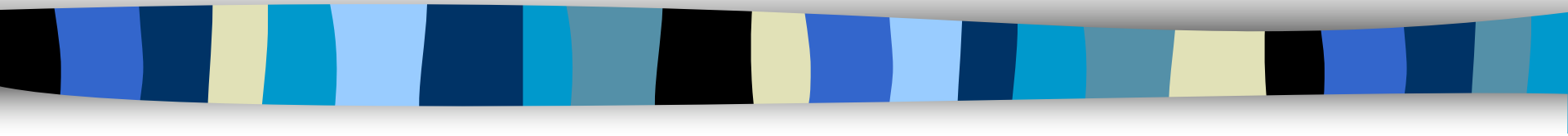
Database Security and Auditing: Protecting Data Integrity and Accessibility



Chapter 3
Administration of Users

Objectives

- Importance of administration documentation
- Concept of operating system authentication
- User Administration using both Oracle and SQL Server
  - Create and remove users and logins
  - Modify an existing user using both Oracle and SQL servers
  - List all default users on Oracle and SQL servers
- Describe best practices for user administration

Documentation of User Administration

- Part of the administration process
- Reasons to document:
  - Provide a paper trail
  - Ensure administration consistency
- What to document:
  - Administration policies, staff and management
  - Security procedures
  - Procedure implementation scripts or programs
  - Predefined roles description

Documentation of User Administration (continued)

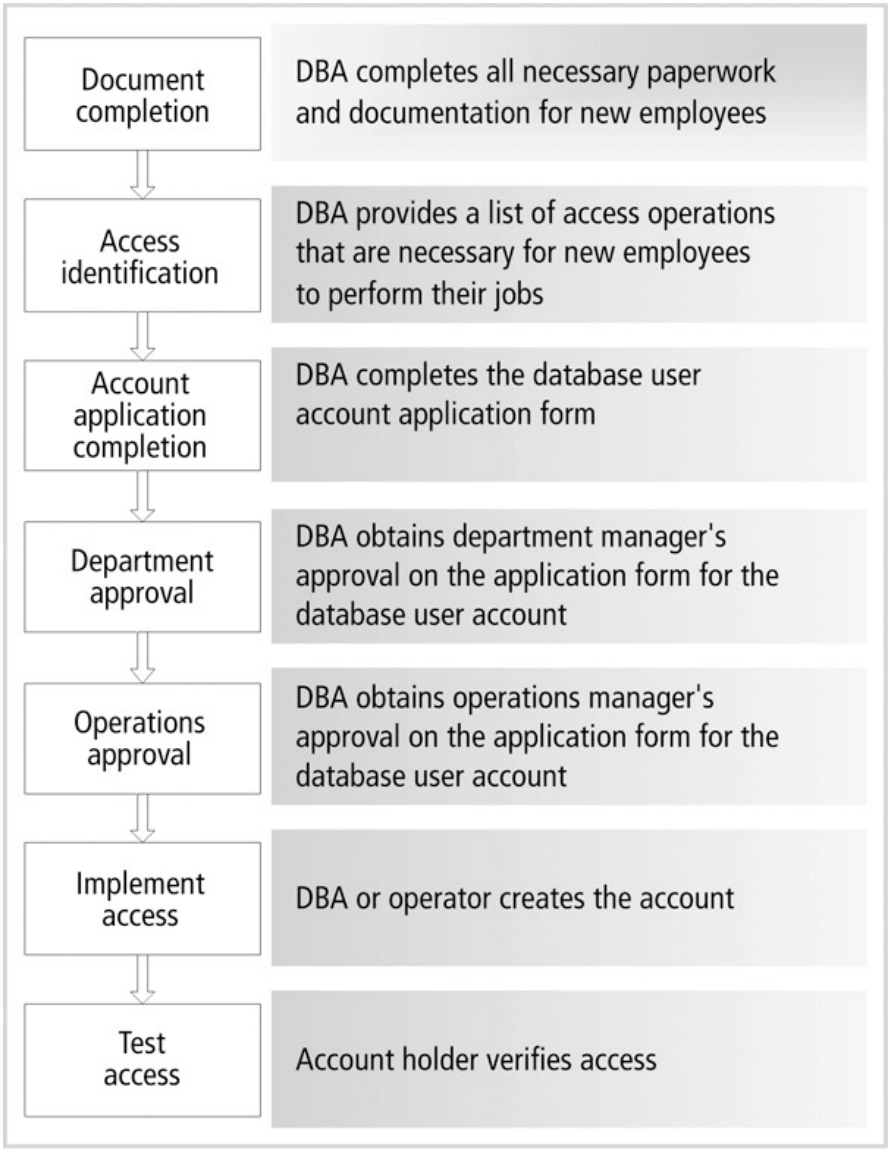


FIGURE 3-1 Database account access procedure

Documentation of User Administration (continued)

Acme Pharmaceutical Company
Database User Account Form

Requested For	
Name (First, MI, Last)	
Employee Type	☐ Employee ☐ Contractor ☐ Temporary ☐ Intern
Title	
Employee# (if available)	

Requested By			
Name (First, MI, Last)			
E-mail		Telephone Ext.	

Date			
Requested		Expected	

Action
☐ Add ☐ Modify ☐ Password Change ☐ Lock ☐ Unlock ☐ Remove

Location & Department	
Location	
Department	

Database Application

Database Role			
☐ Operations Manager	☐ Business Manager	☐ Analyst	☐ Administrator
☐ Developer	☐ Operator	☐ Clerk	☐ QA
☐ Other:			

Reason for the request

Approved by	
Requester Manager:	
Operation Manager:	

Comments

Completed by			
Administrator		Date	

FIGURE 3-2 Database user account application form

Operating System Authentication

- Many databases (including Microsoft SQL Server 2000) depend on OS to authenticate users
- Once an intruder is inside the OS, it is easier to access the database
- Centralize administration of users
- Ideally, users must be authenticated at each level

Operating System Authentication (continued)

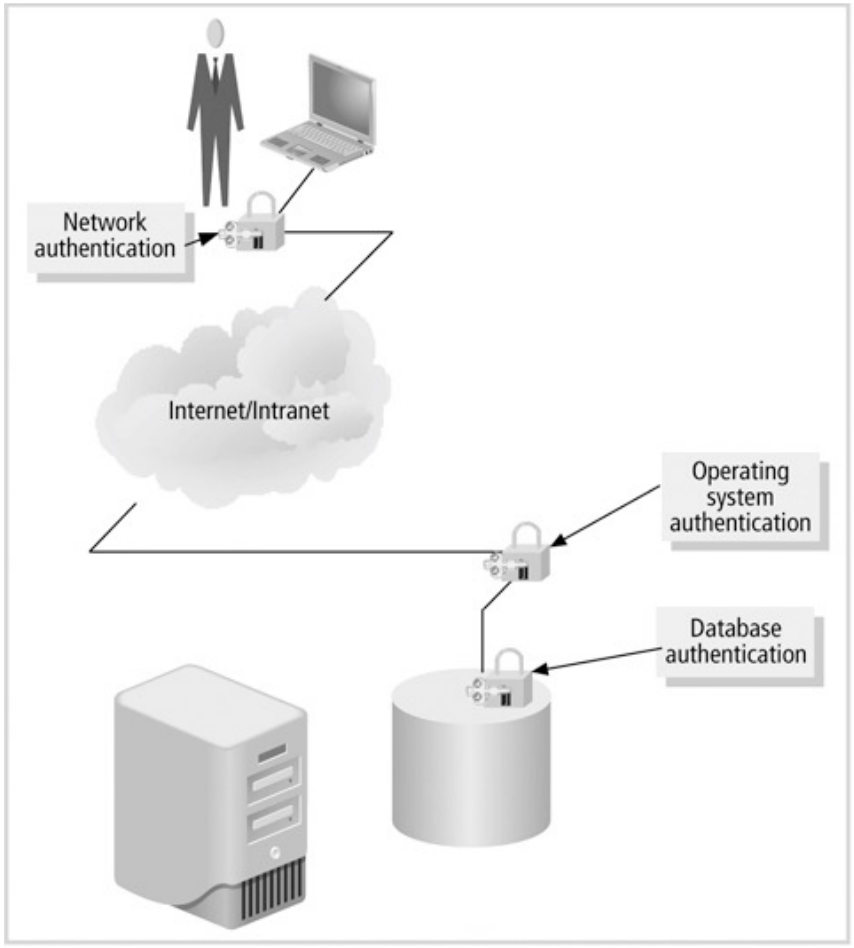


FIGURE 3-3 Ideal authentication levels for database applications

Creating Users

- Must be a standardized, well-documented, and securely managed process
- Several ways in Oracle:
  1. CREATE USER Statement from iSQLPlus
  2. Oracle Enterprise Manager: GUI administration tool using database authentication
  3. Creating an Oracle User Using External (Operating System) Authentication
  4. SQL developer

Creating Users

- In Oracle, use the CREATE USER statement:
  - Part of the a Data Definition Language (DDL)
  - Account can own different objects

```
CREATE USER {name}
IDENTIFIED {BY password | EXTERNALLY | GLOBALLY as
    'external_name'}
[DEFAULT TABLESPACE {tbspname}]
[TEMPORARY TABLESPACE {tmpname}]
[QUOTA {integer {K|M}  ON {tbspname}]
[PROFILE {pname}]
[PASSWORD EXPIRE]
[ACCOUNT {lock | unlock}]
```

Creating an Oracle User

- IDENTIFIED clause
  - Tells Oracle how to authenticate a user account
  - BY PASSWORD option: encrypts and stores an assigned password in the database
  - EXTERNALLY option: user is authenticated by the OS
  - GLOBALLY AS option: depends on authentication through centralized user management method

Creating an Oracle User (continued)

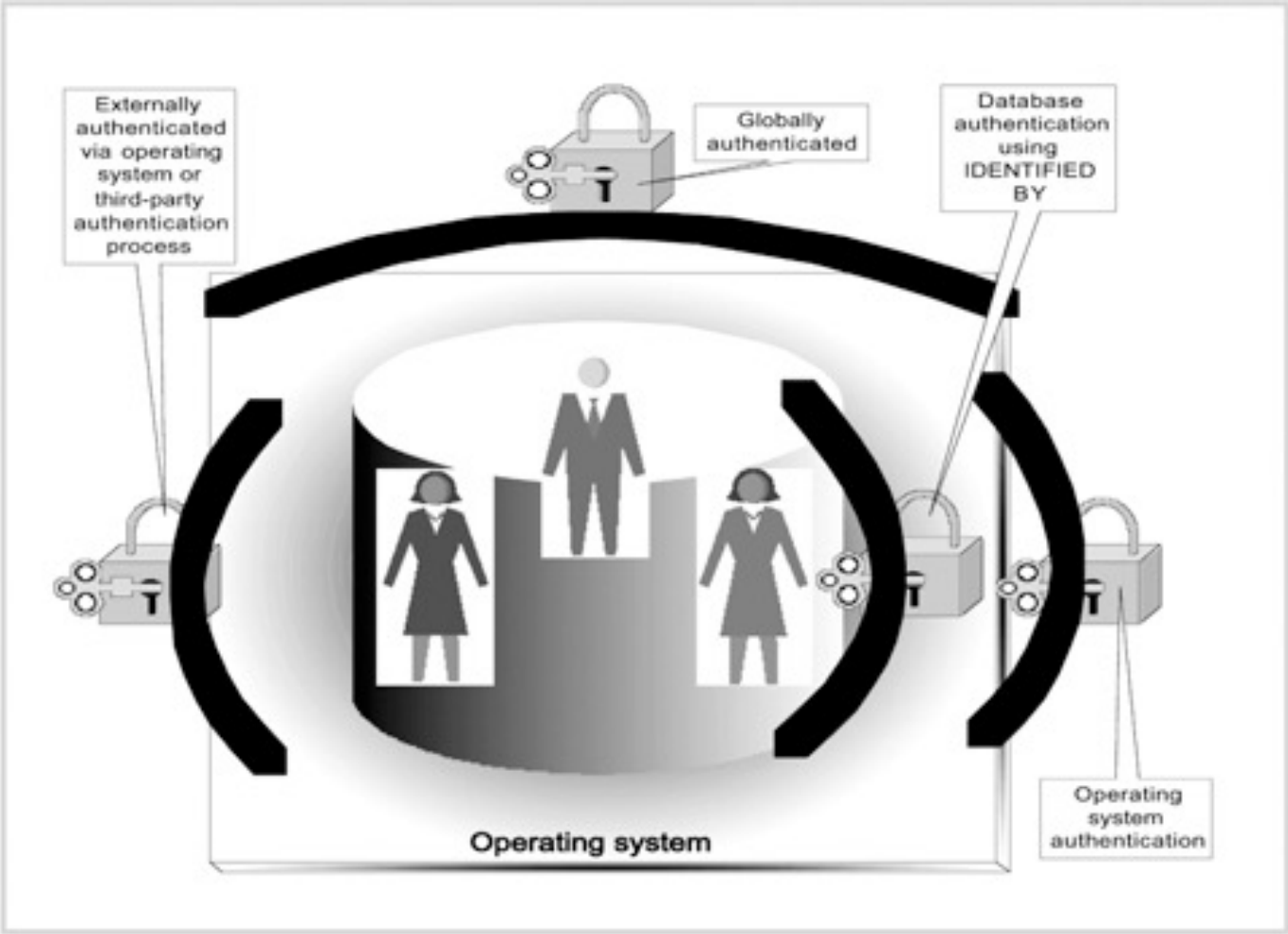


FIGURE 3-4 Architecture of Oracle authentication methods

Creating an Oracle User (continued)

- DEFAULT TABLESPACE clause: specifies default storage for the user
- TEMPORARY TABLESPACE clause
- QUOTA clause: tells Oracle DB how much storage space a user is allowed for a specified tablespace
- PROFILE clause: indicates the profile used for limiting database resources and enforcing password policies

Example

```
CREATE USER STUDENTA
IDENTIFIED BY TRUE#1
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
QUOTA 10M ON USERS
QUOTA 5M ON USER_AUTO
PROFILE DEFAULT
ACCOUNT UNLOCK;
```

Creating an Oracle User (continued)

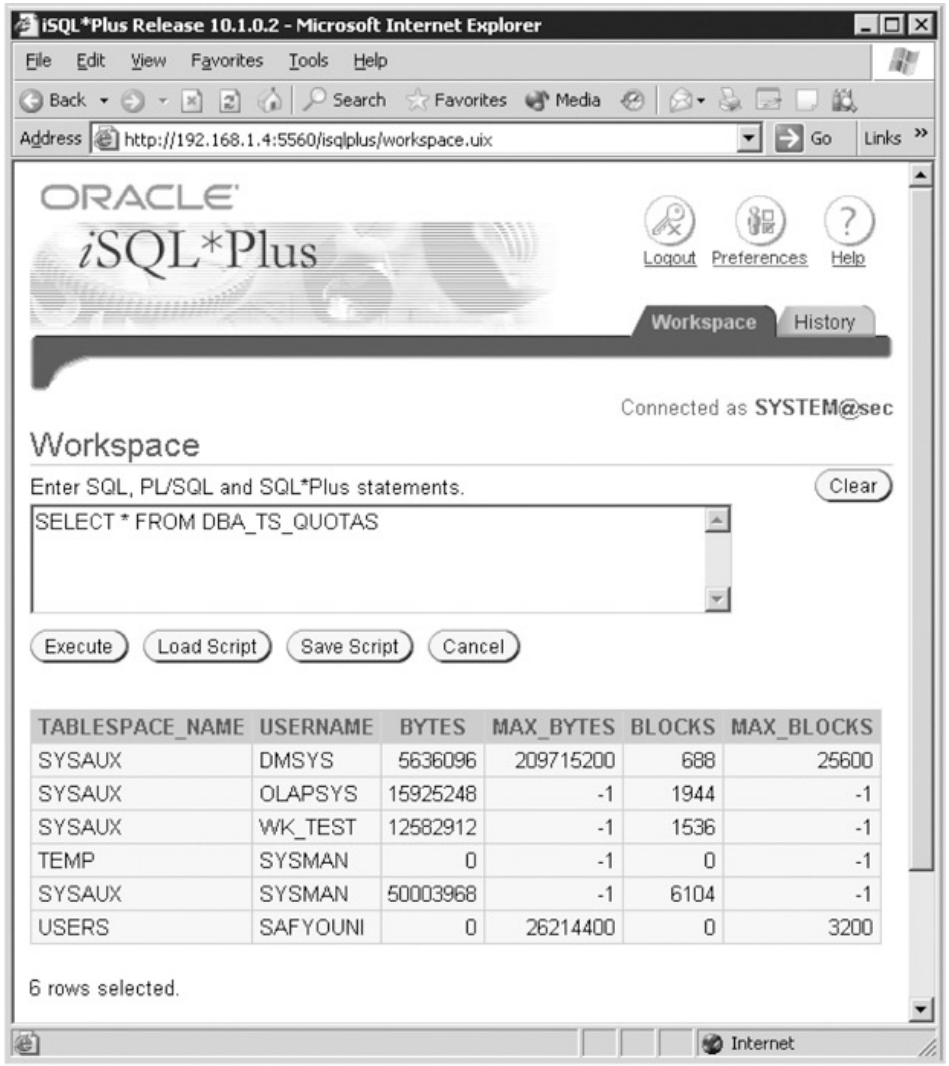


FIGURE 3-5 Contents of data dictionary view DBA_TS_QUOTAS

Creating an Oracle User (continued)

- PASSWORD EXPIRE clause: tells Oracle to expire the user password and prompts the user to enter a new password
- ACCOUNT clause: enable or disable account
- ALTER USER: modifies a user account
- Oracle Enterprise Manager: GUI administration tool

Creating an Oracle User (continued)

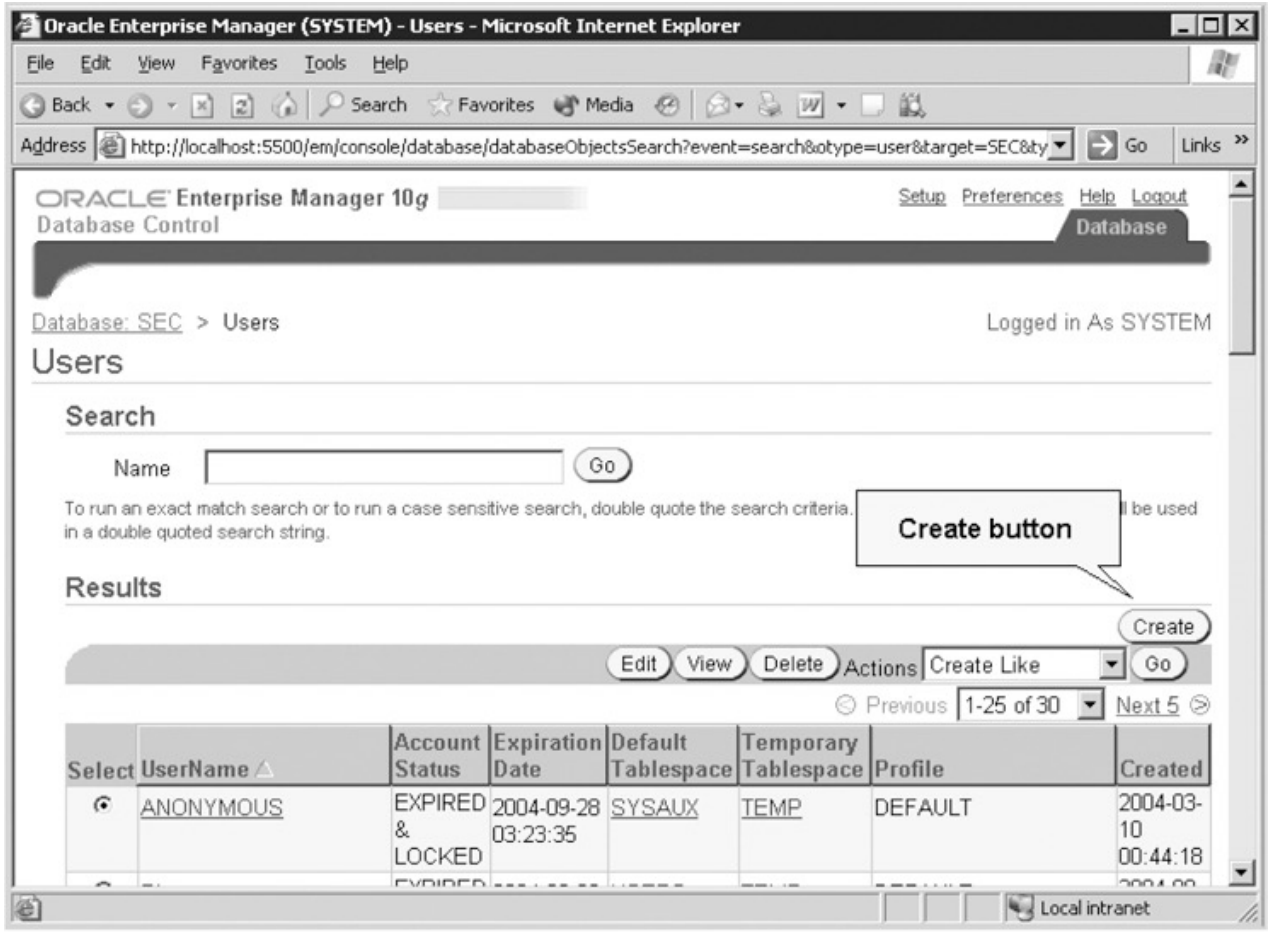


FIGURE 3-7 Oracle Enterprise Manager Console showing the Create Objects button

Creating an Oracle User (continued)

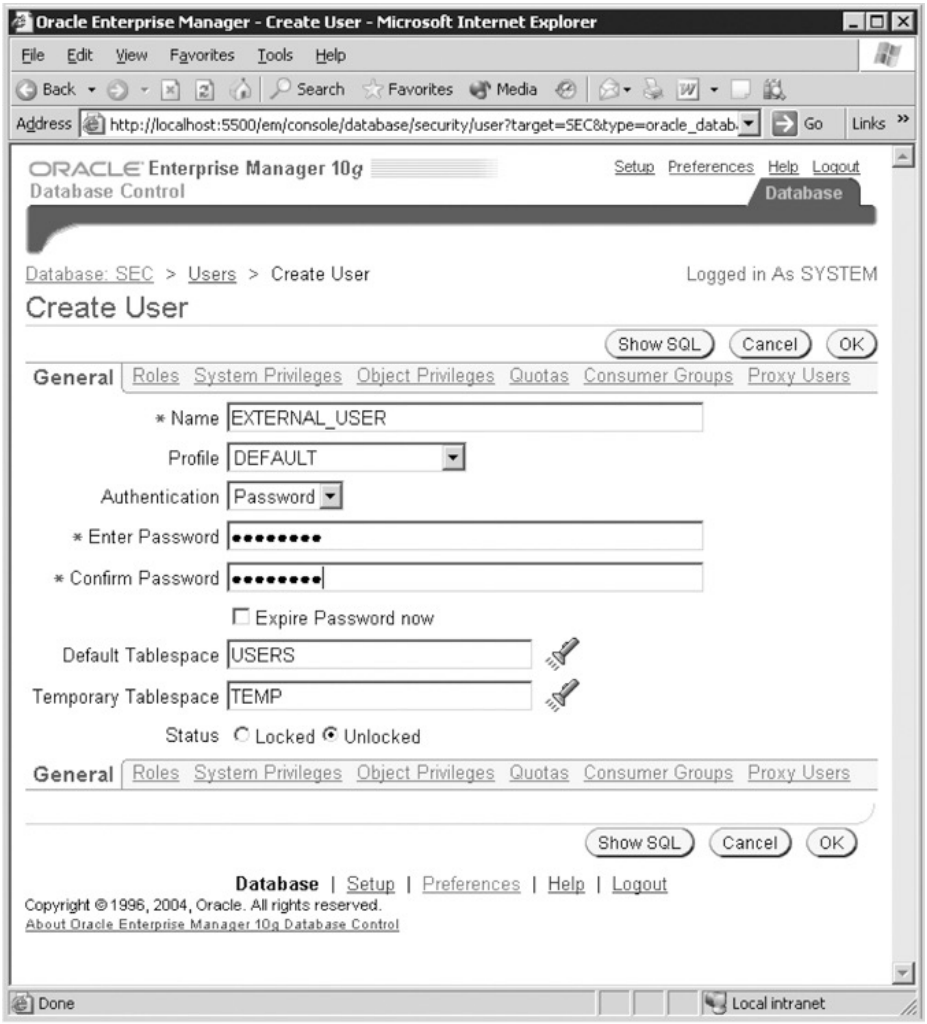


FIGURE 3-8 Creating a new user

Creating an Oracle User Using External (Operating System) Authentication

- Depends on an external party to authenticate the user
- Steps:
  - Verify account belongs to ORA_DBA group
  - Set the Windows registry string OSAUTH_PREFIX_DOMAIN to FALSE
  - View setting of the OS_AUTHENT_PREFIX initialization parameter
  - Change OS_AUTHENT_PREFIX to NULL

Creating an Oracle User Using External (Operating System) Authentication (continued)

Step 1:The window OS account that you want Oracle 10g to use for external authentication must belong to the **ORA_DBA** group. Go to Control Panel → Administrative Tools → Computer Management Tool to verify. You can use one of OS accounts.

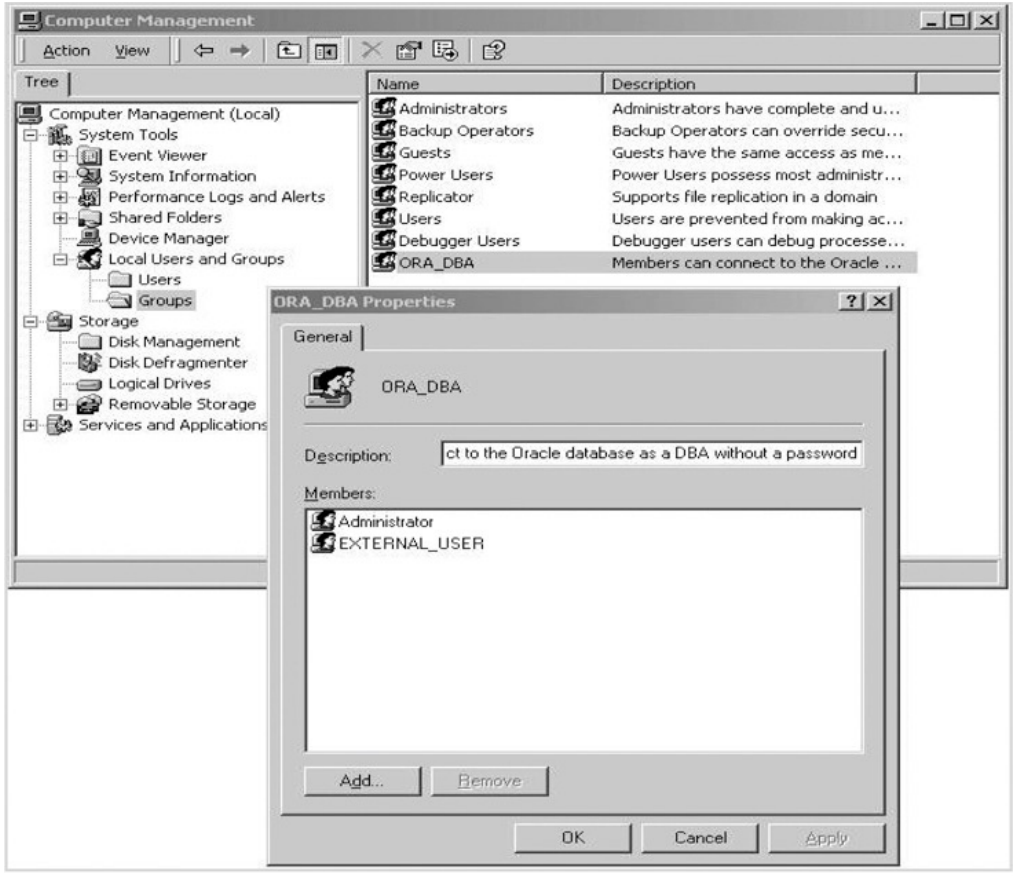


FIGURE 3-11 Computer management tool showing the ORA_DBA group properties

Creating an Oracle User Using External (Operating System) Authentication (continued)

Step 2: You must set the windows registry string OSAUTH_PREFIX-DOMAIN to false. Use "regedit" from run, and navigate to HKEY_LOCAL_MACHINE, SOFTWARE, ORACLE, HOME1 (or 2). Create one if the parameter does not exist.

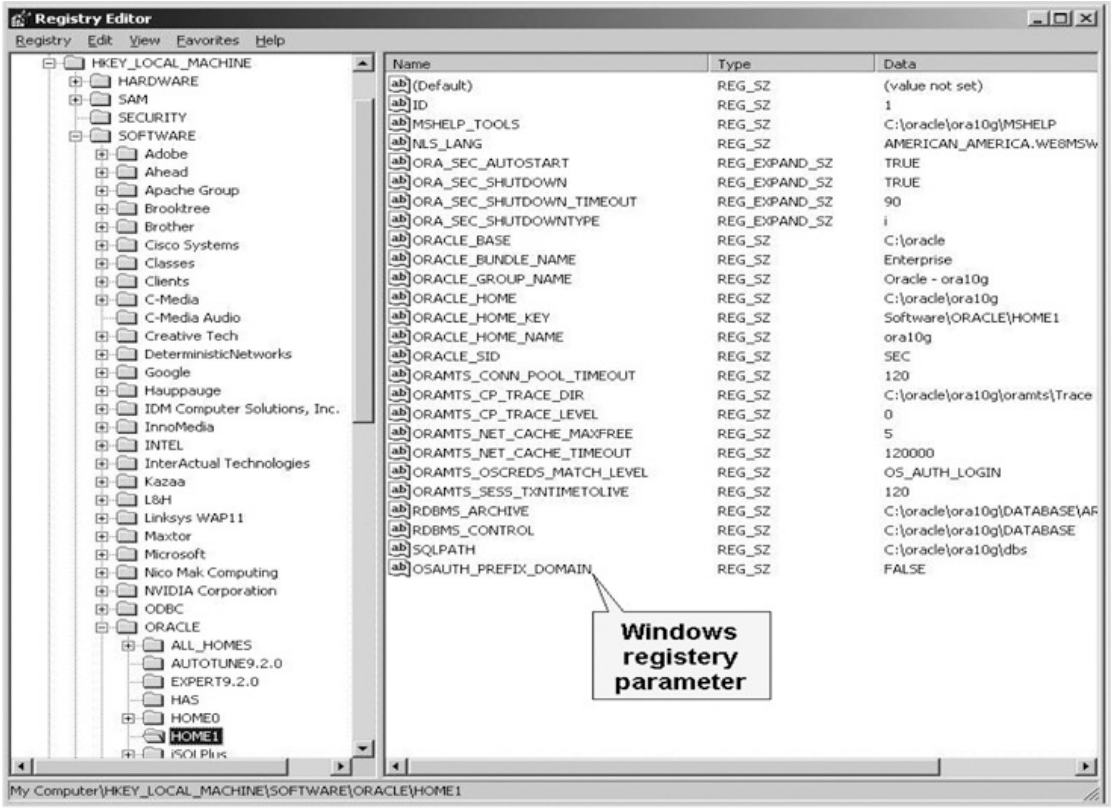


FIGURE 3-12 Windows registry showing the OSAUTH_PREFIX_DOMAIN parameter

Creating an Oracle User Using External (Operating System) Authentication (continued)

Step 3: SQL> **SHOW PARAMETER PREFIX**

Change the O**S_AUTHENT_PREFIX** initialization parameter value to NULL.

Step 4: Create an Oracle user with the same name as the windows user name that is used for external authentication.

SQL> **CREATE USER user_name IDENTIFIED EXTERNALLY**

2 /

User created.

Creating an Oracle User Using External (Operating System) Authentication (continued)

Step 5: Provide new user with CREATE SESSION privilege

SQL>GRANT CREATE SESSION TO EXTERNAL_USER;

Grant succeeded.

Step 6: Log off the Oracle SYS or SYSTEM account and windows account.

Step 7: log in again using *user_name*.

Step 8: From command line type *sqlplus*

- Advantage: allows administrators to use one generic user to run maintenance scripts without a password

More on Password

- Even DBA can not recover real value of password from the database
- You can change the password and inform the user of the new password
- You make the password expire immediately so the user must choose a new password that he finds easier to remember.

```
ALTER USER STUDENTA
IDENTIFIED BY STUDENTA
PASSWORD EXPIRE;
```

Removing Users

- Simple process
- Make a backup first
- Obtain a written request (for auditing purposes)

Removing an Oracle User

- DROP command
- CASCADE option: when user owns database objects

```
DROP USER MELVIN CASCADE;
```

- Recommendations:
  - Backup the account for one to three months
  - Listing all owned objects
  - Lock the account or revoke the CREATE SESSION privilege

Modifying Users

- Modifications involve:
  - Changing passwords
  - Locking an account
  - Increasing a storage quota
- ALTER USER DDL statement

Modifying an Oracle User

- ALTER USER statement
- Oracle Enterprise Manager: graphical tool

Modifying an Oracle User (continued)

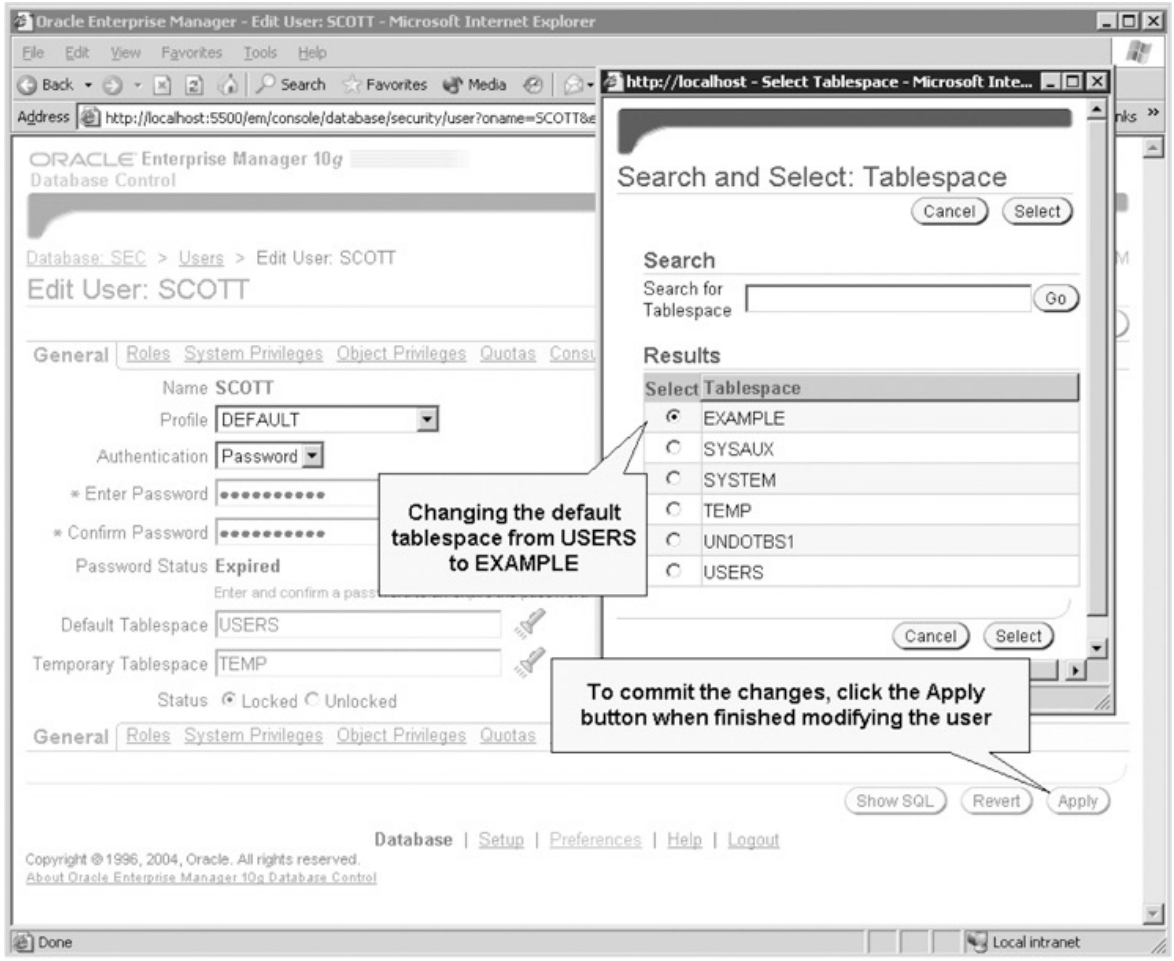


FIGURE 3-20 Illustration of modifying an existing Oracle user account

Default Users

- Oracle default users:
  - SYS, owner of the data dictionary
  - SYSTEM, performs almost all database tasks
  - ORAPWD, creates a password file
- SQL Server default users:
  - SA, system administrator
  - BUILT_IN\Administrators

Practices for Administrators and Managers

- Manage:
  - Accounts
  - Data files
  - Memory
- Administrative tasks:
  - Backup
  - Recovery
  - Performance tuning

Best Practices

- Follow company's policies and procedures
- Always document and create logs
- Educate users
- Keep abreast of database and security technology
- Review and modify procedures

Best Practices (continued)

- Block direct access to database tables
- Limit and restrict access to the server
- Use strong passwords
- Patches, patches, patches

Quick quiz

- These are the top three excuses for failing to incorporate documentation as part of the administration process:
  - _____
  - Belief that the administration process is already documented in the system
  - Reluctance to complicate a process that is simple

- The _____ is the gateway to the database.

- The _____ clause tells Oracle11*g/12c* how to authenticate a user account.
  a. PASSWORD EXPIRE
  b. IDENTIFIED
  c. ACCOUNT
  d. QUOTA

Quick Quiz

- SQL provides a command called _____ that removes a user account from the database

- When a user logs on to the database through the machine where the database is located, the database is called a _____.
  a. local database
  b. remote database
  c. fixed database
  d. database server

Key Terms

- **ACCOUNT UNLOCK** is an Oracle option that indicates that an account is enabled.
- **CREATE USER** statement is a SQL statement that enables database administrators to create a database user account.
- **ODBC (Open Database Connectivity)** is a Microsoft protocol used for connecting Windows applications to different database systems, including other SQL servers and Oracle10*g* servers
- **OLEDB (Object Linking and Embedding Database)** is a Microsoft component that allows Windows applications to connect and access different database systems.
- **Operating system** is the gateway to database access.
- **Windows authentication** is the only type of authentication the default installation of Microsoft SQL Server 2000 supports.

User administration guidelines web sites

- http://www.orafaq.com/faqdba.htm
- http://msdn.microsoft.com/archive/default.asp?url=/archive/en-us/dnarsql7/html/deploybus_appc.asp
- http://www.cadam.com/whitepapers/db_security.htm
- http://www.oracle.com/technology/documentation/ids_arch.html
- https://aurora.vcu.edu/db2help/db2d0/frm3toc.htm

Labs

- Create a database user account:
  - SQL statement
  - GUI in Enterprise Manager
  - A user authenticated by windows OS.
- Modify a user
- Drop a user