



Oracle 11g DBA Fundamentals Overview

Lesson 11: Managing Users and
Securing the Database

Objectives



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
- 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.

Create User

Show SQL Cancel OK

[General](#) [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Groups](#) [Switching Privileges](#) [Proxy Users](#)

* Name

DHAMBY

Profile

HRPROFILE

Authentication

Password

* Enter Password

* Confirm Password

For Password choice, the role is authorized via password.

☒ Expire Password now

Default Tablespace

Temporary Tablespace

Status ☐ Locked ☒ Unlocked

Authenticating Users



Password
External
Global



User
> Authentication
Privilege
Role
Profile
PW Security
Quota

Edit User: HR

Actions Create Like Go Show SQL Revert Apply

General [Roles](#) [System Privileges](#) [Object Privileges](#) [Quotas](#) [Consumer Groups](#) [Switching Privileges](#) [Proxy Users](#)

Name **HR**

Profile DEFAULT

Authentication Password

* Enter Password Password

* Confirm Password External

Global

For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace USERS

Temporary Tablespace TEMP

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

- 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

Edit View Delete Actions Create Like Go							
Previous							
Select	UserName ▲	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	
<input type="radio"/>	ANONYMOUS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	May 2, 2005 3:57:07 PM PST
<input type="radio"/>	BI	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	USERS	TEMP	DEFAULT	May 2, 2005 3:20:28 PM PDT
<input type="radio"/>	CTXSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:56:15 PM PST
<input type="radio"/>	DBSNMP	OPEN		SYSAUX	TEMP	MONITORING_PROFILE	Mar 15, 2005 3:47:59 PM PST
<input type="radio"/>	DHAMBY	OPEN		USERS	TEMP	HRPROFILE	May 5, 2005 8:43:27 PM PDT
<input type="radio"/>	DIP	EXPIRED & LOCKED		USERS	TEMP	DEFAULT	Mar 15, 2005 3:36:04 PM PST
<input type="radio"/>	DMSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:55:30 PM PST
<input type="radio"/>	EXFSYS	EXPIRED & LOCKED	May 2, 2005 3:24:45 PM PDT	SYSAUX	TEMP	DEFAULT	Mar 15, 2005 3:54:58 PM PST
<input type="radio"/>	HR	OPEN		USERS	TEMP	DEFAULT	May 2, 2005 3:20:27 PM PDT

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

Select the user, and click Unlock User.



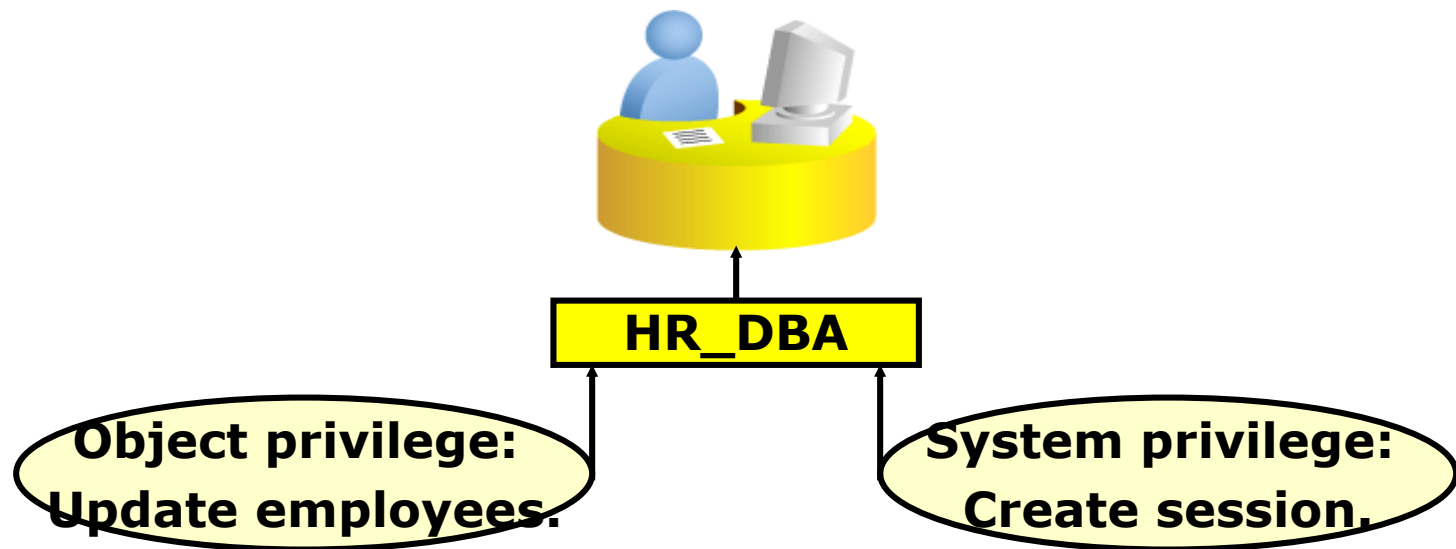
Privileges



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

User
Authentication
> Privilege
Role
Profile
PW Security
Quota



System Privileges



Edit User: HR

Actions

[General](#) [Roles](#) **[System Privileges](#)** [Object Privileges](#) [Quotas](#) [Consumer Groups](#) [Switching 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"/>

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

Modify System Privileges

Available System Privileges

- ACCESS_ANY_WORKSPACE
- ADMINISTER_ANY_SQL_TUNING_SET
- ADMINISTER_DATABASE_TRIGGER
- ADMINISTER_RESOURCE_MANAGER
- ADMINISTER_SQL_TUNING_SET
- ADVISOR
- ALTER_ANY_CLUSTER
- ALTER_ANY_DIMENSION
- ALTER_ANY_EVALUATION_CONTEXT
- ALTER_ANY_INDEX

Selected System Privileges

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



Object Privileges

Object Privileges | Quotas | Consumer Groups | Switching Privileges | Proxy Users

Select Object Type: **Function** | Add

- Function
- Java Class
- Java Source
- Job Classes
- Jobs
- Package
- Procedure
- Programs
- Queue
- Schedules
- Sequence
- Snapshot
- Synonym
- Table**

Add Table Object Privileges

Select Table Objects: OE.CUSTOMERS, OE.INVENTORIES, OE.ORDERS

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

Available Privileges

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

Selected Privileges

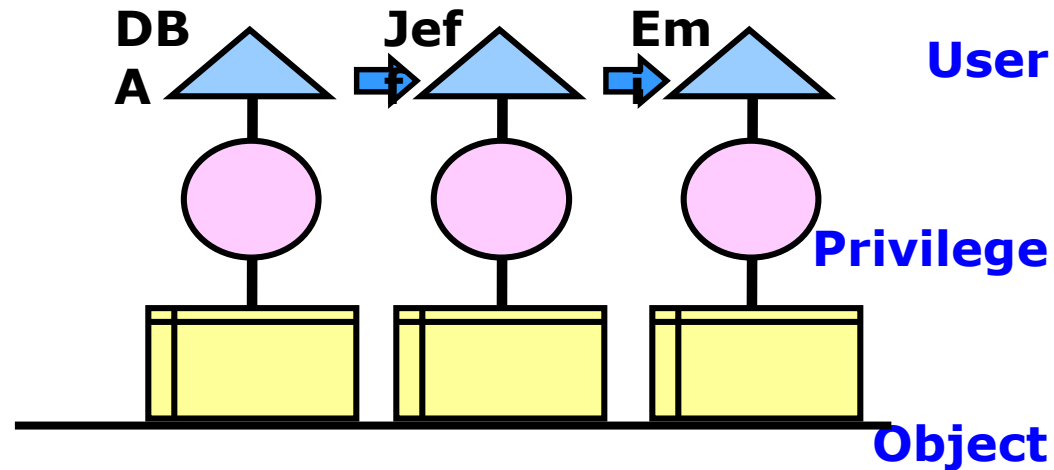
- SELECT**

- To grant object privileges, perform these tasks:
 1. Choose the object type.
 2. Select objects.
 3. Select privileges.



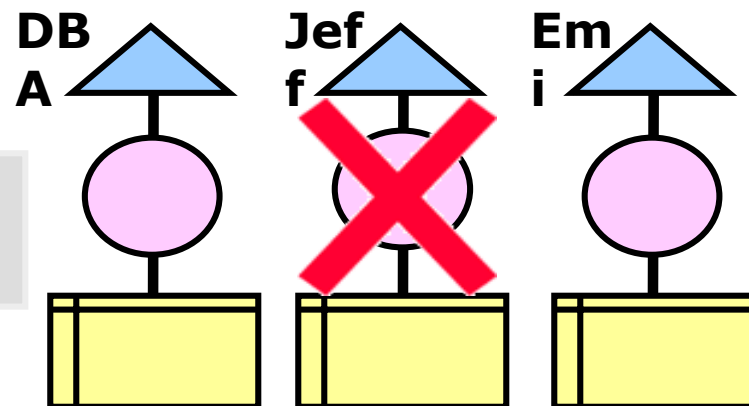
Revoking System Privileges with ADMIN OPTION

GRANT

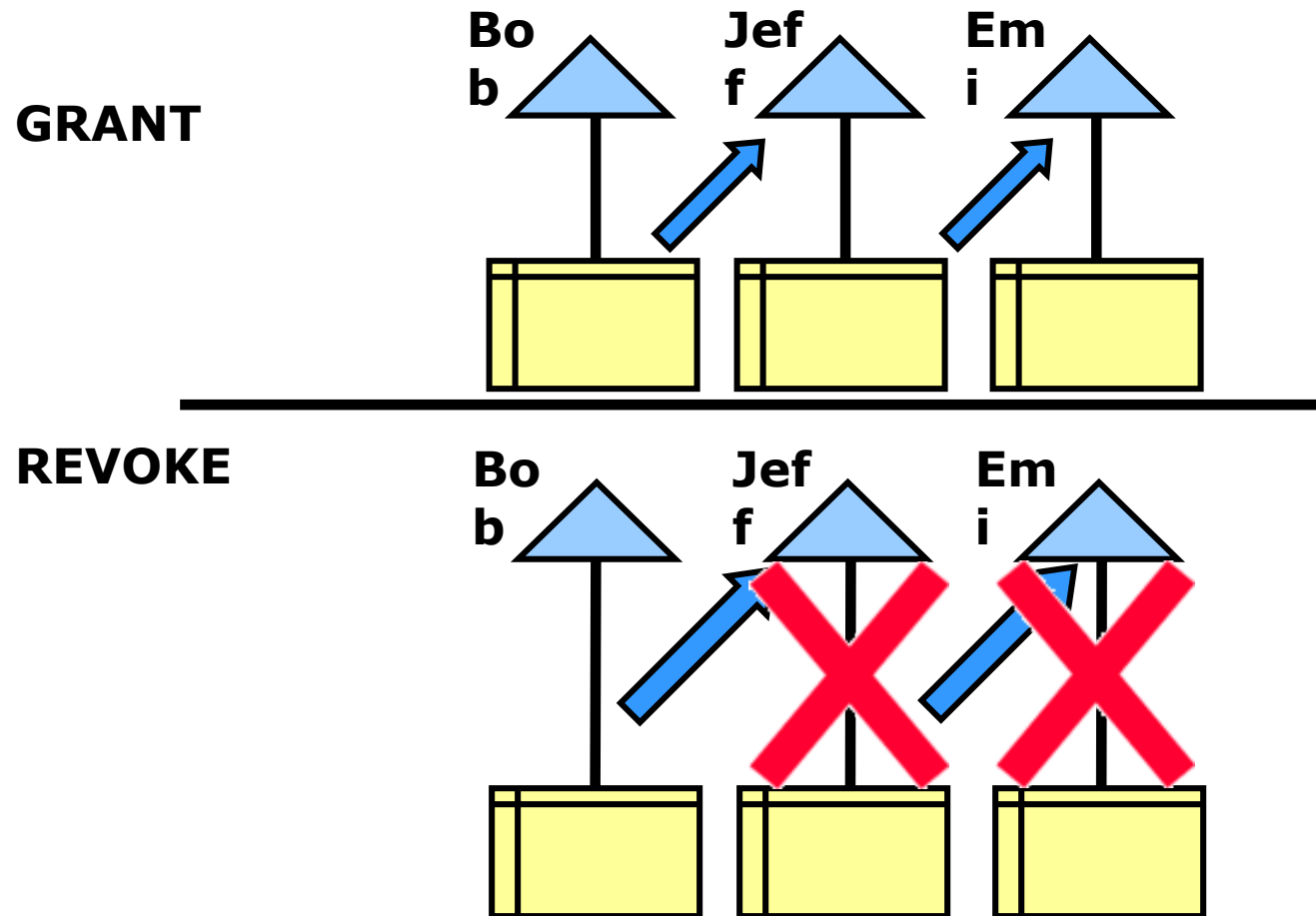


REVOKE

**REVOKE CREATE
TABLE FROM jeff;**



Revoking Object Privileges with GRANT OPTION



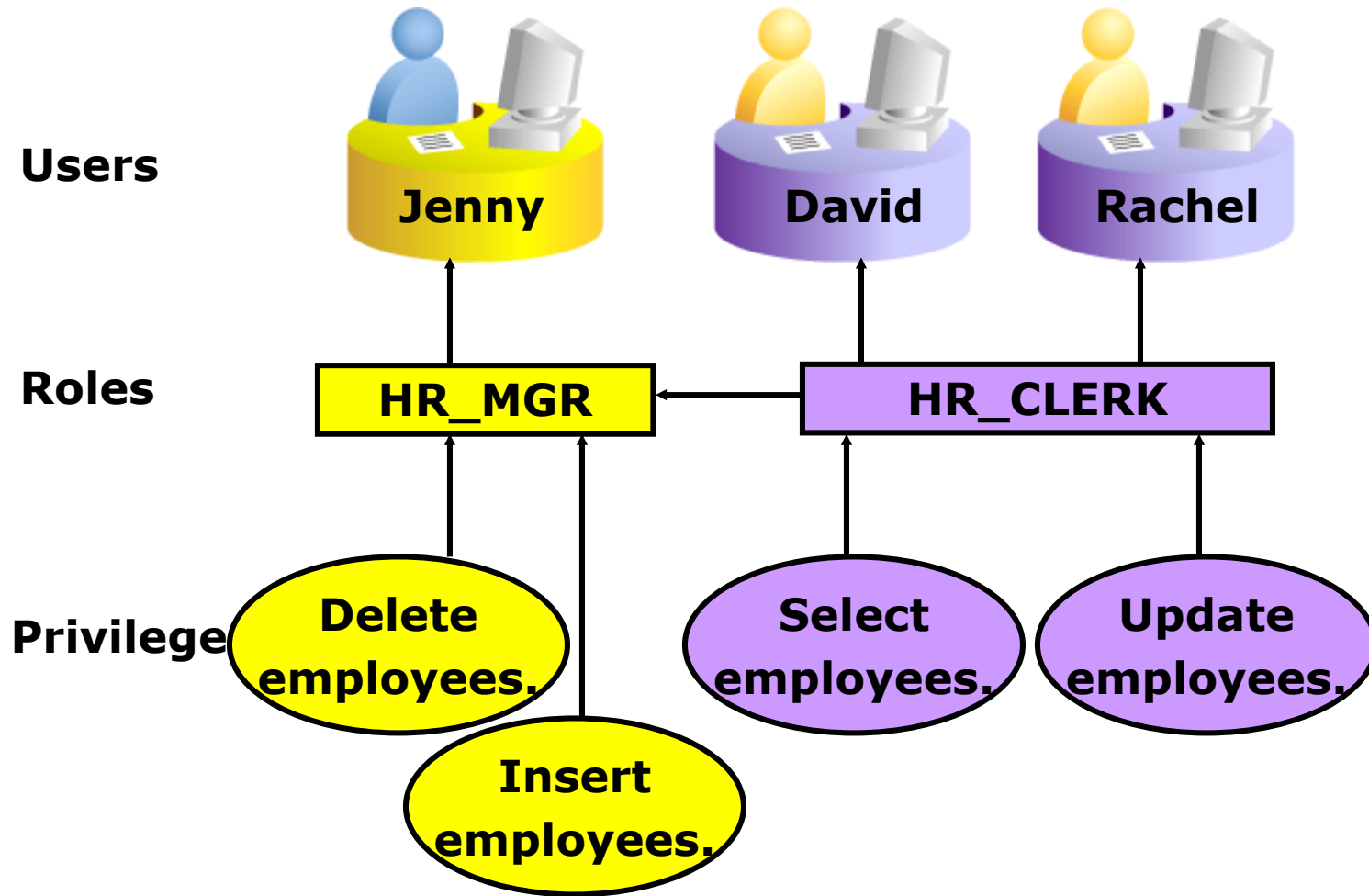
Benefits of Roles



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.

Create Role

Show SQL Cancel OK

General Roles System Privileges **Object Privileges** Consumer Groups Switching Privileges

Select Object Type Function Add

Select	Object Privilege	Schema
	No items found	

General Roles System Privileges **Object Privileges** Consumer Groups Switching Privileges

Show SQL OK

Database | Setup | Preferences | Help | Logout

Copyright © 1996, 2005, Oracle. All rights reserved.
[About Oracle Enterprise Manager 10g Database Control](#)

- Function
- Java Class
- Java Source
- Job Classes
- Jobs
- Package
- Procedure
- Programs
- Queue
- Schedules
- Sequence
- Snapshot
- Synonym
- Table**
- Table Column
- Types
- View
- View Column
- Workspace



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



Database Instance: orcl.oracle.com > Users > Edit User: HR Logged in As DBA1

Modify Roles

Cancel OK

Available Roles

- AQ_ADMINISTRATOR_ROLE
- AQ_USER_ROLE
- AUTHENTICATEDUSER
- CONNECT
- CTXAPP
- DBA**
- DELETE_CATALOG_ROLE
- EJBCLIENT
- EXECUTE_CATALOG_ROLE
- EXP_FULL_DATABASE

>

 Move

>>

 Move All

<

 Remove

<<

 Remove All

Selected Roles

- RESOURCE





Profiles and Users

Users are assigned only one profile at any given time.

Profiles:

- Control resource consumption
- Manage account status and password expiration

User
Authentication
Privilege
Role
> Profile
PW Security
Quota

Create Profile

Show SQLCancelOK

General Password

* Name LIMITED_USER

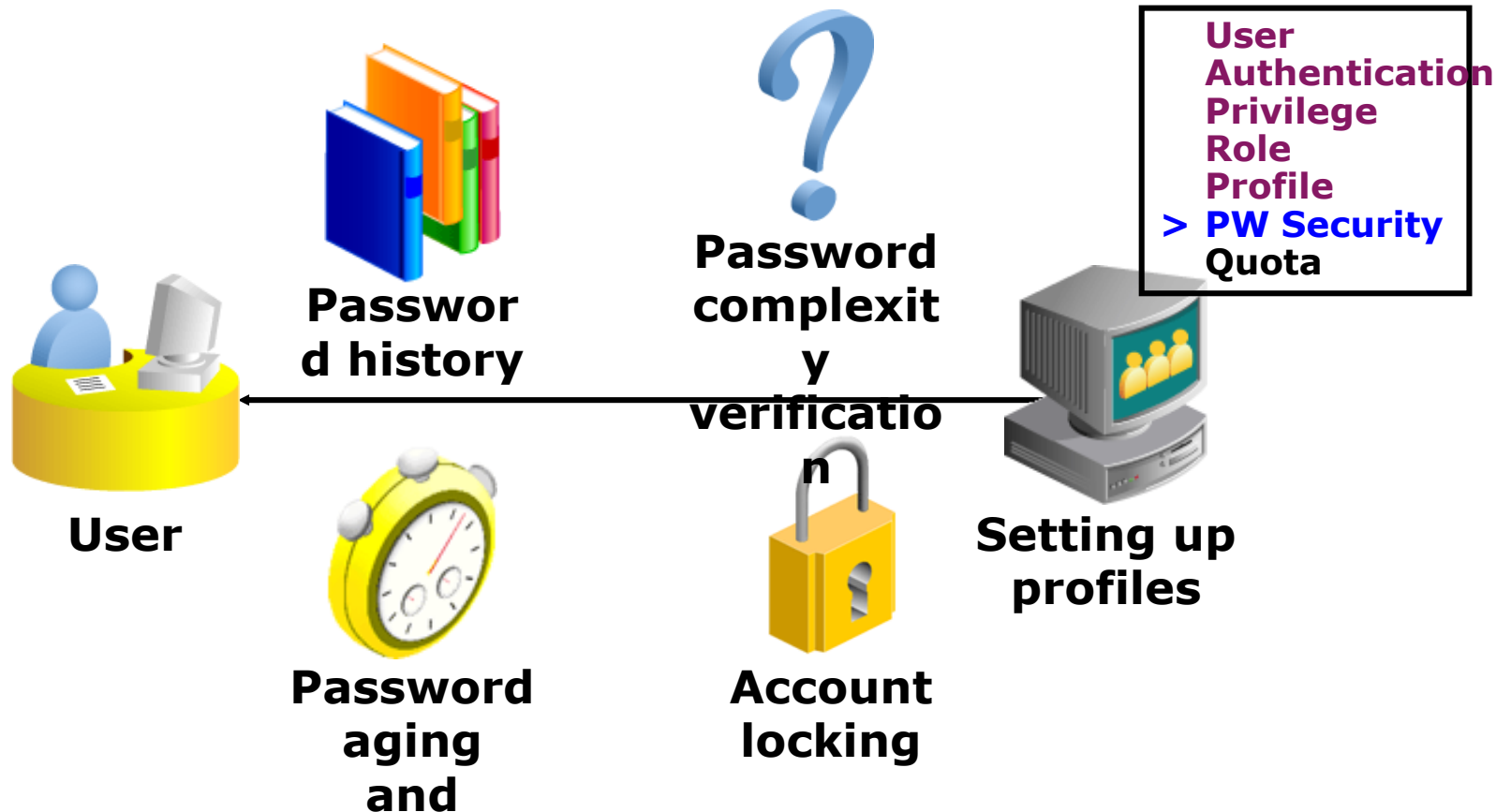
Details

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	

Implementing Password Security Features



Note: Do not use profiles that cause the SYS, SYSMAN, and DBSNMP passwords to expire and the accounts to get 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 keepUNLIMITED

Number of days to keep for120

Complexity

Complexity functionVERIFY_FUNCTION

Failed Login

Number of failed login attempts to lock after3

Number of days to lock for5/1440



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

Edit User: HR

Show SQLRevertApply

GeneralRolesSystem PrivilegesObject Privileges**Quotas**Consumer GroupsProxy Users

Tablespace	Quota	Value	Unit
EXAMPLE	Value <input type="text" value="250"/>	250	MBytes <input type="text" value="M"/>
SYSAUX	None <input type="text" value="None"/>	0	MBytes <input type="text" value="M"/>
SYSTEM	None <input type="text" value="None"/>	0	MBytes <input type="text" value="M"/>
TEMP	None <input type="text" value="None"/>	0	MBytes <input type="text" value="M"/>
UNDOTBS1	None <input type="text" value="None"/>	0	MBytes <input type="text" value="M"/>
USERS (Default)	Unlimited <input type="text" value="Unlimited"/>	0	MBytes <input type="text" value="M"/>

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