Contents

Introduction

This document describes how to configure Identity Services Engine (ISE) with Microsoft Standard Query Language (SQL) Server for ISE authentication using

> **Note**: Open Database Connectivity (ODBC) authentication requires ISE to be able to fetch a plain text user password. The password can be encrypted in the database, but has to be decrypted by the **stored procedure**.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Database and ODBC concepts
- Microsoft SQL Server

Components Used

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

- Identity Services Engine 2.1
- MSSQL Server 2008 R2

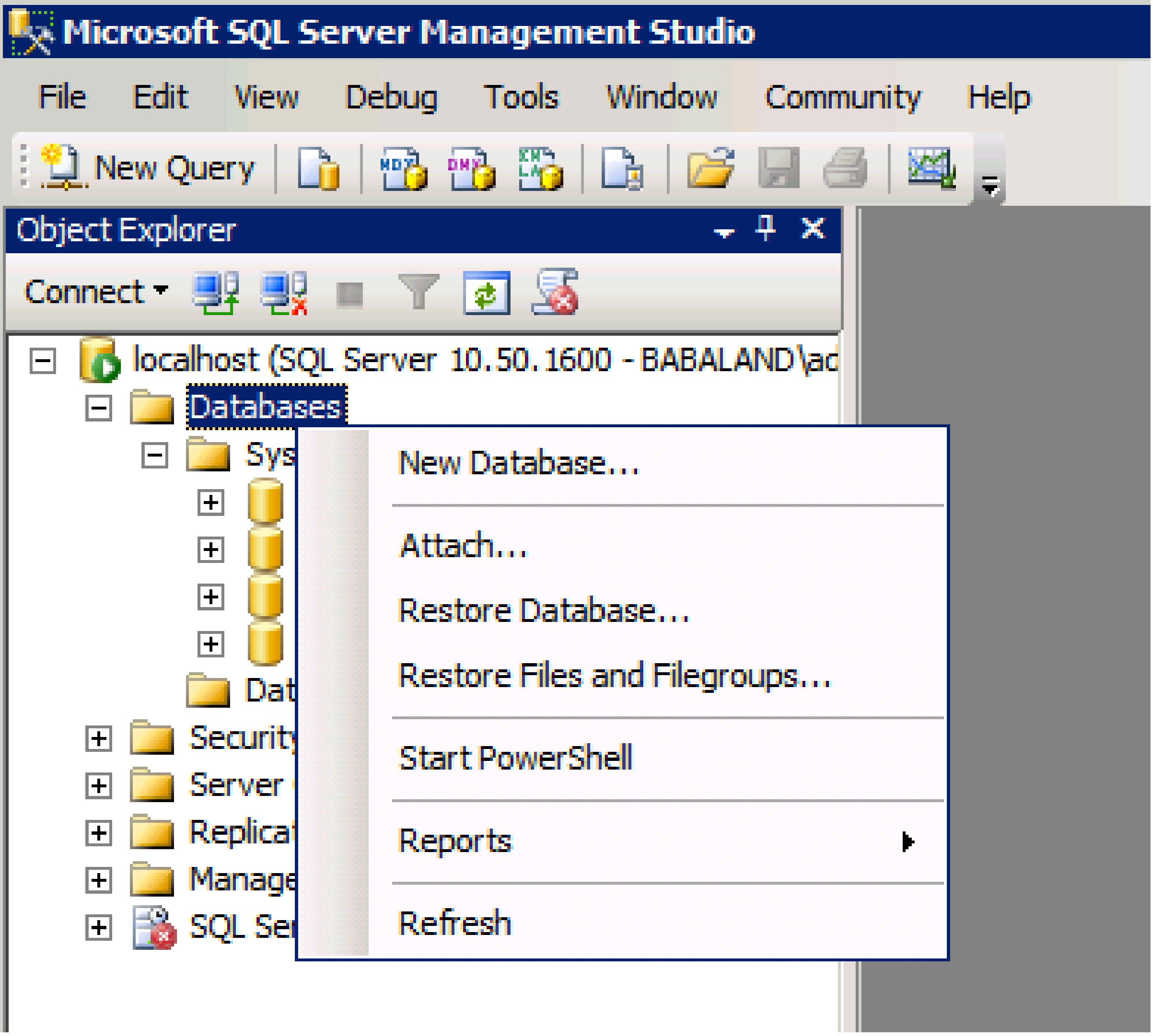
Configure

Step 1. MS SQL Basic Configuration

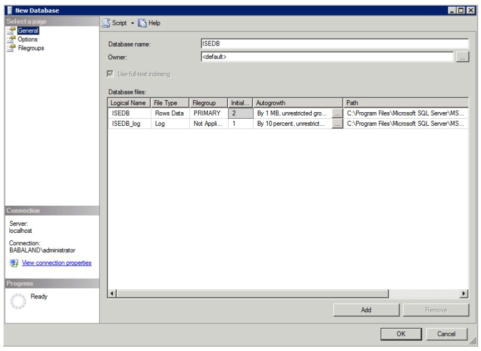
Configuration steps include creating a database and one user for ISE with permissions to access that database.

> **Note**: ISE supports only SQL authentication, not the Windows account. If you need to change authentication mode, please refer to Change Server Authentication Mode

1. Open SQL Server Management Studio (**Start menu > Microsoft SQL Server 2008 R2**) and create a database:



2. Leave default options or adjust database settings as shown in this image:



Database name: ISEDB

Owner: <default>

☑ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial...	Autogrowth	Path
ISEDB	Rows Data	PRIMARY	2	By 1 MB, unrestricted gro...	C:\Program Files\Microsoft SQL Server\MS...
ISEDB_log	Log	Not Appli...	1	By 10 percent, unrestrict...	C:\Program Files\Microsoft SQL Server\MS...

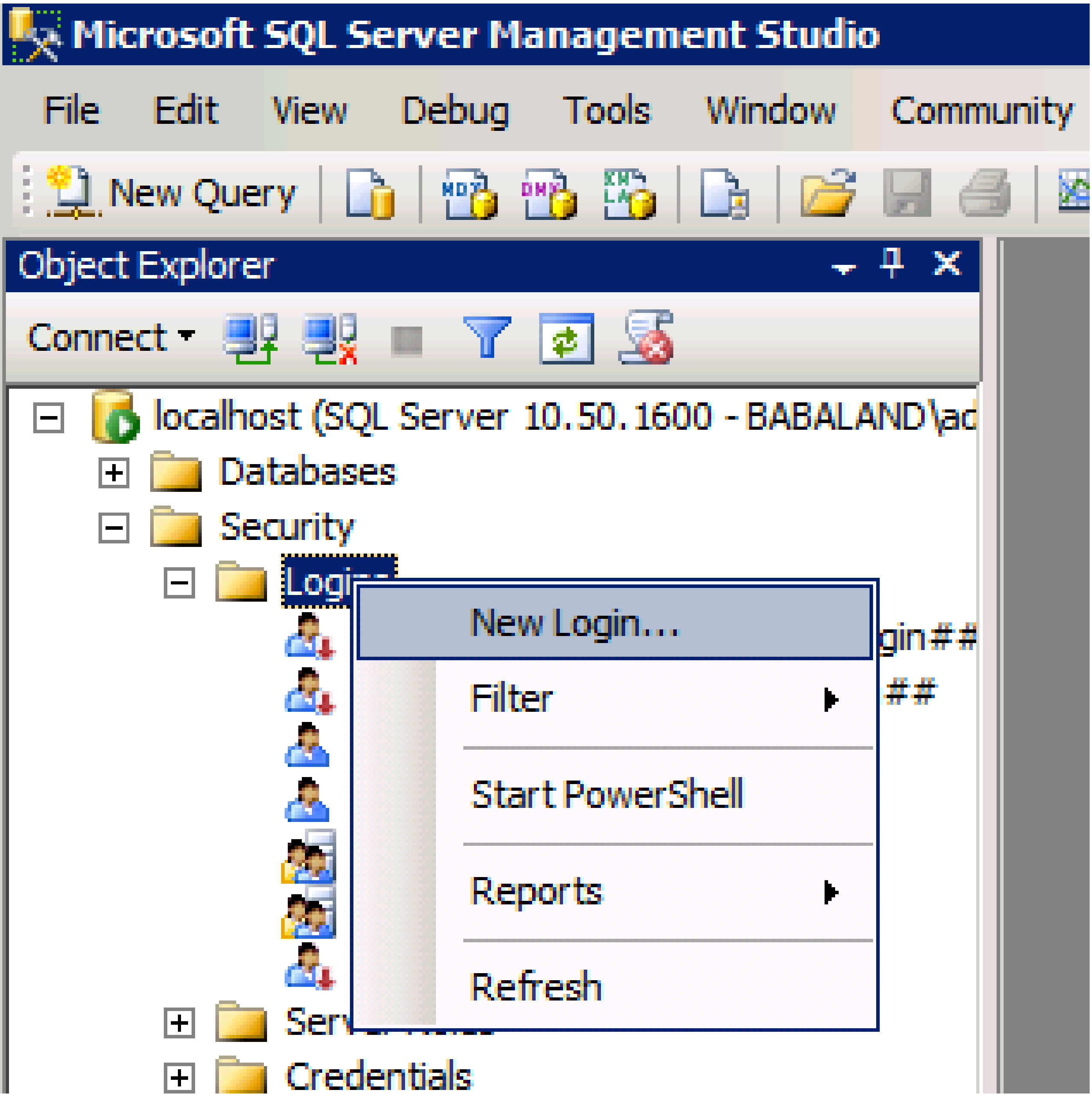
Server:
localhost

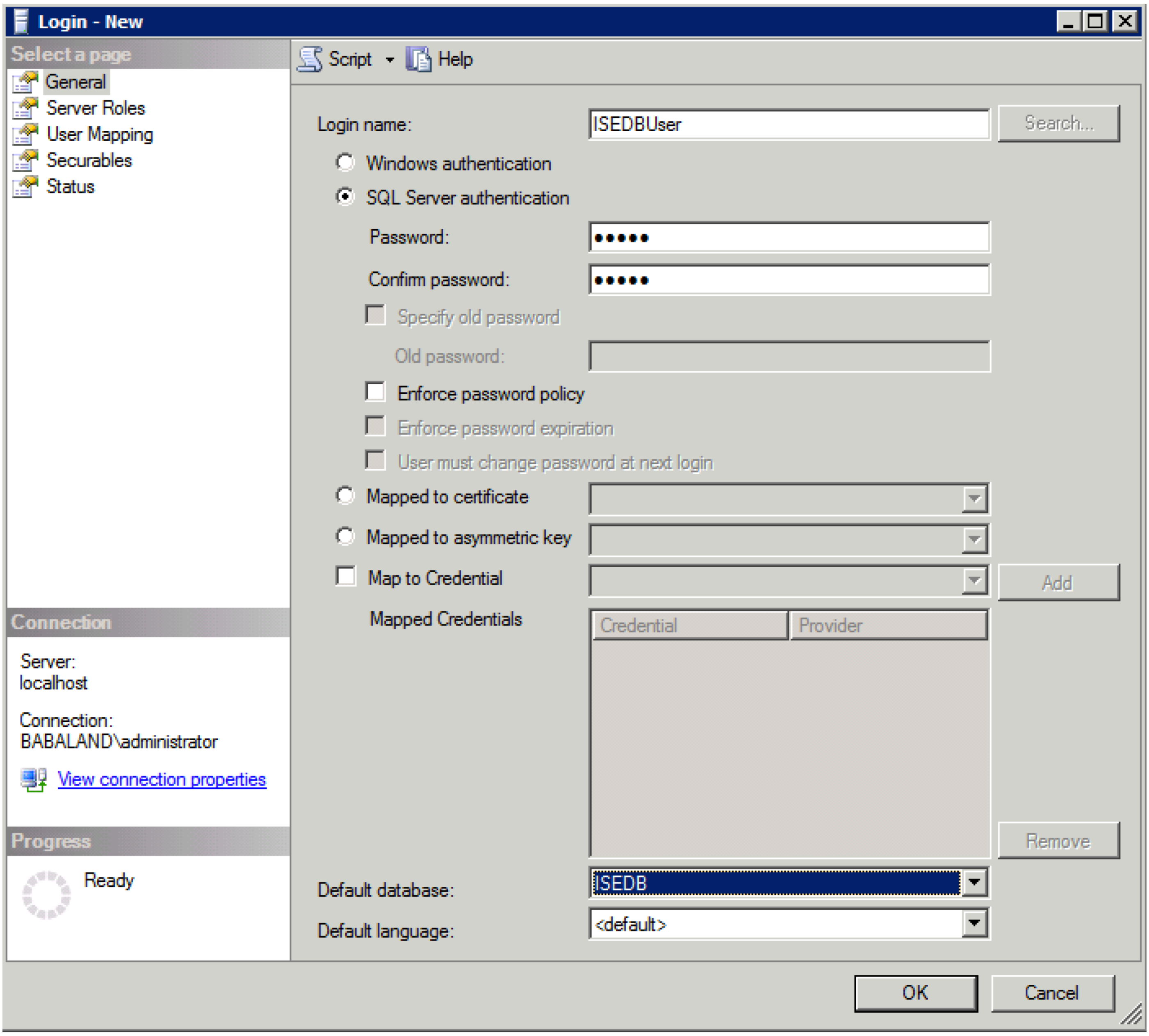
Connection:
BABALAND\administrator

View connection properties

Ready

3. Create a user and set permissions as shown in the images below:





Login - New

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ | Help

Login name: ISEDBUser [Search...]

○ Windows authentication

● SQL Server authentication

Password: •••••

Confirm password: •••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential [Add]

Mapped Credentials

Credential	Provider

[Remove]

Default database: ISEDB

Default language: <default>

Connection

Server:
localhost

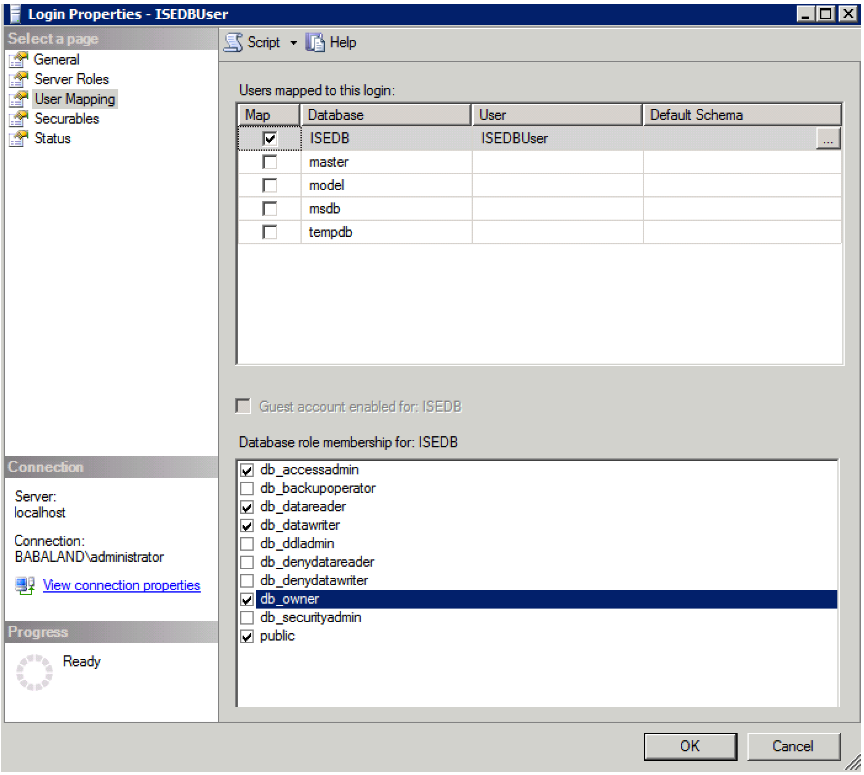
Connection:
BABALAND\administrator

View connection properties

Progress

Ready

[OK] [Cancel]



Login Properties - ISEDBUser

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ | Help

Users mapped to this login:

Map	Database	User	Default Schema
☑	ISEDB	ISEDBUser	...
□	master		
□	model		
□	msdb		
□	tempdb		

□ Guest account enabled for: ISEDB

Database role membership for: ISEDB

- ☑ db_accessadmin
- □ db_backupoperator
- ☑ db_datareader
- ☑ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

Connection

Server:
localhost

Connection:
BABALAND\administrator

View connection properties

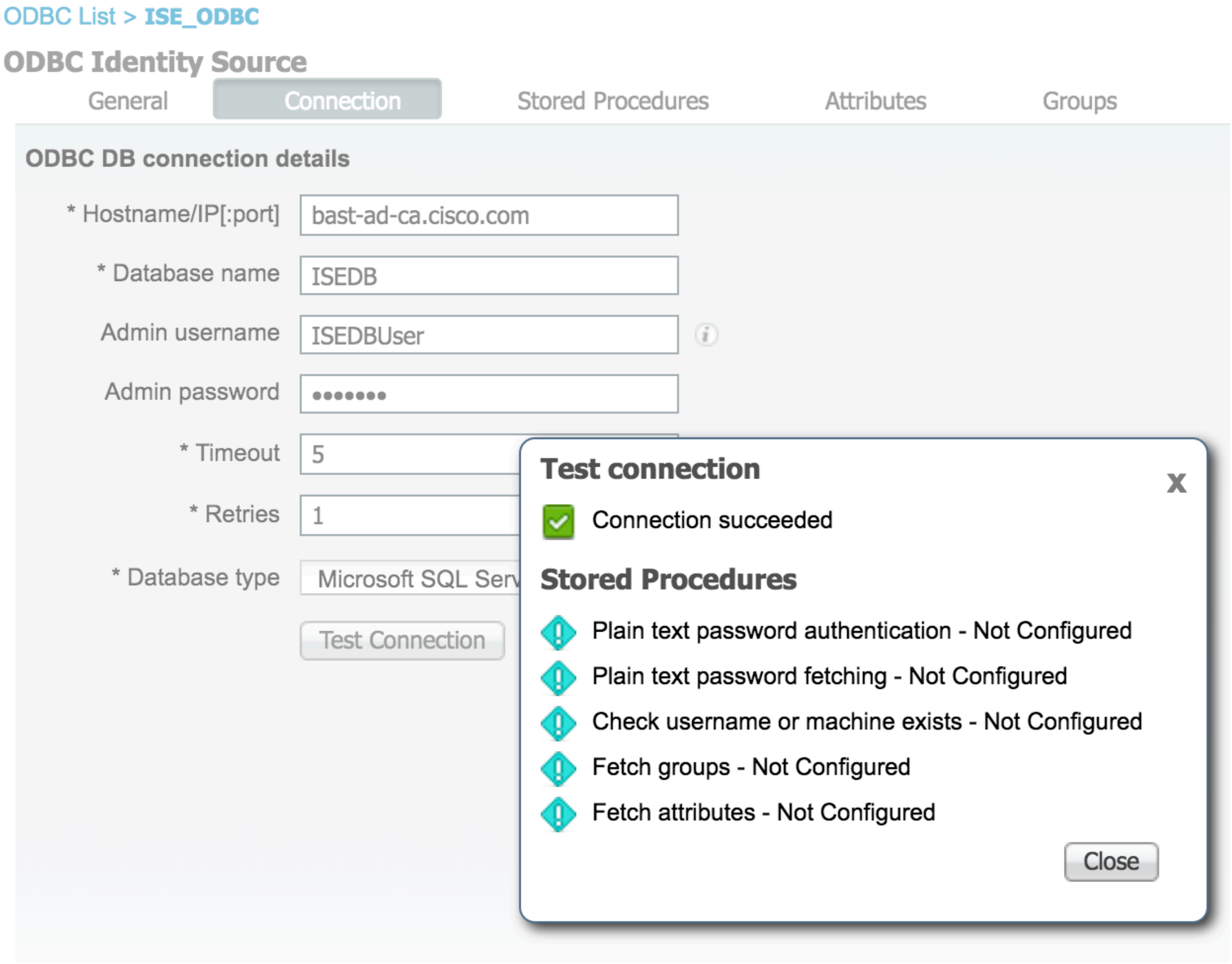
Progress

Ready

[OK] [Cancel]

Step 2. ISE Basic Configuration

Create an **ODBC Identity Source** at **Administration > External Identity Source > ODBC** and test connection:



ODBC Identity Source

ODBC DB connection details

* Hostname/IP[:port]: bast-ad-ca.cisco.com

* Database name: ISEDB

Admin username: ISEDBUser

Admin password: •••••••

* Timeout: 5

* Retries: 1

* Database type: Microsoft SQL Serv

Test connection

✓ Connection succeeded

Stored Procedures

- Plain text password authentication - Not Configured
- Plain text password fetching - Not Configured
- Check username or machine exists - Not Configured
- Fetch groups - Not Configured
- Fetch attributes - Not Configured

Step 3. Configure User Authentication

ISE authentication to ODBC uses stored procedures.The s **resultset** with this syntax:

Value	**Type**
Result	Integer
Group (for compatibility with ACS 4.2 only)	Integer or varchar(255)
Account Info	varchar(255)
Error String	varchar(255)

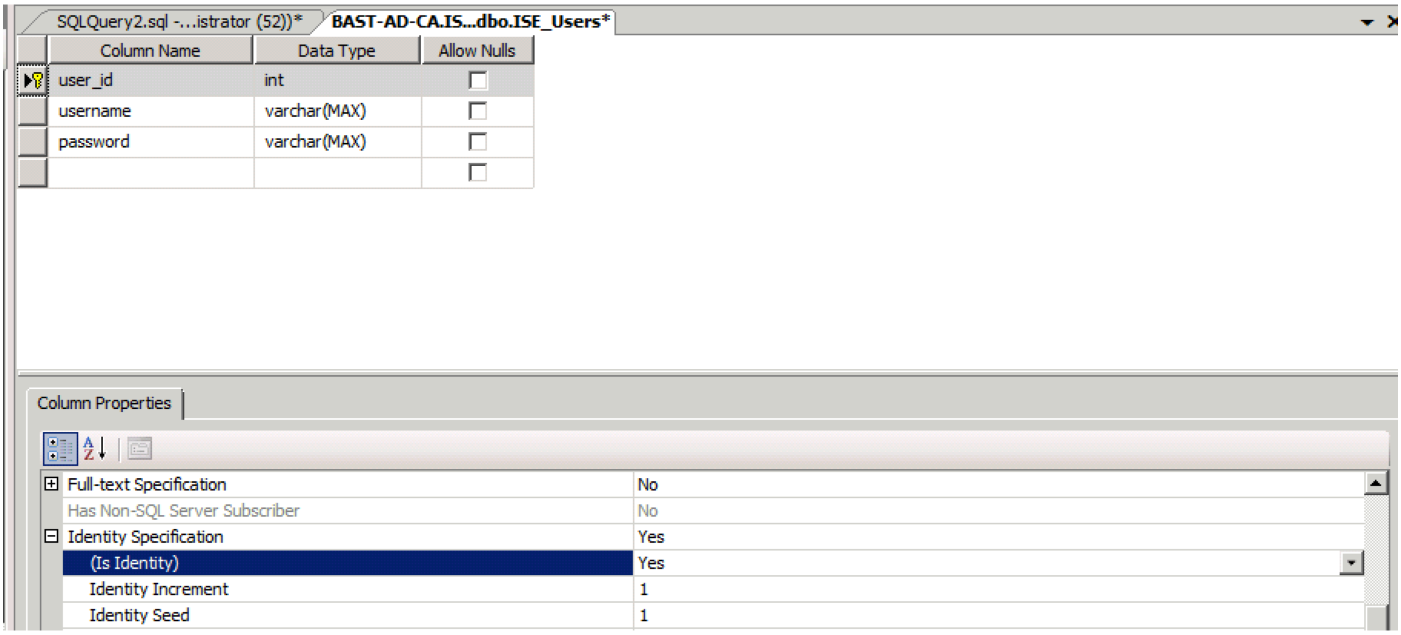
For other procedures, refer to Cisco Identity Services Engine 2.1 Administration Guide

> **Tip**: It is possible to return named parameters instead of resultset. It is just a different type of output, functionality is the same.

1. Navigate to options and uncheck **Prevent saving change that require table re-creation** check box (optional):

2. Create the table. Make sure you set the identity settings on the **primary key**. To set **user_id** as

primary key, right click the **column name:**


SQLQuery2.sql -...istrator (52))*
BAST-AD-CA.IS...dbo.ISE_Users*
Column Properties

Column Name	Data Type	Allow Nulls
user_id	int	□
username	varchar(MAX)	□
password	varchar(MAX)	□
		□

⊞ Full-text Specification	No
Has Non-SQL Server Subscriber	No
⊟ Identity Specification	Yes
(Is Identity)	Yes
Identity Increment	1
Identity Seed	1

Final SQL:

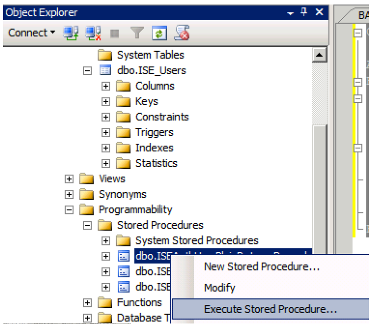
3. Run this query to insert one user:

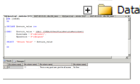
4. Create a procedure for plain text password authentication (used for PAP, EAP-GTC inner method, TACACS):

5. Create a procedure for plain text password fetching (used for CHAP, MSCHAPv1/v2, EAP-MD5, LEAP, EAP-MSCHAPv2 inner method, TACACS

6. Create a procedure for check username or machine exists

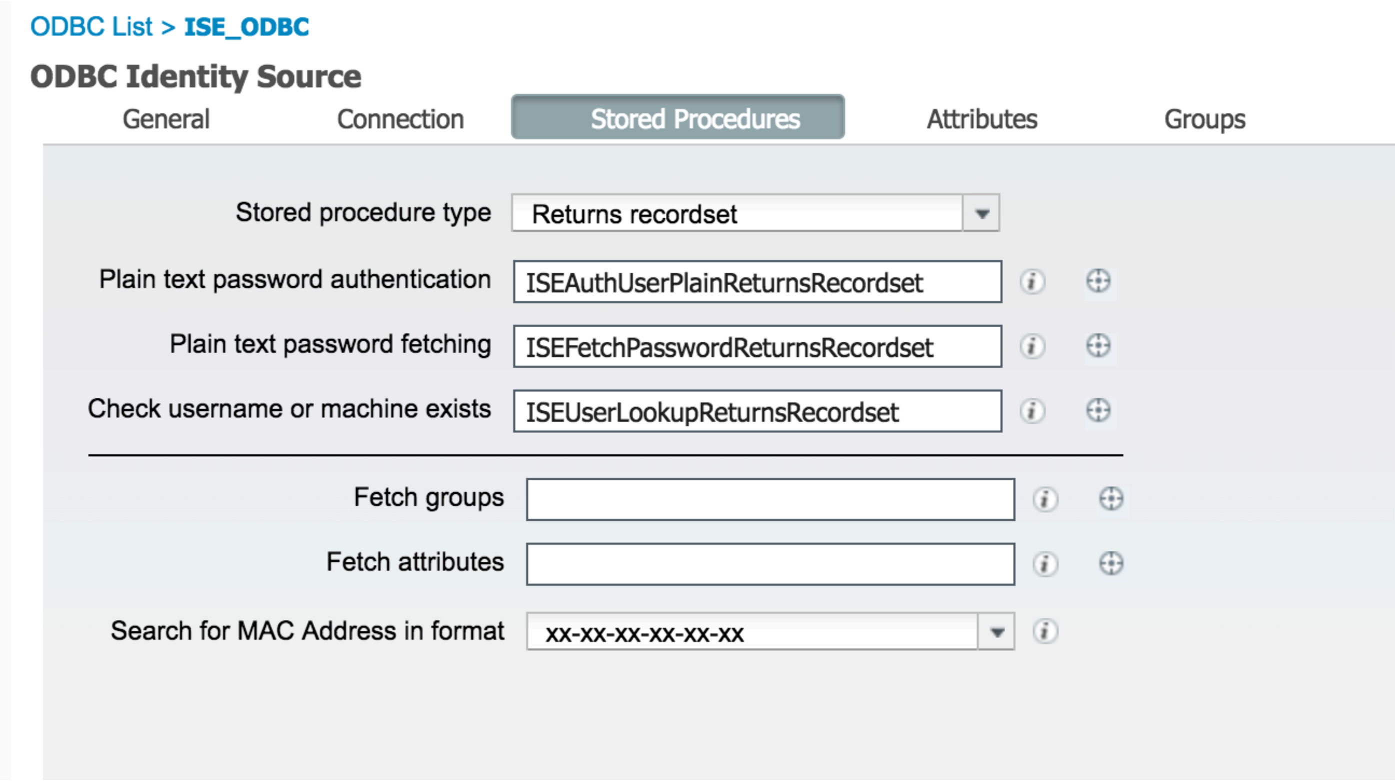
7. Test created procedures:





Test other procedures in the same way.

