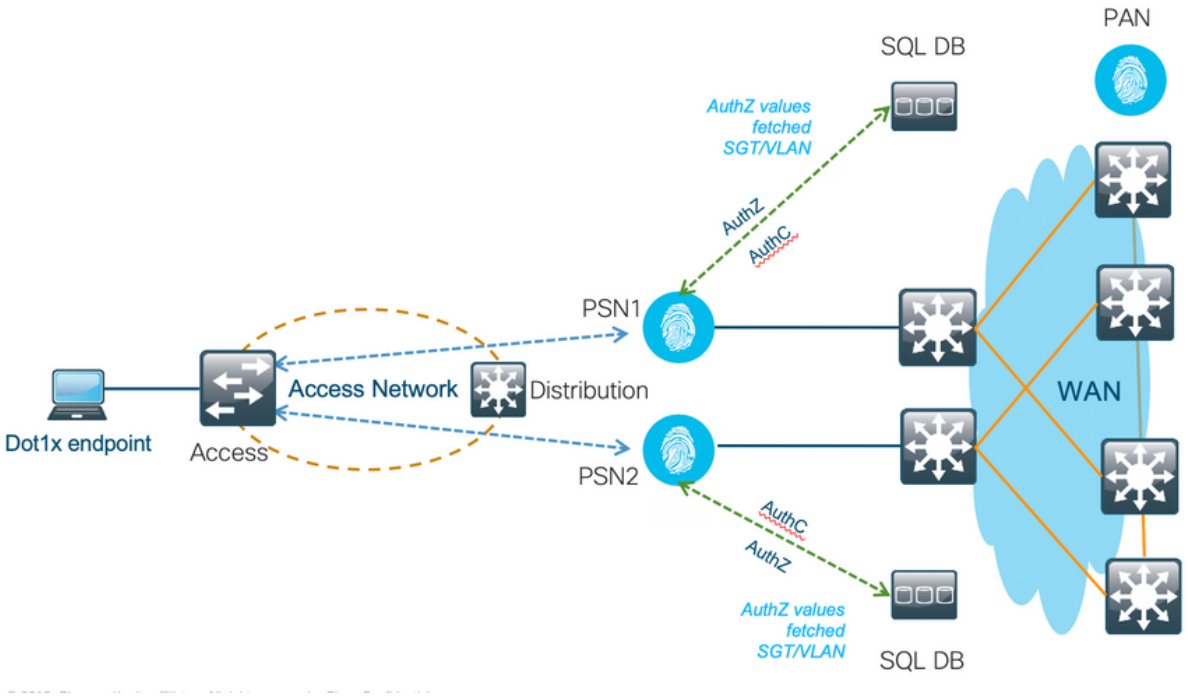
Session Events

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

Lösungs-Workflow (nach ISE 2.7)

Nach ISE 2.7 können Autorisierungsattribute von ODBC abgerufen werden, z. B. Vlan, SGT, ACL, und diese Attribute können in Richtlinien verwendet werden.

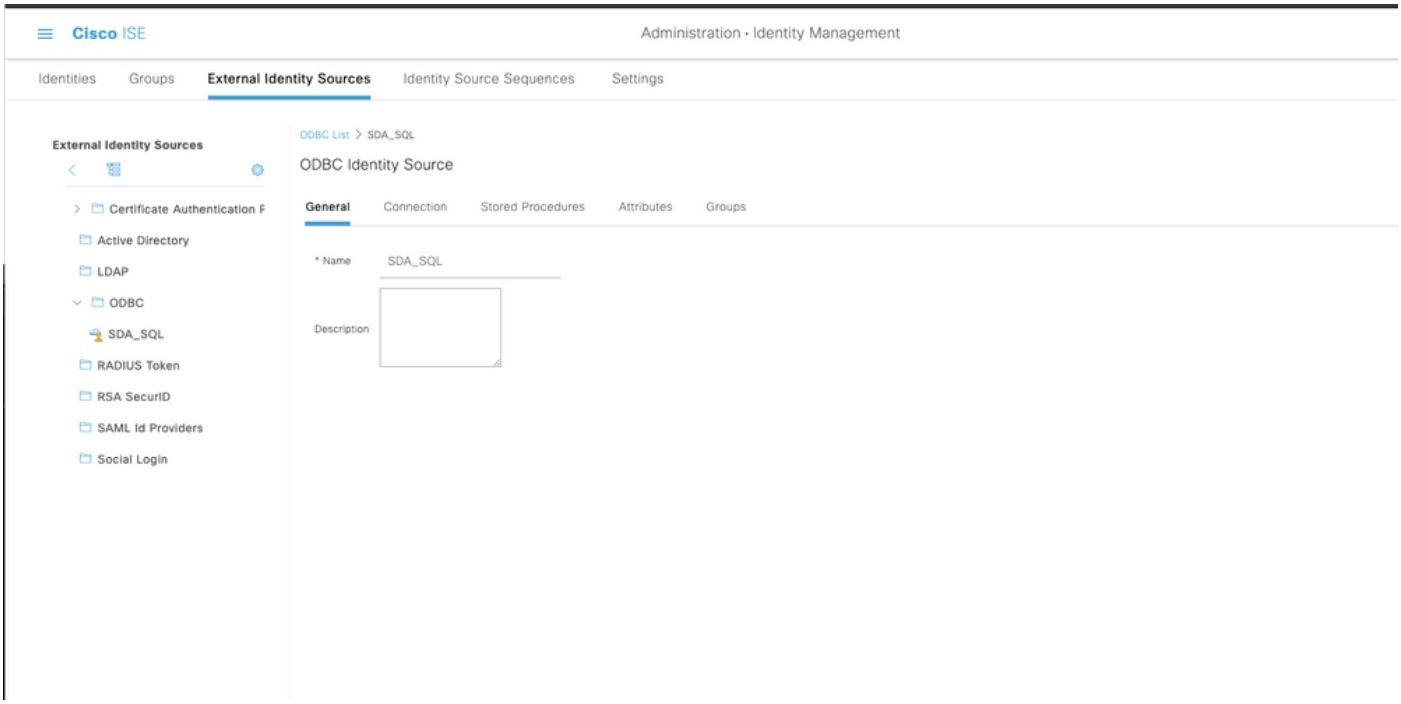
Bei dieser Lösung ist die Cisco ISE in Microsoft SQL integriert. MS SQL wird als ID-Speicher sowohl für die Authentifizierung als auch für die Autorisierung verwendet. Wenn die Anmeldeinformationen von den Endpunkten für PSN bereitgestellt werden, werden die Anmeldeinformationen mit der MS SQL-Datenbank abgeglichen. Die Autorisierungsrichtlinie bezieht sich auf die MS SQL-Datenbank zum Abrufen der autorisierten Ergebnisse wie SGT/VLAN, für die die **Benutzer-ID** als Referenz verwendet wird.



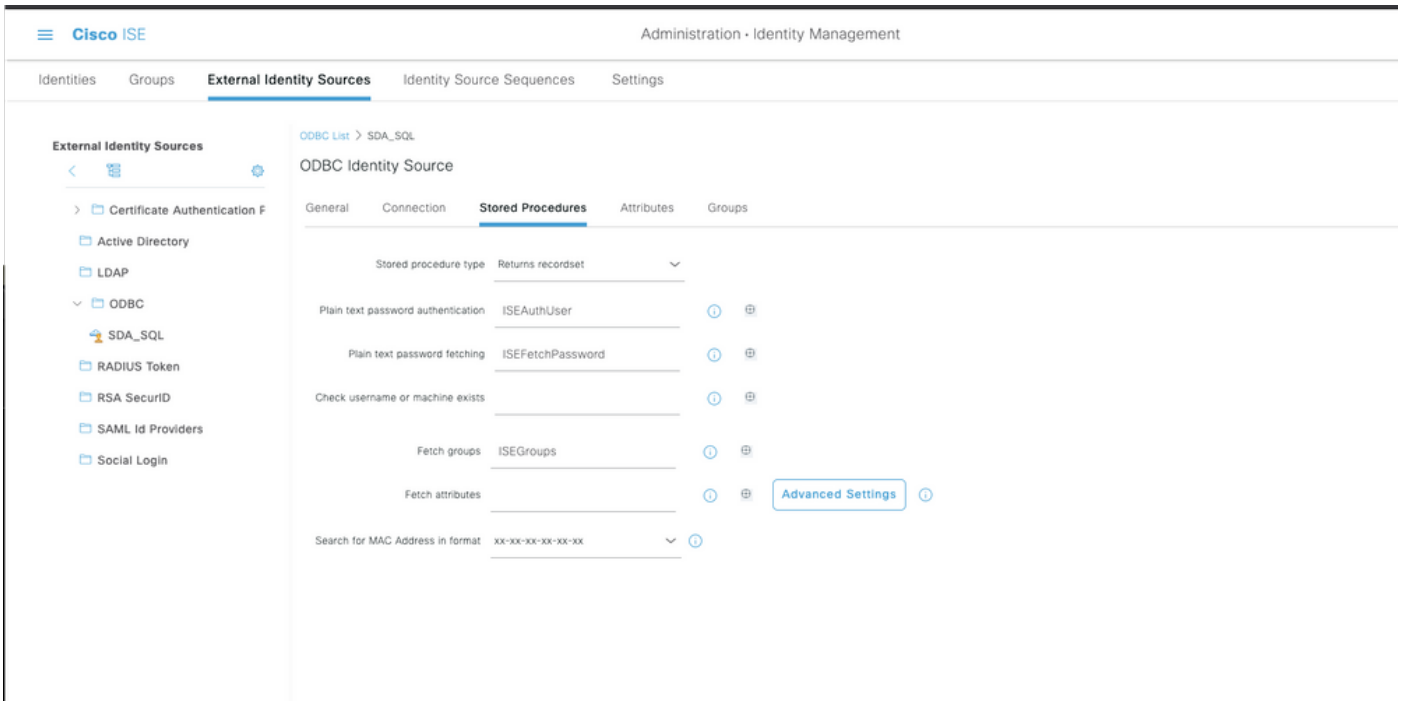
Externe DB - Beispielkonfigurationen

Befolgen Sie die zuvor in diesem Dokument beschriebene Prozedur, um MS SQL DB zusammen mit Username, Password, VLAN ID und SGT zu erstellen.

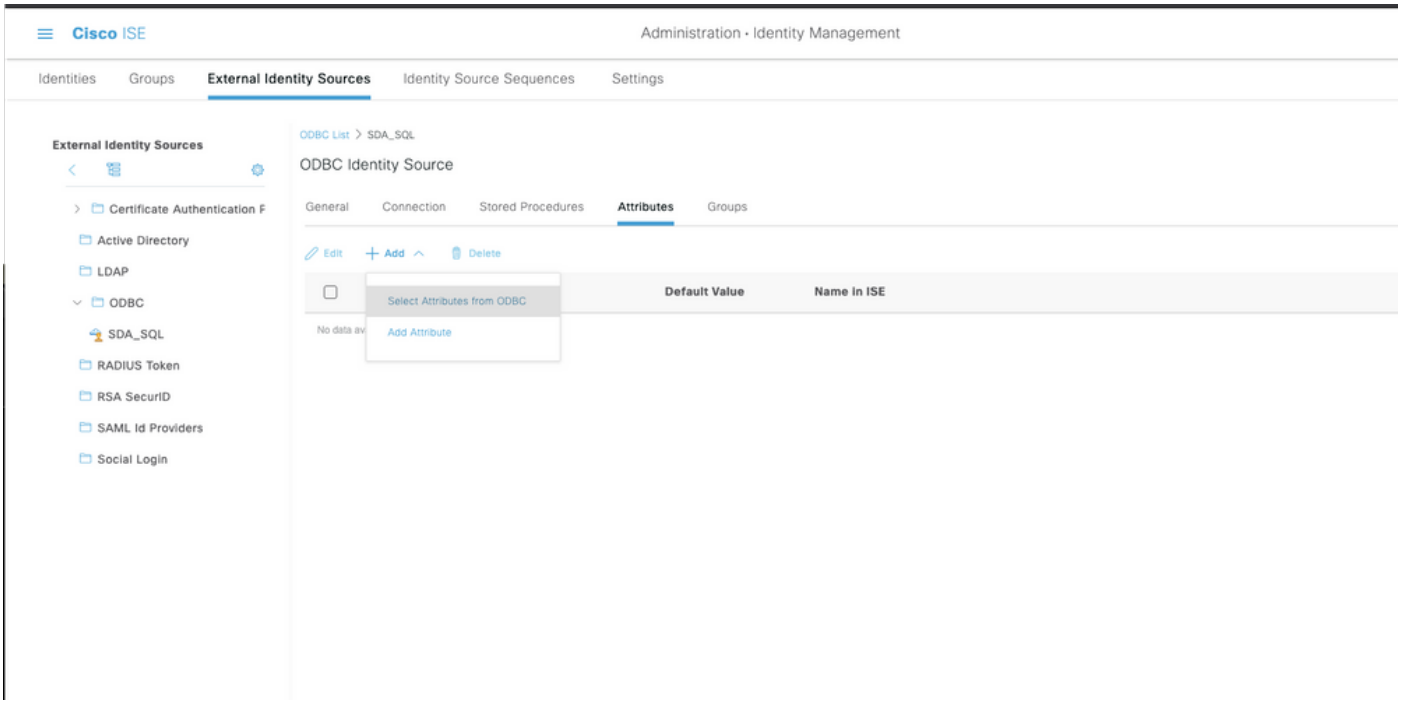
Schritt 1: Erstellen Sie einen ODBC Identity Store in Cisco ISE aus dem Menü **Administration > External Identity Source > ODBC** und testen Sie die Verbindungen.

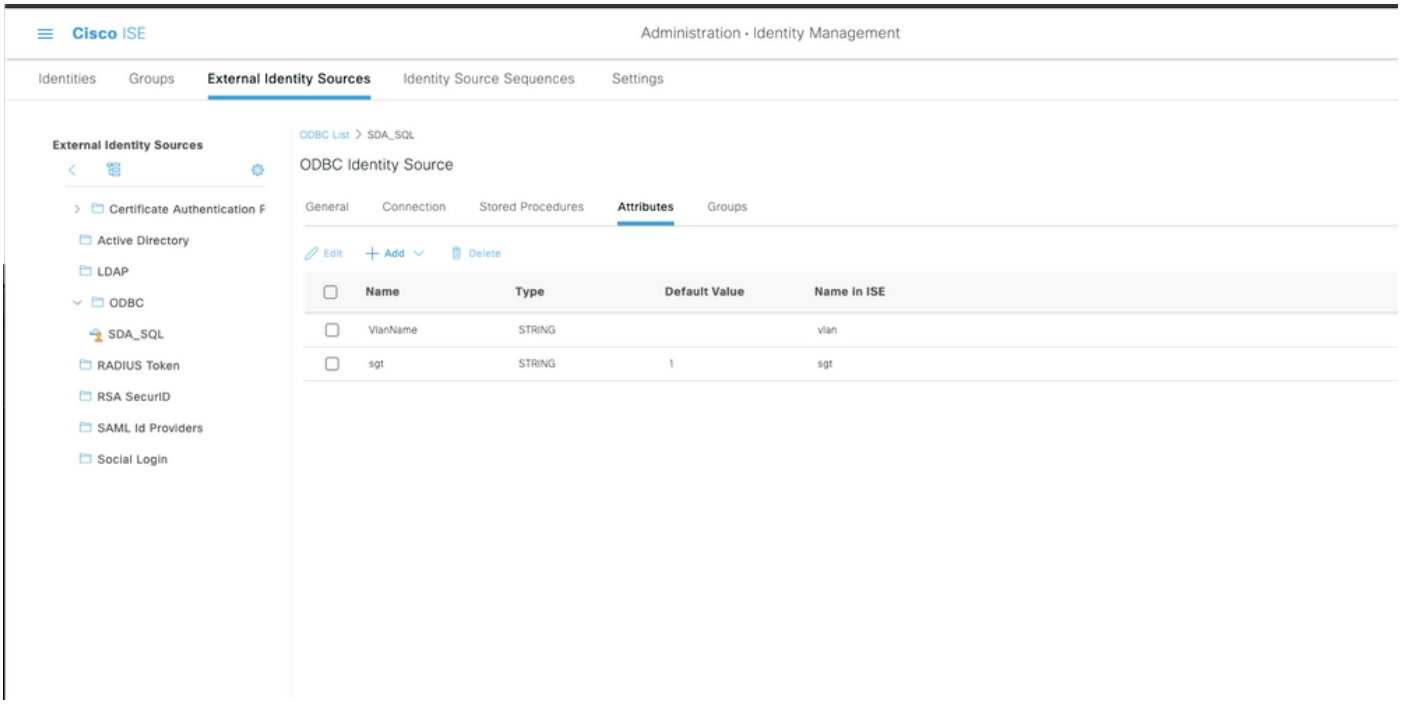


Schritt 2: Navigieren Sie auf der Seite ODBC zur Registerkarte Gespeicherte Prozeduren, um die in Cisco ISE erstellten Prozeduren zu konfigurieren.

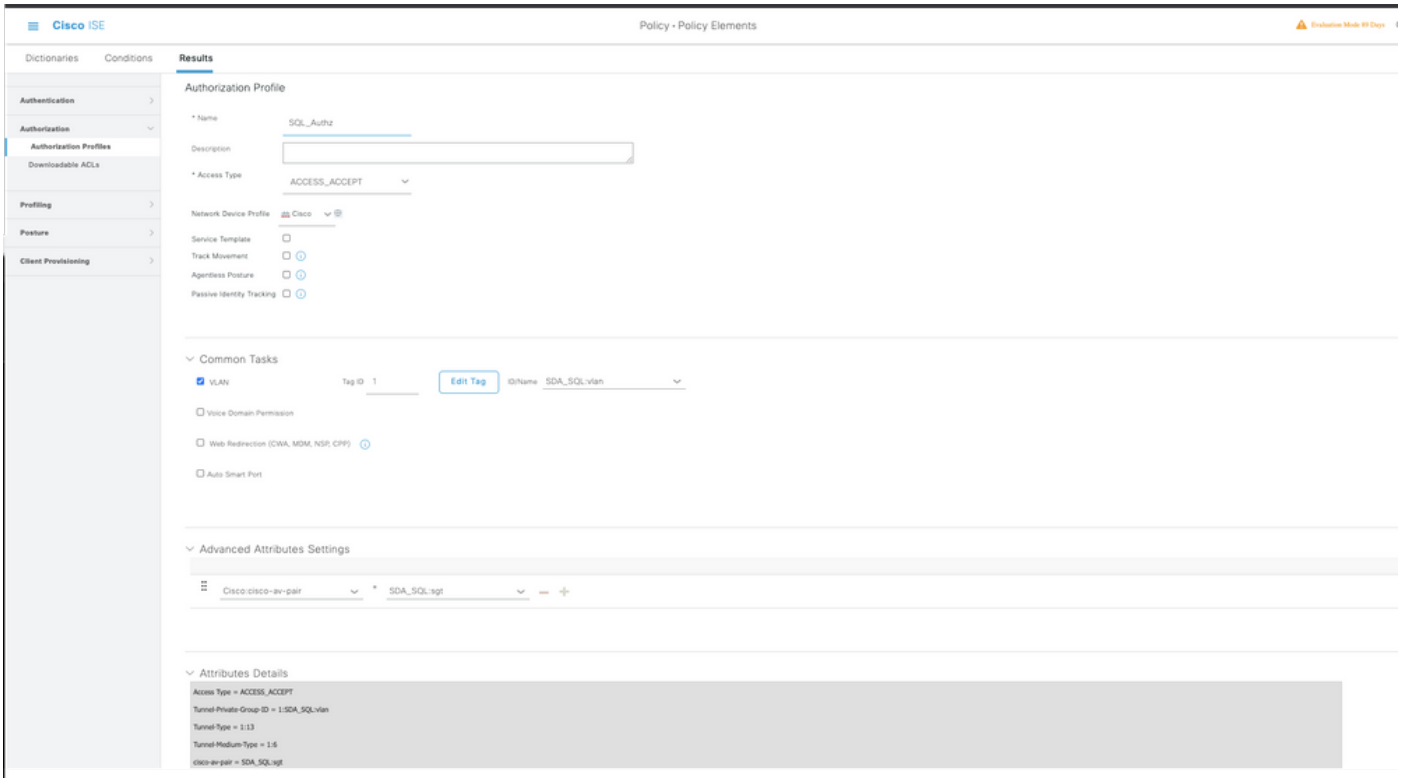


Schritt 3: Holen Sie die Attribute für die Benutzer-ID aus der ODBC-ID-Quelle zur Überprüfung.

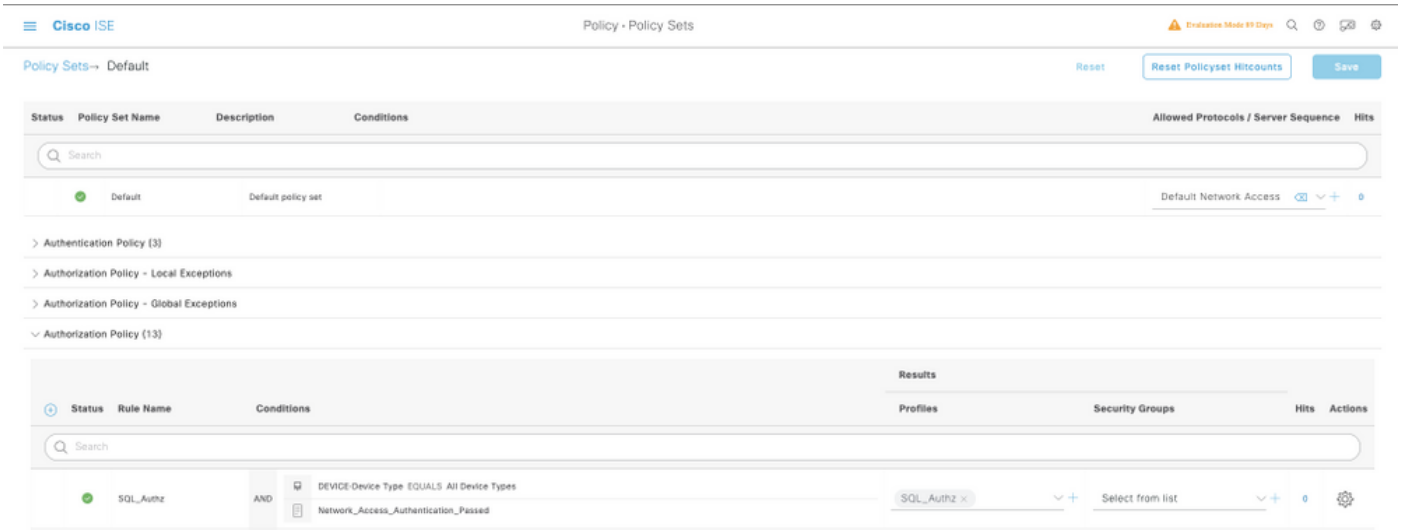




Schritt 4: Erstellen Sie ein **Autorisierungsprofil** und konfigurieren Sie es. Gehen Sie in Cisco ISE zu **Richtlinie > Ergebnisse > Autorisierungsprofil > Erweiterte Attributeinstellungen,** und wählen Sie das Attribut als **Cisco:cisco-av-pair.** Wählen Sie die Werte als <Name der ODBC-Datenbank>:sgt. Wählen Sie unter Allgemeine Aufgaben **VLAN** mit ID/Name als <Name der ODBC-Datenbank>:vlan aus, und speichern Sie es.



Schritt 5: Erstellen Sie eine **Autorisierungsrichtlinie,** und konfigurieren Sie sie. Navigieren Sie in der Cisco ISE zu **Policy > Policy Sets > Authorization Policy > Add.** Setzen Sie die Bedingung als Identity Source auf den SQL-Server. Wählen Sie das Ergebnisprofil als Autorisierungsprofil aus, das zuvor erstellt wurde.



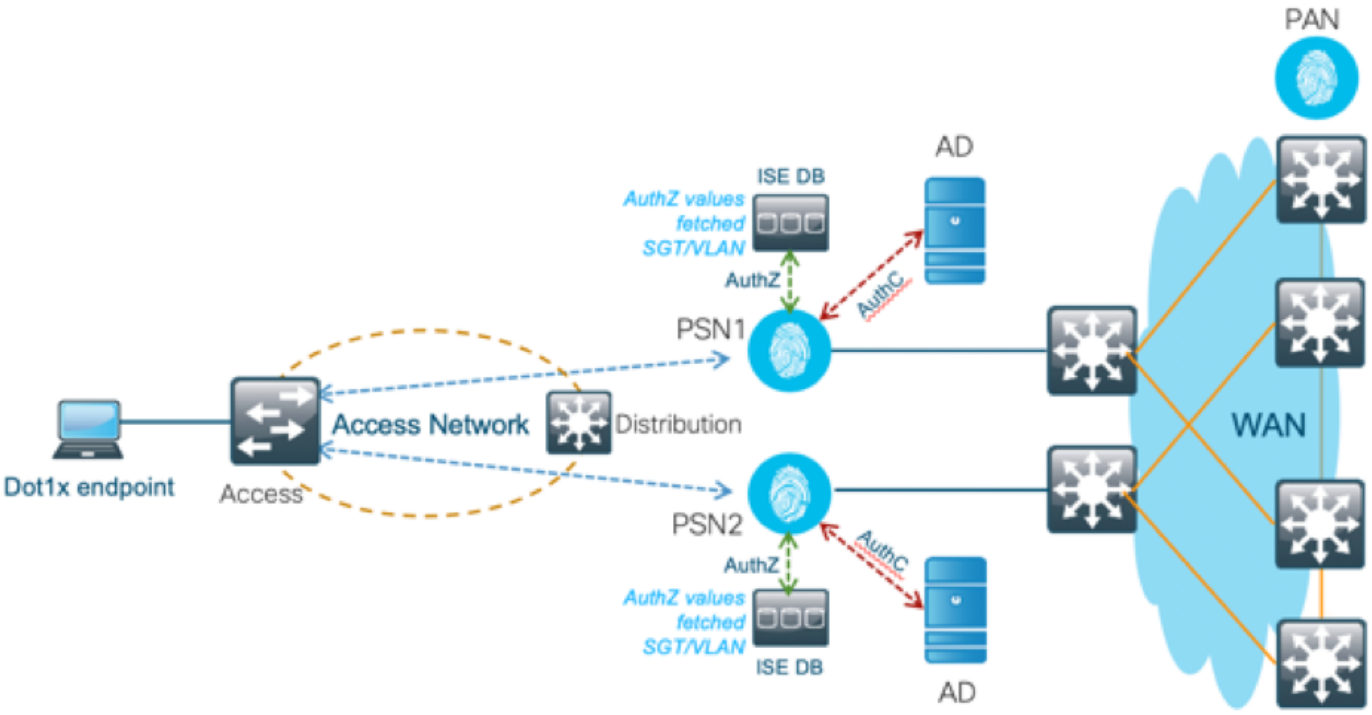
Interne Datenbank verwenden

Die Cisco ISE selbst verfügt über eine integrierte Datenbank, die über Benutzer-IDs zur Autorisierung verfügt.

Lösungs-Workflow

Bei dieser Lösung wird die interne Datenbank der Cisco ISE als Autorisierungspunkt verwendet, während Active Directory (AD) weiterhin die Authentifizierungsquelle ist. Die Benutzer-ID von Endpunkten ist in der Cisco ISE DB enthalten, zusammen mit **benutzerdefinierten Attributen,** die die autorisierten Ergebnisse zurückgeben, wie z. B. SGT oder VLAN. Wenn die

Anmeldeinformationen von den Endpunkten an PSN übermittelt werden, wird die Gültigkeit der Anmeldeinformationen der Endpunkte mit dem Active Directory-ID-Speicher überprüft und der Endpunkt authentifiziert. Die Autorisierungsrichtlinie bezieht sich auf die ISE-DB zum Abrufen der autorisierten Ergebnisse wie SGT/VLAN, für die die Benutzer-ID als Referenz verwendet wird.



Vorteile

Diese Lösung bietet die folgenden Vorteile, die sie zu einer flexiblen Lösung machen:

- Die Cisco ISE DB ist eine integrierte Lösung und bietet daher im Gegensatz zur externen DB-Lösung keinen dritten Fehlerpunkt.
- Da der Cisco ISE-Cluster die Echtzeit-Synchronisierung zwischen allen Personen gewährleistet, besteht keine WAN-Abhängigkeit, da beim PSN alle Benutzer-IDs und benutzerdefinierten Attribute in Echtzeit vom PAN übernommen werden.
- Die Cisco ISE kann alle möglichen zusätzlichen Funktionen nutzen, die die externe DB bietet.
- Für diese Lösung gelten keine Größenbeschränkungen der Cisco ISE.

Nachteile

Diese Lösung hat folgende Nachteile:

- Die maximale Anzahl von Benutzer-IDs, die die Cisco ISE DB zurückhalten kann, beträgt 300.000.
- Fehler, die durch die manuelle Konfiguration der Benutzer-ID für DB verursacht wurden, müssen berücksichtigt werden.

Interne DB-Beispielkonfigurationen

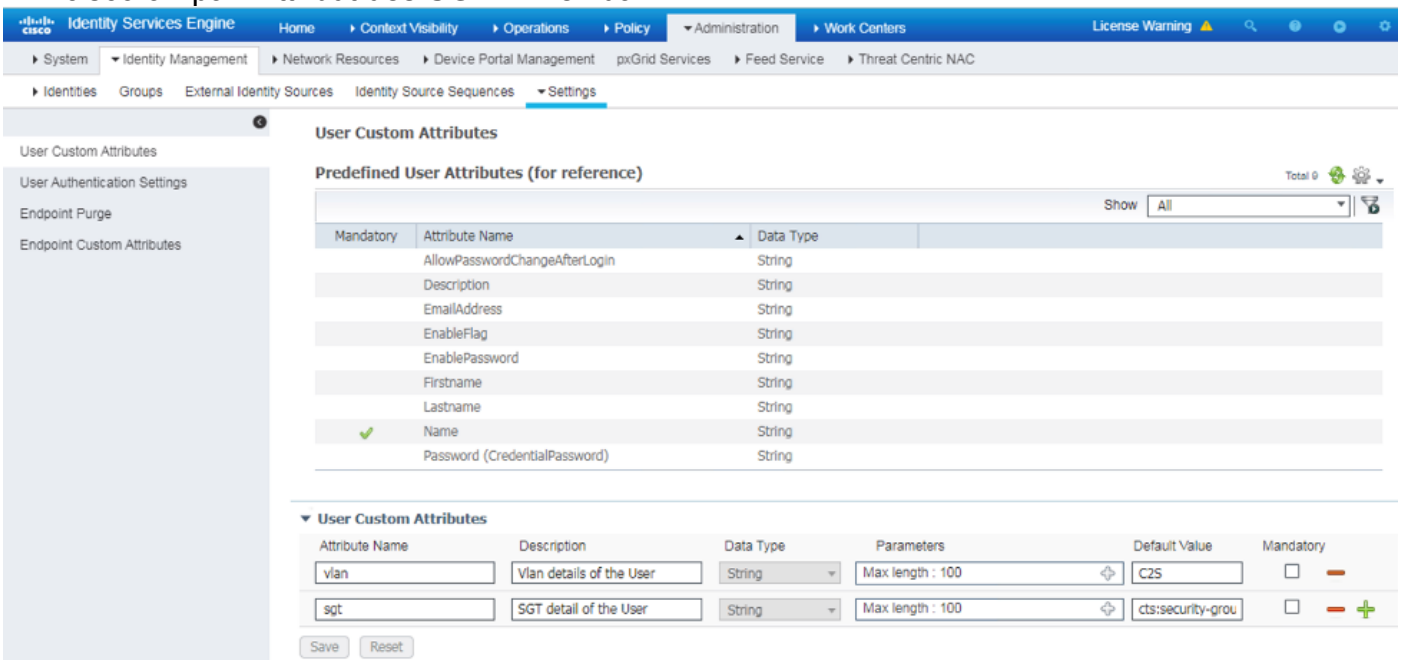
Das benutzerspezifische VLAN und SGT können für jeden Benutzer im internen ID-Speicher mit einem benutzerdefinierten Benutzerattribut konfiguriert werden.

Schritt 1. Erstellen Sie neue benutzerdefinierte Benutzerattribute, um den VLAN- und SGT-Wert der entsprechenden Benutzer darzustellen. Navigieren Sie zu **Administration > Identity Management > Settings > User Custom Attributes.** Erstellen Sie neue benutzerdefinierte Benutzerattribute, wie in dieser Tabelle dargestellt.

Hier wird die ISE-DB-Tabelle mit benutzerdefinierten Attributen angezeigt.

Attributname	Datentyp	Parameter (Länge)	Standardwert
VLAN	String	100	C2S (Standard-VLAN-Name)
Zielgruppe	String	100	cts:security-group-tag=0003-0 (Standard-SGT-Wert)

- In diesem Szenario stellt der VLAN-Wert den VLAN-Namen dar, und der SGT-Wert stellt das cisco-av-pair-Attribut des SGT in Hex dar.

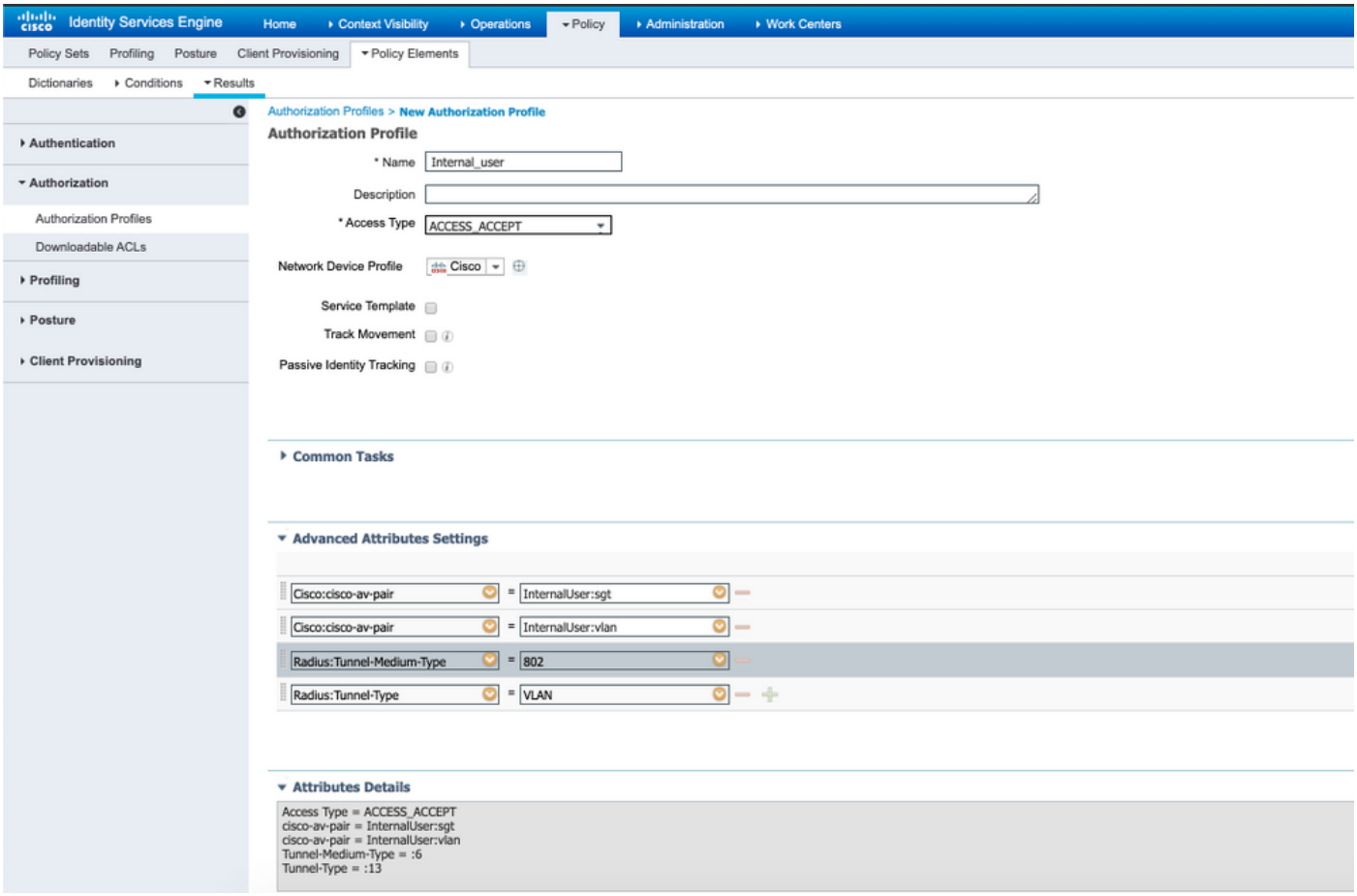


Schritt 2. Erstellen Sie ein Autorisierungsprofil mit benutzerdefinierten Benutzerattributen, um die VLAN- und SGT-Werte der jeweiligen Benutzer zu implizieren. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > Hinzufügen.** Fügen Sie die unten genannten Attribute unter Erweiterte Attributeinstellungen hinzu.

Diese Tabelle zeigt das AuthZ-Profil für interne Benutzer.

Attribut	Wert
Cisco:cisco-av-pair	Interner Benutzer:sgt
Radius:Tunnel-Private-Group-ID	Interner Benutzer:vlan
Radius:Tunnel-Medium-Type	802
Radius:Tunneltyp	VLAN

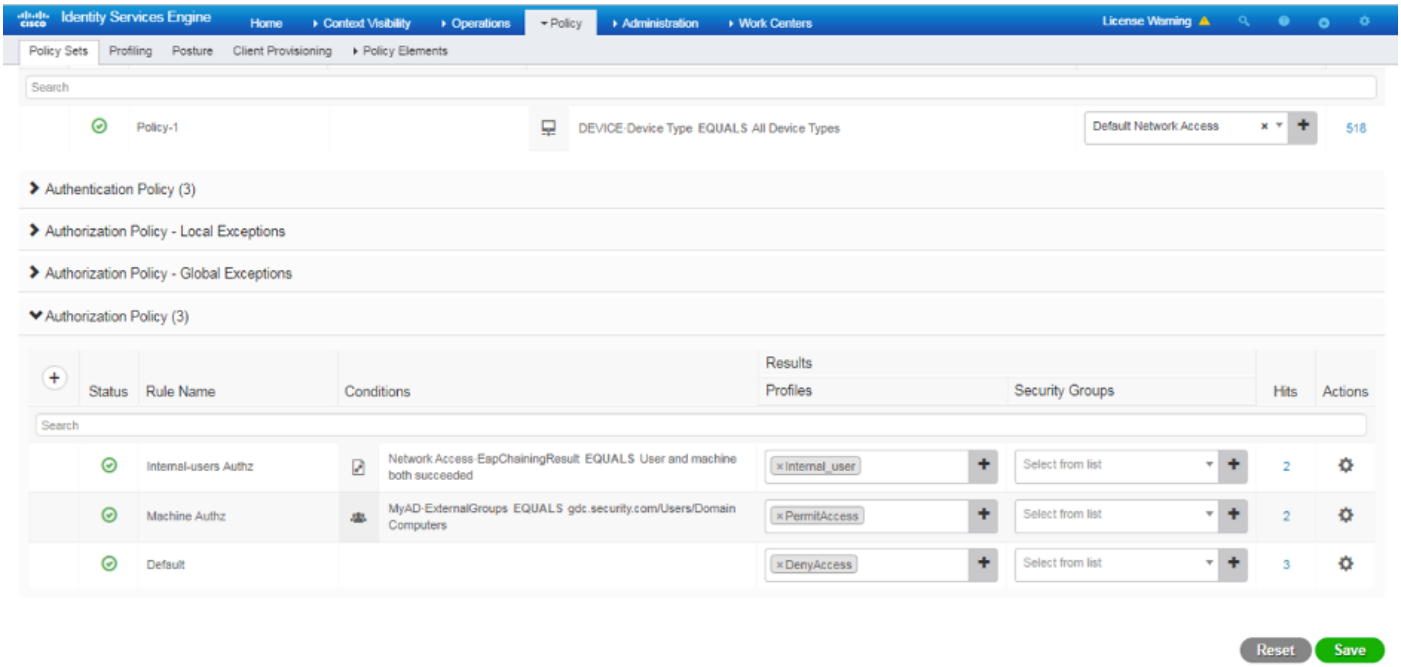
Wie im Bild gezeigt, ist das Profil **Internal_user** für die internen Benutzer so konfiguriert, dass SGT und Vlan jeweils als **InternalUser:sgt** und **InternalUser:vlan** konfiguriert sind.



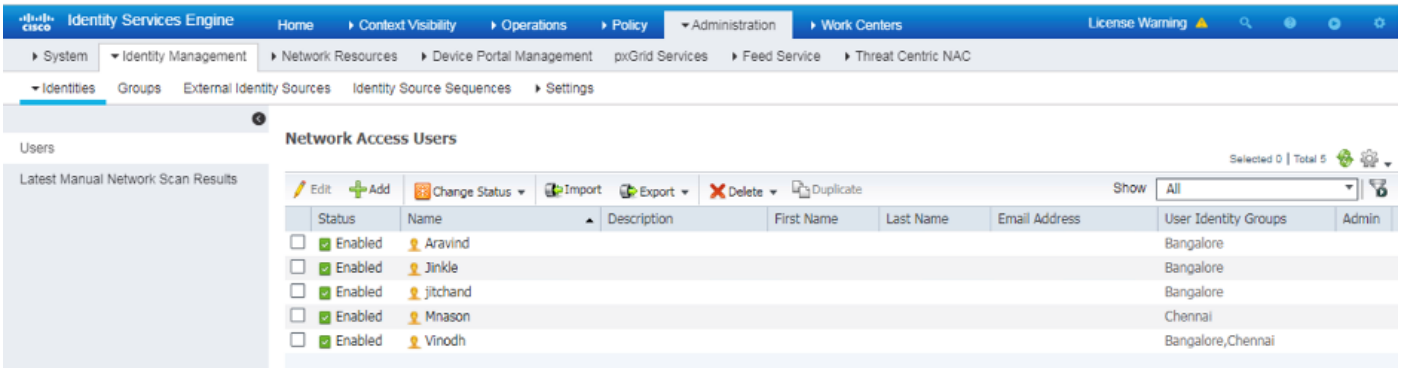
Schritt 3: Autorisierungsrichtlinie erstellen, Navigieren Sie zu **Richtlinie > Policy Sets > Policy-1 > Autorisierung.** Erstellen Sie Autorisierungsrichtlinien mit den unten genannten Bedingungen, und ordnen Sie sie den entsprechenden Autorisierungsprofilen zu.

Diese Tabelle zeigt die AuthZ-Richtlinie für interne Benutzer.

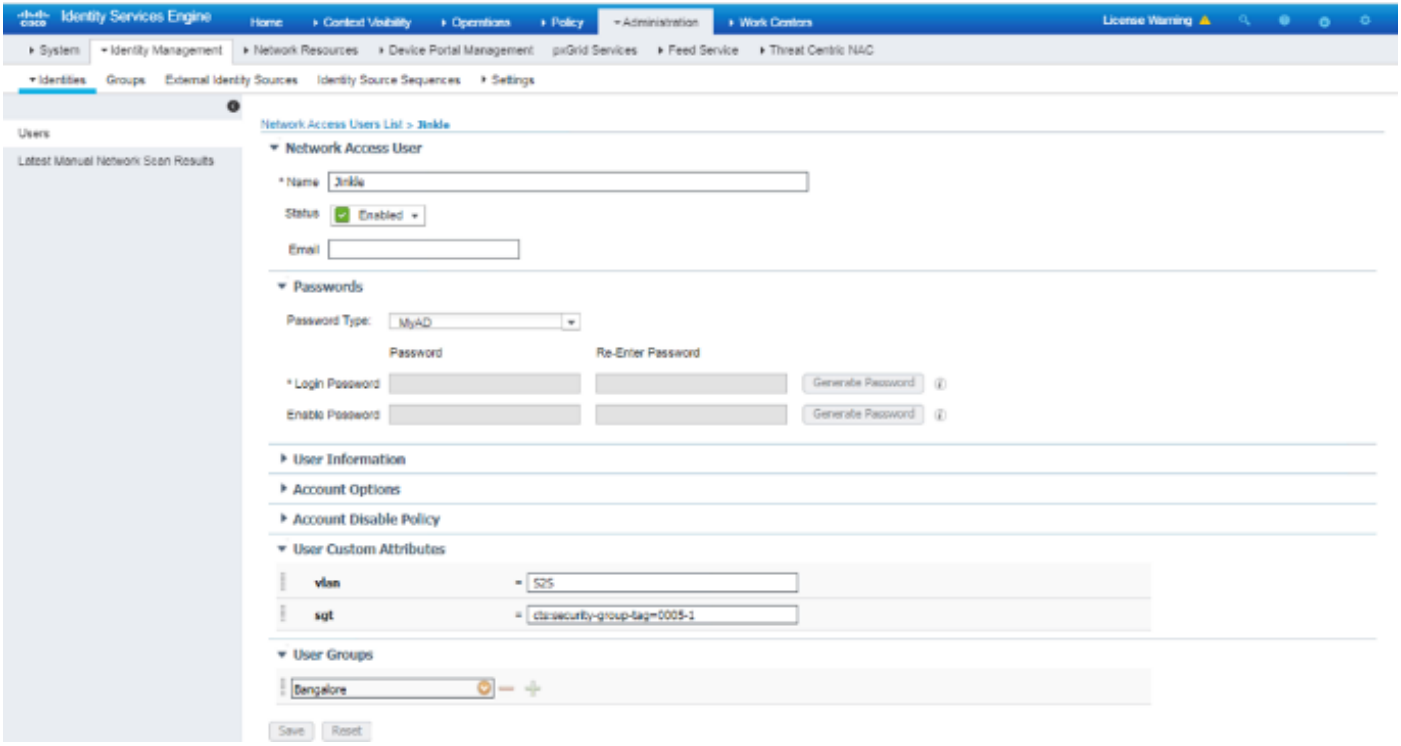
Regelname	Bedingung	Autorisierungsprofil für Ergebnisse
Interne_Benutzer_Authentifizierung	Wenn Netzwerkzugriff.EapChainingResults gleich Benutzer und Computer waren beide erfolgreich	Interner Benutzer
Nur-Computer-Authentifizierung	Wenn MyAD.ExternalGroups GLEICHT gdc.security.com/Users/Domain Computers	Zugriff zulassen



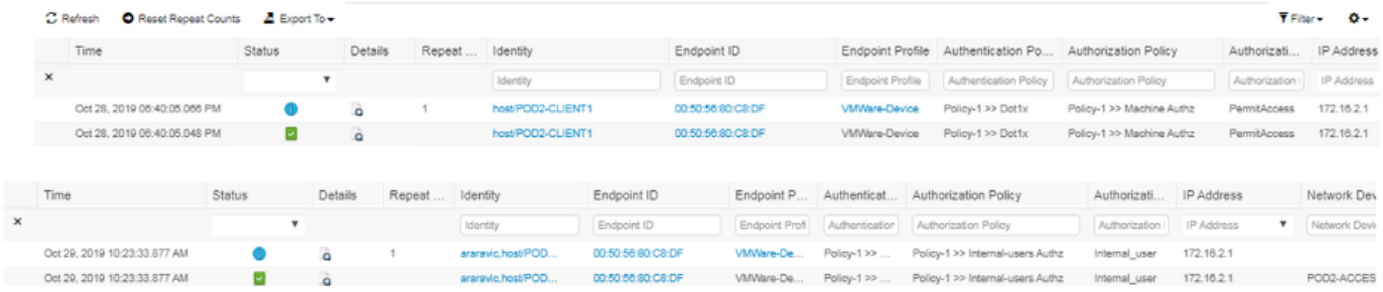
Schritt 4: Erstellen Sie mehrere Benutzeridentitäten mit benutzerdefinierten Attributen mit Benutzerdetails und den entsprechenden benutzerdefinierten Attributen in der CSV-Vorlage. Importieren Sie die CSV, indem Sie zu **Administration > Identity Management > Identities > Users > Import > Choose the file > Import** navigieren.



Dieses Bild zeigt einen Beispielbenutzer mit benutzerdefinierten Attributdetails. Wählen Sie den Benutzer aus, und klicken Sie auf "Bearbeiten", um die benutzerdefinierten Attributdetails anzuzeigen, die dem jeweiligen Benutzer zugeordnet sind.



Schritt 5: Überprüfen Sie die Live-Protokolle:



Überprüfen Sie im Abschnitt **Result** (**Ergebnis**), ob das **Vlan**- und **SGT-**Attribut als Teil von Access-Accept gesendet wird.

Schlussfolgerung

Mit dieser Lösung können einige Großkunden ihre Anforderungen erfüllen. Beim Hinzufügen/Löschen von Benutzer-IDs ist Vorsicht geboten. Werden Fehler ausgelöst, kann dies zu nicht autorisierten Zugriffen für echte Benutzer führen oder umgekehrt.

Zugehörige Informationen

Konfigurieren von Cisco ISE mit MS SQL über 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

Glossar

AAA	Authentifizierung, Autorisierung, Abrechnung
AD	Active Directory
AuthC	Authentifizierung
AuthZ	Autorisierung
DB	Datenbank
PUNKT 1X	802.1x
IBN	Identitätsbasiertes Netzwerk
ID	Identitätsdatenbank
ISE	Identity Services Engine
MnT	Überwachung und Fehlerbehebung

MSSQL	Microsoft SQL
ODBC	Open DataBase-Konnektivität
SCHWENKEN	Knoten "Policy Admin"
PSN	Richtliniendienstknoten
SGT	Secure Group-Tag
SQL	Strukturierte Abfragesprache
VLAN	Virtuelles LAN
WAN	Wide Area Network

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.