Contents

Introduction Prerequisites Requirements Components Used Configure Step 1. MS SQL Basic Configuration Step 2. ISE Basic Configuration Step 3. Configure User Authentication Step 4. Configure Group Retrieval Step 5. Configure Attributes Retrieval Troubleshoot

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

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

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

K Microsoft SQL Serve	er Management Studio							
File Edit View De	bug Tools Window Com	munity Help						
🕴 🔔 New Query 🛛 🛅 🔤	🔁 🔁 🔂 📴 🔙 (3 🕰 🖕						
Object Explorer	+ † ×							
Connect 🕶 📑 📑	Connect 🕶 📑 📑 👕 📷 🔊							
 Iocalhost (SQL Ser Databases 	rver 10.50.1600 - BABALAND\a							
🗆 🧰 Sys	New Database							
	Attach							
	Restore Database							
Dat	Restore Files and Filegroups							
	Start PowerShell							
E E Replica	Reports	•						
 Manage SQL Set 	Refresh							

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

Classic of	Database name	c	ISEDB	_		
neycops	Owner:		default	,		
	Database files:					
	Logical Name	File Type	Flegroup	Intial	Autogrowth	Path
	ISEDB	Rows Data	PRIMARY	2	By 1 MB, unrestricted gro	C:\Program Files\Microsoft SQL Server\MS
	ISED8_log	Log	Not Appl	1	By 10 percent, unrestrict	C:\Program Files\Microsoft SQL Server\MS
section Mr:						
nocion ver: necion: RAMO'administrator						
nection wr: shoet rection: NLNIO administrator Wex connection properties						

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



🚪 Login - New			
Select a page	🛒 Script 👻 📑 Help		
General			
Server Roles	Login name:	ISEDBUser	Search
Securables	O Windows authentication		
🚰 Status	SQL Server authentication		
	Password:	•••••	
	Confirm password:	••••	
	Specify old password		
	Old password:		
	Enforce password policy	/	
	Enforce password expira	ation	
	🔲 User must change passv	word at next login	
	O Mapped to certificate		
	O Mapped to asymmetric key		
	Map to Credential	X	Add
Connection	Mapped Credentials	Credential Provider	
Server: localhost			
Connection: BABALAND\administrator			
View connection properties			
Progress			Remove
Ready	Default database:	ISEDB	
	Default language:	<default></default>	
		ОК	Cancel

Login Properties - ISEDBUser					
Select a page	🖁 Script 👻	📑 Help			
General		<u></u>			
Server Roles	Users mad	ped to this login:			
Securables	Мар	Database	User	Default Schema	
Status		ISEDB	ISEDBUser		
		master			
		model			
	L n	msdb			
		tempdb			
	Database	role membership for: ISEDB			
Connection	db_ac	cessadmin			
Server: localhost Connection: BABALAND\administrator Wew connection properties	db_ba ✓ db_da ✓ db_da db_dd db_dd db_de ✓ db_ow db_se	ckupoperator tareader tawriter ladmin nydatareader nydatawriter mer curityadmin			_
Progress	✓ public				
Ready					
					1
				OK	Cancel

Step 2. ISE Basic Configuration

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

ODBC List > ISE_ODBC										
ODBC Identity Source										
General	Connection	Stored Procedu	res	Attributes	Groups					
ODBC DB connection d	etails									
* Hostname/IP[:port]	bast-ad-ca.cisco.com	n]							
* Database name	ISEDB]							
Admin username	ISEDBUser		(i)							
Admin password	•••••]							
* Timeout	5	Test conn	ection			x				
* Retries	1	🔽 Connec	tion succeede	ed		~				
* Database type	Microsoft SQL Serv	Stored Pro	ocedures							
	Test Connection	Plain tex	kt password a	uthentication -	Not Configured					
		Plain te	kt password f	etching - Not C	configured					
		🕕 Check ເ	isername or r	nachine exists	 Not Configured 					
		🛛 🕕 Fetch gi	roups - Not C	onfigured						
		🌒 🐠 Fetch at	tributes - Not	Configured						
					Close					
						-				

