Oracle Databaseを使用したISE 2.3でのODBCの設定

内容

概要

このドキュメントでは、Open Database Connectivity(ODBC)を使用して、ISE認証用にOracle Database(ISE)を使用してIdentity Services Engine(ISE)を設定する方法について説明します。

Open Database Connectivity（ODBC）認証では、ISE がプレーン テキストのパスワードを取得できることが必要です。データベース内でパスワードを暗号化できますが、ストアド プロシージャで復号する必要があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engine 2.3
- データベースと ODBC の概念
- Oracle

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)2.3.0.298
- サントス7
- Oracle Database 12.2.0.1.0
- Oracle SQL Developer 4.1.5

設定

> **注**：このドキュメントで説明するSQLプロシージャを例として扱います。これは、Oracle DBの公式かつ推奨される設定方法ではありません。コミットするすべてのSQLクエリーの結果と影響を理解していることを確認します。

ステップ1: Oracle基本設定

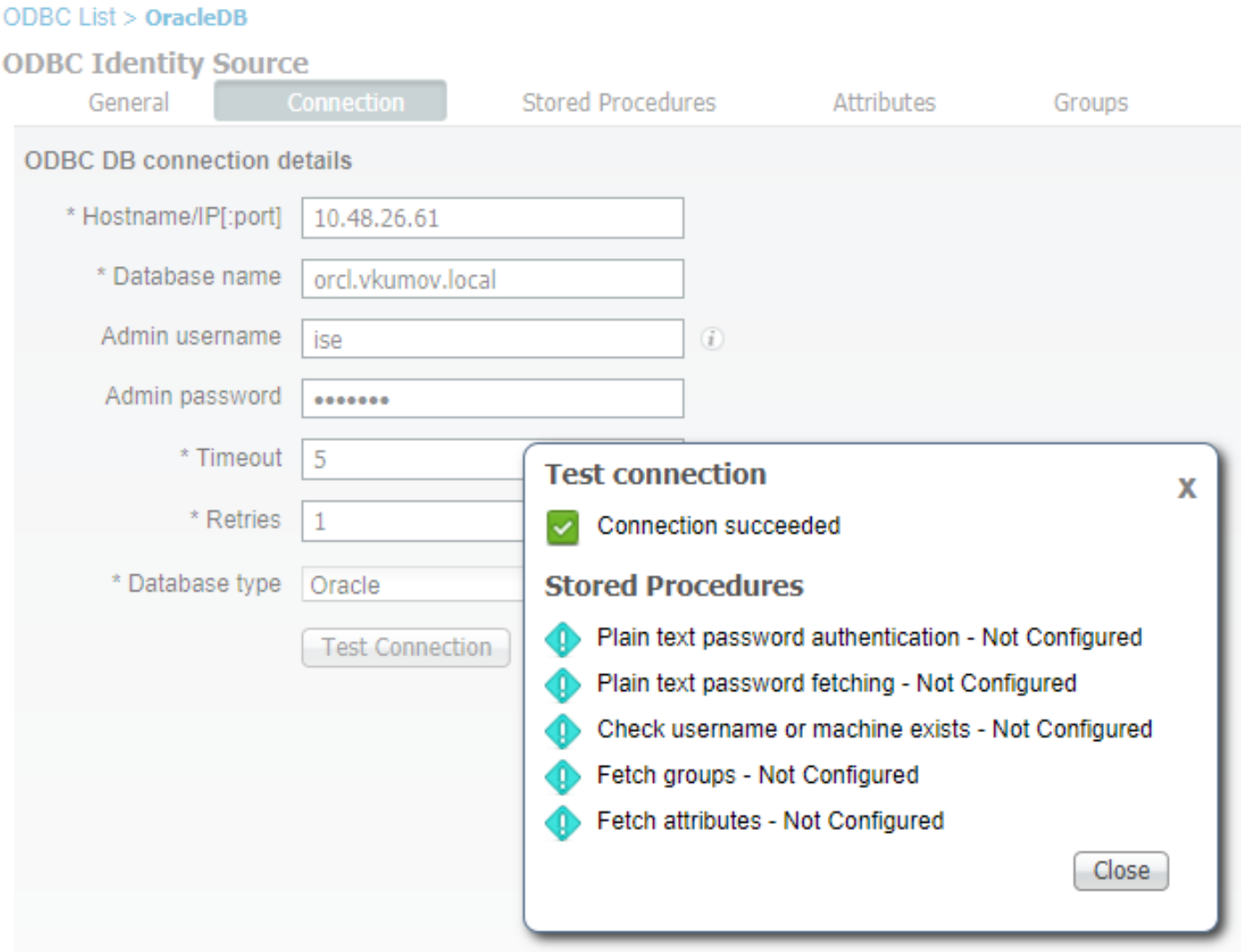
この例では、Oracleは次のパラメータで設定されています。

- データベース名：**ORCL**
- Service name :**orcl.vkumov.local**
- [Port]：**1521 (デフォルト)**
- ユーザ名iseを使用してISEのアカウントを作成**します**

先に進む前に、Oracleデータベースを構成します。

ステップ 2：ISE の基本設定

[Administration] > [External Identity Source] > [ODBC] で ODBC Identity Source を作成し、接続をテストします。



注： ISEはサービス名を使用してOracleに接続するため、[Database name]フィールドにはSID（またはDB名）ではなくOracleに存在するサービス名を入力する必要があります。 バグCSCvf06497のドット(.)は[データベース名]フィールドでは使用できません。このバグはISE 2.3で修正されています。

ステップ 3：ユーザ認証の設定

ODBC の ISE 認証では、ストアド プロシージャを使用します。手順の種類を選択できます。この例では、返り値としてrecordsetsを使用します。

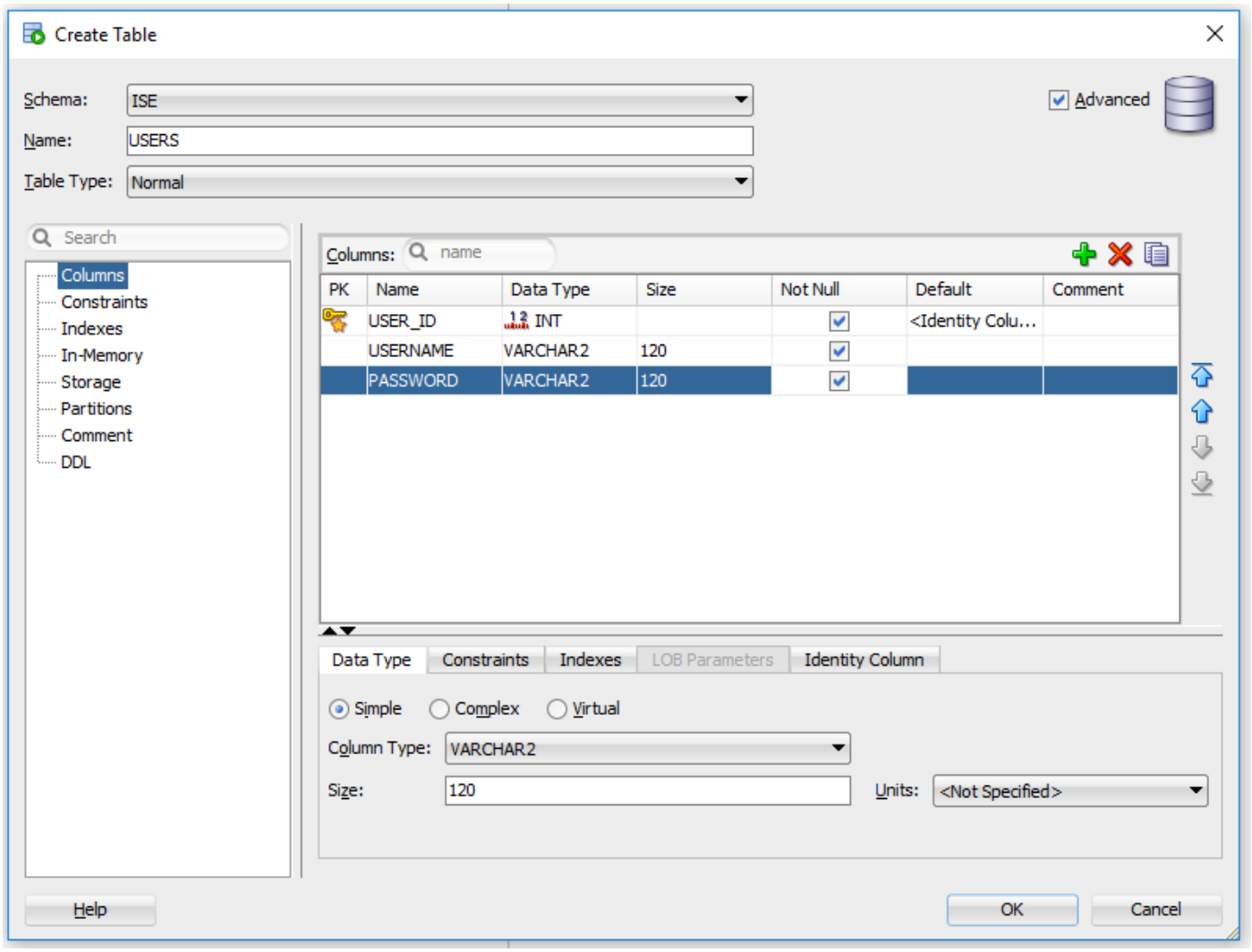
その他の手順については、『Cisco Identity Services Engine管理者ガイド、リリース2.3』を参照してください

ヒント：resultset の代わりに名前付きパラメータが返されることがあります。これは別のタイプの出力ですが、機能は同じです。

1.ユーザーの資格情報を使用してテーブルを作成します。**プライマリ キーに ID 設定が行われていることを確認します。**

```
--  DDL for Table USERS
--------------------------------------------------------

  CREATE TABLE "ISE"."USERS"
   ("USER_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
99999999999999999999999999999 INCREMENT BY 1 START WITH 1 CACHE 20 NOORDER  NOCYCLE  NOKEEP
NOSCALE ,
"USERNAME" VARCHAR2(120 BYTE),
"PASSWORD" VARCHAR2(120 BYTE)
   ) SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
 NOCOMPRESS LOGGING
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  DDL for Index USERS_PK
--------------------------------------------------------

  CREATE UNIQUE INDEX "ISE"."USERS_PK" ON "ISE"."USERS" ("USER_ID")
  PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  Constraints for Table USERS
--------------------------------------------------------

  ALTER TABLE "ISE"."USERS" MODIFY ("USER_ID" NOT NULL ENABLE);
  ALTER TABLE "ISE"."USERS" MODIFY ("USERNAME" NOT NULL ENABLE);
  ALTER TABLE "ISE"."USERS" MODIFY ("PASSWORD" NOT NULL ENABLE);
  ALTER TABLE "ISE"."USERS" ADD CONSTRAINT "USERS_PK" PRIMARY KEY ("USER_ID")
  USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS"  ENABLE;
```

またはSQL Developer GUIから：



2.ユーザの追加

```
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('alice', 'password1')
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('bob', 'password1')
INSERT INTO "ISE"."USERS" (USERNAME, PASSWORD) VALUES ('admin', 'password1')
```

3.プレーンテキストパスワード認証の手順を作成します（PAP、EAP-GTC内部方式、TACACSに使用）。

```
create or replace function ISEAUTH_R
(
  ise_username IN VARCHAR2,
  ise_userpassword IN VARCHAR2
) return sys_refcursor AS
BEGIN
  declare
    c integer;
    resultSet SYS_REFCURSOR;
  begin
    select count(*) into c from USERS where USERS.USERNAME = ise_username and USERS.PASSWORD =
ise_userpassword;
    if c > 0 then
      open resultSet for select 0 as code, 11, 'good user', 'no error' from dual;
    ELSE
      open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
    END IF;
```

```
    return resultSet;
  end;
END ISEAUTH_R;
```

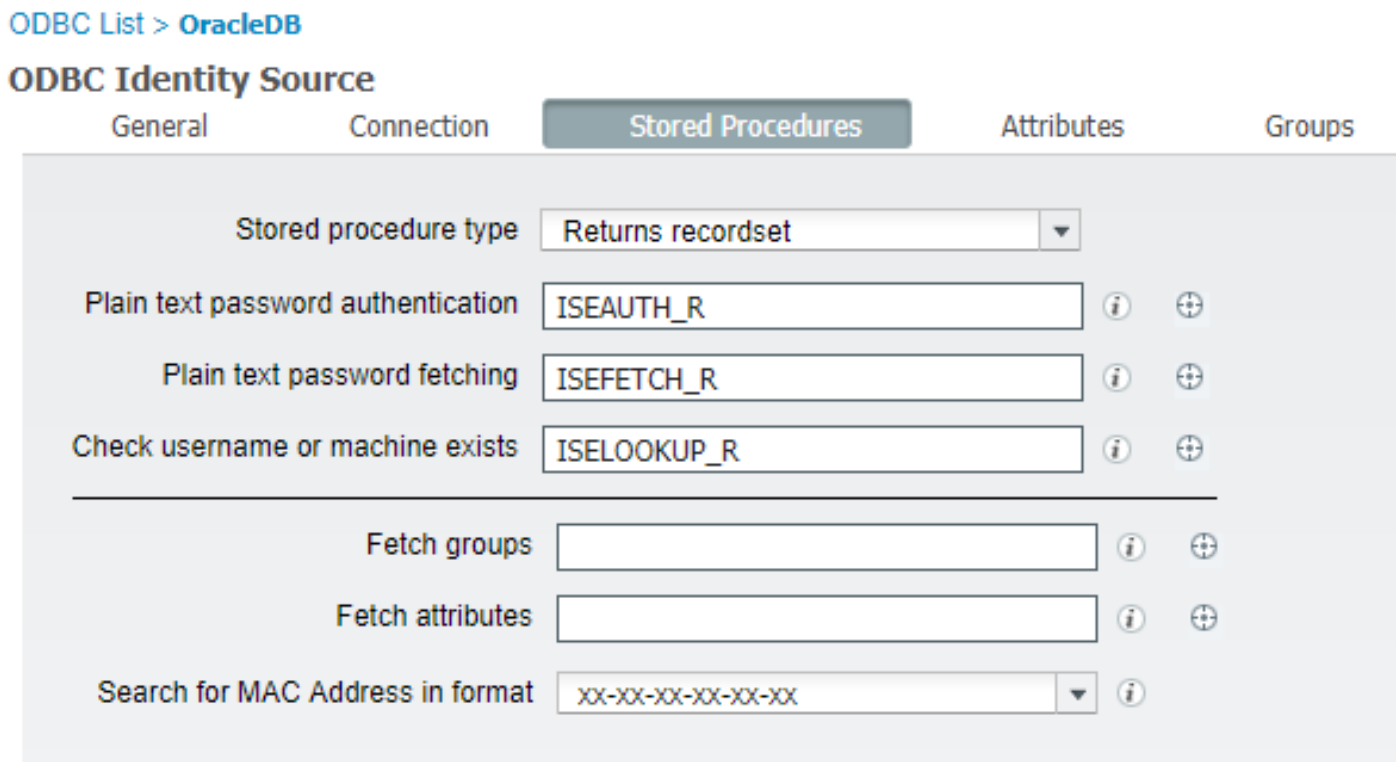
4.プレーンテキストのパスワード取得の手順を作成します（CHAP、MSCHAPv1/v2、EAP-MD5、LEAP、EAP-MSCHAPv2内部方式、TACACSに使用）。

```
create or replace function ISEFETCH_R
(
  ise_username IN VARCHAR2
) return sys_refcursor AS
BEGIN
  declare
    c integer;
    resultSet SYS_REFCURSOR;
  begin
    select count(*) into c from USERS where USERS.USERNAME = ise_username;
    if c > 0 then
      open resultSet for select 0, 11, 'good user', 'no error', password from USERS where
USERS.USERNAME = ise_username;
      DBMS_OUTPUT.PUT_LINE('found');
    ELSE
      open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
      DBMS_OUTPUT.PUT_LINE('not found');
    END IF;
    return resultSet;
  end;
END;
```

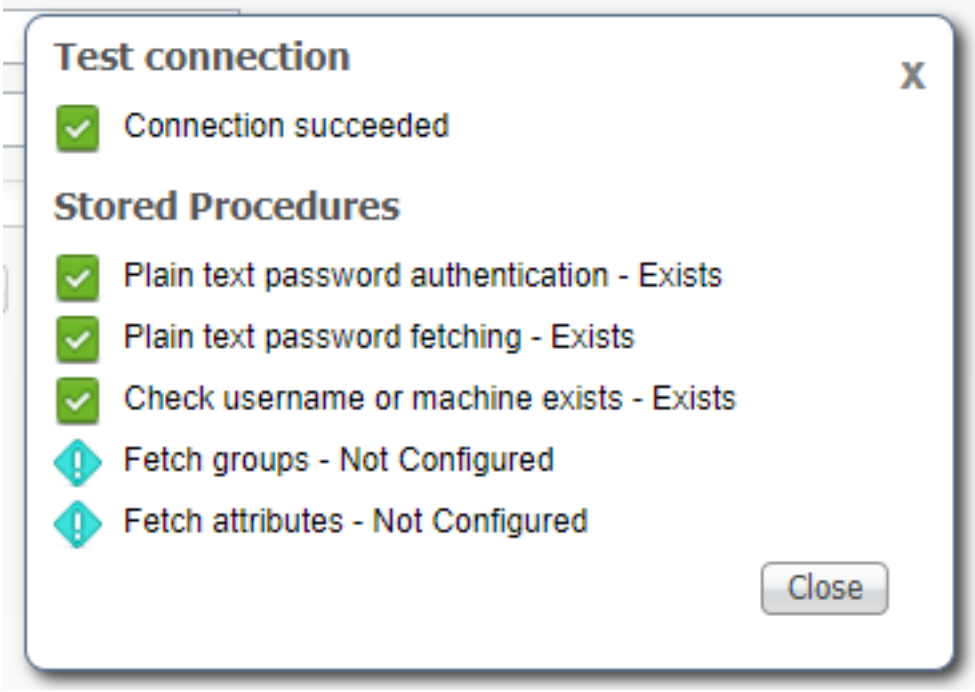
5.ユーザ名またはマシンの存在を確認する手順を作成します（MAB、PEAPの高速再接続、EAP-FASTおよびEAP-TTLSに使用）。

```
create or replace function ISELOOKUP_R
(
  ise_username IN VARCHAR2
) return sys_refcursor AS
BEGIN
  declare
    c integer;
    resultSet SYS_REFCURSOR;
  begin
    select count(*) into c from USERS where USERS.USERNAME = ise_username;
    if c > 0 then
      open resultSet for select 0, 11, 'good user', 'no error' from USERS where USERS.USERNAME =
ise_username;
    ELSE
      open resultSet for select 3, 0, 'odbc','ODBC Authen Error' from dual;
    END IF;
    return resultSet;
  end;
END;
```

6. ISEでの手順の設定と保存



7. [Connection]タブに戻り、[Test Connection]ボタンをクリックします



ステップ 4：グループ取得の設定

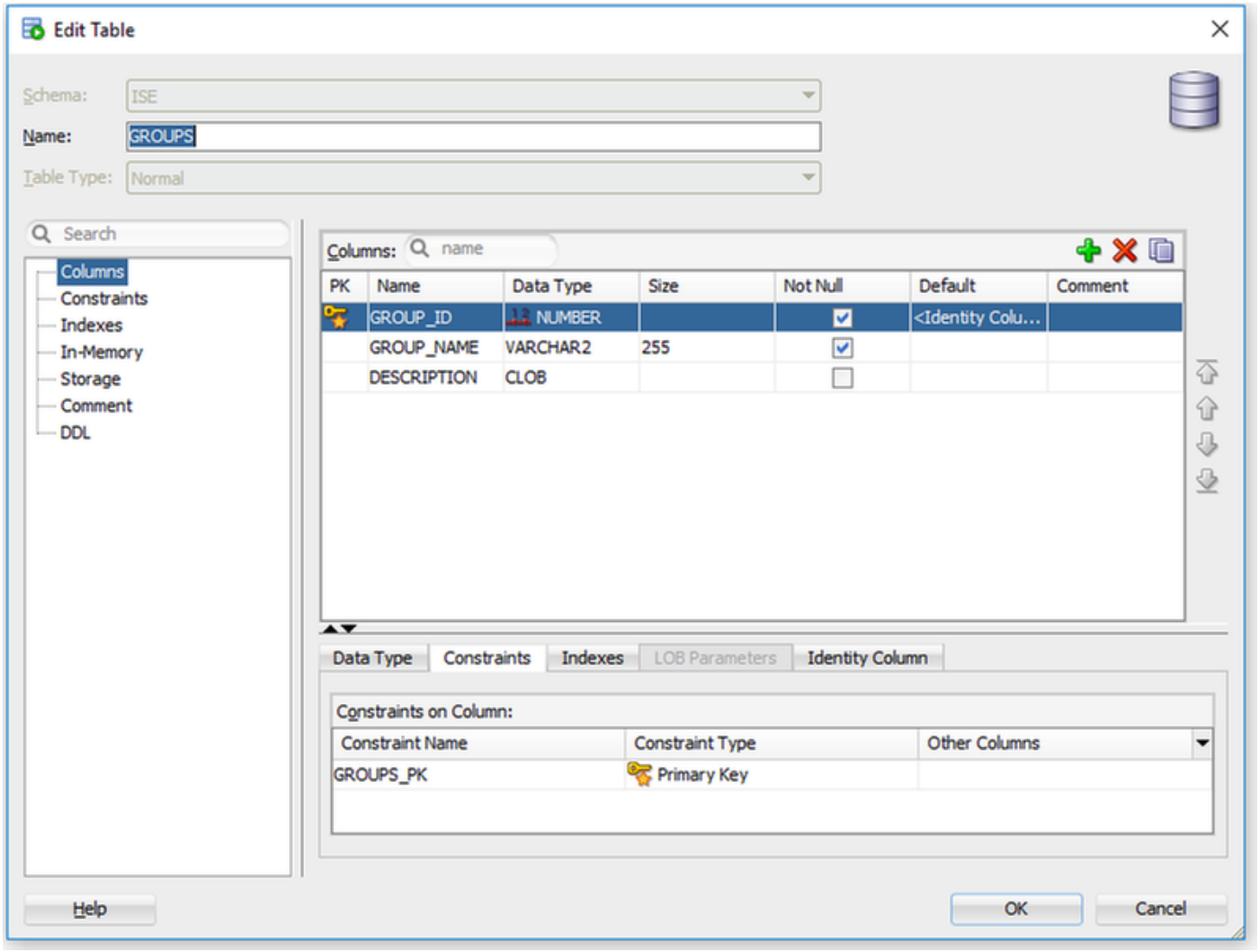
1.ユーザグループを含むテーブルと、多対多マッピングに使用するテーブルを作成します

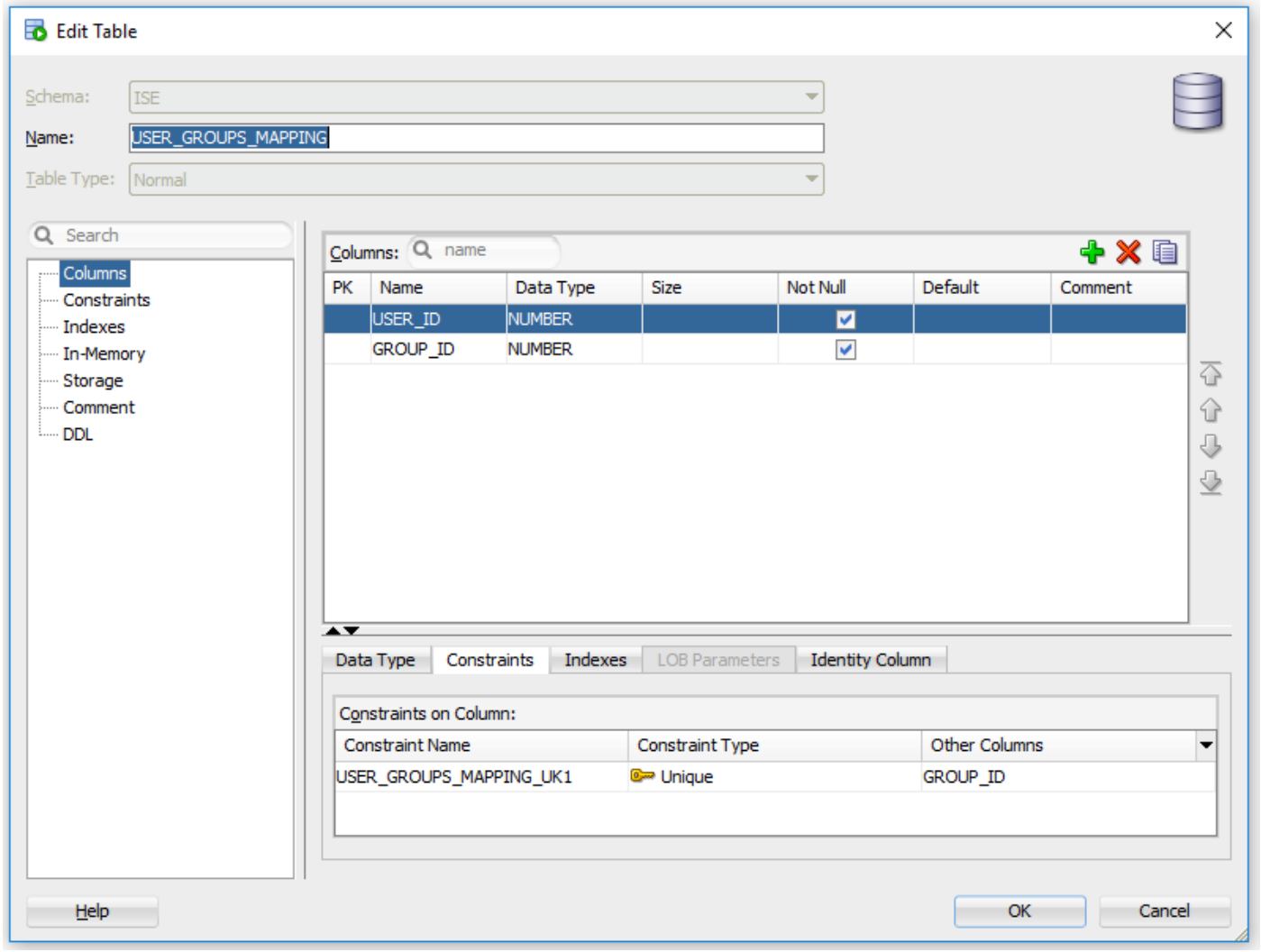
```
--------------------------------------------------------
--  DDL for Table GROUPS
--------------------------------------------------------

  CREATE TABLE "ISE"."GROUPS"
   ("GROUP_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
99999999999999999999999999999 INCREMENT BY 1 START WITH 1 CACHE 20 NOORDER  NOCYCLE  NOKEEP
```

```
NOSCALE ,
"GROUP_NAME" VARCHAR2(255 BYTE),
"DESCRIPTION" CLOB
   ) SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
 NOCOMPRESS LOGGING
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS"
 LOB ("DESCRIPTION") STORE AS SECUREFILE (
  TABLESPACE "USERS" ENABLE STORAGE IN ROW CHUNK 8192
  NOCACHE LOGGING  NOCOMPRESS  KEEP_DUPLICATES
  STORAGE(INITIAL 106496 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)) ;
--------------------------------------------------------
--  DDL for Table USER_GROUPS_MAPPING
--------------------------------------------------------

  CREATE TABLE "ISE"."USER_GROUPS_MAPPING"
   ("USER_ID" NUMBER(*,0),
"GROUP_ID" NUMBER(*,0)
   ) SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
 NOCOMPRESS LOGGING
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  DDL for Index GROUPS_PK
--------------------------------------------------------

  CREATE UNIQUE INDEX "ISE"."GROUPS_PK" ON "ISE"."GROUPS" ("GROUP_ID")
  PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  DDL for Index USER_GROUPS_MAPPING_UK1
--------------------------------------------------------

  CREATE UNIQUE INDEX "ISE"."USER_GROUPS_MAPPING_UK1" ON "ISE"."USER_GROUPS_MAPPING" ("USER_ID",
"GROUP_ID")
  PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  Constraints for Table GROUPS
--------------------------------------------------------

  ALTER TABLE "ISE"."GROUPS" MODIFY ("GROUP_ID" NOT NULL ENABLE);
  ALTER TABLE "ISE"."GROUPS" MODIFY ("GROUP_NAME" NOT NULL ENABLE);
  ALTER TABLE "ISE"."GROUPS" ADD CONSTRAINT "GROUPS_PK" PRIMARY KEY ("GROUP_ID")
  USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS"  ENABLE;
--------------------------------------------------------
```

```
--  Constraints for Table USER_GROUPS_MAPPING
------------------------------------------------------

  ALTER TABLE "ISE"."USER_GROUPS_MAPPING" MODIFY ("USER_ID" NOT NULL ENABLE);
  ALTER TABLE "ISE"."USER_GROUPS_MAPPING" MODIFY ("GROUP_ID" NOT NULL ENABLE);
  ALTER TABLE "ISE"."USER_GROUPS_MAPPING" ADD CONSTRAINT "USER_GROUPS_MAPPING_UK1" UNIQUE
("USER_ID", "GROUP_ID")
  USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS"  ENABLE;
```

GUI から：





2.グループとマッピングを追加し、aliceとbobがグループUsersに属し、adminがグループAdminsに属する

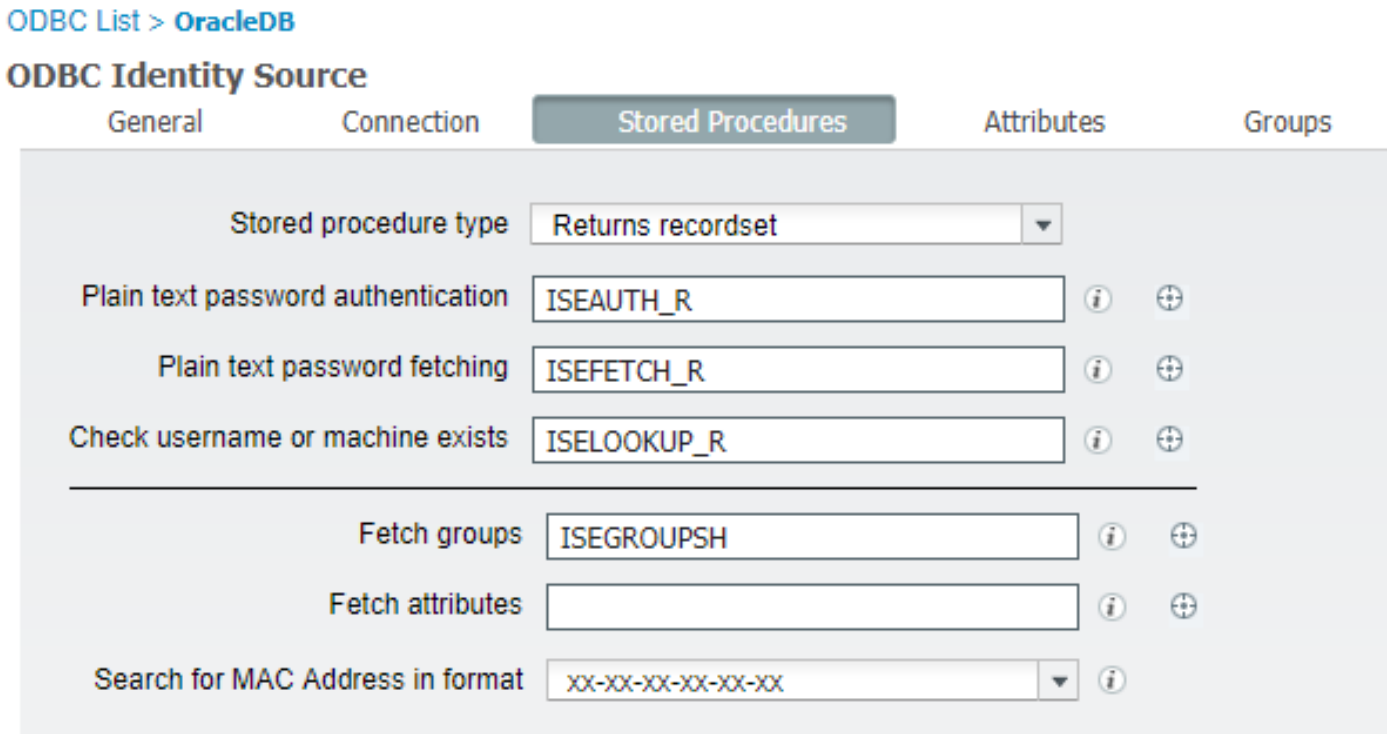
```
-- Adding groups
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Admins', 'Group for
administrators')
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Users', 'Corporate users')

-- Alice and Bob are users
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('1', '2')
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('2', '2')

-- Admin is in Admins group
INSERT INTO "ISE"."USER_GROUPS_MAPPING" (USER_ID, GROUP_ID) VALUES ('3', '1')
```

3.グループ取得手順を作成します。ユーザ名が「*」の場合、すべてのグループが返されます

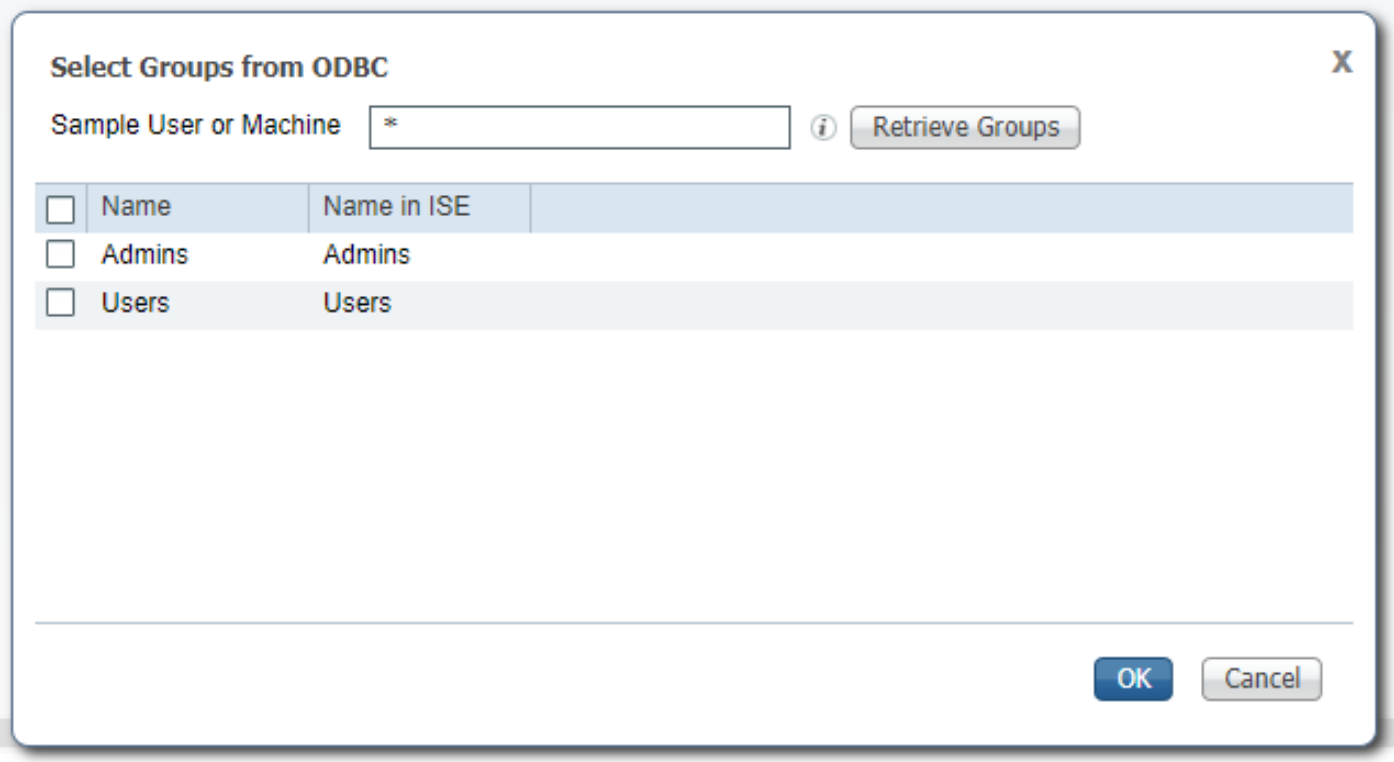
```
create or replace function ISEGROUPSH
(
  ise_username IN VARCHAR2,
  ise_result OUT int
) return sys_refcursor as
BEGIN
  declare
    c integer;
    userid integer;
```

```
    resultSet SYS_REFCURSOR;
  begin
    IF ise_username = '*' then
      ise_result := 0;
      open resultSet for select GROUP_NAME from GROUPS;
    ELSE
      select count(*) into c from USERS where USERS.USERNAME = ise_username;
      select USER_ID into userid from USERS where USERS.USERNAME = ise_username;
      IF c > 0 then
          ise_result := 0;
          open resultSet for select GROUP_NAME from GROUPS where GROUP_ID IN ( SELECT m.GROUP_ID
from USER_GROUPS_MAPPING m where m.USER_ID = userid );
      ELSE
          ise_result := 3;
          open resultSet for select 0 from dual where 1=2;
      END IF;
    END IF;
    return resultSet;
  end;
END ;
```

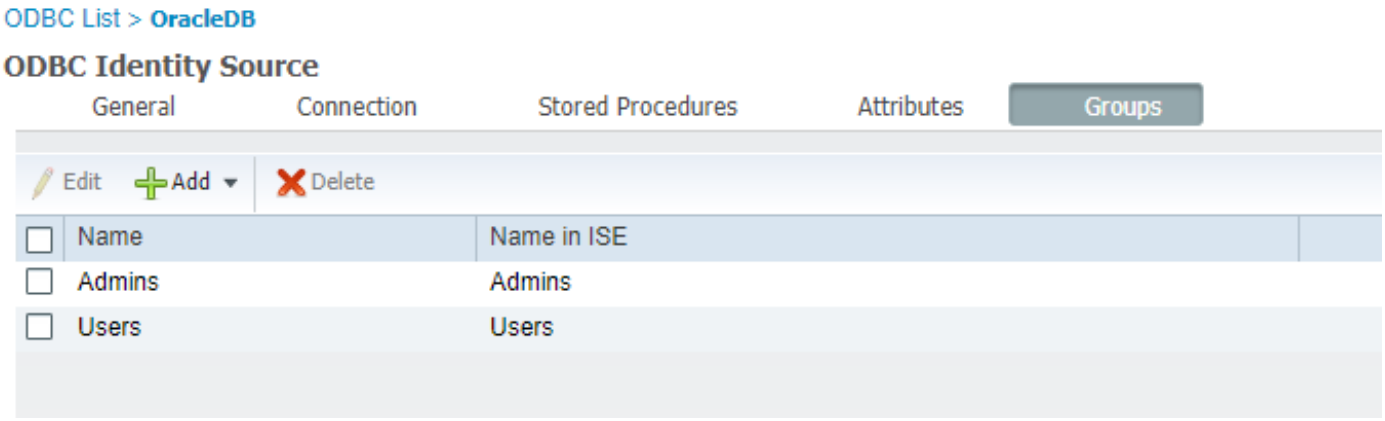
4.フェッチグループにマップします。



5.グループを取得し、ODBC Identity Sourceに追加します



必要なグループを選択して[OK]をクリックすると、[グループ]タブに表示されます



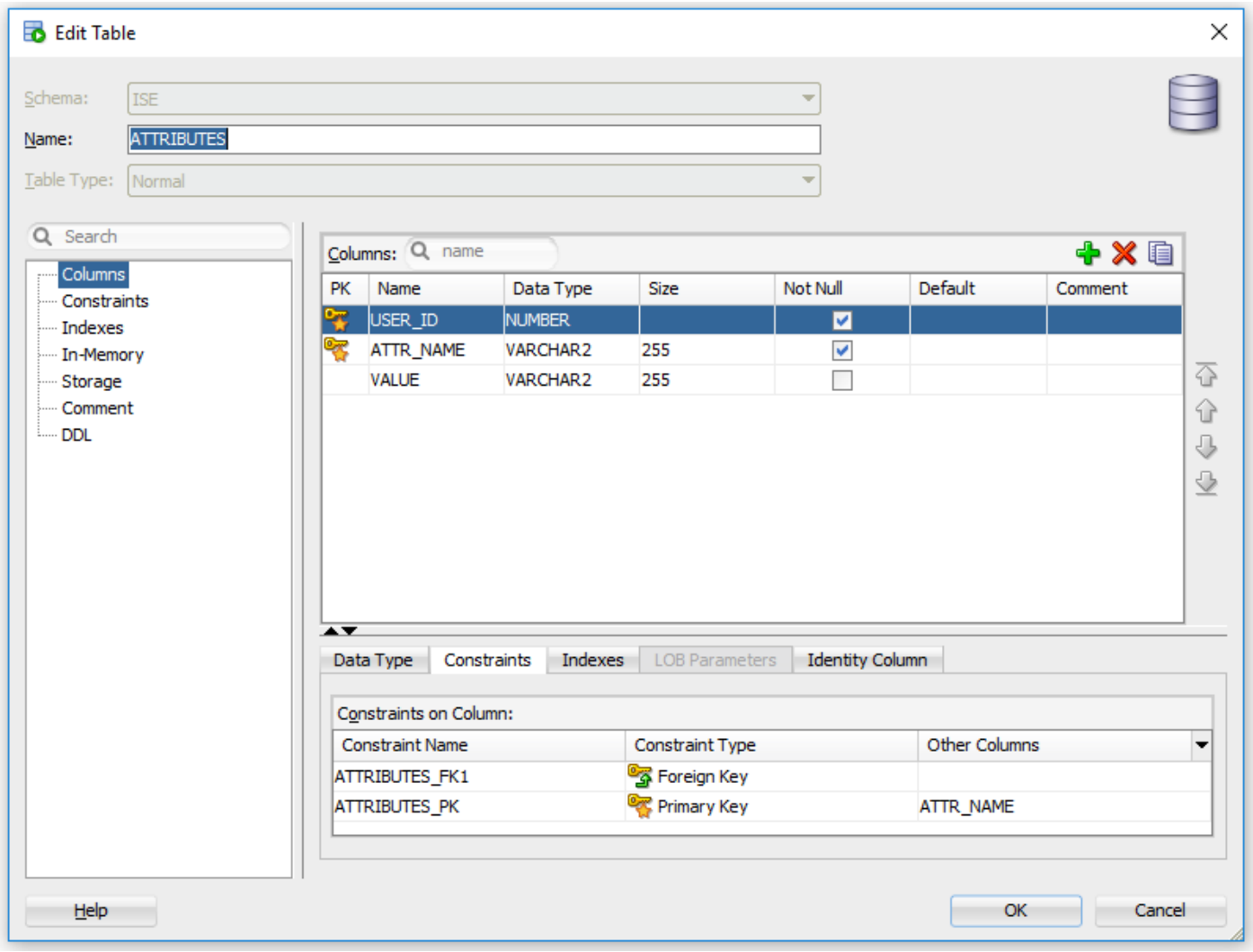
ステップ 5：属性取得の設定

1.この例を簡略化するために、属性にはフラットなテーブルを使用します

```
-------------------------------------------------------
--  DDL for Table ATTRIBUTES
-------------------------------------------------------

  CREATE TABLE "ISE"."ATTRIBUTES"
   ("USER_ID" NUMBER(*,0),
"ATTR_NAME" VARCHAR2(255 BYTE),
"VALUE" VARCHAR2(255 BYTE)
   ) SEGMENT CREATION IMMEDIATE
  PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255
 NOCOMPRESS LOGGING
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
```

```
--------------------------------------------------------
--  DDL for Index ATTRIBUTES_PK
--------------------------------------------------------

  CREATE UNIQUE INDEX "ISE"."ATTRIBUTES_PK" ON "ISE"."ATTRIBUTES" ("ATTR_NAME", "USER_ID")
  PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS" ;
--------------------------------------------------------
--  Constraints for Table ATTRIBUTES
--------------------------------------------------------

  ALTER TABLE "ISE"."ATTRIBUTES" MODIFY ("USER_ID" NOT NULL ENABLE);
  ALTER TABLE "ISE"."ATTRIBUTES" MODIFY ("ATTR_NAME" NOT NULL ENABLE);
  ALTER TABLE "ISE"."ATTRIBUTES" ADD CONSTRAINT "ATTRIBUTES_PK" PRIMARY KEY ("ATTR_NAME",
"USER_ID")
  USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255
  STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
  PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1
  BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
  TABLESPACE "USERS"  ENABLE;
```

GUI から：



2.ユーザーの属性の作成

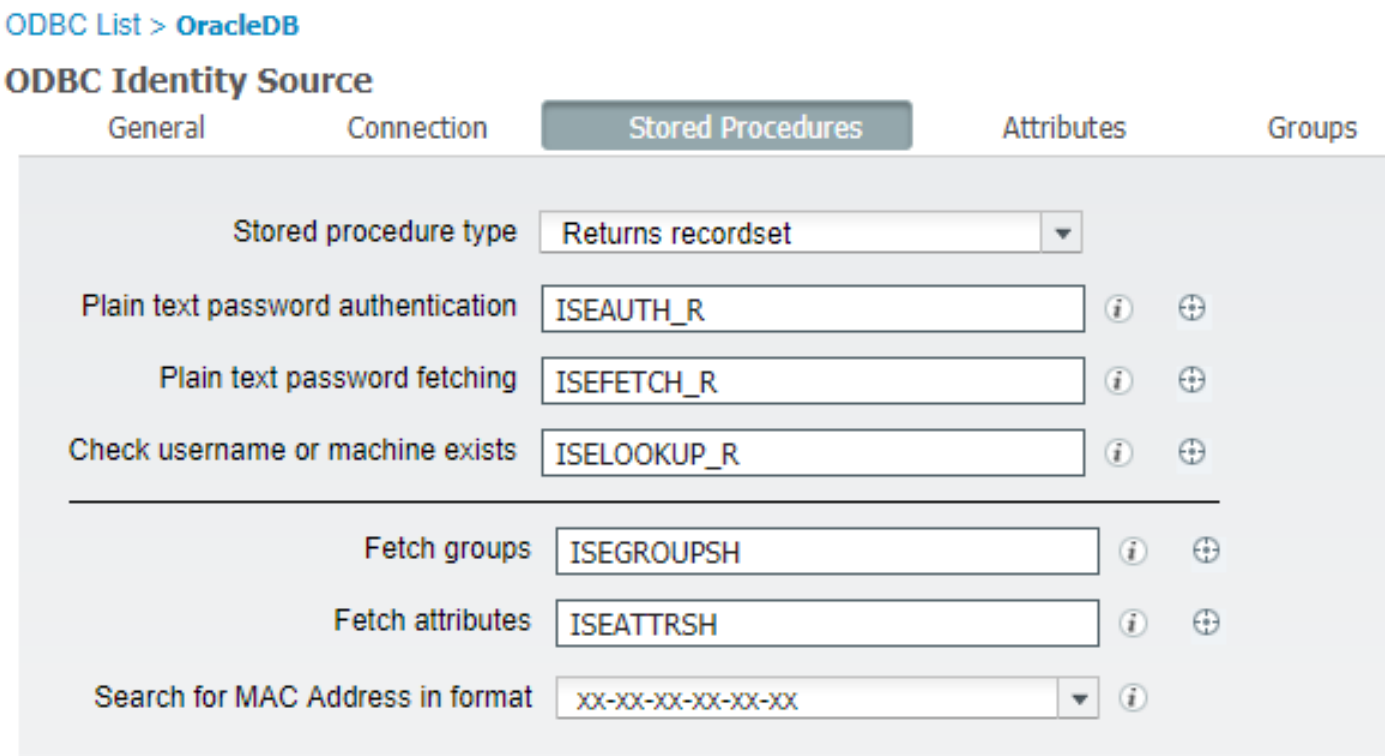
```
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('3', 'SecurityLevel', '15')
```

```
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('1', 'SecurityLevel', '5')
INSERT INTO "ISE"."ATTRIBUTES" (USER_ID, ATTR_NAME, VALUE) VALUES ('2', 'SecurityLevel', '10')
```

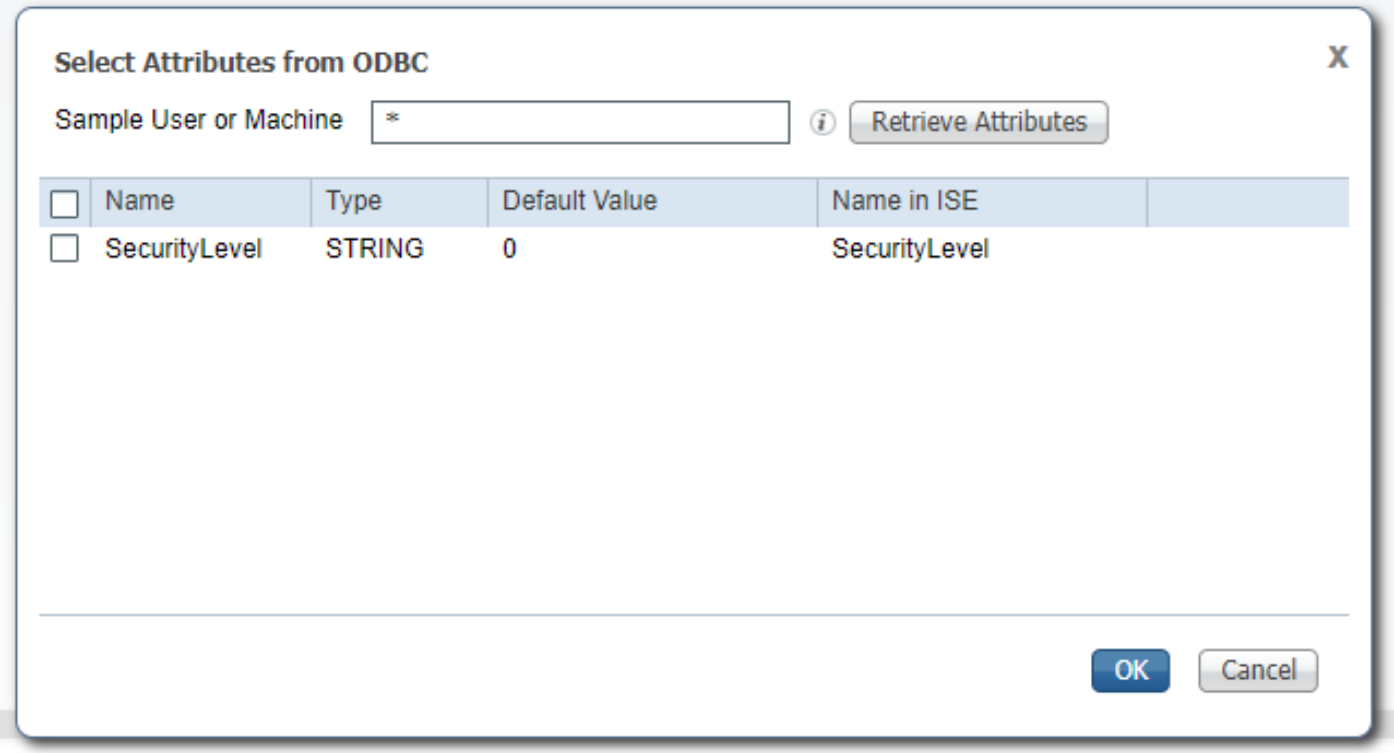
3.プロシージャを作成します。グループの取得と同様に、usernameが「*」の場合は、すべての異なる属性を返します

```
create or replace function ISEATTRSH
(
  ise_username IN VARCHAR2,
  ise_result OUT int
) return sys_refcursor as
BEGIN
  declare
    c integer;
    userid integer;
    resultSet SYS_REFCURSOR;
  begin
    IF ise_username = '*' then
      ise_result := 0;
      open resultSet for select DISTINCT ATTR_NAME, '0' as "VAL" from ATTRIBUTES;
    ELSE
      select count(*) into c from USERS where USERS.USERNAME = ise_username;
      select USER_ID into userid from USERS where USERS.USERNAME = ise_username;
      if c > 0 then
          ise_result := 0;
          open resultSet for select ATTR_NAME, VALUE from ATTRIBUTES where USER_ID = userid;
      ELSE
          ise_result := 3;
          open resultSet for select 0 from dual where 1=2;
      END IF;
    END IF;
    return resultSet;
  end;
END ;
```

4. Fetch属性にマップします



5.属性の取得



属性を選択し、[OK]をクリックします。

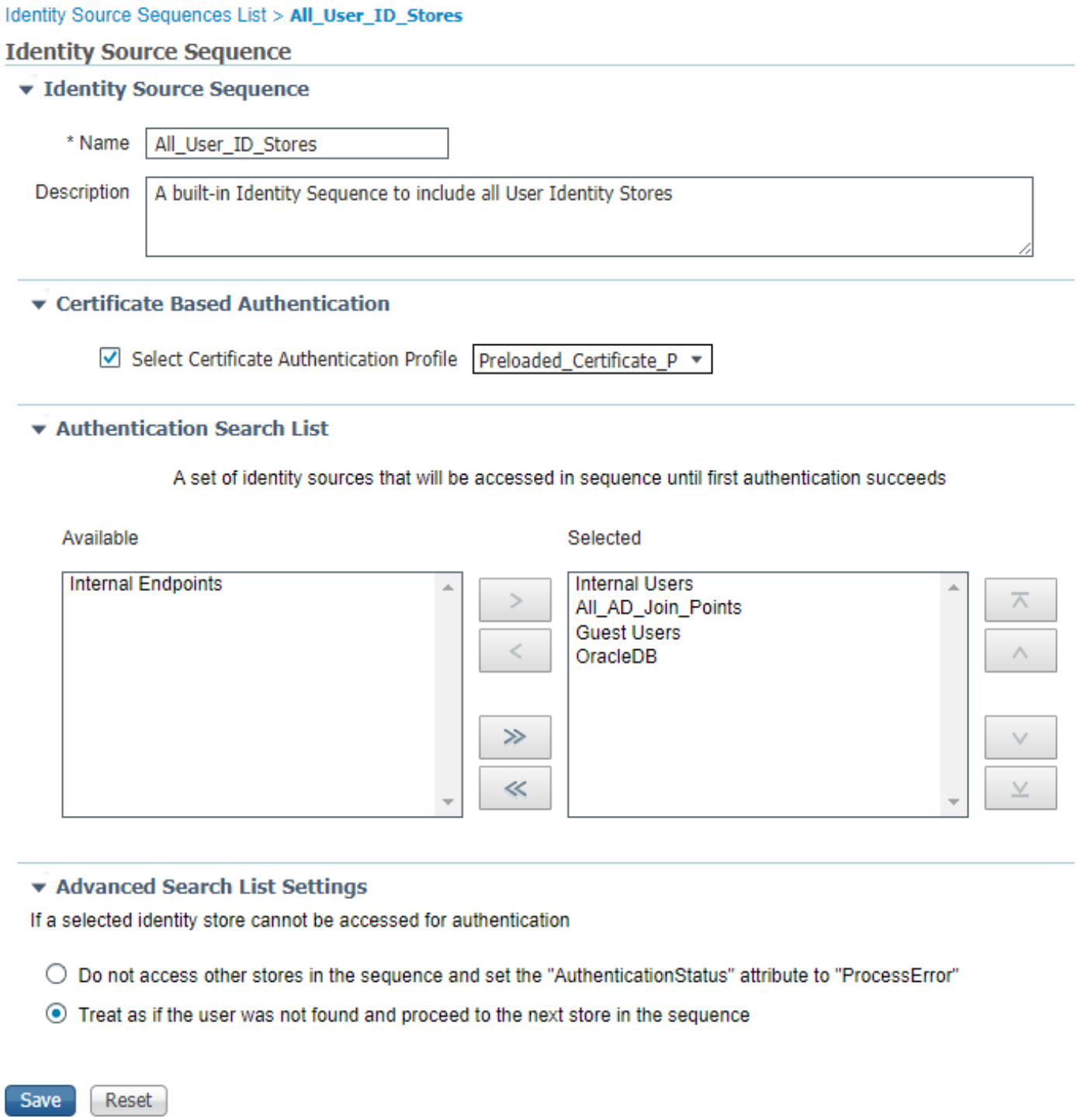
ステップ6：認証/認可ポリシーの設定

この例では、次の簡単な認可ポリシーが設定されています。

SecurityLevel = 5の**ユーザーは拒否**されます。

ステップ7：アイデンティティ・ソース・シーケンスへのOracle ODBCの追加

[*Administration*] > [*Identity Management*] > *[Identity Source Sequences]に移動し、シーケンスを選択し、*シーケンスにODBCを追加します。



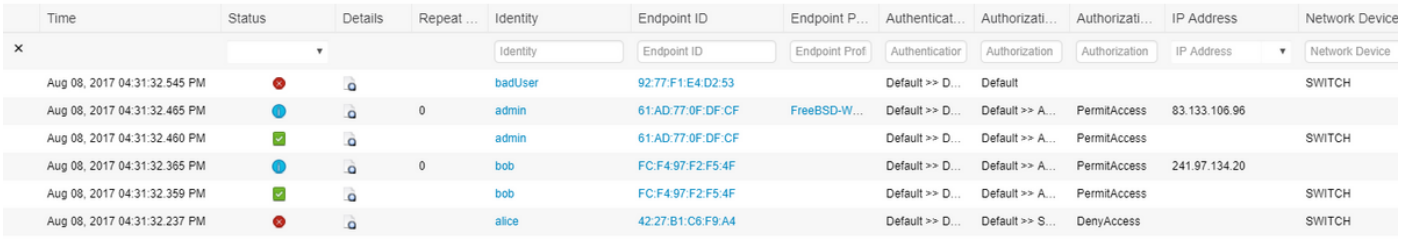
保存します。

確認

これで、ODBCに対してユーザを認証し、ユーザのグループと属性を取得できるようになります。

RADIUS ライブ ログ

いくつかの認証を実行し、*[Operations] > [RADIUS] > [Live Logs]に移動します*



	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
×					Identity	Endpoint ID	Endpoint Prof	Authentication	Authorization	Authorization	IP Address	Network Device
	Aug 08, 2017 04:31:32.545 PM	✗			badUser	92:77:F1:E4:D2:53		Default >> D...	Default			SWITCH
	Aug 08, 2017 04:31:32.465 PM	?		0	admin	61:AD:77:0F:DF:CF	FreeBSD-W...	Default >> D...	Default >> A...	PermitAccess	83.133.106.96	
	Aug 08, 2017 04:31:32.460 PM	✓			admin	61:AD:77:0F:DF:CF		Default >> D...	Default >> A...	PermitAccess		SWITCH
	Aug 08, 2017 04:31:32.365 PM	?		0	bob	FC:F4:97:F2:F5:4F		Default >> D...	Default >> A...	PermitAccess	241.97.134.20	
	Aug 08, 2017 04:31:32.359 PM	✓			bob	FC:F4:97:F2:F5:4F		Default >> D...	Default >> A...	PermitAccess		SWITCH
	Aug 08, 2017 04:31:32.237 PM	✗			alice	42:27:B1:C6:F9:A4		Default >> D...	Default >> S...	DenyAccess		SWITCH

ご覧のように、ユーザAliceには**SecurityLevel** = 5**が設定されているため、**アクセスは拒否されました。

詳細レポート

対象セッション**の[詳細]列**の[詳細**レポート]**をクリックして、フローを確認します。

ユーザAliceの詳細レポート（セキュリティレベルが低いため拒否）: