# 配置在ISE 2.3的ODBC与Oracle数据库

## 目录



## 简介

本文描述如何配置身份服务引擎(ISE)使用开放数据库连接(ODBC)，有ISE验证的Oracle数据库的。

开放数据库连接(ODBC)验证要求ISE能拿来纯文本用户密码。密码在数据库加密，但是必须由存储过程解密。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎2.3
- 数据库和ODBC概念
- Oracle

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎2.3.0.298
- Centos 7
- Oracle数据库12.2.0.1.0
- Oracle SQL开发者4.1.5

# 配置

> **注意：**对待在本文提交的SQL存储过程作为示例。这不是Oracle DB配置一个正式和推荐的方式。保证您了解您做每SQL查询的结果和影响。

## 步骤1. Oracle基本配置

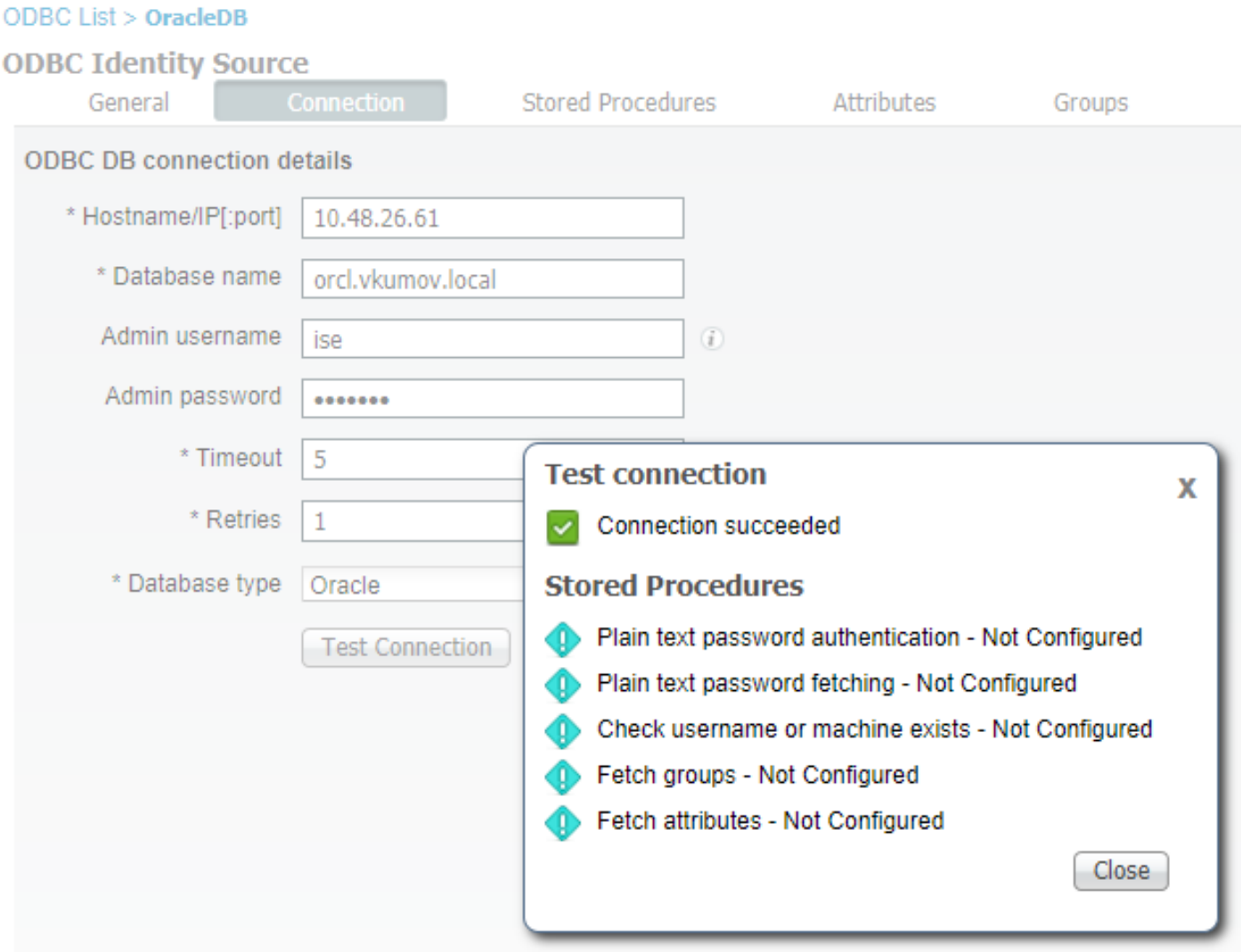
在本例中Oracle配置与以下参数：

- DB名称：**ORCL**
- 服务名称：**orcl.vkumov.local**
- 波尔特：**1521** (默认)
- ISE的已创建帐户与用户名**ise**

您应该在将来发生前配置您的Oracle。

## 步骤2. ISE基本配置

创建ODBC标识来源在*Administration >外部标识来源> ODBC*和测试连接：




**注意**：使用服务名称， ISE连接对Oracle，因此在Oracle中存在，不是SID应该充满的[Database name]字段服务名称(或DB请命名)。由于bug CSCvf06497小点(。)不能用于[Database name]字段。此bug在ISE 2.3修复。

## 步骤3.配置用户认证

对ODBC用途存储过程的ISE验证。选择步骤的类型是可能的。在本例中我们使用recordsets作为返回。

对于其他步骤，参考思科身份服务引擎管理员指南，版本2.3

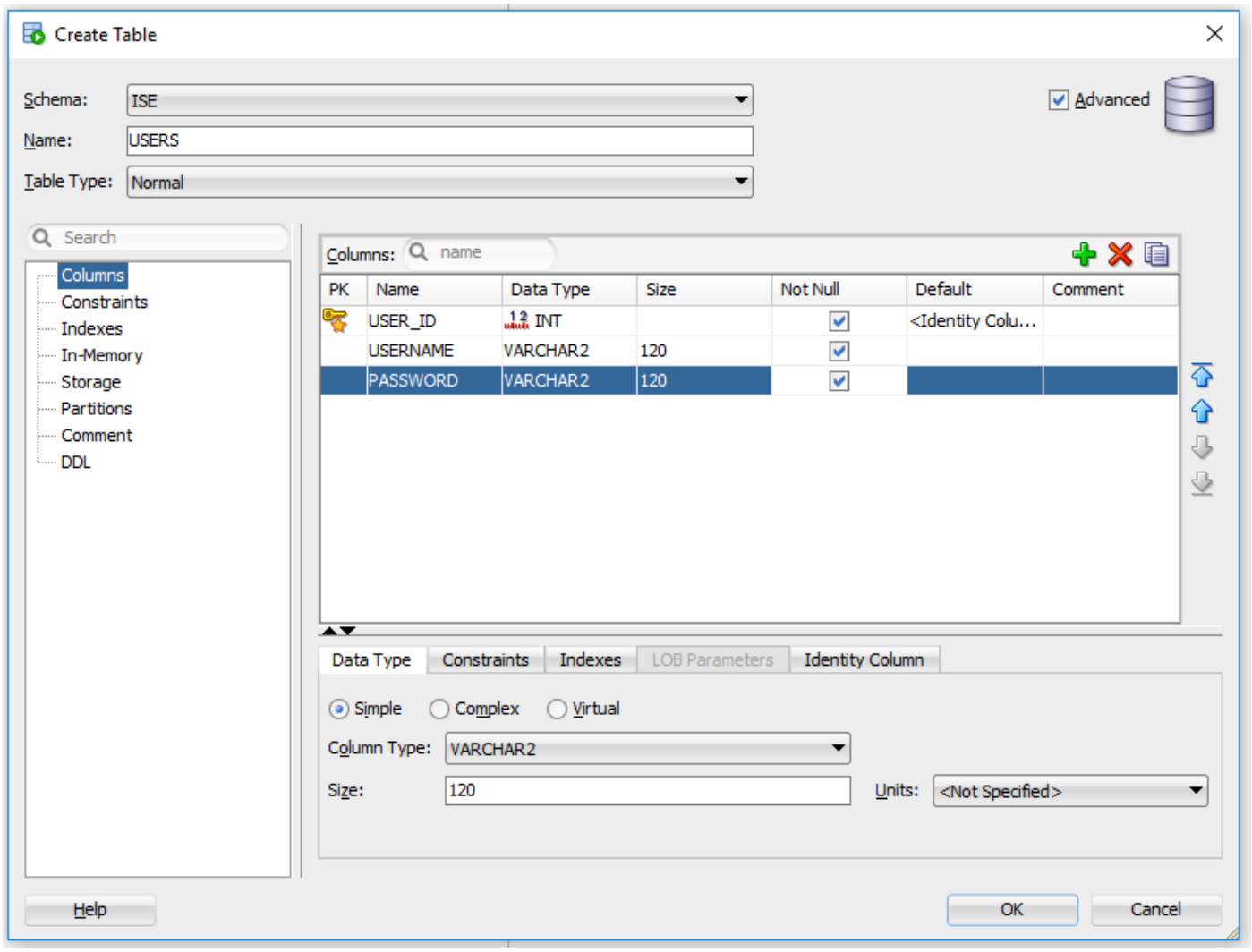
**提示**：返回指定参数而不是resultset是可能的。它是不同种输出，功能是相同的。

1. 创建与用户的凭证的表。确保您设在**主键的**标识设置。

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

  CREATE TABLE "ISE"."USERS"
   ("USER_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
9999999999999999999999999999 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;
```

或者从SQL开发者GUI ：




2. 添加用户

```
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. 创建纯文本密码验证的一个步骤(用于PAP， EAP-GTC内在方法， TACACS)

```
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. 创建纯文本密码拿来的一个步骤(用于CHAP， MSCHAPv1/v2， EAP-MD5， LEAP， EAP-

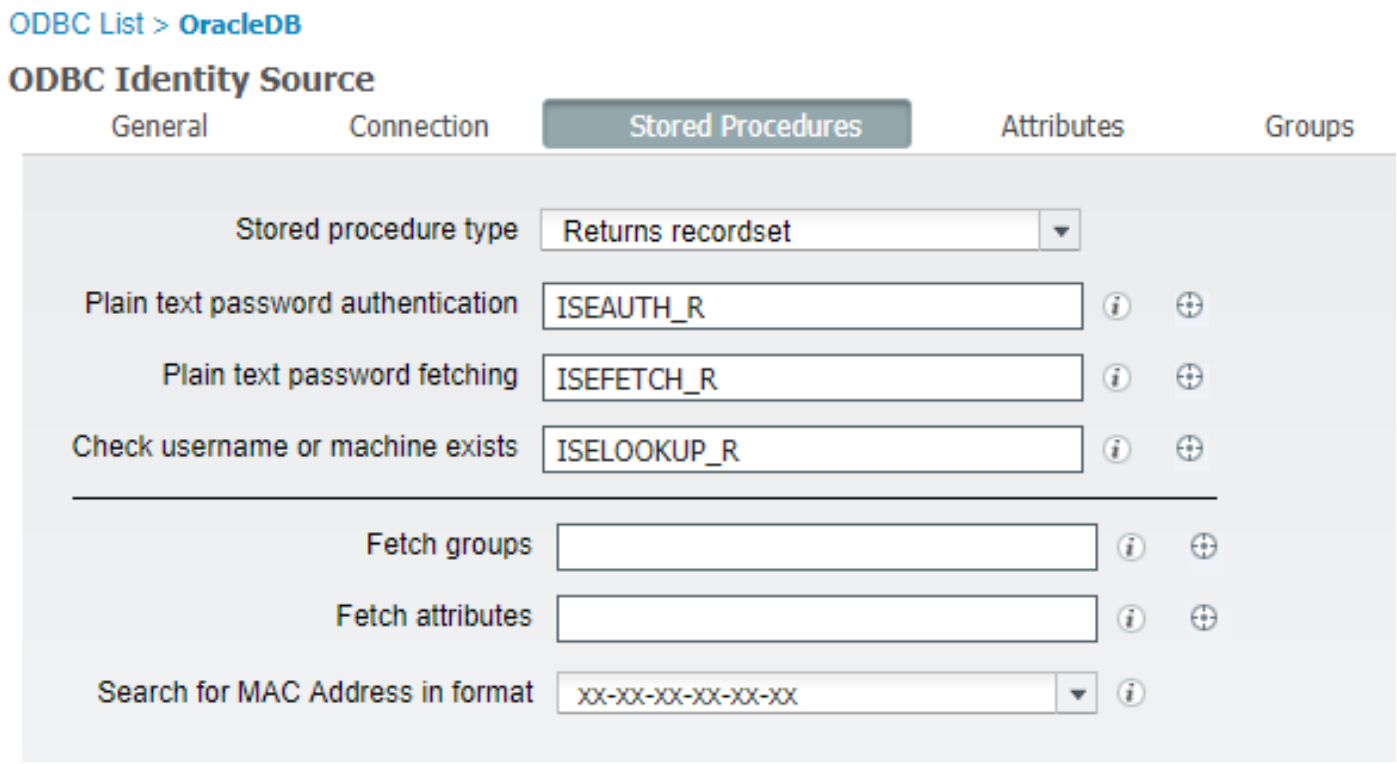
MSCHAPv2内在方法， TACACS)

```
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. 创建检查用户名的一个步骤或计算机存在(使用MAB，快速请重新连接PEAP、EAP-FAST和EAP-TTLS)

```
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. 配置在ISE的步骤并且保存




7. 去上一步Connection选项并且点击[Test Connection]按钮


## 步骤4.配置组检索

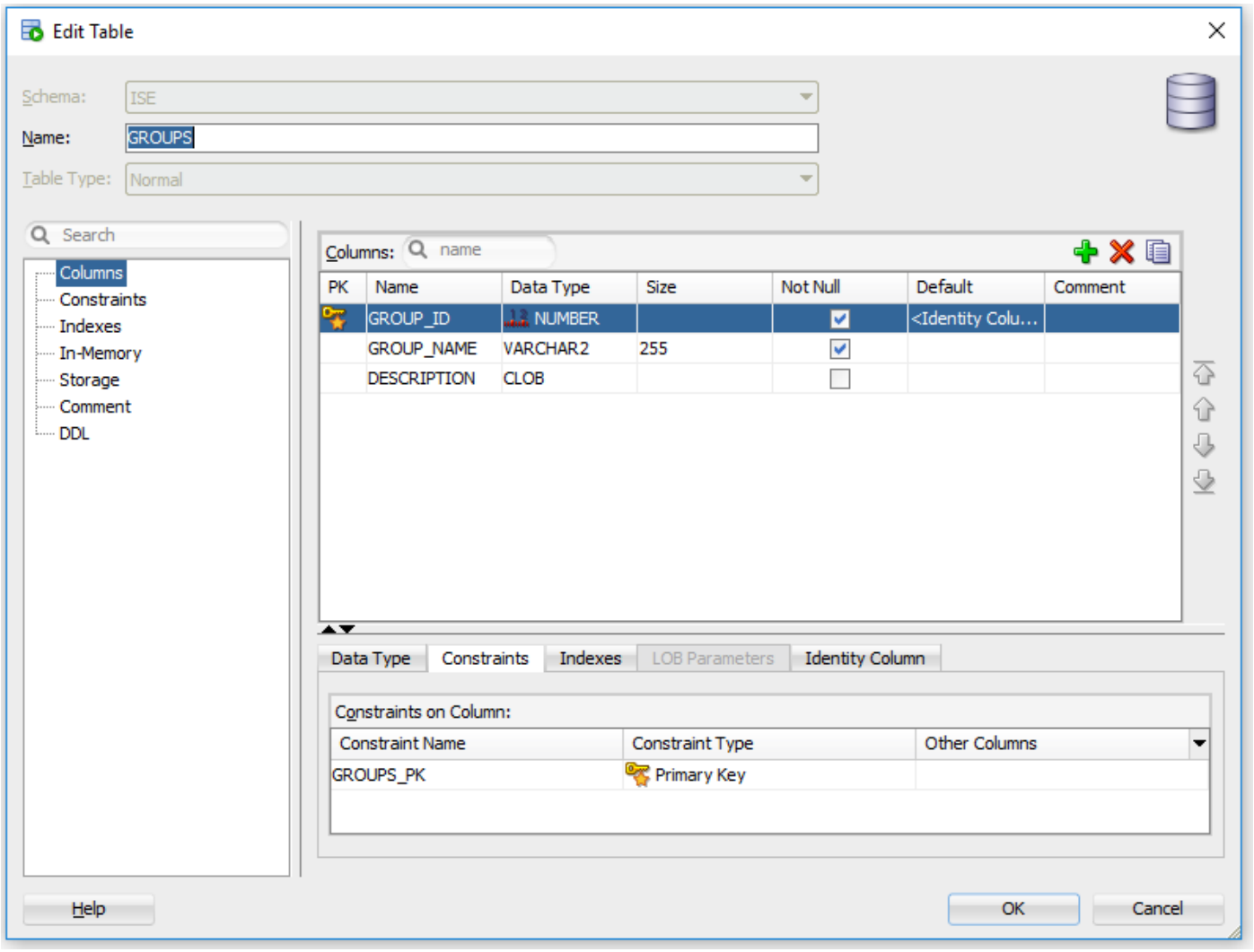
1. 创建用于越来越多的映射的表包含用户组的和别的

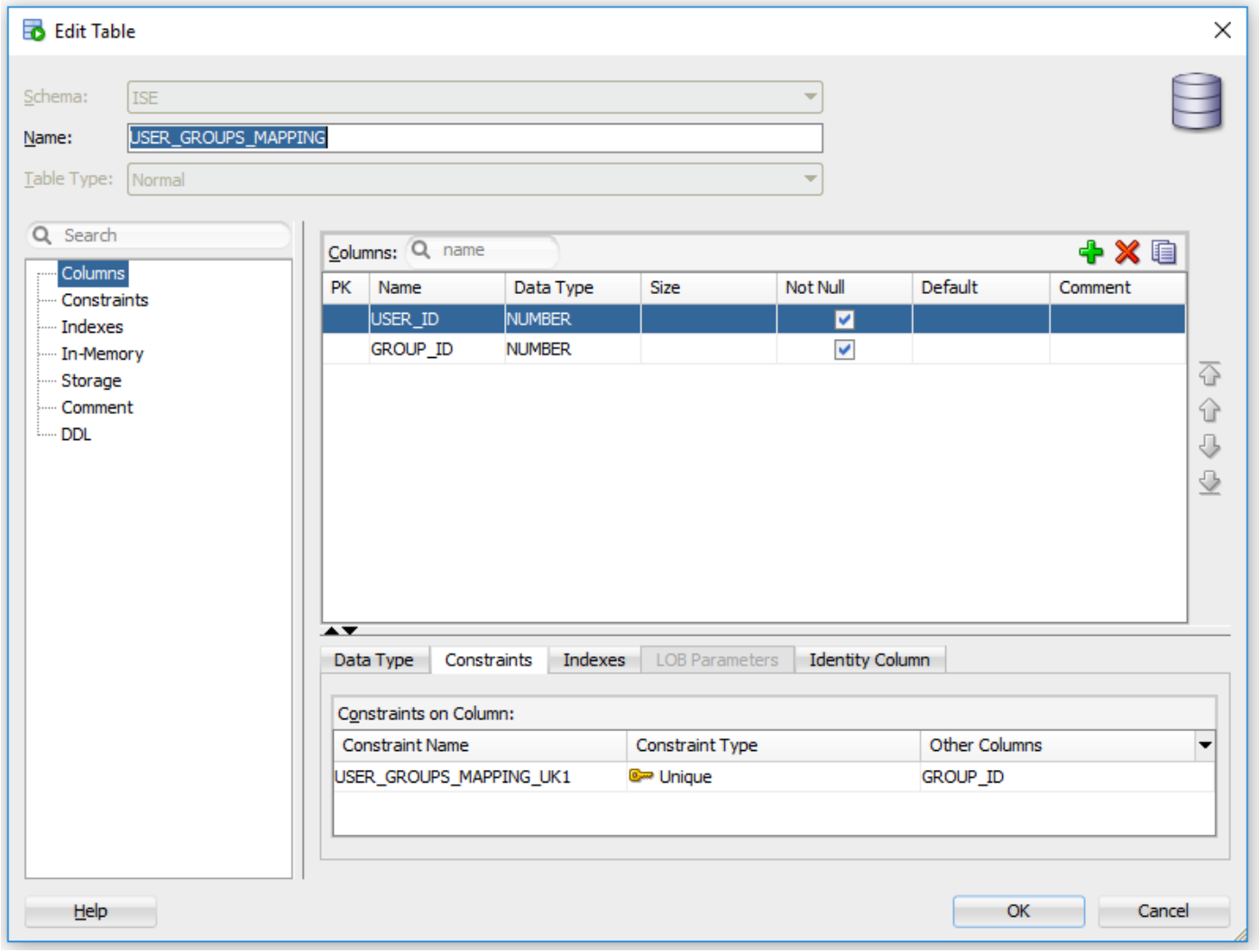
```
-------------------------------------------------------
--  DDL for Table GROUPS
-------------------------------------------------------

  CREATE TABLE "ISE"."GROUPS"
   ("GROUP_ID" NUMBER(*,0) GENERATED ALWAYS AS IDENTITY MINVALUE 1 MAXVALUE
9999999999999999999999999999 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;
```

从GUI ：






2. 添加组和映射，因此**阿丽斯**和**Bob**属于分组**用户**，并且admin属于分组**管理员**

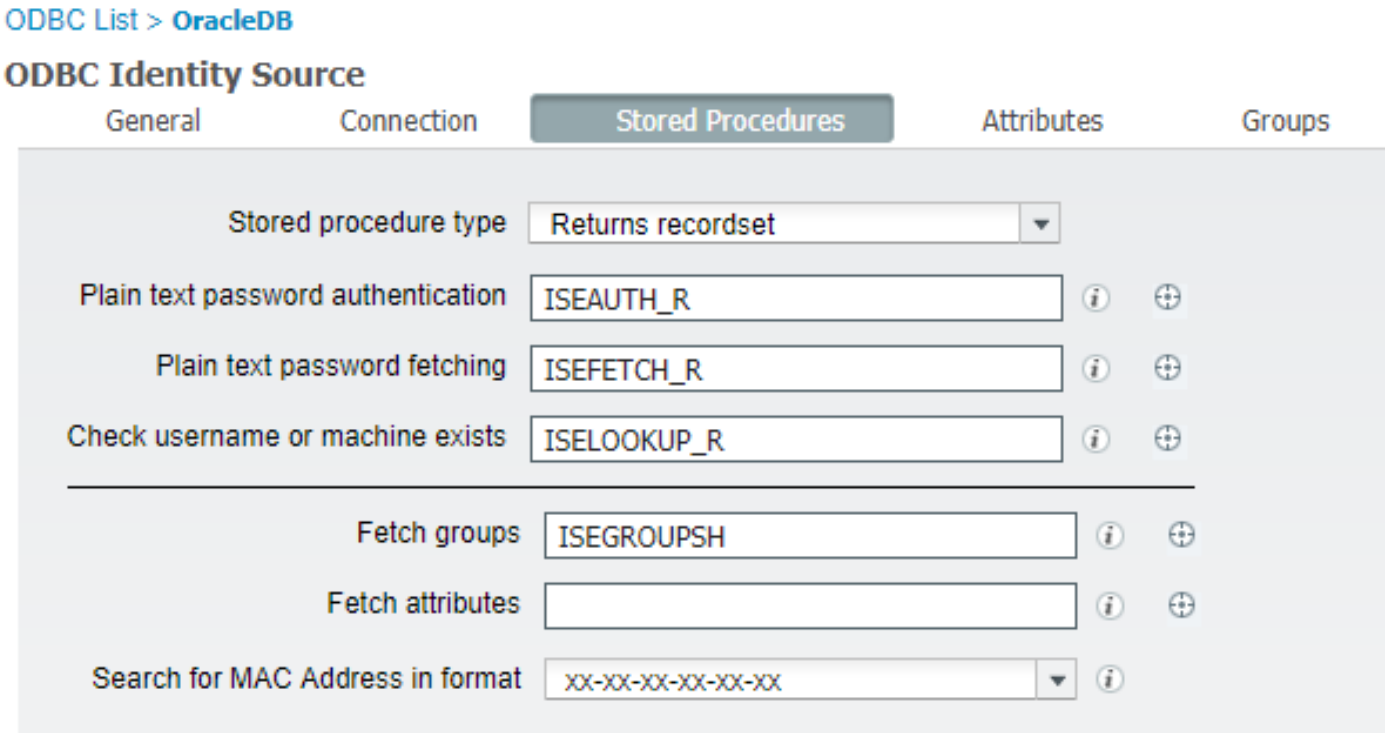
```
-- Adding groups
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Admins', 'Group for
administrators')
INSERT INTO "ISE"."GROUPS" (GROUP_NAME, DESCRIPTION) VALUES ('Users', 'Corporate users')

-- 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. 创建组检索步骤。它返回所有组，如果用户名是“*”

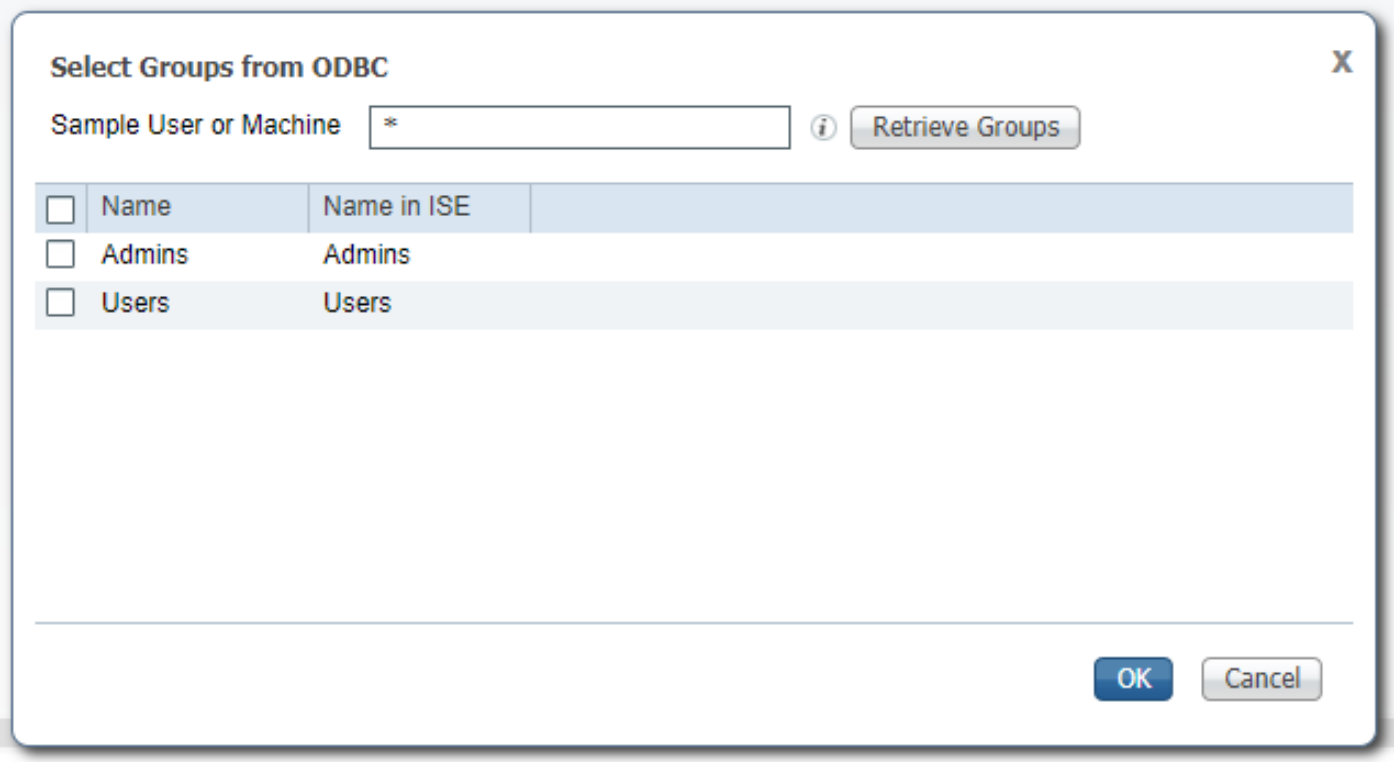
```
create or replace function ISEGROUPSH
(
  ise_username IN VARCHAR2,
  ise_result OUT int
) return sys_refcursor as
BEGIN
  declare
    c integer;
    userid integer;
    resultSet SYS_REFCURSOR;
  begin
    IF ise_username = '*' then
      ise_result := 0;
      open resultSet for select GROUP_NAME 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 ;
```

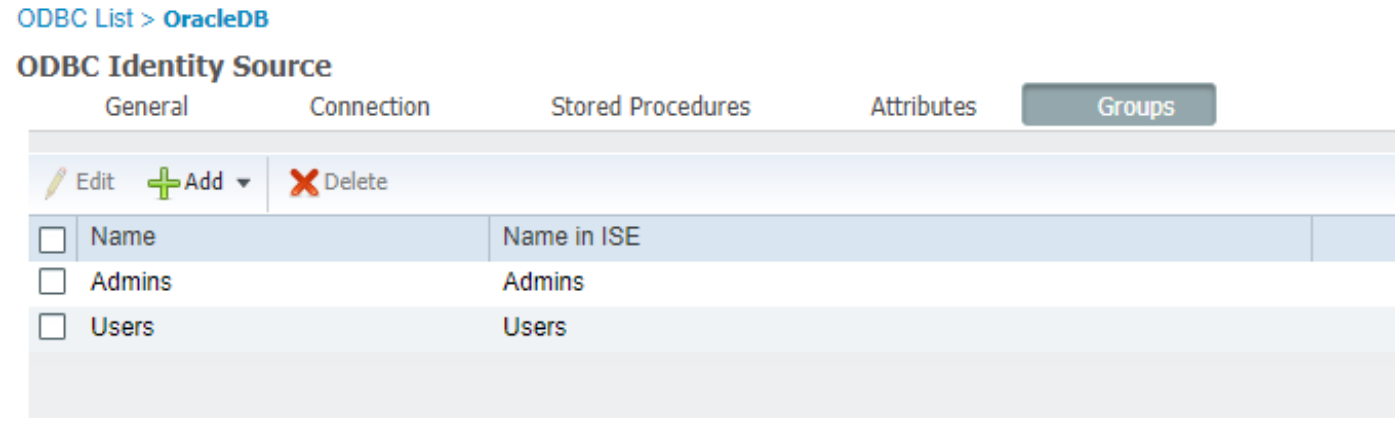
4. 映射它**拿来组**




5. 拿来组并且添加他们到**ODBC标识来源**




select需要组并且点击[OK]，他们将出现在**“组”**选项卡



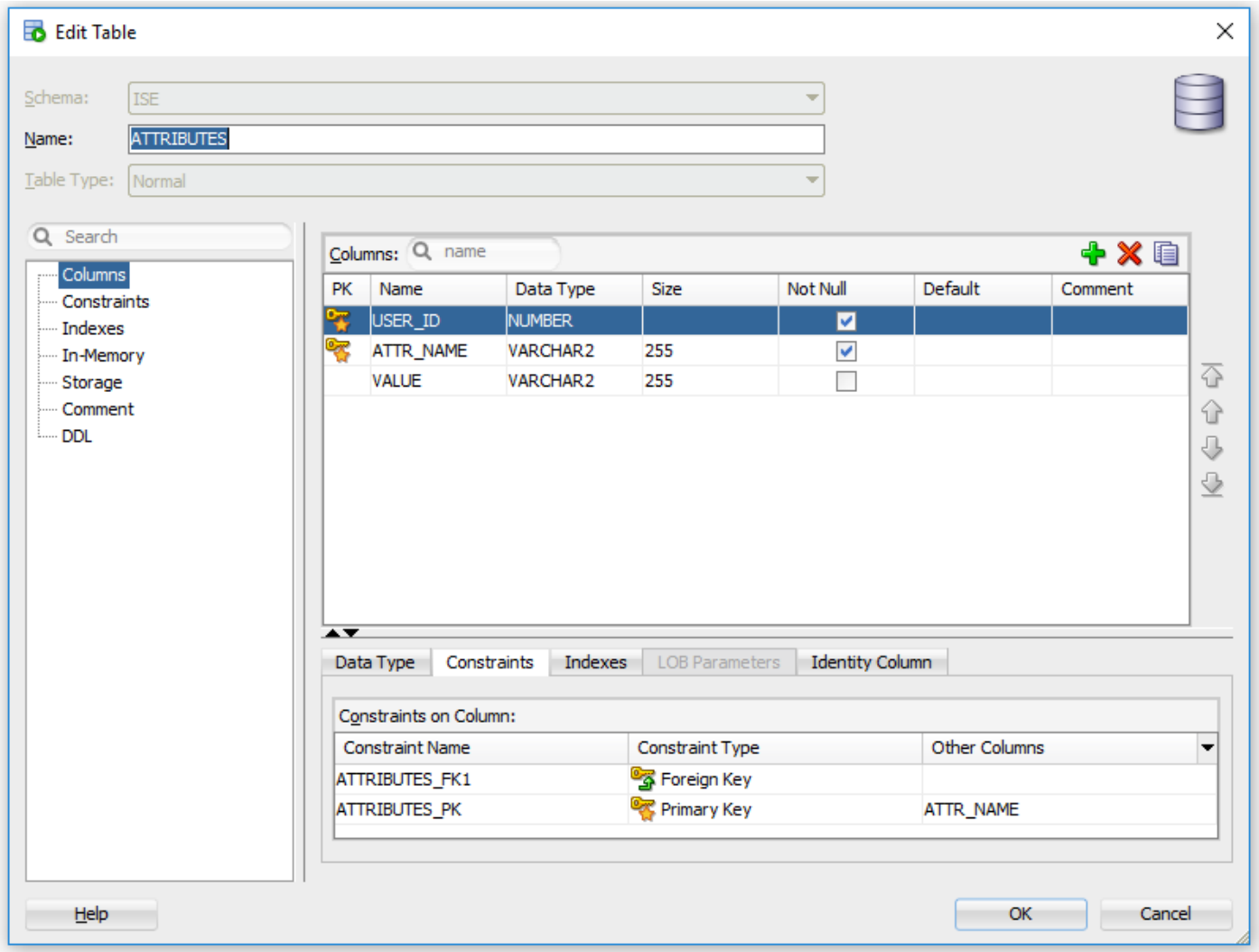

## 步骤5.配置属性检索

1. 为了简化此示例，一个平面的表使用属性

```
-------------------------------------------------------
--  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;
```

从GUI ：



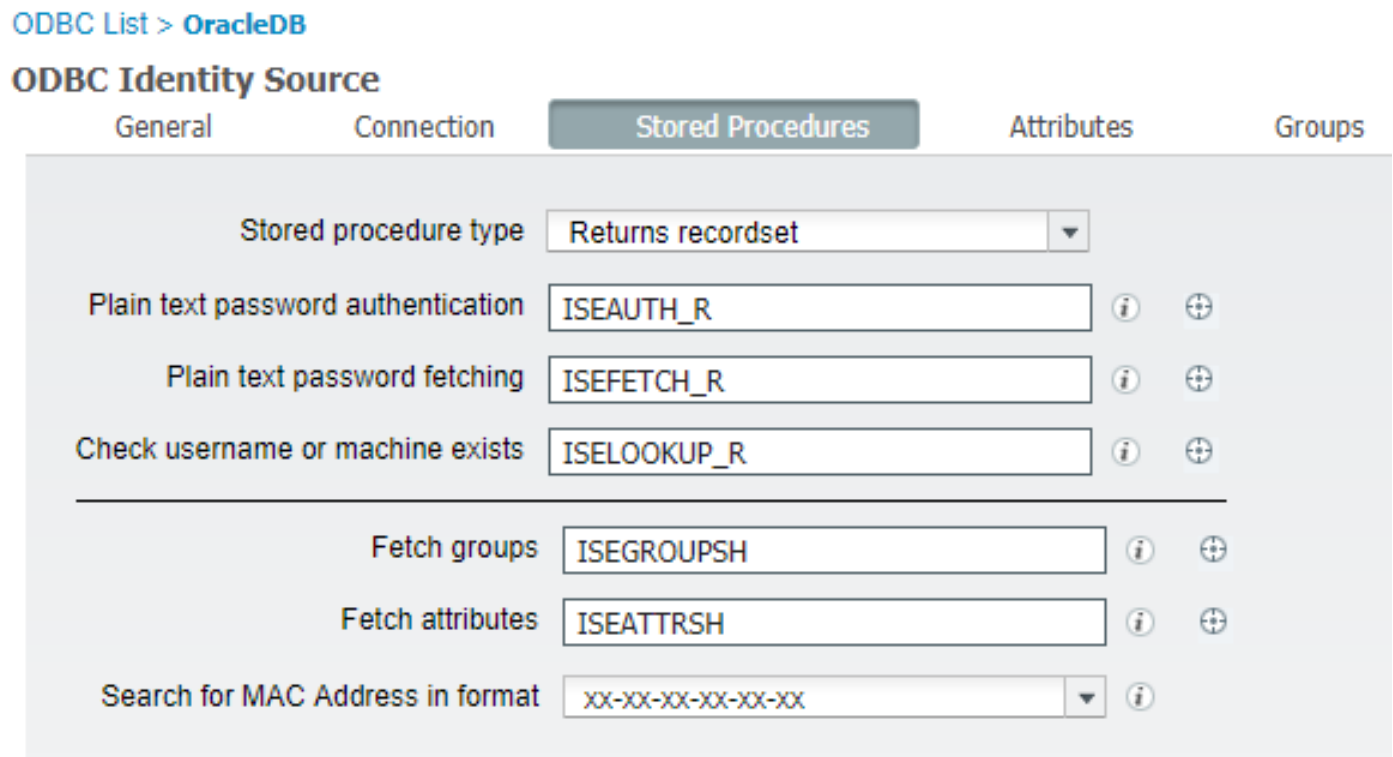

## 2. 创建用户的一些属性

```
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')
```

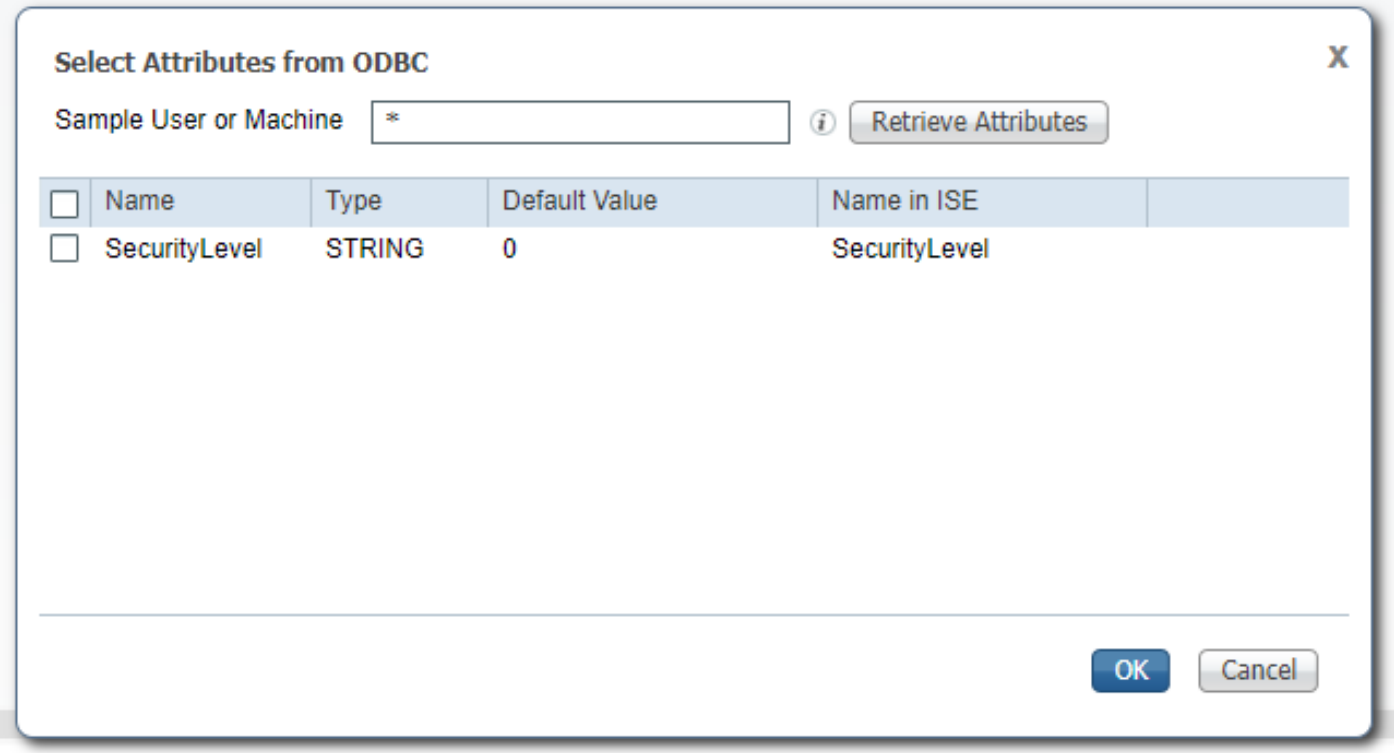
3. 创建步骤。同一样与组检索，它将返回所有明显的属性，如果用户名是“*”

```
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. 映射它**拿来属性**




5. 拿来属性




选择属性并且点击[OK]。

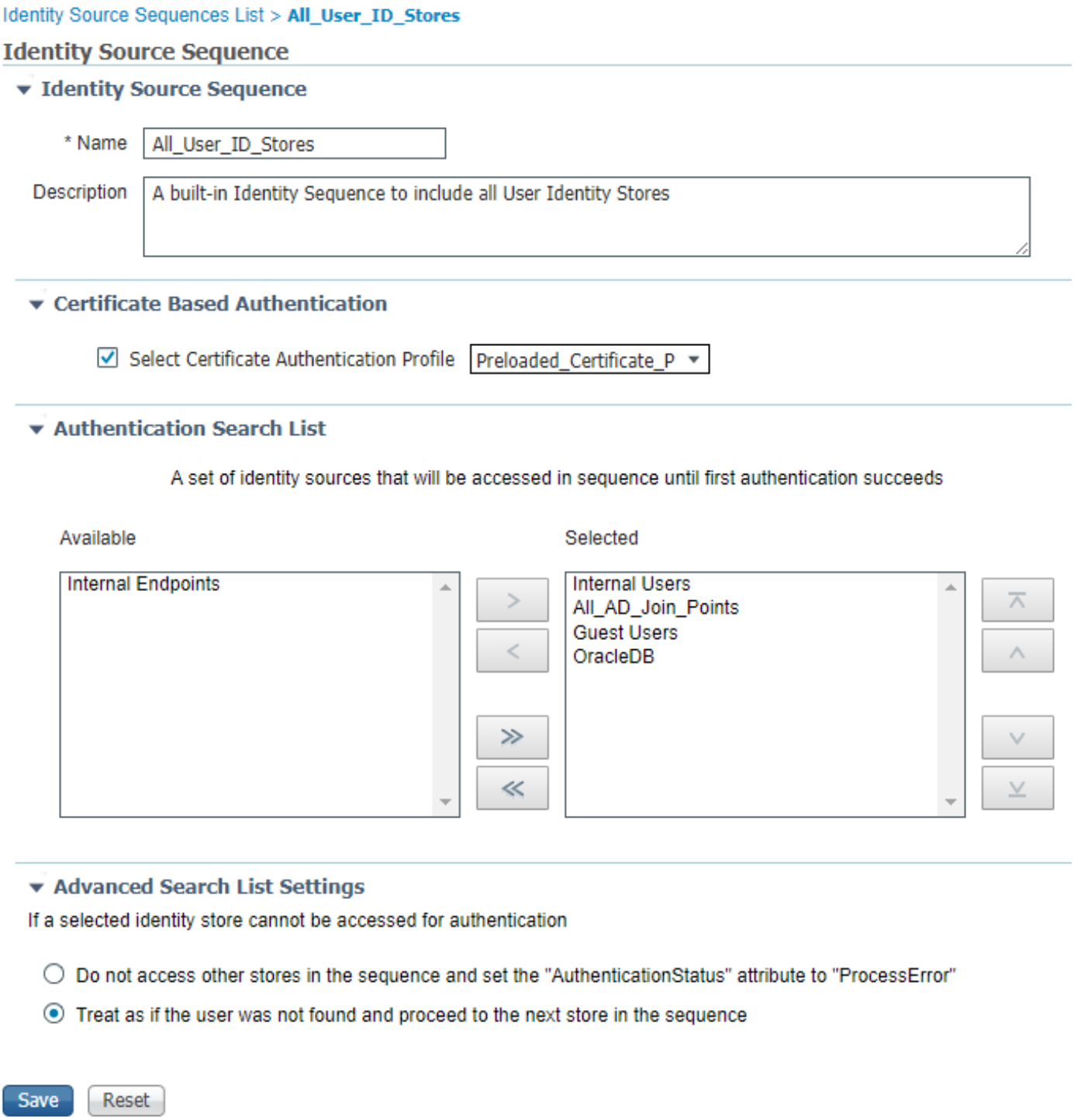
## 步骤6.配置认证/授权策略

在本例中以下简单授权策略配置：


有**SecurityLevel的**用户**= 5将**拒绝。

## 步骤7.添加Oracle ODBC到标识来源顺序

导航对*Administration >身份管理>标识来源顺序*，选择您的顺序并且添加ODBC到顺序：



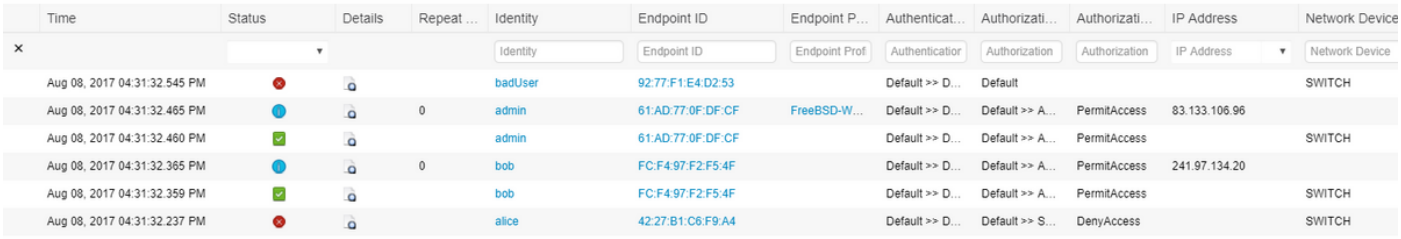

保存它。

# 验证

您应该当前能利用ODBC现在验证用户和获取他们的组和属性。

## RADIUS Live日志

进行一些认证并且导航对*操作> RADIUS> Live日志*



| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authenticat... | Authorizati... | Authorizati... | IP Address | Network Device |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Identity | Endpoint ID | Endpoint Prof | Authenticatior | 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 |

正如你看到的用户阿丽斯有**SecurityLevel = 5**，因此访问拒绝。

## 详细报表

点击在**Details列的详细报表**有趣的会话的能检查流。

用户的阿丽斯(已拒绝由于详细的报告低SecurityLevel) ：