Step 3. Configure User Authentication

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

Value	Туре
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 <u>Cisco Identity Services Engine 2.1 Administration Guide</u>

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.sqlistrator	(52))* BAST-AD	-CA.ISdbo.IS	_Users*		
	Column Name	Data Type	Allow Nulls			
▶8	user_id	int				
	username	varchar(MAX)				
	password	varchar(MAX)				
C	olumn Properties					
	∄ ≹↓ ⊂					
[∃ Full-text Specification				No	<u> </u>
	Has Non-SQL Server Sub	scriber			No	
[∃ Identity Specification				Yes	
	(Is Identity)				Yes	<u> </u>
	Identity Increment					
	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:

OD	BC List > ISE_ODB	С						
00	BC Identity So	urce						
	General	Connection	Stored Procedures	Attribute	es	Grou	lps	
	Store	d procedure type	Returns recordset	-				
	Plain text passwo	ord authentication	ISEAuthUserPlainReturnsRecord	dset	i	\oplus		
	Plain text p	assword fetching	ISEFetchPasswordReturnsRecor	rdset	i	\oplus		
	Check username o	or machine exists	ISEUserLookupReturnsRecordse	et	i	\oplus		
		Fetch groups			i	\oplus		
		Fetch attributes			(i)	\oplus		
	Search for MAC	Address in format	xx-xx-xx-xx-xx	٣	i			

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

¥	Aut	hent	tication Policy					
		~	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			
	ø		test_aaa	: If	Radius:Service-Type EQUALS Login	Allow Protocols : Default Network Access	and	Edit 🕶
			Default		use ISE_ODBC			

erview		
Event	5200 Authentication succeeded	
leerneme	odhousort	
semane	oubcuseri	
ndpoint Id		
ndpoint Profile		
uthentication Policy	Default >> test, asa >> Default	
unentication Folicy		
uthorization Policy	Default >> Default	
uthorization Result	PermitAccess	
thentication Details		
thentication Details	2016-06-08 11:04:07.004	
thentication Details ource Timestamp eceived Timestamp	2016-06-08 11:04:07.004 2016-06-08 11:04:07.005	
thentication Details ource Timestamp eceived Timestamp olicy Server	2016-06-08 11:04:07.004 2016-06-08 11:04:07.005 bise236	
thentication Details ource Timestamp eceived Timestamp olicy Server vent	2016-06-08 11:04:07.004 2016-06-08 11:04:07.005 bise236 5200 Authentication succeeded	
thentication Details ource Timestamp teceived Timestamp olicy Server vent	2016-06-08 11:04:07.004 2016-06-08 11:04:07.005 bise236 5200 Authentication succeeded odbcuser1	
thentication Details source Timestamp teceived Timestamp Policy Server svent	2016-06-08 11:04:07.004 2016-06-08 11:04:07.005 bise236 5200 Authentication succeeded odbcuser1	

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

OD	BC Identity	Source					
	General	Connection	Stored Procedures	Attribute	es		Groups
	Sto	ored procedure type	Returns recordset	*			
	Plain text pass	word authentication	ISEAuthUserPlainReturnsRec	cordset	i	Ð	
	Plain tex	t password fetching	ISEFetchPasswordReturnsRe	cordset	i	Ð	
	Check usernam	ne or machine exists	ISEUserLookupReturnsRecor	dset	i	Ð	
		Fetch groups	ISEGroupsRetrieval		i	\oplus	
		Fetch attributes	ISEAttrsRetrieval		(i)	\oplus	
	Search for MA	AC Address in format	xx-xx-xx-xx-xx	•	i		

- 5. Fetch the groups and add them into the ODBC Identity Source:
- Stepseconighteightighteretes Reprievating group:



4. Map it to Fetch attributes:

ODBC List > ISE_ODBC

ODBC Identity Source

General	Connection	Stored Procedures	Attributes	Groups
St	ored procedure type	Returns recordset	•	
Plain text pas	sword authentication	ISEAuthUserPlainReturnsRec	cordset	\oplus
Plain te	xt password fetching	ISEFetchPasswordReturnsRe	ecordset	\oplus
Check usernar	ne or machine exists	ISEUserLookupReturnsRecor	rdset	\oplus
	Fetch groups	ISEGroupsRetrieval	(i)	Ð
	Fetch attributes	ISEAttrsRetrieval	i	\oplus
Search for M	AC Address in format	xx-xx-xx-xx-xx	• (i)	

5. Fetch the attributes:

Select Attributes from ODBC					
Sample User or Machine	odbcuser2 Retrieve Attributes				
Name	Туре 🔺	Default Value	Name in ISE		
AwsomenessLevel	STRING	100	AwsomenessLevel		
UserType	STRING	admin	UserType		



6. Adjust ISE rules:

		Statu	s Rule Name	Conditions (identity groups and other conditions) Permissions	
		~	Group1Access	if ISE_ODBC:ExternalGroups EQUALS then PermitAccess ODBCGroup1	Edit 🕶
	ø	~	AwesomeUser	If ISE_ODBC:AwsomenessLevel EQUALS 100 then PermitAccess	Edit 🕶
		 	Default	if no matches, then DenyAccess	Edit 🕶
Tee		late .	Onlah. Report. Merrity Endpoint D	Expert N. Advetus. Manuter Nay Advetus.	
-		e ~ 0	3	Nadar 5 - Nadar Managara	

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:

🛃 Event Viewer						
File Action View Help						
🗢 🔿 🔀 🖬 🖬						
Event Viewer (Local)	Application Number of	fevents: 29,048 (!) New events available				
Custom Views	Lovel	Data and Time	Course	Event ID	Task Catagory	
Windows Logs	Level Disformation	Clore and time	Source	Event ID	Task Category	
Application	Toformation	6/8/2016 11:08:07 AM	MSSQLSERVER	19456	Server	
Security	Information	6/8/2016 11:03:36 AM	MSSQLSERVER MSSQL SERVER	10450	Logon	·
Eustern	Information	6/8/2016 11:03:35 AM	MSSQLSERVER	10430	Server	
Ecowarded Events	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
	Information	6/8/2016 11:02:22 AM	MSSQLSERVER	5004	Server	
Active Directory Web Services	Information	6/8/2016 11:02:25 AM	MSSQLSERVER	5084	Server	
DES Replication	Tafamatian	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
Directory Service	Information	6/8/2016 11:02:25 AM	MSSQLSERVER	5004	Server	
DNS Server	Tafamatian	6/8/2016 11:02:23 AM	MSSQLSERVER	5064	Server	
Hardware Events	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5004	Server	
🛃 Internet Explorer	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
🛃 Key Management Service	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5004	Server	
Microsoft	Information	6/8/2016 11:02:25 AM	MSSQLSERVER	5084	Server	
🖃 🚞 Windows	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
API-Tracing	Information	6/8/2016 11:02:25 AM	MSSQLSERVER	5004	Server	
AppID	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
Application Server-Applications	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
Application-Experience	Information	6/8/2016 11:02:23 AM	MSSQLSERVER MSSQLSERVER	5084	Server	
AppLocker	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5004	Server	
Auton Autonication Liner Interface	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
Bits-Client	Information	6/8/2016 11:02:22 AM	MSSQLSERVER	5004	Server	
	Information	6/8/2016 11:02:25 AM	MSSQLSERVER	5084	Server	
CertificateServicesClient-Creden	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	
🕀 🧰 CertPolEng	Information	6/8/2016 11:02:23 AM	MSSQLSERVER	5084	Server	-
🗉 🧮 CodeIntegrity				20.0	Service	
	Event 18450, MISSQLSER	(VEK				
	General Details					
DateTimeControlPanel	Details					1
DeviceSync		Habita Bada State and Bases A		1. J. C	MC 1	_
🕀 🧮 Dhcp-Client	Login failed for use	r papaiang\administrator', Keason: An attem	ipt to login using SQL authentication f	alled. Server is configured for	windows	
Dhcp-Nap-Enforcement-Client	authentication only	. [CELEINT: 10.40.59.250]				
T DHCP-Server						

Example of user missing permissions to open database:

🛃 Event Viewer					
File Action View Help					
🗢 🔿 🖄 💽 🚺					
🛃 Event Viewer (Local)	Application Number of	events: 29,048 (!) New events available			Ac
Custom Views	Lavel	Data and Time	Course	Event ID Task Catagory	
Windows Logs	Toformation	Gla (2016 11, 12, 56 AM	MCCOLCEDVED	19456 Loope	
Application		6/8/2016 11:13:35 AM	MSSQLSERVER MSSQLSERVER	2408 Server	1 🛛 🖾
E Security	Information	6/8/2016 11:13:21 AM	MSSOLSERVER	9688 Server	
System	Information	6/8/2016 11:13:21 AM	MSSOLSERVER	9666 Server	
Eorwarded Events	Information	6/8/2016 11:13:21 AM	MSSQLSERVER	9666 Server	
Applications and Services Logs	Information	6/8/2016 11:13:21 AM	MSSOLSERVER	17137 Server	
Active Directory Web Services	Information	6/8/2016 11:13:21 AM	MSSOLSERVER	17126 Server	
DFS Replication	(i) Information	6/8/2016 11:13:21 AM	MSSOLSERVER	26059 Server	
Directory Service	(i) Information	6/8/2016 11:13:21 AM	MSSOLSERVER	26059 Server	
DNS Server	(i) Information	6/8/2016 11:13:21 AM	MSSOLSERVER	17201 Server	
🛃 Hardware Events	(i) Information	6/8/2016 11:13:21 AM	MSSOLSERVER	26022 Server	
Internet Explorer	(i) Information	6/8/2016 11:13:21 AM	MSSOLSERVER	26022 Server	
Key Management Service	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26048 Server	
E Microsoft	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26048 Server	
API Tracing	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022 Server	
	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26022 Server	<u> </u>
Application Server-Applications	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17136 Server	2
Application-Experience	(i) Information	6/8/2016 11:13:21 AM	MSSQLSERVER	26013 Server	
🗄 🧮 AppLocker	 Information 	6/8/2016 11:13:21 AM	MSSQLSERVER	17137 Server	Ev
🕀 🧮 Audio	 Information 	6/8/2016 11:13:21 AM	MSSQLSERVER	17137 Server	
🕀 🧮 Authentication User Interface	 Information 	6/8/2016 11:13:21 AM	MSSQLSERVER	17663 Server	
🕀 🧮 Bits-Client	Information	6/8/2016 11:13:21 AM	MSSQLSERVER	17137 Server	
E CAPI2	Information	6/8/2016 11:13:20 AM	MSSQLSERVER	958 Server	
CertificateServicesClient-Creden	Information	6/8/2016 11:13:20 AM	MSSQLSERVER	17137 Server	
CertPolEng	Information	6/8/2016 11:13:20 AM	MSSOLSER/JED	19030 Server	_ "
CodeIntegrity	Event 18456, MSSQLSER	VER			× Q
Corrupted-leikecovery-Olent				- 2	
Control and contro and control and control and control and control and control and co					
Dhco-Client	Login failed for user	'ISEDBUser'. Reason: Failed to open the expli	citly specified database. [CLIENT: 10.48.]	39.236]	
🗊 🦳 DHCP-Server					

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**: