6

Administering User Security

Objectives

After completing this lesson, you should be able to do the following:

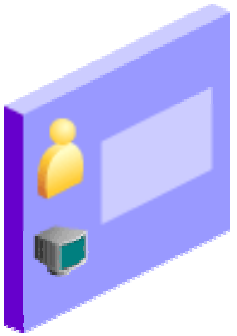
- Create and manage database user accounts
  - Authenticate users
  - Assign default storage areas (tablespaces)
- Grant and revoke privileges
- Create and manage roles
- Create and manage profiles
  - Implement standard password security features
  - Control resource usage by users

Database User Accounts

> User
Authentication
Privilege
Role
Profile
PW Security
Quota

Each database user account has:

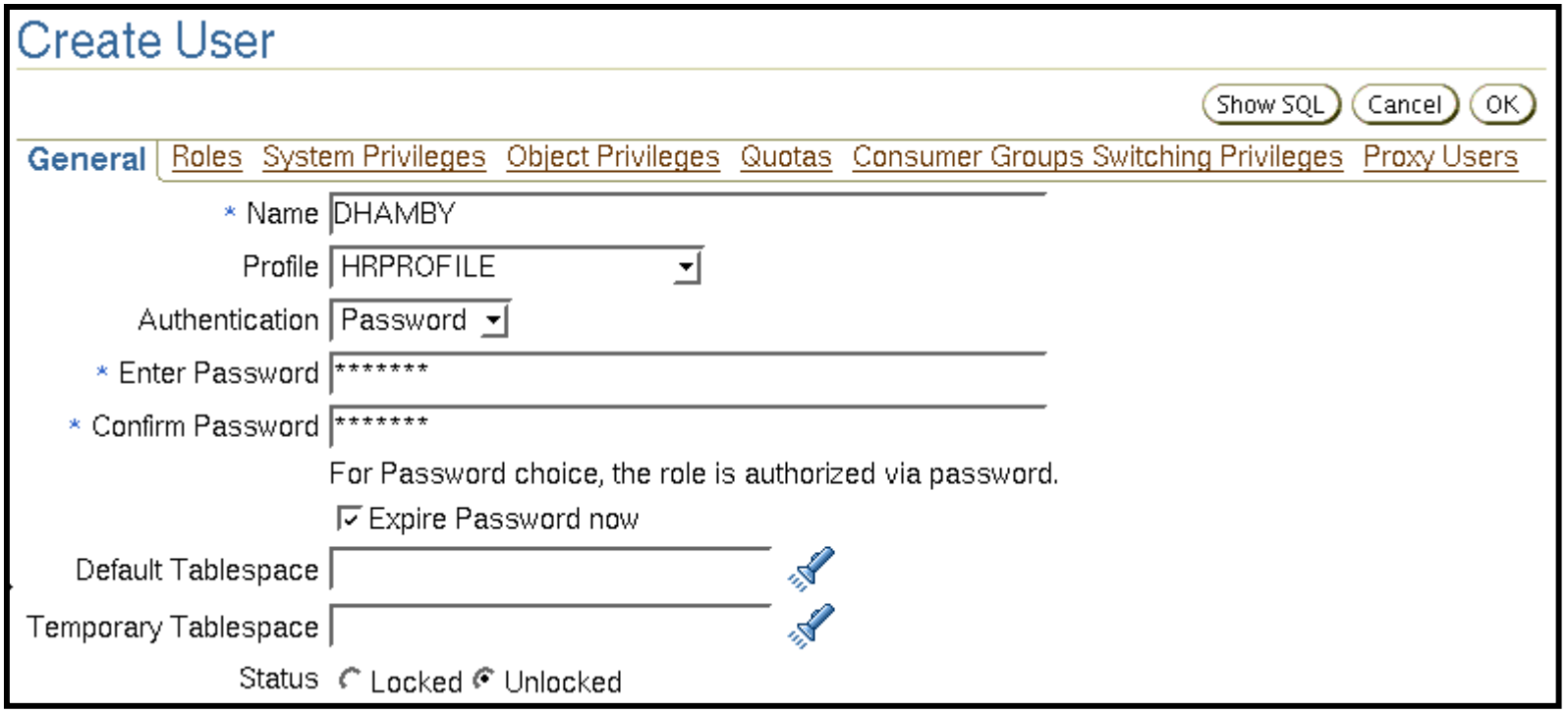
- A unique username
- An authentication method
- A default tablespace
- A temporary tablespace
- A user profile
- A consumer group
- A lock status



Predefined Accounts: SYS and SYSTEM

- The SYS account:
  - Is granted the DBA role
  - Has all privileges with ADMIN OPTION
  - Is required for startup, shutdown, and some maintenance commands
  - Owns the data dictionary
  - Owns the Automatic Workload Repository (AWR)
- The SYSTEM account is granted the DBA role.
- These accounts are not used for routine operations.

Creating a User

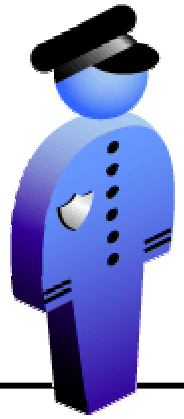


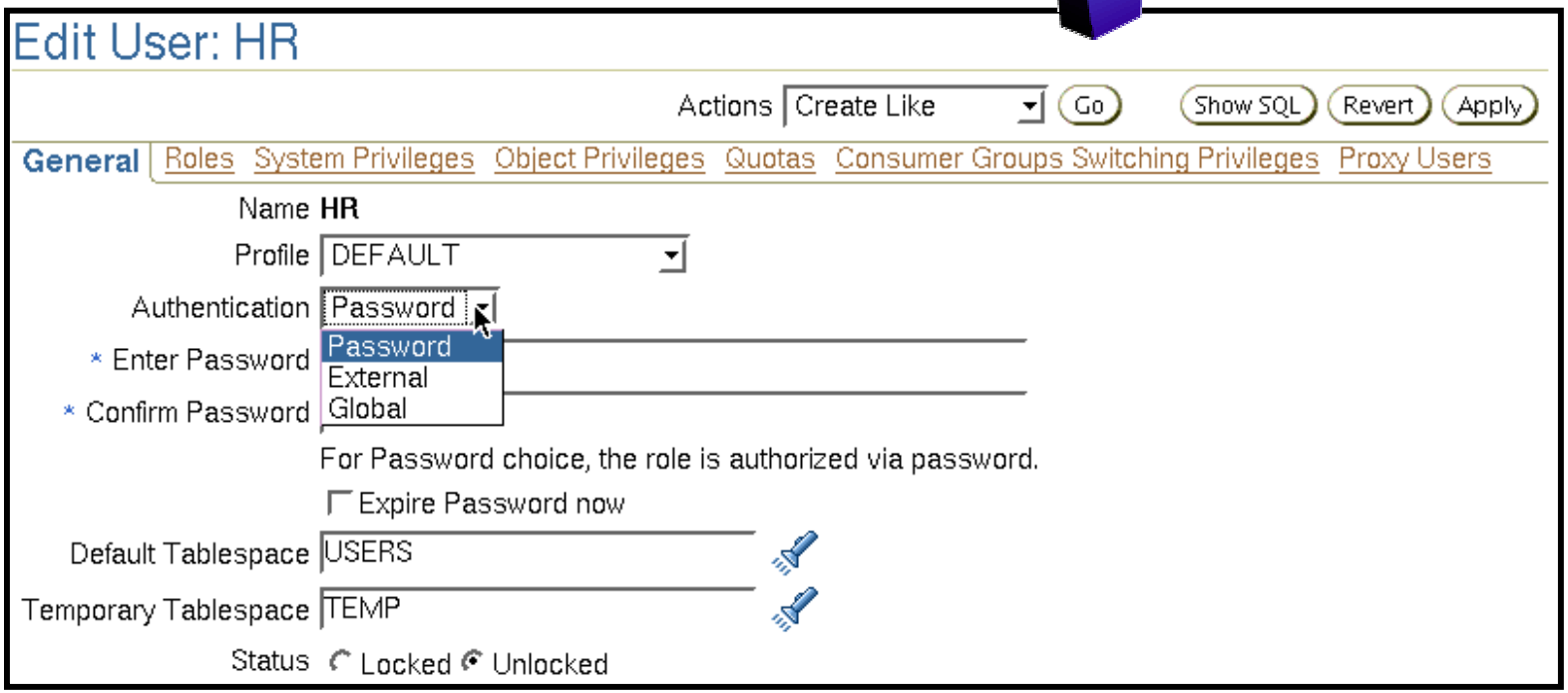
Select Administration > Schema > Users & Privileges > Users, and then click the Create button.

Authenticating Users

- User
- **Authentication**
- Privilege
- Role
- Profile
- PW Security
- Quota

- **Password**
- **External**
- **Global**





Administrator Authentication

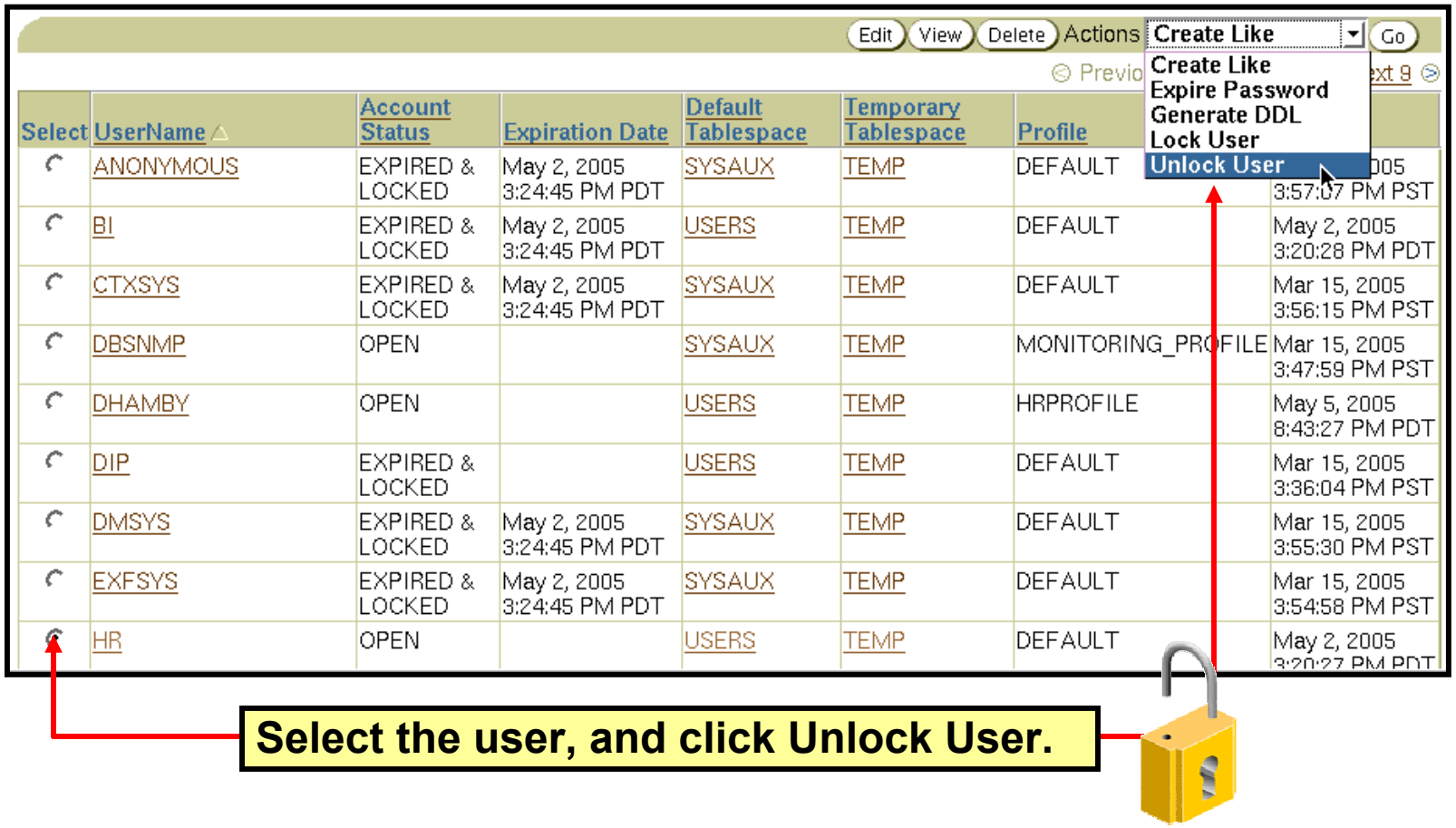
Operating System Security

- DBAs must have the OS privileges to create and delete files.
- Typical database users should not have the OS privileges to create or delete database files.

Administrator Security

- `SYSBA` and `SYSOPER` connections are authorized via password file or OS.
  - Password file authentication records the DBA user by name.
  - OS authentication does not record the specific user.
  - OS authentication takes precedence over password file authentication for `SYSDBA` and `SYSOPER`.

Unlocking a User Account and Resetting the Password

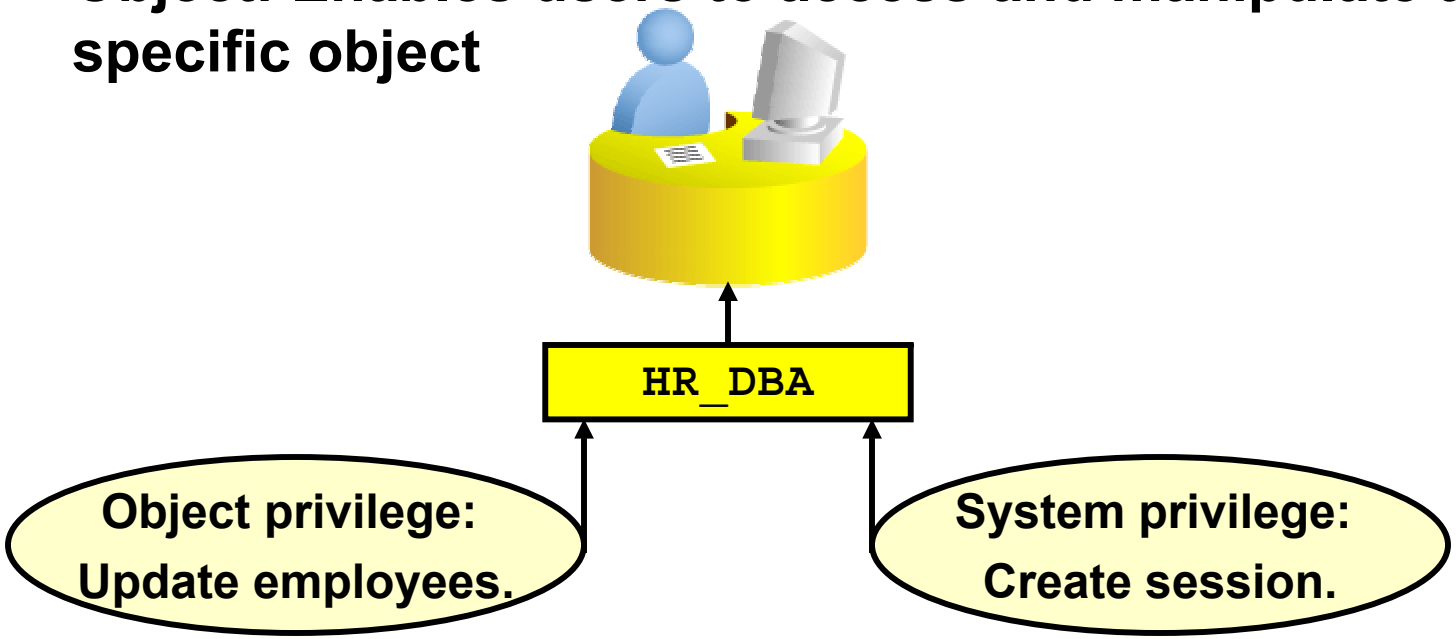


Privileges

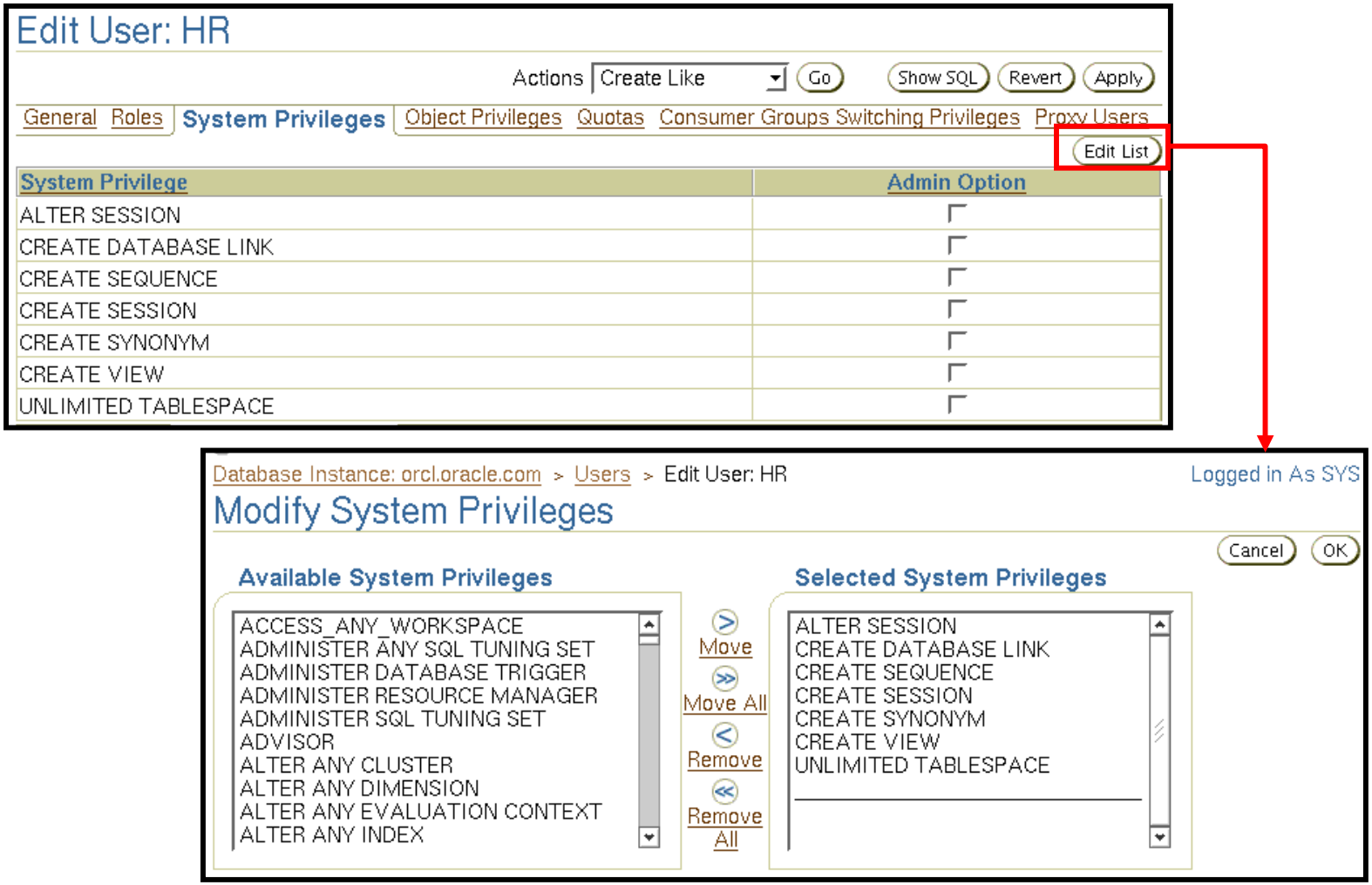
- User Authentication
- > Privilege
- Role
- Profile
- PW Security
- Quota

There are two types of user privileges:

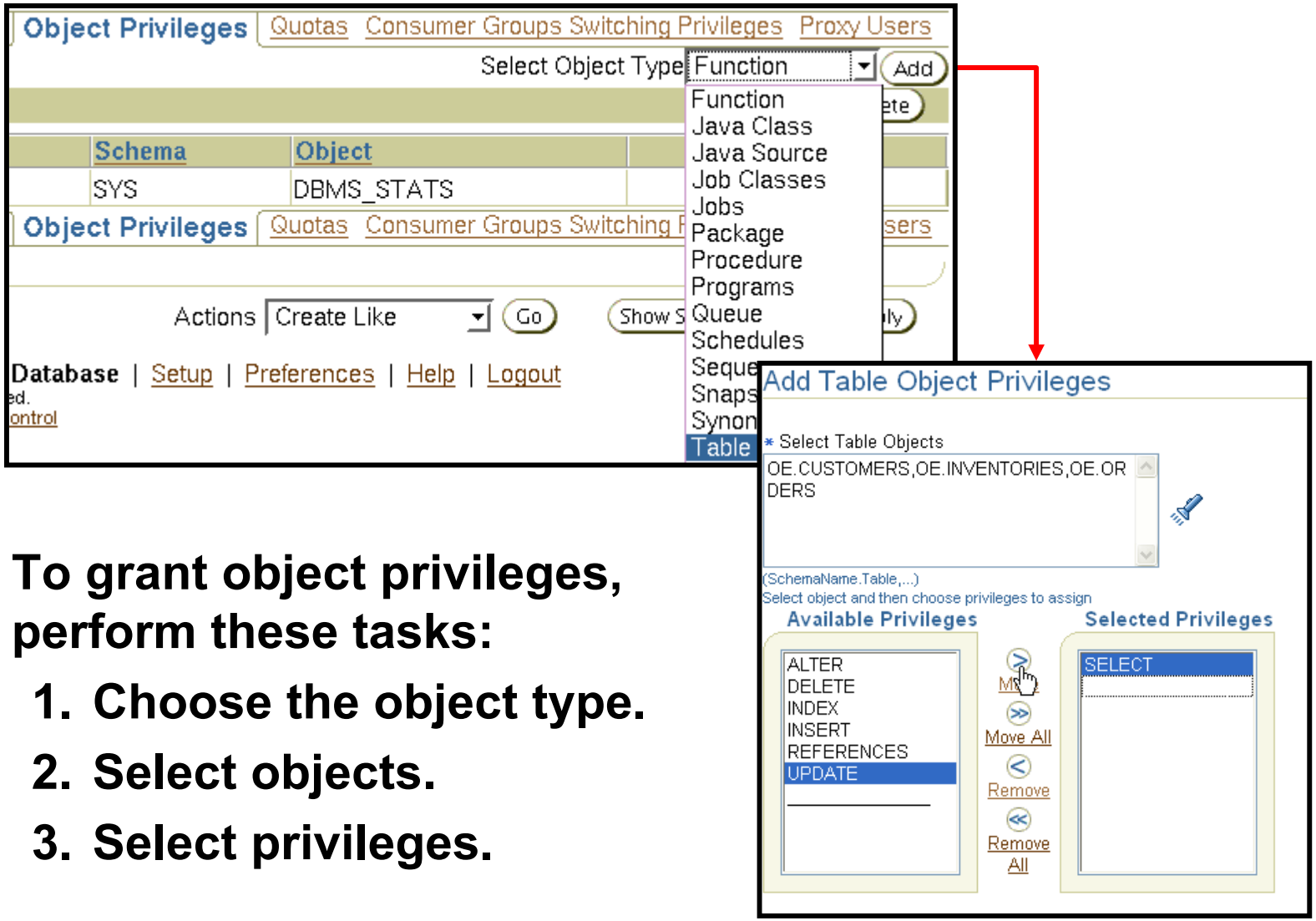
- System: Enables users to perform particular actions in the database
- Object: Enables users to access and manipulate a specific object



System Privileges



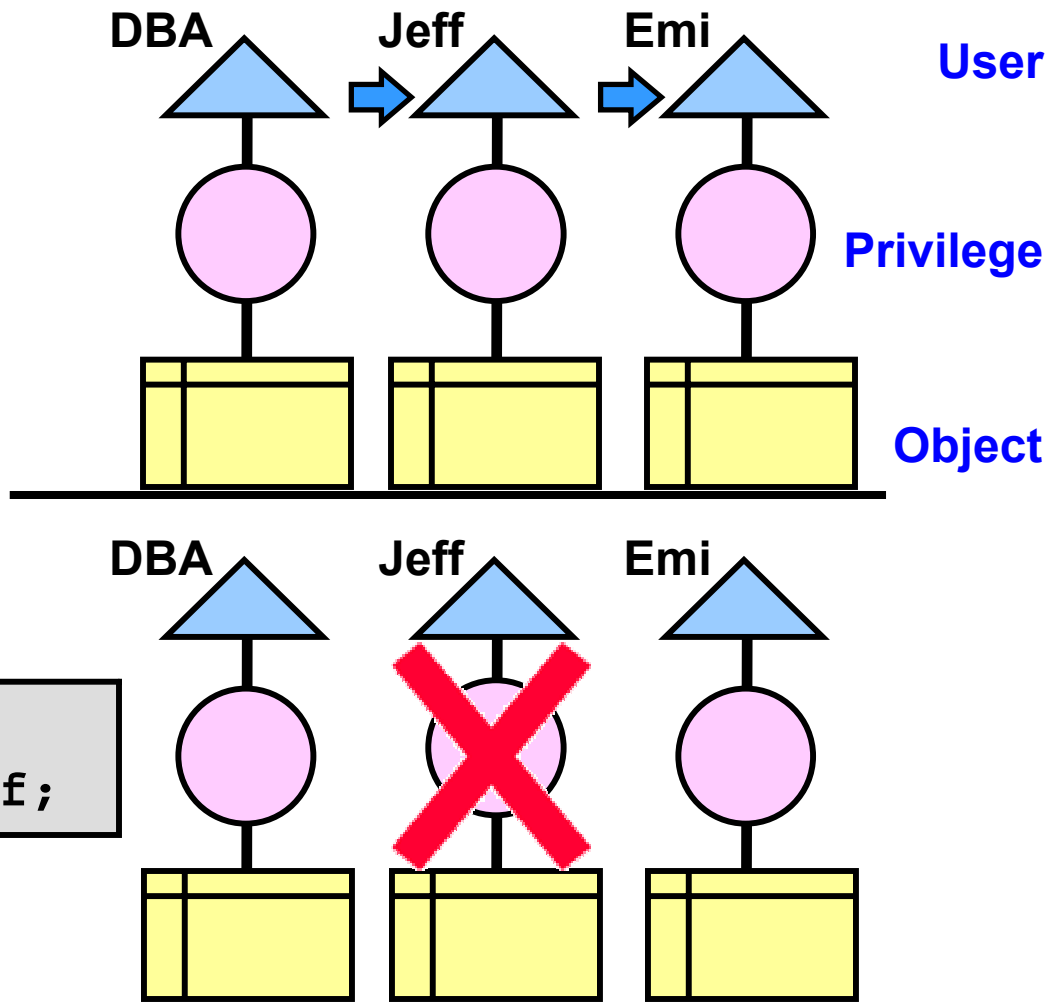
Object Privileges



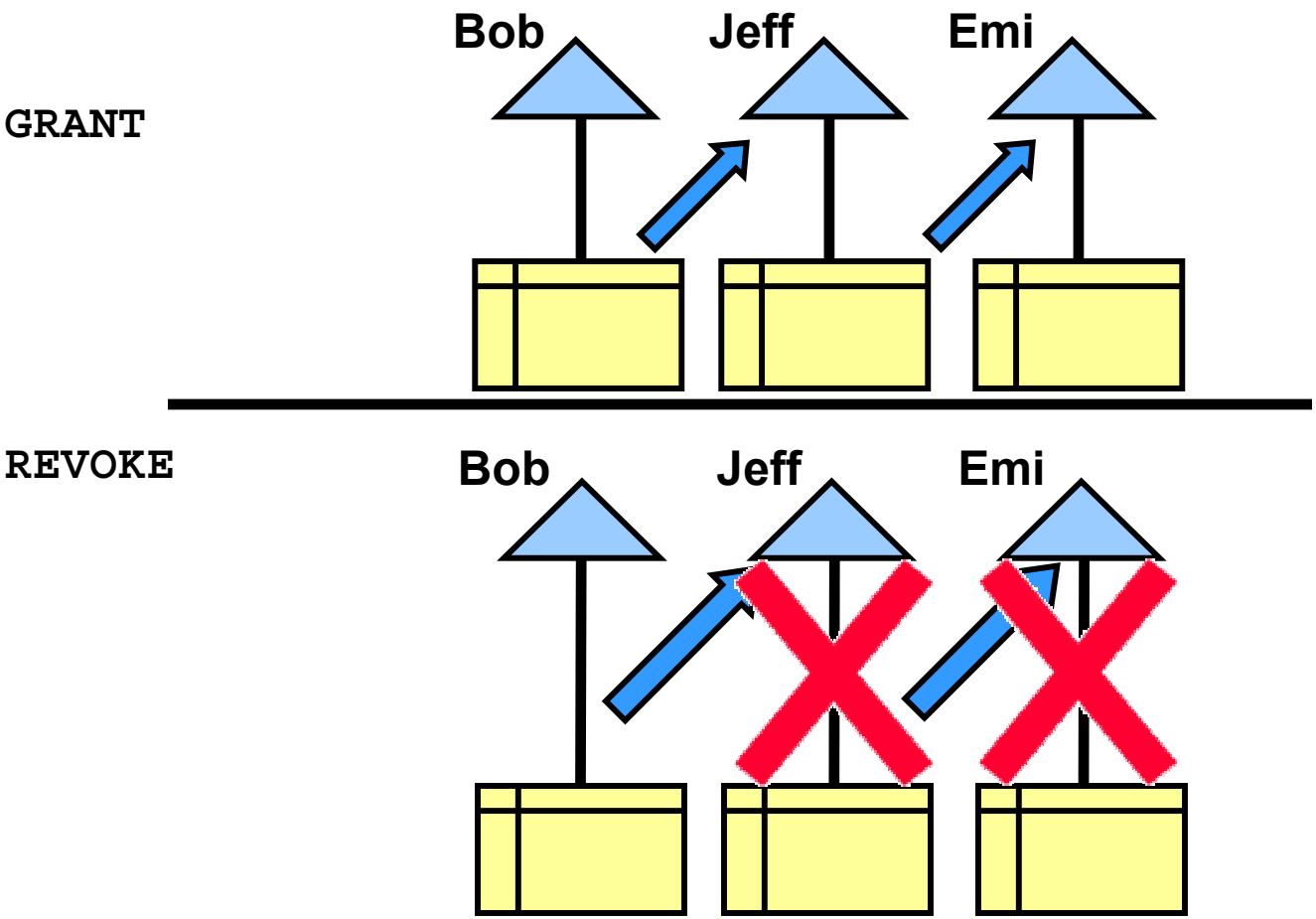
To grant object privileges, perform these tasks:

1. **Choose the object type.**
2. **Select objects.**
3. **Select privileges.**

Revoking System Privileges with ADMIN OPTION



Revoking Object Privileges with GRANT OPTION

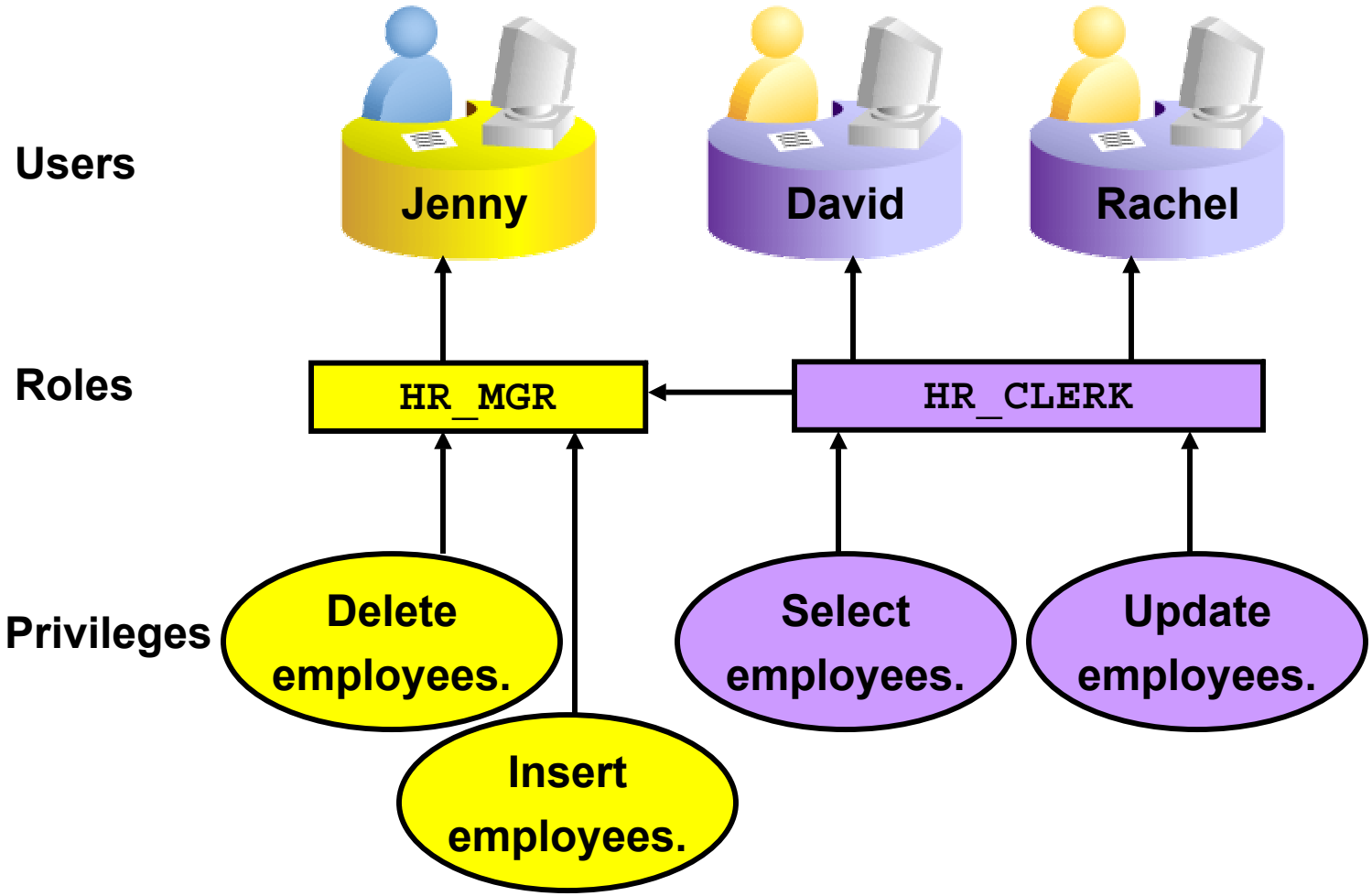


Benefits of Roles

User
Authentication
Privilege
> Role
Profile
PW Security
Quota

- Easier privilege management
- Dynamic privilege management
- Selective availability of privileges

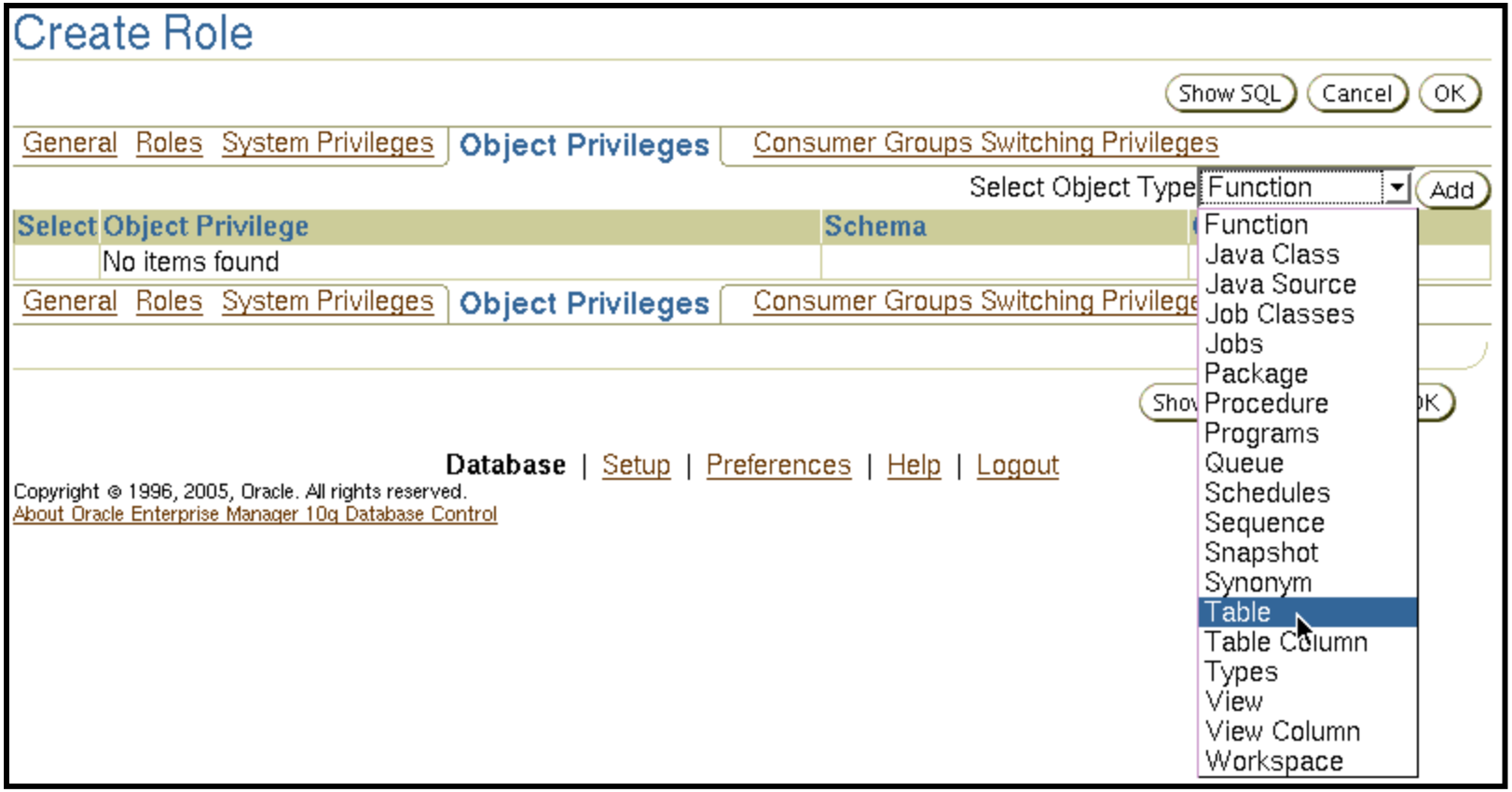
Assigning Privileges to Roles and Roles to Users



Predefined Roles

CONNECT	CREATE SESSION
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	Most system privileges, several other roles. Do not grant to nonadministrators.
SELECT_ CATALOG_ ROLE	No system privileges, but HS_ADMIN_ROLE and over 1,700 object privileges on the data dictionary

Creating a Role



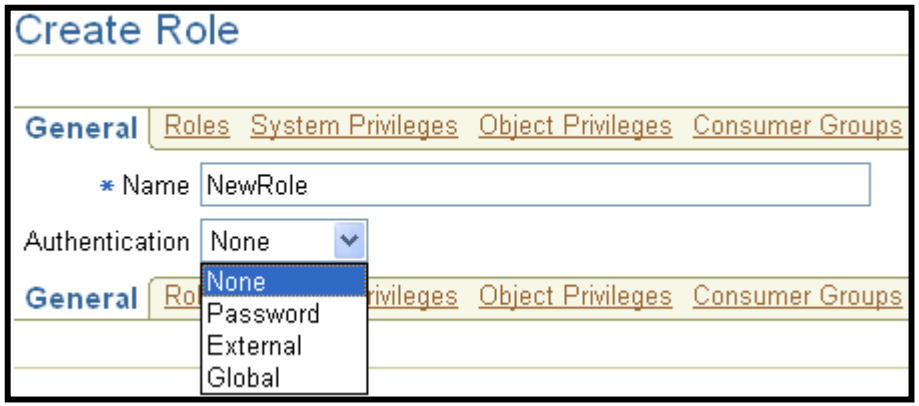
Select Administration > Schema > Users & Privileges > Roles.

Secure Roles

- **Roles may be nondefault.**

```
SET ROLE vacationdba;
```

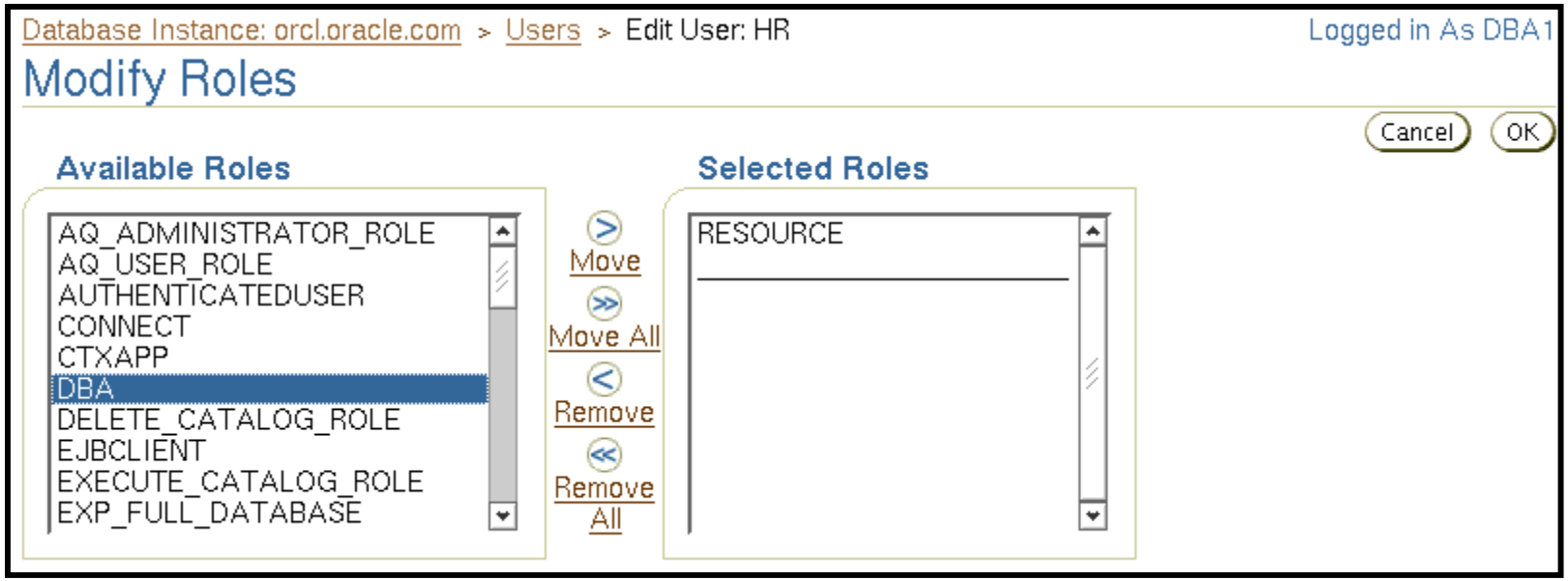
- **Roles may be protected through authentication.**



- **Roles may also be secured programmatically.**

```
CREATE ROLE secure_application_role
IDENTIFIED USING <security_procedure_name>;
```

Assigning Roles to Users



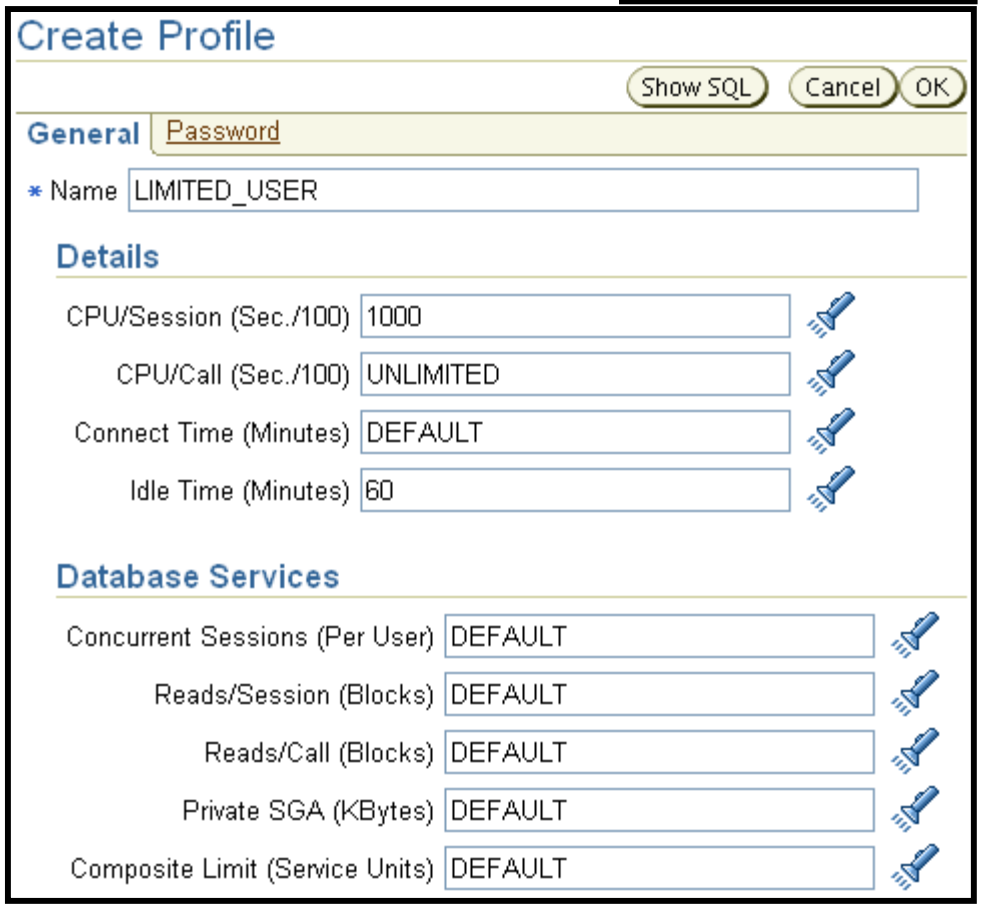
Profiles and Users

- User
- Authentication
- Privilege
- Role
- > Profile
- PW Security
- Quota

Users are assigned only one profile at any given time.

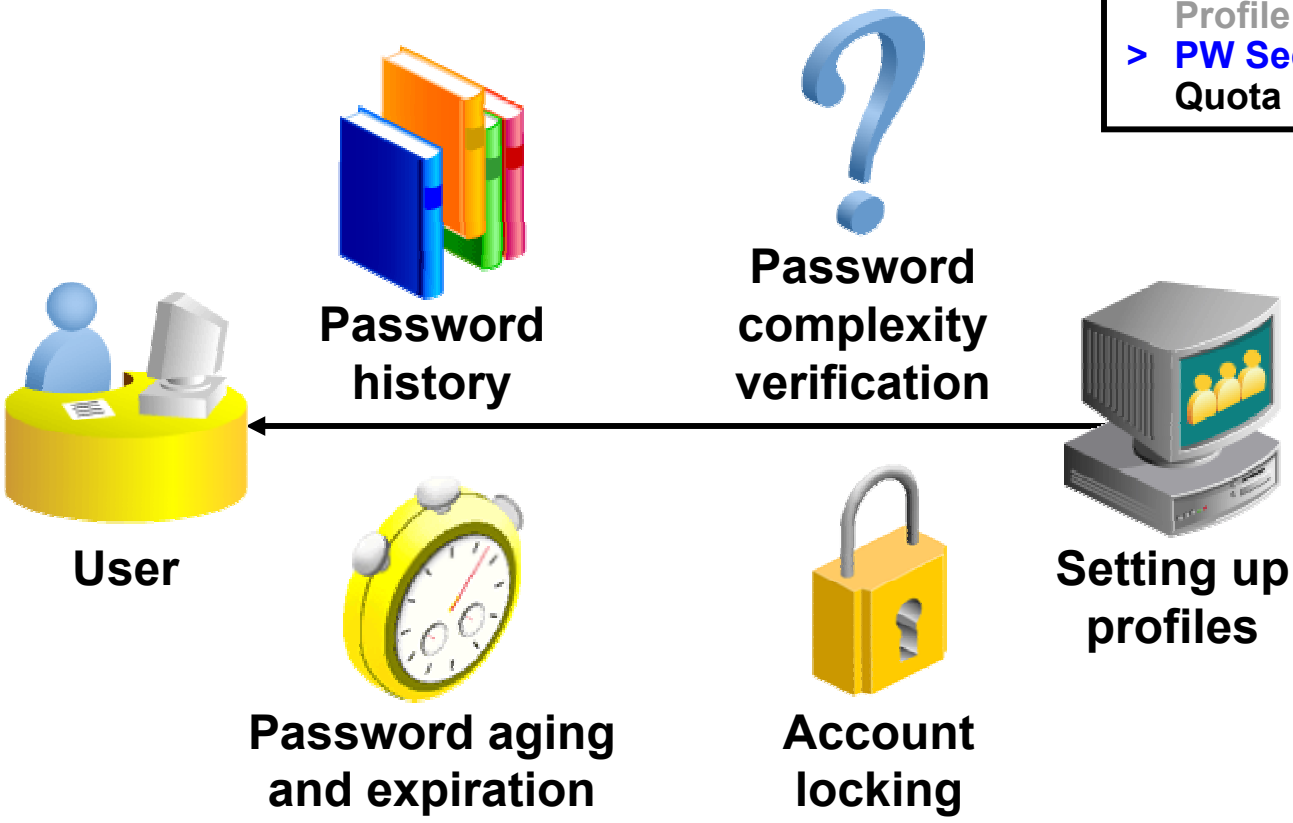
Profiles:

- **Control resource consumption**
- **Manage account status and password expiration**



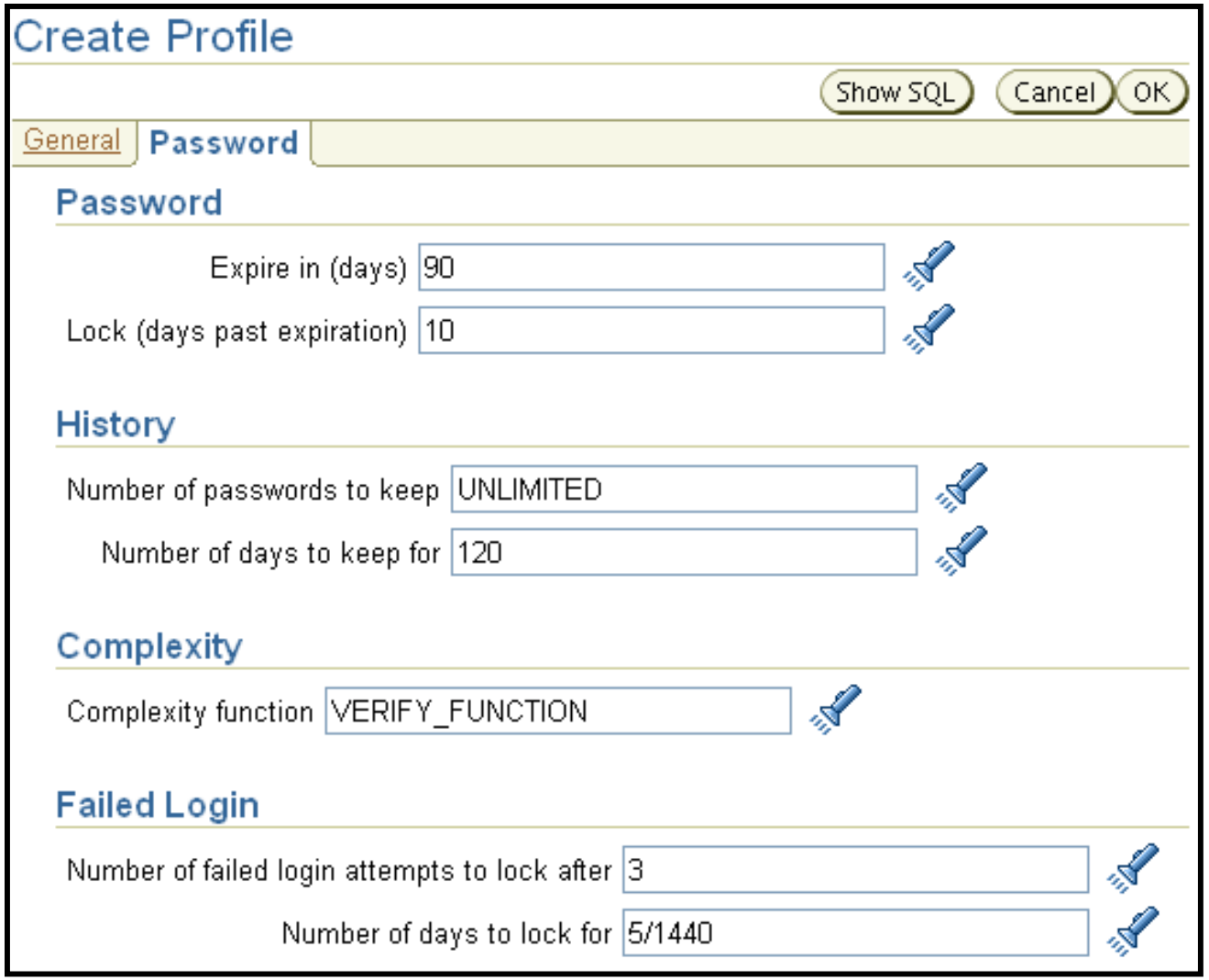
Implementing Password Security Features

- User
- Authentication
- Privilege
- Role
- Profile
- > PW Security
- Quota



Note: Do not use profiles that cause the passwords for `SYS`, `SYSMAN`, and `DBSNMP` to expire and, subsequently, cause those accounts to get locked.

Creating a Password Profile

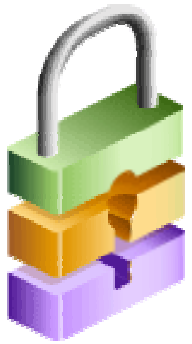


Supplied Password Verification Function: VERIFY_FUNCTION

The supplied password verification function enforces these password restrictions:

- The minimum length is four characters.
- The password cannot be the same as the username.
- The password must have at least one alphabetic, one numeric, and one special character.
- The password must differ from the previous password by at least three letters.

Tip: Use this function as a template to create your own customized password verification.

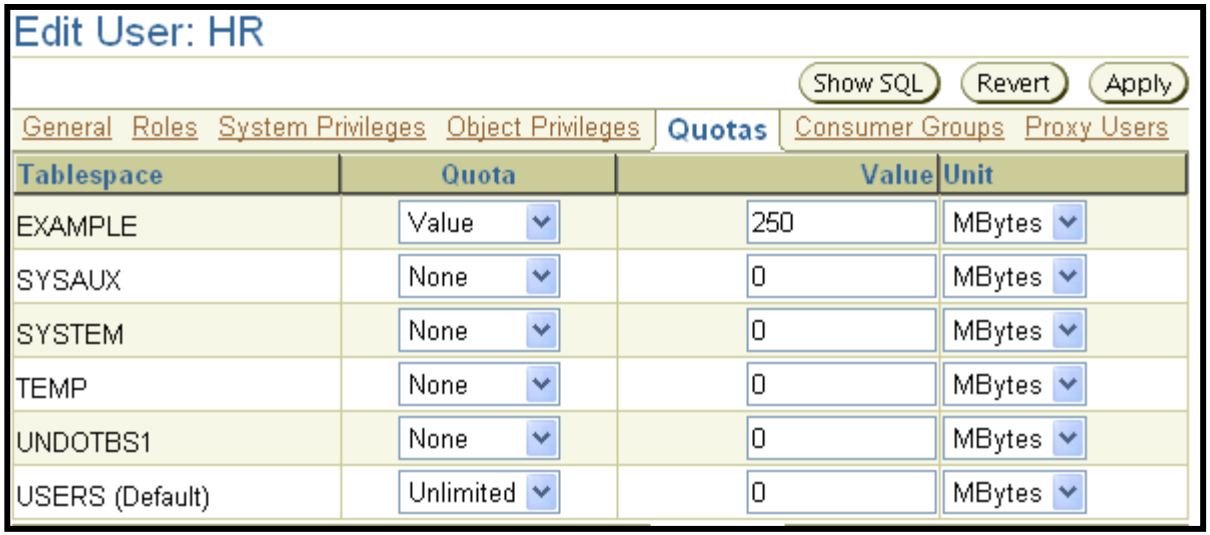


Assigning Quota to Users

- User Authentication
- Privilege
- Role
- Profile
- PW Security
- > Quota

Users who do not have the `UNLIMITED TABLESPACE` system privilege must be given a quota before they can create objects in a tablespace. Quotas can be:

- **A specific value in megabytes or kilobytes**
- **Unlimited**



Summary

In this lesson, you should have learned how to:

- Create and manage database user accounts
  - Authenticate users
  - Assign default storage areas (tablespaces)
- Grant and revoke privileges
- Create and manage roles
- Create and manage profiles
  - Implement standard password security features
  - Control resource usage by users

Practice Overview: Administering Users

This practice covers the following topics:

- Creating a profile to limit resource consumption
- Creating two roles:
  - `HRCLERK`
  - `HRMANAGER`
- Creating four new users:
  - One manager and two clerks
  - One schema user for the next practice session