8. Configure procedures on ISE and save:



ODBC Identity Source

Stored procedure type: Returns recordset

Plain text password authentication: ISEAuthUserPlainReturnsRecordset

Plain text password fetching: ISEFetchPasswordReturnsRecordset

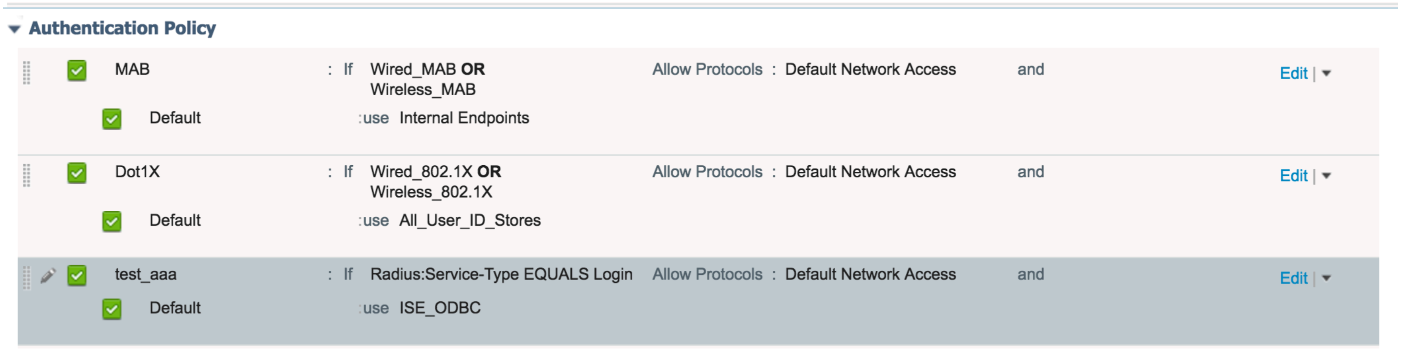
Check username or machine exists: ISEUserLookupReturnsRecordset

Fetch groups:

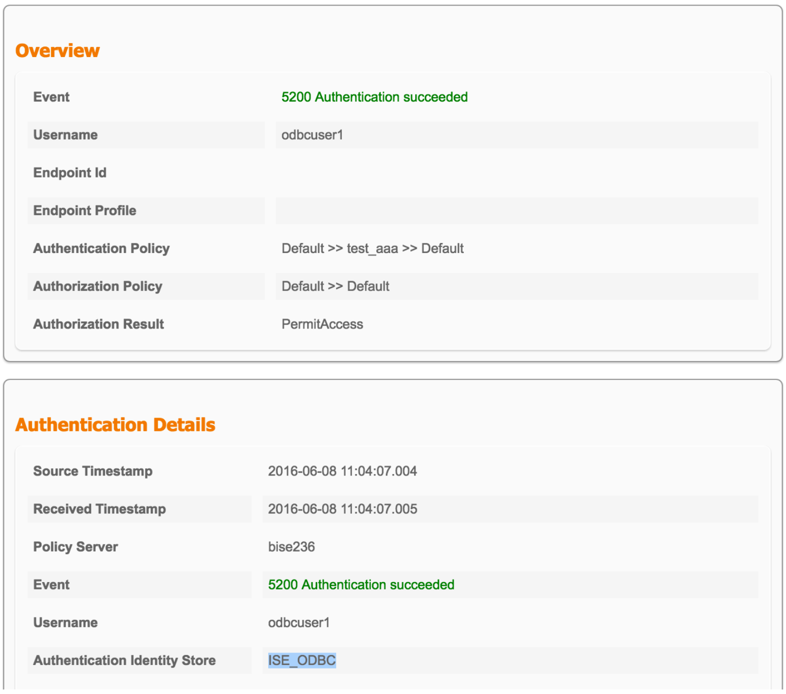
Fetch attributes:

Search for MAC Address in format: xx-xx-xx-xx-xx-xx

9. Create a simple authentication rule using ODBC and test it:



☑ MAB	: If	Wired_MAB **OR** Wireless_MAB	Allow Protocols : Default Network Access	and	Edit | ▾
☑ Default	:use	Internal Endpoints			
☑ Dot1X	: If	Wired_802.1X **OR** Wireless_802.1X	Allow Protocols : Default Network Access	and	Edit | ▾
☑ Default	:use	All_User_ID_Stores			
☑ test_aaa	: If	Radius:Service-Type EQUALS Login	Allow Protocols : Default Network Access	and	Edit | ▾
☑ Default	:use	ISE_ODBC			

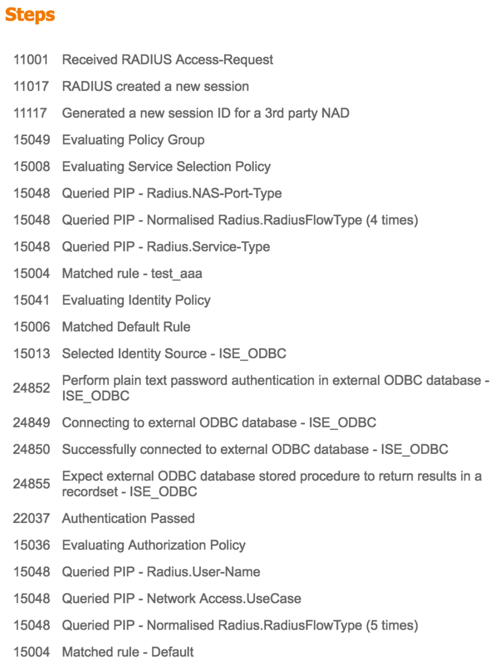


Overview

Event	5200 Authentication succeeded
Username	odbcuser1
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> test_aaa >> Default
Authorization Policy	Default >> Default
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2016-06-08 11:04:07.004
Received Timestamp	2016-06-08 11:04:07.005
Policy Server	bise236
Event	5200 Authentication succeeded
Username	odbcuser1
Authentication Identity Store	ISE_ODBC



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID for a 3rd party NAD
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Radius.NAS-Port-Type
15048	Queried PIP - Normalised Radius.RadiusFlowType (4 times)
15048	Queried PIP - Radius.Service-Type
15004	Matched rule - test_aaa
15041	Evaluating Identity Policy
15006	Matched Default Rule
15013	Selected Identity Source - ISE_ODBC
24852	Perform plain text password authentication in external ODBC database - ISE_ODBC
24849	Connecting to external ODBC database - ISE_ODBC
24850	Successfully connected to external ODBC database - ISE_ODBC
24855	Expect external ODBC database stored procedure to return results in a recordset - ISE_ODBC
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Radius.User-Name
15048	Queried PIP - Network Access.UseCase
15048	Queried PIP - Normalised Radius.RadiusFlowType (5 times)
15004	Matched rule - Default

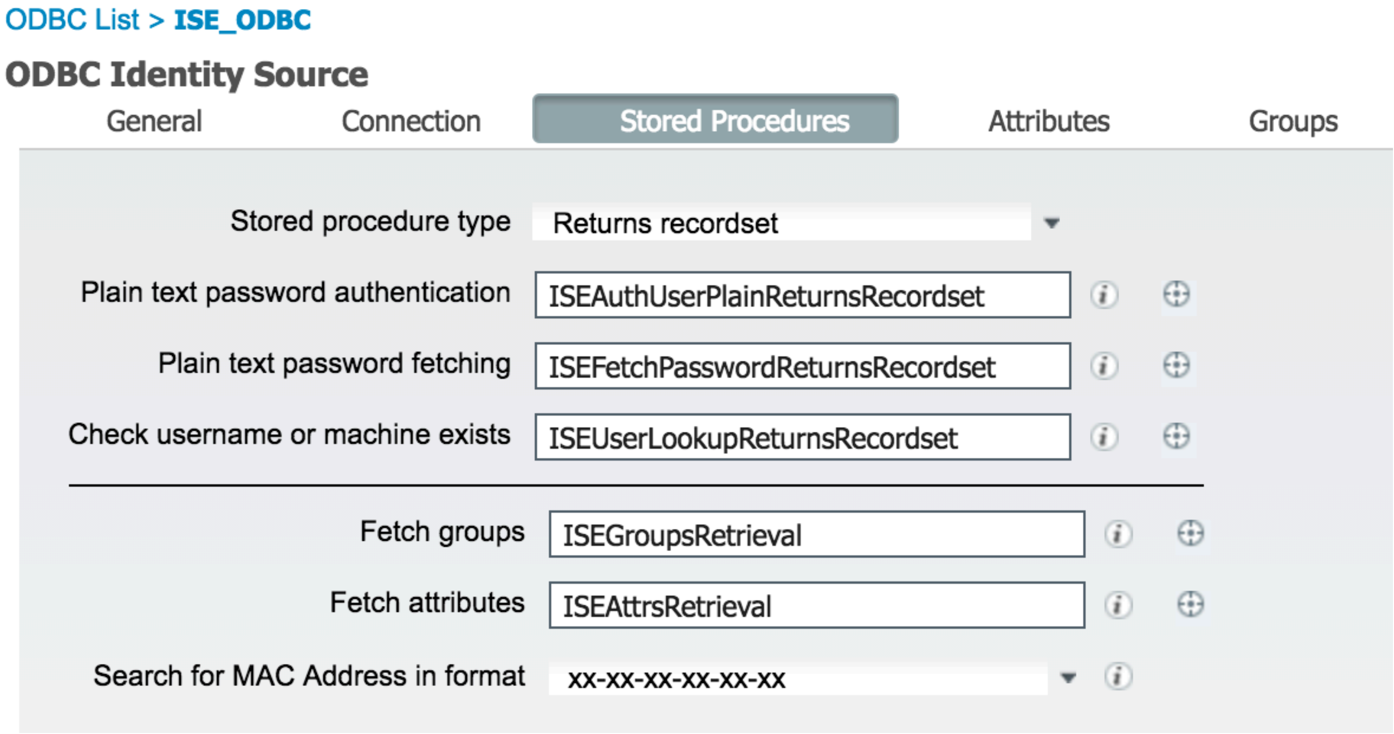
Step 4. Configure Group Retrieval

1. Create tables containing user groups and another used for many-to-many mapping:

2. Add groups and mappings, so that **ODBCUSER1** belongs to both groups:

3. Create group retrieval procedure:

4. Map it to **Fetch groups:**



ODBC List > **ISE_ODBC**

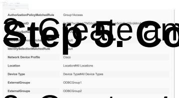
ODBC Identity Source

Stored procedure type	Returns recordset
Plain text password authentication	ISEAuthUserPlainReturnsRecordset
Plain text password fetching	ISEFetchPasswordReturnsRecordset
Check username or machine exists	ISEUserLookupReturnsRecordset
Fetch groups	ISEGroupsRetrieval
Fetch attributes	ISEAttrsRetrieval
Search for MAC Address in format	xx-xx-xx-xx-xx-xx

5. Fetch the groups and add them into the **ODBC Identity Source:**

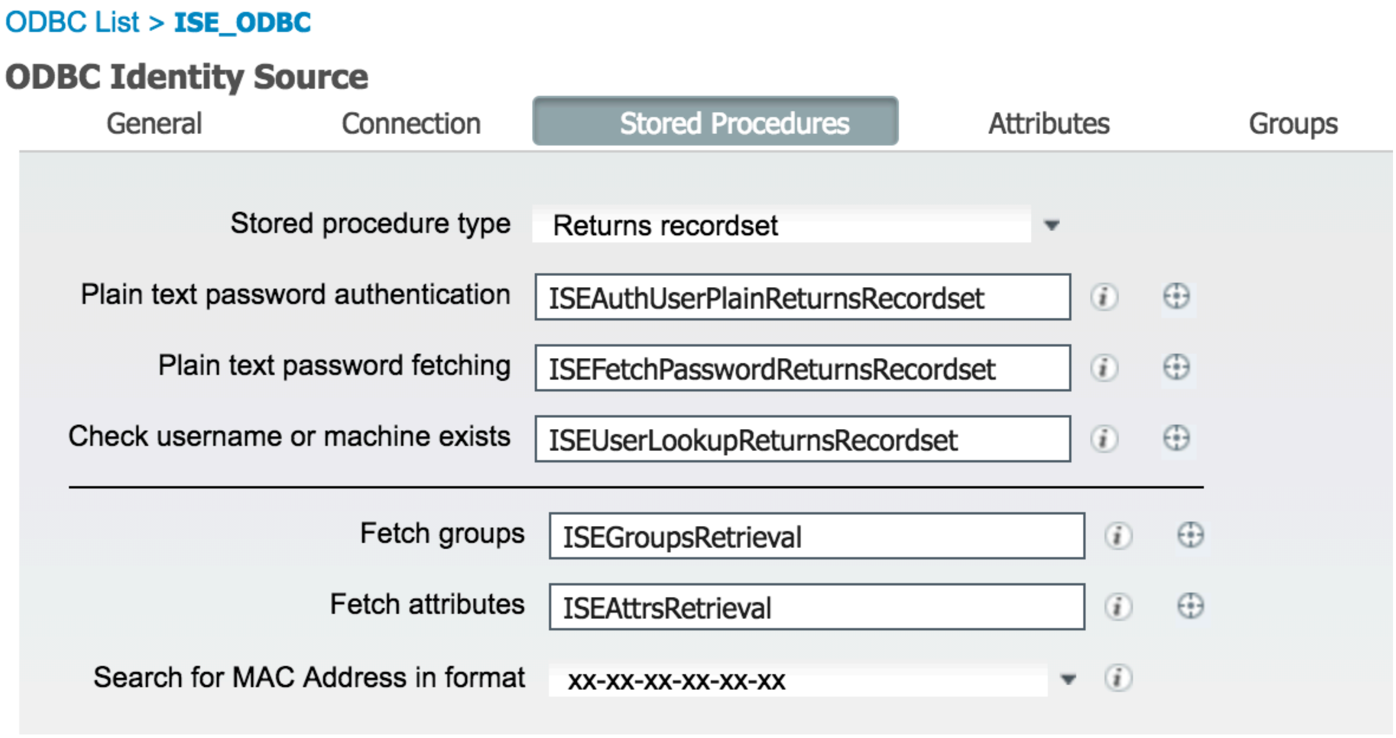
Step 5. Configure Attributes Retrieval

2. Create an [illegible] any group:



AuthorizationPolicyMatchedRule	Group1Access
IdentitySelectionMatchedRule	[illegible]
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
ExternalGroups	ODBCGroup1
ExternalGroups	ODBCGroup2

4. Map it to **Fetch attributes:**

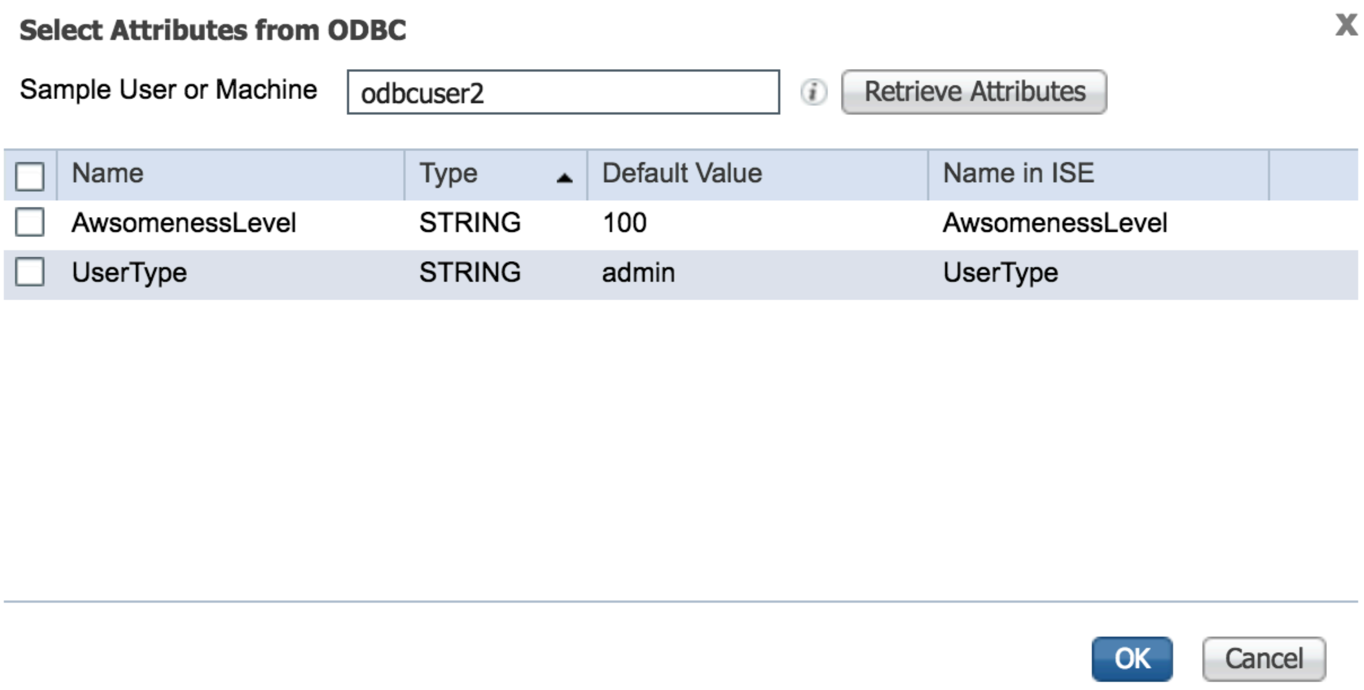


ODBC List > **ISE_ODBC**

ODBC Identity Source

Stored procedure type	Returns recordset
Plain text password authentication	ISEAuthUserPlainReturnsRecordset
Plain text password fetching	ISEFetchPasswordReturnsRecordset
Check username or machine exists	ISEUserLookupReturnsRecordset
Fetch groups	ISEGroupsRetrieval
Fetch attributes	ISEAttrsRetrieval
Search for MAC Address in format	xx-xx-xx-xx-xx-xx

5. Fetch the attributes:

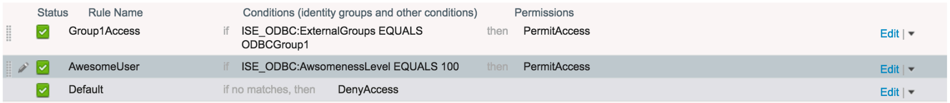


Select Attributes from ODBC

Sample User or Machine: odbcuser2

☐	Name	Type ▲	Default Value	Name in ISE
☐	AwsomenessLevel	STRING	100	AwsomenessLevel
☐	UserType	STRING	admin	UserType

6. Adjust ISE rules:

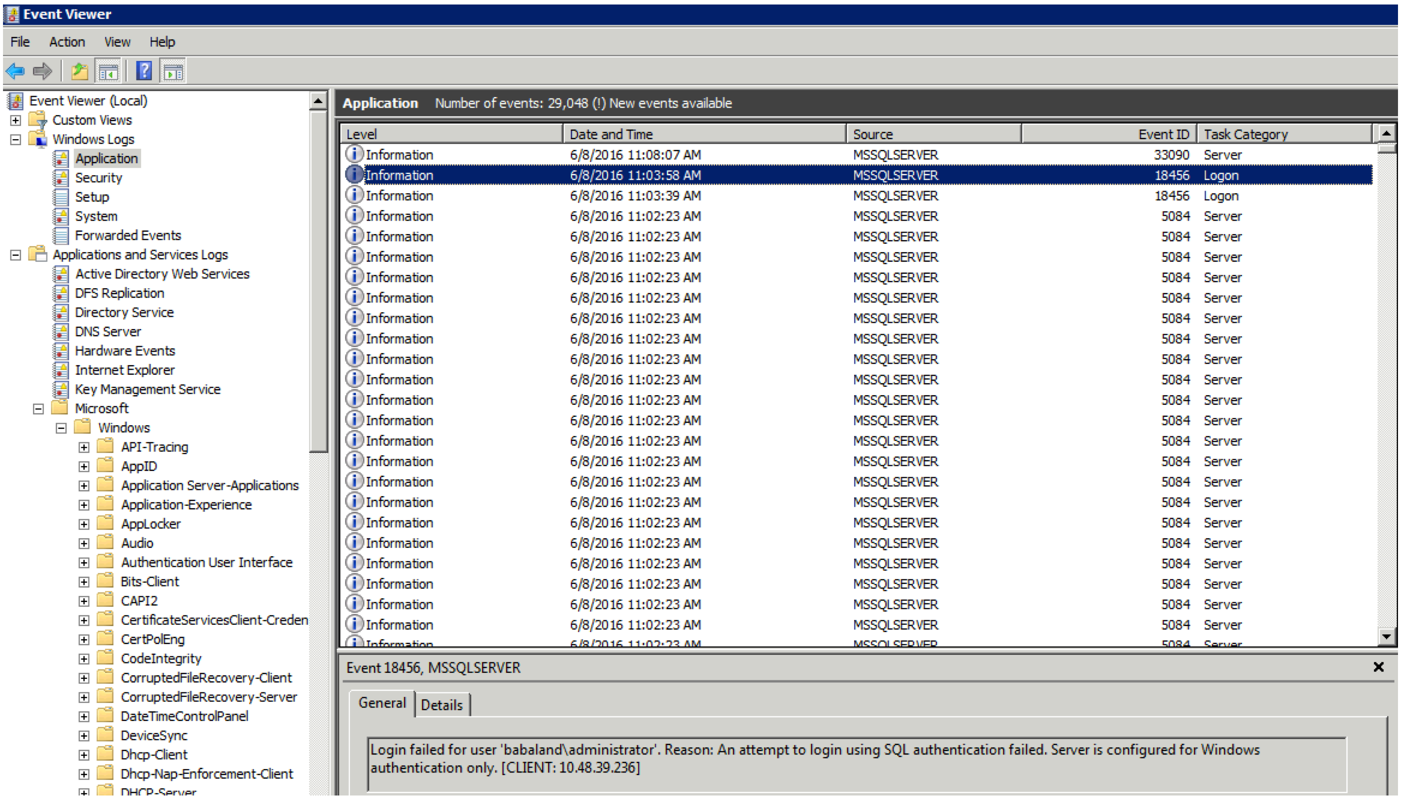


Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Group1Access	if	ISE_ODBC:ExternalGroups EQUALS ODBCGroup1	then	PermitAccess	Edit | ▾
✓	AwesomeUser	if	ISE_ODBC:AwsomenessLevel EQUALS 100	then	PermitAccess	Edit | ▾
✓	Default	if no matches, then	DenyAccess			Edit | ▾

Troubleshoot

If the connection is not successful, check windows event log. On ISE use command **show logging application prrt-management.log tail** while attempting to connect.

Example of bad authentication mode:



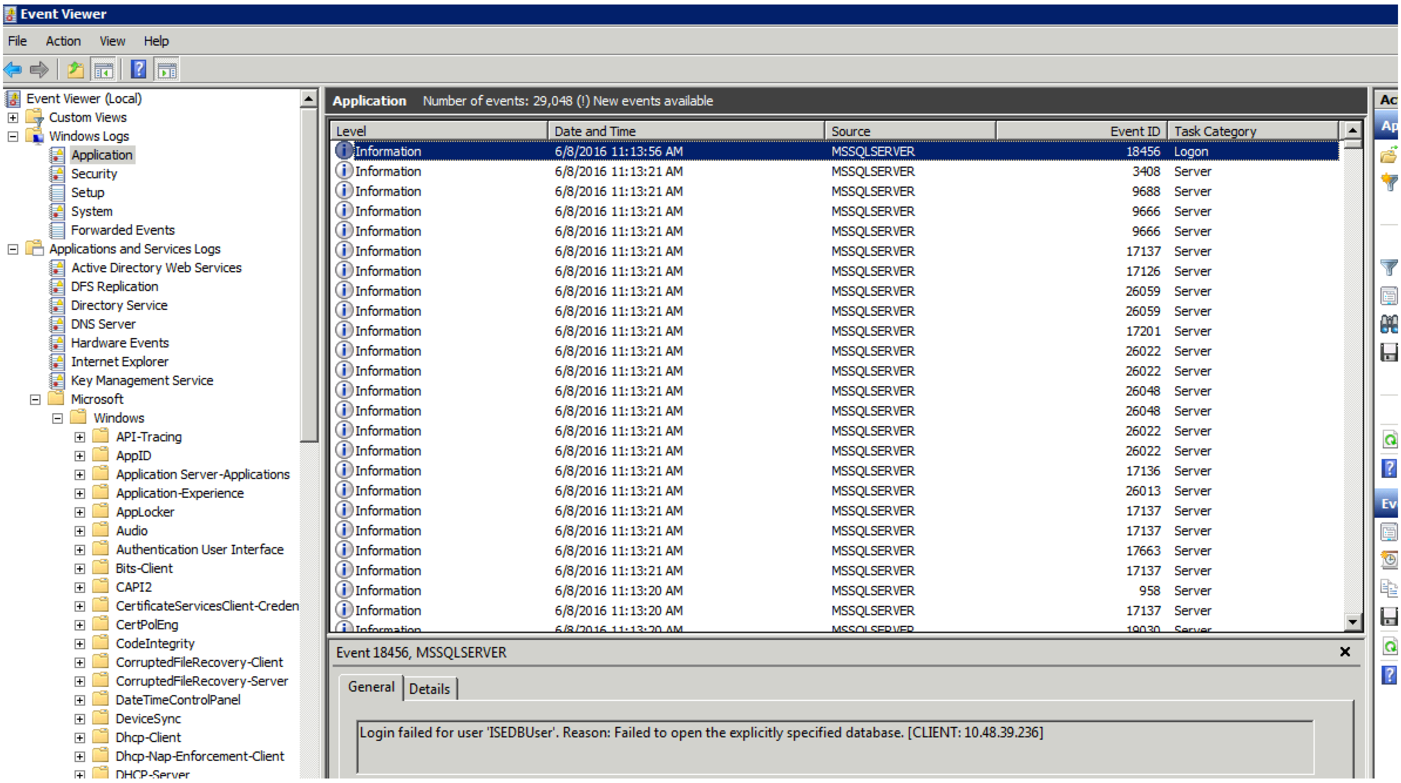
Application Number of events: 29,048 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	6/8/2016 11:08:07 AM	MSSQLSERVER	33090	Server
Information	6/8/2016 11:03:58 AM	MSSQLSERVER	18456	Logon
Information	6/8/2016 11:03:39 AM	MSSQLSERVER	18456	Logon
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server
Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server

Event 18456, MSSQLSERVER

Login failed for user 'babaland\administrator'. Reason: An attempt to login using SQL authentication failed. Server is configured for Windows authentication only. [CLIENT: 10.48.39.236]

Example of user missing permissions to open database:



Application Number of events: 29,048 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	6/8/2016 11:13:56 AM	MSSQLSERVER	18456	Logon
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	3408	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	9688	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	9666	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	9666	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17137	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17126	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26059	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26059	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17201	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26048	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26048	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17136	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26013	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17137	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17137	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17663	Server
Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17137	Server
Information	6/8/2016 11:13:20 AM	MSSQLSERVER	958	Server
Information	6/8/2016 11:13:20 AM	MSSQLSERVER	17137	Server
Information	6/8/2016 11:13:20 AM	MSSQLSERVER	19030	Server

Event 18456, MSSQLSERVER

Login failed for user 'ISEDBUser'. Reason: Failed to open the explicitly specified database. [CLIENT: 10.48.39.236]

In order to troubleshoot DB operations, enable logging components **odbc-id-store** to DEBUG level under **Administration > System > Logging > Debug Log Configuation**.

Logs are placed in **prrt-management.log** file.

Example for **odbuser2**: