

# 8

## **Administering User Security**

# Objectives

After completing this lesson, you should be able 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

# Database User Accounts

Each database user account has:

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



A schema:

- Is a collection of database objects that are owned by a database user
- Has the same name as the user account

# Predefined Administrative Accounts

- **SYS account:**
  - Is granted the DBA role, as well as several other roles.
  - Has all privileges with `ADMIN OPTION`
  - Is required for startup, shutdown, and some maintenance commands
  - Owns the data dictionary and the Automatic Workload Repository (AWR)
- **SYSTEM account is granted the DBA, MGMT\_USER, and AQ\_ADMINISTRATOR\_ROLE roles.**
- **DBSNMP account is granted the OEM\_MONITOR role.**
- **SYSMAN account is granted the MGMT\_USER, RESOURCE and SELECT\_CATALOG\_ROLE roles.**
- **These accounts are not used for routine operations.**

# Creating a User

Database Instance: orcl.oracle.com > Users > Logged in As SYS

## Create User

[Show SQL](#) [Cancel](#) [OK](#)

**General** [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Group Privileges](#) [Proxy Users](#)

\* Name

Profile


Authentication


\* Enter Password

\* Confirm Password

For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace  

Temporary Tablespace  

Status ☐ Locked ☒ Unlocked

[Show SQL](#)

[Return](#)

```
CREATE USER "MYDBA" PROFILE "DEFAULT" IDENTIFIED BY "*****" DEFAULT
TABLESPACE "USERS" TEMPORARY TABLESPACE "TEMP" ACCOUNT UNLOCK
GRANT "CONNECT" TO "MYDBA"
```

Select Server > Users, and then click the Create button.

# Authenticating Users

- Password
- External
- Global

**Edit User: HR**

Actions

**General** [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Group Privileges](#) [Proxy Users](#)

Name **HR**

Profile


Authentication


\* Enter Password

\* Confirm Password


For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace  

Temporary Tablespace  

Status ☐ Locked ☒ Unlocked



# 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:

- For `SYSDBA`, `SYSOPER`, and `SYSASM` connections:
  - DBA user by name is audited for password file and strong authentication methods
  - OS account name is audited for OS authentication
  - OS authentication takes precedence over password file authentication for privileged users
  - Password file uses case-sensitive passwords

# Unlocking a User Account and Resetting the Password

**Users**

Object Type:

**Search**

Enter an object name to filter the data that is displayed in your results set.

Object Name:

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode:

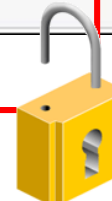
Select	UserName	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created
<input type="checkbox"/>	<a href="#">ANONYMOUS</a>	EXPIRED & LOCKED	Aug 3, 2007 1:34:38 AM MDT	<a href="#">SYSAUX</a>	<a href="#">TEMP</a>	DEFAULT	Aug 3, 2007 1:34:38 AM MDT
<input type="checkbox"/>	<a href="#">APEX_PUBLIC_USER</a>	EXPIRED & LOCKED	Aug 3, 2007 2:04:08 AM MDT	<a href="#">USERS</a>	<a href="#">TEMP</a>	DEFAULT	Aug 3, 2007 2:04:08 AM MDT
<input type="checkbox"/>	<a href="#">BI</a>	EXPIRED & LOCKED	Aug 4, 2008 7:04:49 PM MDT	<a href="#">USERS</a>	<a href="#">TEMP</a>	DEFAULT	Aug 4, 2008 7:04:49 PM MDT

Actions:       1-25 of 39

Lock User dropdown menu:

- Create Like
- Expire Password
- Generate DDL
- Lock User
- Unlock User**

**Select the user, select Unlock User, and click Go.**

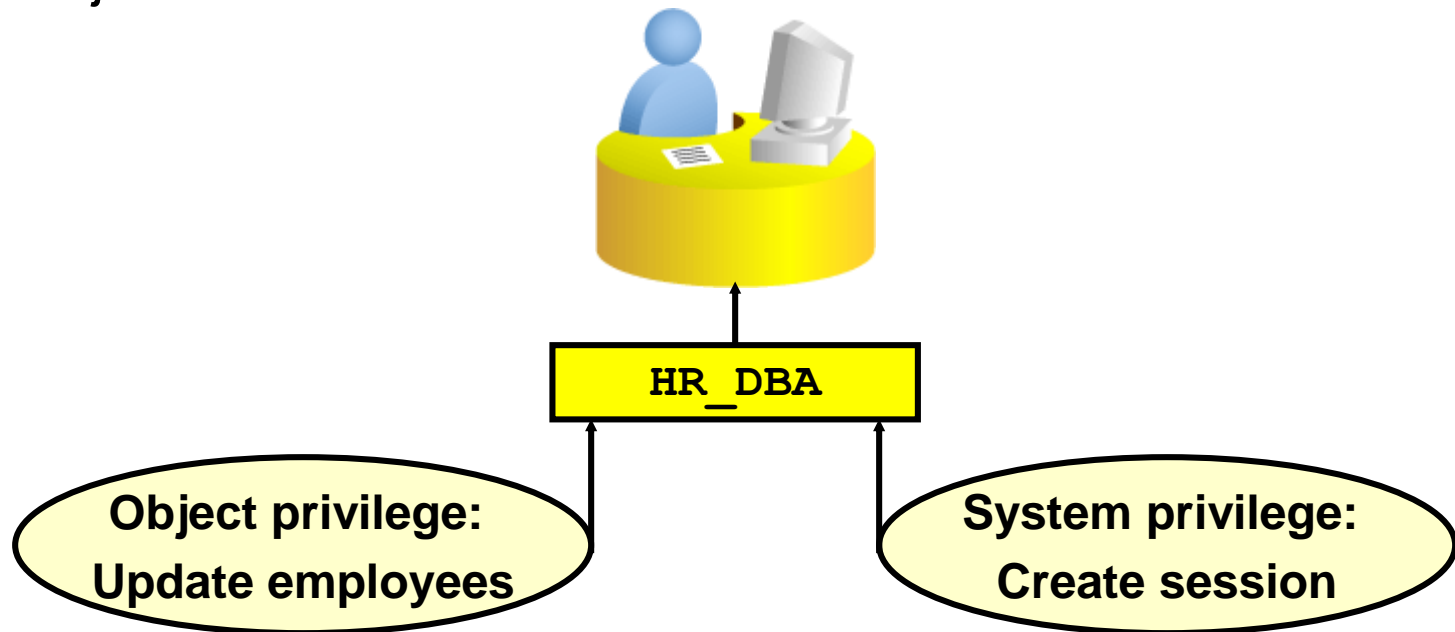




# Privileges

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

**Edit User: HR**

Actions: Create Like Go Show SQL Revert Apply

[General](#) [Roles](#) **System Privileges** [Object Privileges](#) [Quotas](#) [Consumer Group Privileges](#) [Proxy Users](#)

System Privilege	Admin Option
ALTER SESSION	<input type="checkbox"/>
CREATE DATABASE LINK	<input type="checkbox"/>
CREATE SEQUENCE	<input type="checkbox"/>
CREATE SESSION	<input type="checkbox"/>
CREATE SYNONYM	<input type="checkbox"/>
CREATE VIEW	<input type="checkbox"/>
UNLIMITED TABLESPACE	<input type="checkbox"/>

[Edit List](#)

### Modify System Privileges

Cancel OK

#### Available System Privileges

- ACCESS\_ANY\_WORKSPACE
- ADMINISTER ANY SQL TUNING SET
- ADMINISTER DATABASE TRIGGER
- ADMINISTER RESOURCE MANAGER
- ADMINISTER SQL MANAGEMENT OBJECT
- ADMINISTER SQL TUNING SET
- ADVISOR
- ALTER ANY ASSEMBLY
- ALTER ANY CLUSTER
- ALTER ANY CUBE

> [Move](#)

>> [Move All](#)

< [Remove](#)

<< [Remove All](#)

#### Selected System Privileges

- ALTER SESSION
- CREATE DATABASE LINK
- CREATE SEQUENCE
- CREATE SESSION
- CREATE SYNONYM
- CREATE VIEW
- UNLIMITED TABLESPACE

# Object Privileges

**Edit User: HR**

Actions: Create Like [Go] [Show SQL] [Revert] [Apply]

General Roles System Privileges **Object Privileges** Quotas Consumer Group Privileges Proxy Users

Select Object Type: Table [Add]

Delete

Select	Object Privilege	Schema	Object	Grant Option
<input type="checkbox"/>	EXECUTE	SYS	DBMS_STATS	

General Roles System Privileges **Object Privileges** Quotas

**Add Table Object Privileges**

Cancel OK

\* Select Table Objects

OE.CUSTOMERS, OE.INVENTORIES, OE.ORDERS, OE.ORDER\_ITEMS

(SchemaName.Table,...)  
Select object and then choose privileges to assign

**Available Privileges**

- ALTER
- DELETE
- INDEX
- INSERT
- REFERENCES
- UPDATE

Move Move All Remove Remove All

**Selected Privileges**

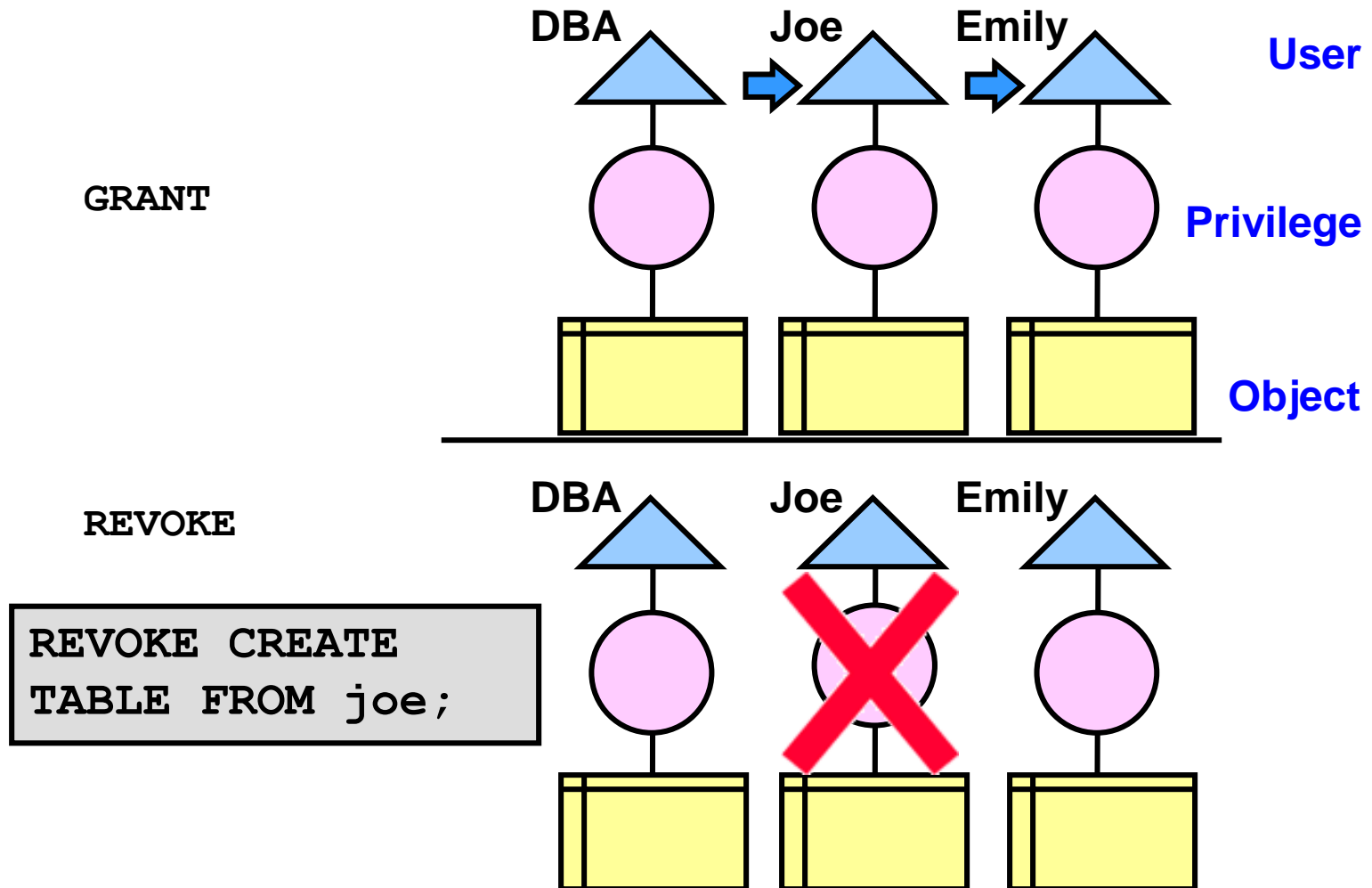
- SELECT

Search and select objects.

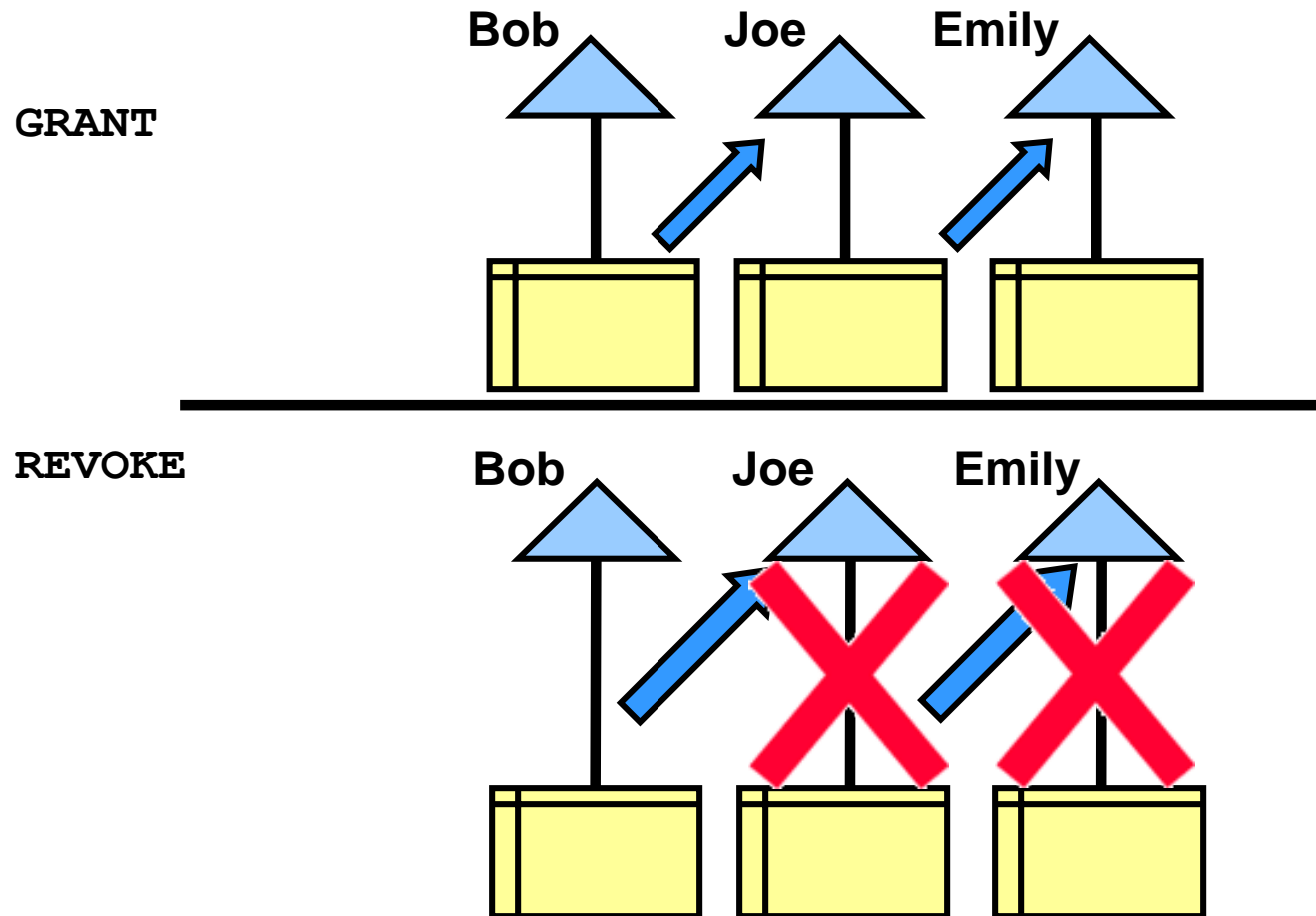
To grant object privileges:

- Choose the object type.
- Select objects.
- Select privileges.

# Revoking System Privileges with ADMIN OPTION



# Revoking Object Privileges with GRANT OPTION

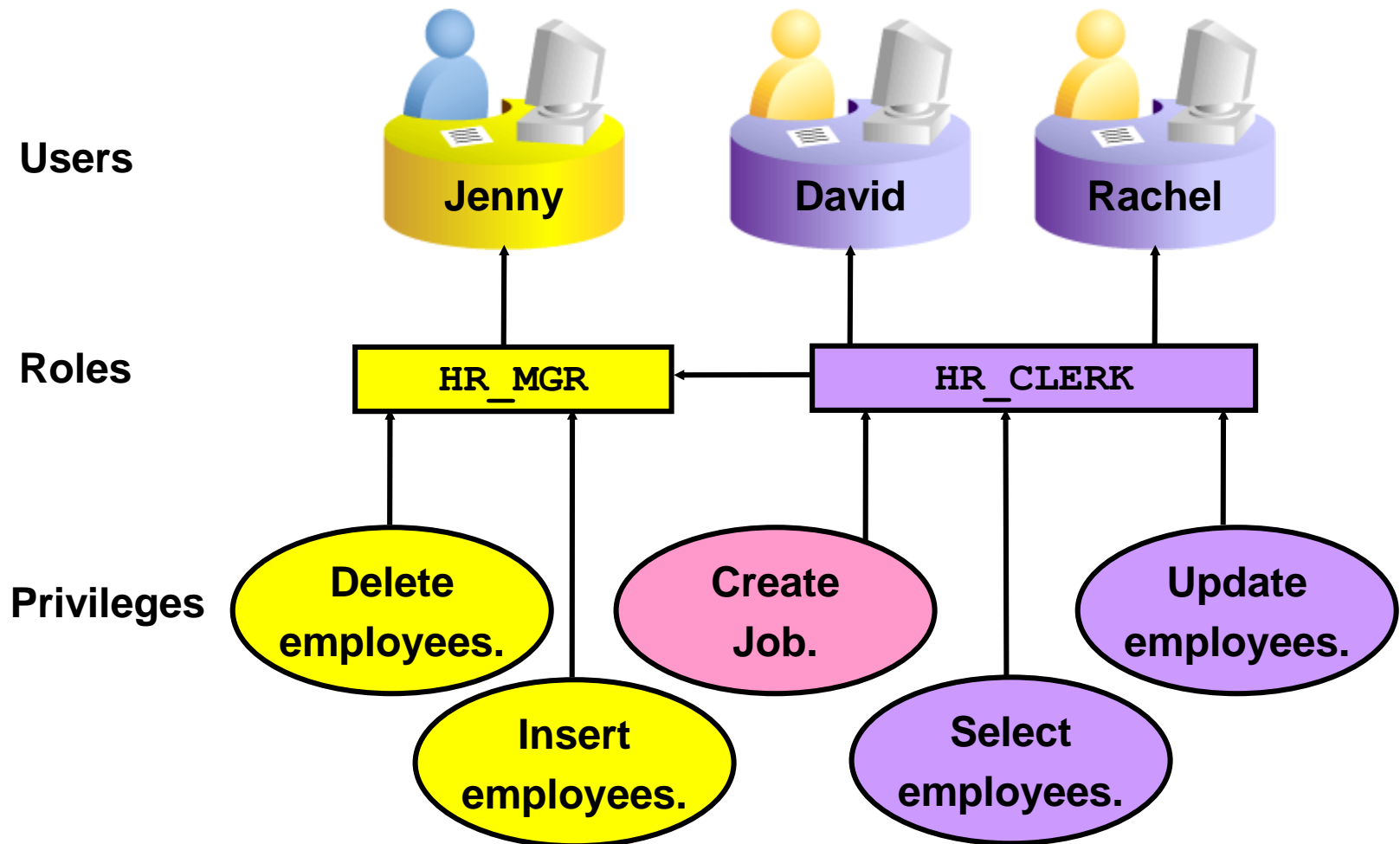


# Benefits of Roles

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



# Assigning Privileges to Roles and Assigning Roles to Users



# Predefined Roles

Role	Privileges Included
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; HS_ADMIN_ROLE and over 1,700 object privileges on the data dictionary



# Creating a Role

Select Server > Roles.

Add privileges and roles from the appropriate tab.

Click OK when finished.

**Create Role**

General Roles System Privileges Object Privileges Consumer Group Privileges

\* Name **OE\_READER**

Authentication None

There is no authentication.

Show SQL Cancel OK

**Create Role**

General Roles System Privileges **Object Privileges** Consumer Group Privileges

Select Object Type Table Add

Delete

Select	Object Privilege	Schema	Object
<input checked="" type="radio"/>	SELECT	OE	CUSTOMERS
<input type="radio"/>	SELECT	OE	INVENTORIES
<input type="radio"/>	SELECT	OE	ORDERS
<input type="radio"/>	SELECT	OE	ORDER_ITEMS

# Secure Roles

- Roles can be nondefault and enabled when required.

```
SET ROLE vacationdba;
```

- Roles can be protected through authentication.



- Roles can also be secured programmatically.

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

# Assigning Roles to Users

**Edit User: BERNST**

Actions

[General](#) **[Roles](#)** [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Group Privileges](#) [Proxy Users](#)

Role	Admin Option	Default
CONNECT	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Modify Roles**

**Available Roles**

- JAVA\_DEPLOY
- JMXSERVER
- LOGSTDBY\_ADMINISTRATOR
- MGMT\_USER
- OEM\_ADVISOR
- OEM\_MONITOR
- OE\_READER**
- OLAPI\_TRACE\_USER
- OLAP\_DBA
- OLAP\_USER

**Selected Roles**

- CONNECT



# Quiz

All passwords created in Oracle Database 11g are not case-sensitive by default.

1. True
2. False

# Quiz

A database role:

1. Can be enabled or disabled
2. Can consist of system and object privileges
3. Is owned by its creator
4. Cannot be protected by a password

# Profiles and Users

Users are assigned only one profile at a time.

Profiles:

- Control resource consumption
- Manage account status and password expiration





**Create Profile**

Show SQL Cancel OK






**General** Password

\* Name LIMITED\_USER

**Details**

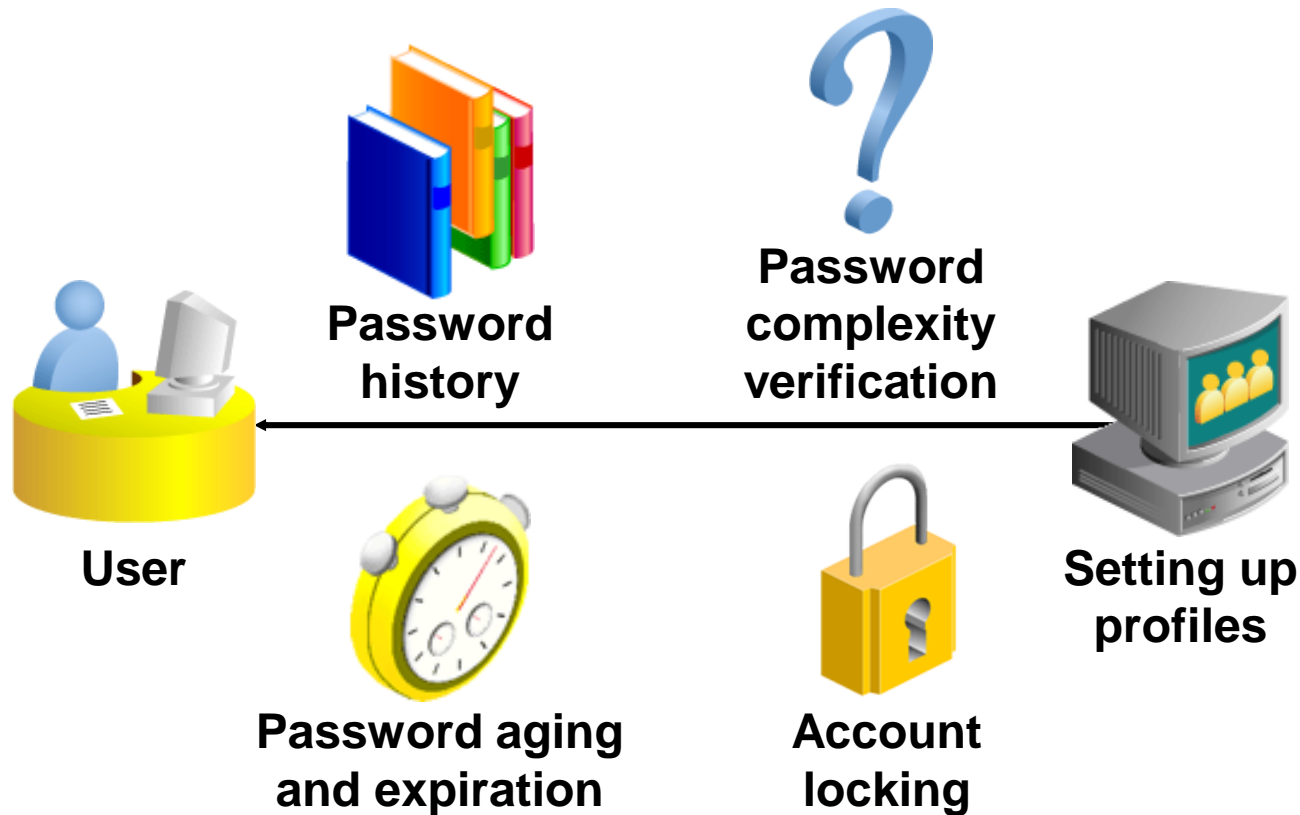
CPU/Session (Sec./100)	1000	
CPU/Call (Sec./100)	UNLIMITED	
Connect Time (Minutes)	DEFAULT	
Idle Time (Minutes)	60	

**Database Services**

Concurrent Sessions (Per User)	DEFAULT	
Reads/Session (Blocks)	DEFAULT	
Reads/Call (Blocks)	DEFAULT	
Private SGA (KBytes)	DEFAULT	
Composite Limit (Service Units)	DEFAULT	

**Note: RESOURCE\_LIMIT must be set to TRUE before profiles can impose resource limitations.**

# Implementing Password Security Features



**Note: Do not use profiles that cause the SYS, SYSMAN, and DBSNMP passwords to expire and the accounts to be locked.**

# Creating a Password Profile

**Create Profile**

Show SQLCancelOK

General

Password

**Password**

Expire in (days)90

Lock (days past expiration)10

**History**

Number of passwords to keep2

Number of days to keep forUNLIMITED

**Complexity**

Complexity functionVERIFY\_FUNCTION\_11G

**Failed Login**

Number of failed login attempts to lock after3

Number of days to lock for5/1440



# Supplied Password Verification Function: `VERIFY_FUNCTION_11G`

The `VERIFY_FUNCTION_11G` function insures that the password is:

- At least eight characters
- Different from the username, username with a number, or username reversed
- Different from the database name or the database name with a number
- A string with at least one alphabetic and one numeric character
- Different from the previous password by at least three letters

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



# Assigning Quotas to Users

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

**Edit User: BERNST**

Actions:

[General](#) [Roles](#) [System Privileges](#) [Object Privileges](#) **Quotas** [Consumer Group Privileges](#)

Tablespace	Quota	Value	Unit
EXAMPLE	<input type="text" value="Value"/> <input type="button" value="v"/>	<input type="text" value="20"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
INVENTORY	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
SYSAUX	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
SYSTEM	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
TEMP	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
UNDOTBS1	<input type="text" value="None"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>
USERS (Default)	<input type="text" value="Unlimited"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="MBytes"/> <input type="button" value="u"/>

# Applying the Principle of Least Privilege

- Protect the data dictionary:

```
O7_DICTIONARY_ACCESSIBILITY=FALSE
```

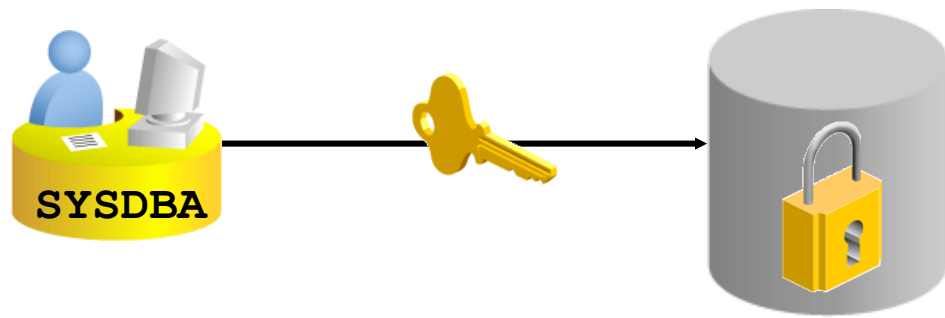
- Revoke unnecessary privileges from PUBLIC.
- Use access control lists (ACL) to control network access.
- Restrict the directories accessible by users.
- Limit users with administrative privileges.
- Restrict remote database authentication:

```
REMOTE_OS_AUTHENT=FALSE
```

# Protect Privileged Accounts

Privileged accounts can be protected by:

- Using password file with case-sensitive passwords
- Enabling strong authentication for administrator roles



# Quiz

Applying the principle of least privilege is not enough to harden the Oracle database.

1. True
2. False

# Quiz

With `RESOURCE_LIMIT` set at its default value of `FALSE`, profile password limitations are ignored.

1. True
2. False

# 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 8 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