GRANT

Purpose

Use the GRANT statement to grant:

- System privileges to users and roles.
- Roles to users and roles. Both privileges and roles are either local, global, or external. Table 18 1 lists the system privileges (organized by the database object operated upon). Table 18 2 lists Oracle Database predefined roles.
- Object privileges for a particular object to users, roles, and PUBLIC. Table 18 3 summarizes the object privileges that you can grant on each type of object. Table 18 4 lists object privileges and the operations that they authorize.

Notes on Authorizing Database Users You can authorize database users through means other than the database and the GRANT statement.

- Many Oracle Database privileges are granted through supplied PL/ SQL and Java packages. For information on those privileges, please refer to the documentation for the appropriate package.
- Some operating systems have facilities that let you grant roles to Oracle Database users with the initialization parameter OS_ROLES. If you choose to grant roles to users through operating system facilities, then you cannot also grant roles to users with the GRANT statement, although you can use the GRANT statement to grant system privileges to users and system privileges and roles to other roles.

See Also:

- CREATE USER on page 17-26 and CREATE ROLE on page 15-63 for definitions of local, global, and external privileges
- *Oracle Database Security Guide* for information about other authorization methods and for information about privileges
- REVOKE on page 18-84 for information on revoking grants

Prerequisites

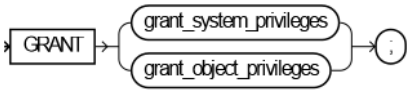
To grant a system privilege, you must either have been granted the system privilege with the ADMIN OPTION or have been granted the GRANT ANY PRIVILEGE system privilege.

To grant a role, you must either have been granted the role with the ADMIN OPTION or have been granted the GRANT ANY ROLE system privilege, or you must have created the role.

To grant an object privilege, you must own the object, or the owner of the object must have granted you the object privileges with the GRANT OPTION, or you must have been granted the GRANT ANY OBJECT PRIVILEGE system privilege. If you have the GRANT ANY OBJECT PRIVILEGE, then you can grant the object privilege only if the object owner could have granted the same object privilege. In this case, the GRANTOR column of the DBA_TAB_PRIVS view displays the object owner rather than the user who issued the GRANT statement.

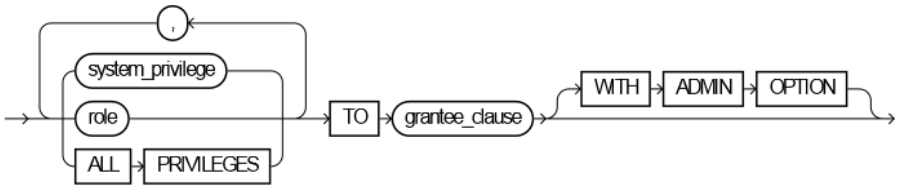
Syntax

grant::=



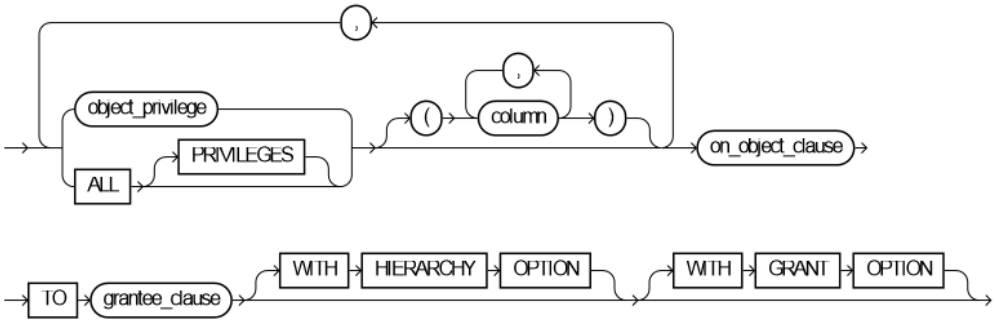
(*grant_system_privileges::=* on page 18-33, *grant_object_privileges::=* on page 18-33)

grant_system_privileges::=



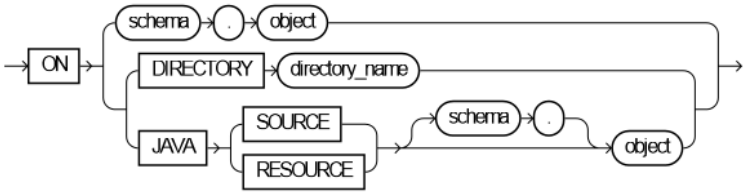
(*grantee_clause::=* on page 18-33)

grant_object_privileges::=

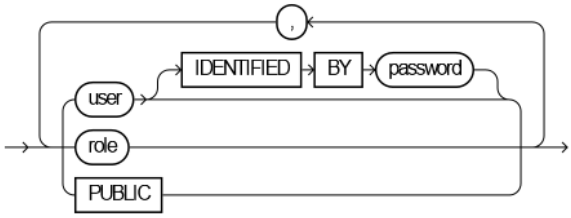


(*on_object_clause::=* on page 18-33, *grantee_clause::=* on page 18-33)

on_object_clause::=



grantee_clause::=



Semantics

grant_system_privileges

Use these clauses to grant system privileges.

system_privilege

Specify the system privilege you want to grant. Table 18 1 lists the system privileges, organized by the database object operated upon.

- If you grant a privilege to a **user**, then the database adds the privilege to the user s privilege domain. The user can immediately exercise the privilege.
- If you grant a privilege to a **role**, then the database adds the privilege to the privilege domain of the role. Users who have been granted and have enabled the role can immediately exercise the privilege. Other users who have been granted the role can enable the role and exercise the privilege.

  > See Also: Granting a System Privilege to a User: Example on page 18-48 and "Granting System Privileges to a Role: Example" on page 18-48

- If you grant a privilege to **PUBLIC**, then the database adds the privilege to the privilege domains of each user. All users can immediately perform operations authorized by the privilege.

Oracle Database provides the ALL PRIVILEGES shortcut for granting all the system privileges listed in Table 18 1 on page 18-37, except the SELECT ANY DICTIONARY privilege.

role

Specify the role you want to grant. You can grant an Oracle Database predefined role or a user-defined role. Table 18 2 lists the predefined roles.

- If you grant a role to a **user**, then the database makes the role available to the user. The user can immediately enable the role and exercise the privileges in the privilege domain of the role.
- If you grant a role to another **role**, then the database adds the privilege domain of the granted role to the privilege domain of the grantee role. Users who have been granted the grantee role can enable it and exercise the privileges in the granted role s privilege domain.
- If you grant a role to **PUBLIC**, then the database makes the role available to all users. All users can immediately enable the role and exercise the privileges in the privilege domain of the role.

  > See Also: "Granting a Role to a Role: Example" on page 18-49 and CREATE ROLE on page 15-63 for information on creating a user-defined role

IDENTIFIED BY Clause

Use the IDENTIFIED BY clause to specifically identify an existing user by password or to create a nonexistent user. This clause is not valid if the grantee is a role or PUBLIC. If the user specified in the *grantee_clause* does not exist, then the database creates the user with the password and with the privileges and roles specified in this clause.

> See Also: CREATE USER on page 17-26 for restrictions on usernames and passwords

WITH ADMIN OPTION

Specify WITH ADMIN OPTION to enable the grantee to:

- Grant the role to another user or role, unless the role is a GLOBAL role
- Revoke the role from another user or role
- Alter the role to change the authorization needed to access it
- Drop the role

If you grant a system privilege or role to a user without specifying WITH ADMIN OPTION, and then subsequently grant the privilege or role to the user WITH ADMIN OPTION, then the user has the ADMIN OPTION on the privilege or role.

To revoke the ADMIN OPTION on a system privilege or role from a user, you must revoke the privilege or role from the user altogether and then grant the privilege or role to the user without the ADMIN OPTION.

> See Also: "Granting a Role with the Admin Option: Example" on page 18-48

grantee_clause

TO *grantee_clause* identifies users or roles to which the system privilege, role, or object privilege is granted.

Restriction on Grantees A user, role, or PUBLIC cannot appear more than once in TO *grantee_clause*

PUBLIC Specify PUBLIC to grant the privileges to all users.

Restrictions on Granting System Privileges and Roles Privileges and roles are subject to the following restrictions:

- A privilege or role cannot appear more than once in the list of privileges and roles to be granted.
- You cannot grant a role to itself.
- You cannot grant a role IDENTIFIED GLOBALLY to anything.
- You cannot grant a role IDENTIFIED EXTERNALLY to a global user or global role.
- You cannot grant roles circularly. For example, if you grant the role banker to the role teller, then you cannot subsequently grant teller to banker.

grant_object_privileges

Use these clauses to grant object privileges.

object_privilege

Specify the object privilege you want to grant. You can specify any of the values shown in Table 18 3. See also Table 18 4.

Restriction on Object Privileges A privilege cannot appear more than once in the list of privileges to be granted.

ALL [PRIVILEGES]

Specify ALL to grant all the privileges for the object that you have been granted with the GRANT OPTION. The user who owns the schema containing an object automatically has all privileges on the object with the GRANT OPTION. The keyword PRIVILEGES is provided for semantic clarity and is optional.

column

Specify the table or view column on which privileges are to be granted. You can specify columns only when granting the INSERT, REFERENCES, or UPDATE privilege. If you do not list columns, then the grantee has the specified privilege on all columns in the table or view.

For information on existing column object grants, query the USER_, ALL_, or DBA_COL_PRIVS data dictionary view.

> See Also: *Oracle Database Reference* for information on the data dictionary views and "Granting Multiple Object Privileges on Individual Columns: Example" on page 18-49

on_object_clause

The *on_object_clause* identifies the object on which the privileges are granted. Directory schema objects and Java source and resource schema objects are identified separately because they reside in separate namespaces.

If you can make this grant only because you have the GRANT ANY OBJECT PRIVILEGE system privilege--that is, you are not the owner of *object*, nor do you have *object_privilege* on *object* WITH GRANT OPTION--then the effect of this grant is that you are acting on behalf of the object owner. The *_TAB_PRIVS data dictionary views will reflect that this grant was made by the owner of *object*.

> See Also:
>
> - "Granting Object Privileges to a Role: Example" on page 18-49
> - "Revoke Operations that Use GRANT ANY OBJECT PRIVILEGE: Example" on page 18-91 for more information on using the GRANT ANY OBJECT PRIVILEGE system privilege for revoke operations

WITH GRANT OPTION

Specify WITH GRANT OPTION to enable the grantee to grant the object privileges to other users and roles.

Restriction on Granting WITH GRANT OPTION You can specify WITH GRANT OPTION only when granting to a user or to PUBLIC, not when granting to a role.

WITH HIERARCHY OPTION

Specify WITH HIERARCHY OPTION to grant the specified object privilege on all subobjects of *object*, such as subviews created under a view, including subobjects created subsequent to this statement.

This clause is meaningful only in combination with the SELECT object privilege.

object Specify the schema object on which the privileges are to be granted. If you do not qualify *object* with *schema*, then the database assumes the object is in your own schema. The object can be one of the following types:

- Table, view, or materialized view

- Sequence
- Procedure, function, or package
- User-defined type
- Synonym for any of the preceding items
- Directory, library, operator, or indextype
- Java source, class, or resource

You cannot grant privileges directly to a single partition of a partitioned table.

> See Also: "Granting Object Privileges on a Table to a User: Example" on page 18-49, "Granting Object Privileges on a View: Example" on page 18-49, and "Granting Object Privileges to a Sequence in Another Schema: Example" on page 18-49

DIRECTORY ***directory_name*** Specify a directory schema object on which privileges are to be granted. You cannot qualify *directory_name* with a schema name.

> See Also: CREATE DIRECTORY on page 14-42 and "Granting an Object Privilege on a Directory: Example" on page 18-49

JAVA SOURCE | RESOURCE The JAVA clause lets you specify a Java source or resource schema object on which privileges are to be granted.

> See Also: CREATE JAVA on page 14-84

Listings of System and Object Privileges

> Note: When you grant a privilege on ANY object, such as CREATE ANY CLUSTER, the result is determined by the value of the O7_DICTIONARY_ACCESSIBILITY initialization parameter. By default, this parameter is set to FALSE, so that ANY privileges give the grantee access to that type of object in all schemas except the SYS schema. If you set O7_DICTIONARY_ACCESSIBILITY to TRUE, then the ANY privileges also give the grantee access, in the SYS schema, to all objects except Oracle Scheduler objects. For security reasons, Oracle recommends that you use this setting only with great caution.

Table 18–1 System Privileges

System Privilege Name	Operations Authorized
Advisor Framework Privileges: All of the advisor framework privileges are part of the DBA role.	--
ADVISOR	Access the advisor framework through PL/ SQL packages such as DBMS_ADVISOR and DBMS_SQLTUNE. Please refer to *Oracle Database PL/SQL Packages and Types Reference* for information on these packages.
ADMINISTER SQL TUNING SET	Create, drop, select (read), load (write), and delete a SQL tuning set owned by the grantee through the DBMS_SQLTUNE package.
ADMINISTER ANY SQL TUNING SET	Create, drop, select (read), load (write), and delete a SQL tuning set owned by any user through the DBMS_SQLTUNE package.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
CREATE ANY SQL PROFILE	Accept a SQL Profile recommended by the SQL Tuning Advisor, which is accessed through Enterprise Manager or by the DBMS_SQLTUNE package.
DROP ANY SQL PROFILE	Drop an existing SQL Profile.
ALTER ANY SQL PROFILE	Alter the attributes of an existing SQL Profile.
CLUSTERS:	--
CREATE CLUSTER	Create clusters in the grantee s schema.
CREATE ANY CLUSTER	Create a cluster in any schema. Behaves similarly to CREATE ANY TABLE.
ALTER ANY CLUSTER	Alter clusters in any schema.
DROP ANY CLUSTER	Drop clusters in any schema.
CONTEXTS:	--
CREATE ANY CONTEXT	Create any context namespace.
DROP ANY CONTEXT	Drop any context namespace.
DATABASE:	--
ALTER DATABASE	Alter the database.
ALTER SYSTEM	Issue ALTER SYSTEM statements.
AUDIT SYSTEM	Issue AUDIT statements.
DATABASE LINKS:	--
CREATE DATABASE LINK	Create private database links in the grantee s schema.
CREATE PUBLIC DATABASE LINK	Create public database links.
DROP PUBLIC DATABASE LINK	Drop public database links.
DEBUGGING:	--
DEBUG CONNECT SESSION	Connect the current session to a debugger.
DEBUG ANY PROCEDURE	Debug all PL/ SQL and Java code in any database object. Display information on all SQL statements executed by the application. **Note:** Granting this privilege is equivalent to granting the DEBUG object privilege on all applicable objects in the database.
DIMENSIONS:	--
CREATE DIMENSION	Create dimensions in the grantee s schema.
CREATE ANY DIMENSION	Create dimensions in any schema.
ALTER ANY DIMENSION	Alter dimensions in any schema.
DROP ANY DIMENSION	Drop dimensions in any schema.
DIRECTORIES:	--
CREATE ANY DIRECTORY	Create directory database objects.
DROP ANY DIRECTORY	Drop directory database objects.
INDEXTYPES:	--
CREATE INDEXTYPE	Create an indextype in the grantee s schema.
CREATE ANY INDEXTYPE	Create an indextype in any schema and create a comment on an indextype in any schema.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
ALTER ANY INDEXTYPE	Modify indextypes in any schema.
DROP ANY INDEXTYPE	Drop an indextype in any schema.
EXECUTE ANY INDEXTYPE	Reference an indextype in any schema.
INDEXES:	--
CREATE ANY INDEX	Create in any schema a domain index or an index on any table in any schema.
ALTER ANY INDEX	Alter indexes in any schema.
DROP ANY INDEX	Drop indexes in any schema.
JOB SCHEDULER OBJECTS:	The following privileges are needed to execute procedures in the DBMS_SCHEDULER package.
CREATE JOB	Create jobs, schedules, or programs in the grantee s schema.
CREATE ANY JOB	Create, alter, or drop jobs, schedules, or programs in any schema. **Note:** This extremely powerful privilege allows the grantee to execute code as any other user. It should be granted with caution.
CREATE EXTERNAL JOB	Create in the grantee's schema an executable scheduler job that runs on the operating system.
EXECUTE ANY PROGRAM	Use any program in a job in the grantee s schema.
EXECUTE ANY CLASS	Specify any job class in a job in the grantee s schema.
MANAGE SCHEDULER	Create, alter, or drop any job class, window, or window group.
LIBRARIES:	--
CREATE LIBRARY	Create external procedure or function libraries in the grantee s schema.
CREATE ANY LIBRARY	Create external procedure or function libraries in any schema.
DROP ANY LIBRARY	Drop external procedure or function libraries in any schema.
MATERIALIZED VIEWS:	--
CREATE MATERIALIZED VIEW	Create a materialized view in the grantee s schema.
CREATE ANY MATERIALIZED VIEW	Create materialized views in any schema.
ALTER ANY MATERIALIZED VIEW	Alter materialized views in any schema.
DROP ANY MATERIALIZED VIEW	Drop materialized views in any schema.
QUERY REWRITE	This privilege has been deprecated. No privileges are needed for a user to enable rewrite for a materialized view that references tables or views in the user s own schema.
GLOBAL QUERY REWRITE	Enable rewrite using a materialized view when that materialized view references tables or views in any schema.
ON COMMIT REFRESH	Create a refresh-on-commit materialized view on any table in the database. Alter a refresh-on-demand materialized on any table in the database to refresh-on-commit.
FLASHBACK ANY TABLE	Issue a SQL Flashback Query on any table, view, or materialized view in any schema. This privilege is not needed to execute the DBMS_FLASHBACK procedures.
OPERATORS:	--

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
CREATE OPERATOR	Create an operator and its bindings in the grantee s schema.
CREATE ANY OPERATOR	Create an operator and its bindings in any schema and create a comment on an operator in any schema.
ALTER ANY OPERATOR	Modify an operator in any schema.
DROP ANY OPERATOR	Drop an operator in any schema.
EXECUTE ANY OPERATOR	Reference an operator in any schema.
OUTLINES:	--
CREATE ANY OUTLINE	Create public outlines that can be used in any schema that uses outlines.
ALTER ANY OUTLINE	Modify outlines.
DROP ANY OUTLINE	Drop outlines.
PROCEDURES:	--
CREATE PROCEDURE	Create stored procedures, functions, and packages in the grantee s schema.
CREATE ANY PROCEDURE	Create stored procedures, functions, and packages in any schema.
ALTER ANY PROCEDURE	Alter stored procedures, functions, or packages in any schema.
DROP ANY PROCEDURE	Drop stored procedures, functions, or packages in any schema.
EXECUTE ANY PROCEDURE	Execute procedures or functions, either standalone or packaged. Reference public package variables in any schema.
PROFILES:	--
CREATE PROFILE	Create profiles.
ALTER PROFILE	Alter profiles.
DROP PROFILE	Drop profiles.
ROLES:	--
CREATE ROLE	Create roles.
ALTER ANY ROLE	Alter any role in the database.
DROP ANY ROLE	Drop roles.
GRANT ANY ROLE	Grant any role in the database.
ROLLBACK SEGMENTS:	--
CREATE ROLLBACK SEGMENT	Create rollback segments.
ALTER ROLLBACK SEGMENT	Alter rollback segments.
DROP ROLLBACK SEGMENT	Drop rollback segments.
SEQUENCES:	--
CREATE SEQUENCE	Create sequences in the grantee s schema.
CREATE ANY SEQUENCE	Create sequences in any schema.
ALTER ANY SEQUENCE	Alter any sequence in the database.
DROP ANY SEQUENCE	Drop sequences in any schema.
SELECT ANY SEQUENCE	Reference sequences in any schema.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
SESSIONS:	--
CREATE SESSION	Connect to the database.
ALTER RESOURCE COST	Set costs for session resources.
ALTER SESSION	Issue ALTER SESSION statements.
RESTRICTED SESSION	Logon after the instance is started using the SQL*Plus STARTUP RESTRICT statement.
SNAPSHOTS:	See MATERIALIZED VIEWS
SYNONYMS:	--
CREATE SYNONYM	Create synonyms in the grantee s schema.
CREATE ANY SYNONYM	Create private synonyms in any schema.
CREATE PUBLIC SYNONYM	Create public synonyms.
DROP ANY SYNONYM	Drop private synonyms in any schema.
DROP PUBLIC SYNONYM	Drop public synonyms.
TABLES:	**Note:** For external tables, the only valid privileges are CREATE ANY TABLE, ALTER ANY TABLE, DROP ANY TABLE, and SELECT ANY TABLE.
CREATE TABLE	Create tables in the grantee s schema.
CREATE ANY TABLE	Create tables in any schema. The owner of the schema containing the table must have space quota on the tablespace to contain the table.
ALTER ANY TABLE	Alter any table or view in any schema.
BACKUP ANY TABLE	Use the Export utility to incrementally export objects from the schema of other users.
DELETE ANY TABLE	Delete rows from tables, table partitions, or views in any schema.
DROP ANY TABLE	Drop or truncate tables or table partitions in any schema.
INSERT ANY TABLE	Insert rows into tables and views in any schema.
LOCK ANY TABLE	Lock tables and views in any schema.
SELECT ANY TABLE	Query tables, views, or materialized views in any schema.
FLASHBACK ANY TABLE	Issue a SQL Flashback Query on any table, view, or materialized view in any schema. This privilege is not needed to execute the DBMS_FLASHBACK procedures.
UPDATE ANY TABLE	Update rows in tables and views in any schema.
TABLESPACES:	--
CREATE TABLESPACE	Create tablespaces.
ALTER TABLESPACE	Alter tablespaces.
DROP TABLESPACE	Drop tablespaces.
MANAGE TABLESPACE	Take tablespaces offline and online and begin and end tablespace backups.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
UNLIMITED TABLESPACE	Use an unlimited amount of any tablespace. This privilege overrides any specific quotas assigned. If you revoke this privilege from a user, then the user s schema objects remain but further tablespace allocation is denied unless authorized by specific tablespace quotas. You cannot grant this system privilege to roles.
TRIGGERS:	--
CREATE TRIGGER	Create a database trigger in the grantee s schema.
CREATE ANY TRIGGER	Create database triggers in any schema.
ALTER ANY TRIGGER	Enable, disable, or compile database triggers in any schema.
DROP ANY TRIGGER	Drop database triggers in any schema.
ADMINISTER DATABASE TRIGGER	Create a trigger on DATABASE. You must also have the CREATE TRIGGER or CREATE ANY TRIGGER system privilege.
TYPES:	--
CREATE TYPE	Create object types and object type bodies in the grantee s schema.
CREATE ANY TYPE	Create object types and object type bodies in any schema.
ALTER ANY TYPE	Alter object types in any schema.
DROP ANY TYPE	Drop object types and object type bodies in any schema.
EXECUTE ANY TYPE	Use and reference object types and collection types in any schema, and invoke methods of an object type in any schema if you make the grant to a specific user. If you grant EXECUTE ANY TYPE to a role, then users holding the enabled role will not be able to invoke methods of an object type in any schema.
UNDER ANY TYPE	Create subtypes under any nonfinal object types.
USERS:	--
CREATE USER	Create users. This privilege also allows the creator to: ■ Assign quotas on any tablespace. ■ Set default and temporary tablespaces. ■ Assign a profile as part of a CREATE USER statement.
ALTER USER	Alter any user. This privilege authorizes the grantee to: ■ Change another user s password or authentication method. ■ Assign quotas on any tablespace. ■ Set default and temporary tablespaces. ■ Assign a profile and default roles.
DROP USER	Drop users
VIEWS:	--
CREATE VIEW	Create views in the grantee s schema.
CREATE ANY VIEW	Create views in any schema.
DROP ANY VIEW	Drop views in any schema.
UNDER ANY VIEW	Create subviews under any object views.
FLASHBACK ANY TABLE	Issue a SQL Flashback Query on any table, view, or materialized view in any schema. This privilege is not needed to execute the DBMS_FLASHBACK procedures.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
MERGE ANY VIEW	If a user has been granted the MERGE ANY VIEW privilege, then for any query issued by that user, the optimizer can use view merging to improve query performance without performing the checks that would otherwise be performed to ensure that view merging does not violate any security intentions of the view creator. See also *Oracle Database Reference* for information on the OPTIMIZER_SECURE_VIEW_MERGING parameter and *Oracle Database Performance Tuning Guide* for information on view merging.
MISCELLANEOUS:	--
ANALYZE ANY	Analyze any table, cluster, or index in any schema.
AUDIT ANY	Audit any object in any schema using AUDIT *schema_objects* statements.
CHANGE NOTIFICATION	Create a registration on queries and receive database change notifications in response to DML or DDL changes to the objects associated with the registered queries. Please refer to *Oracle Database Application Developer's Guide - Fundamentals* for more information on database change notification.
COMMENT ANY TABLE	Comment on any table, view, or column in any schema.
EXEMPT ACCESS POLICY	Bypass fine-grained access control. **Caution:** This is a very powerful system privilege, as it lets the grantee bypass application-driven security policies. Database administrators should use caution when granting this privilege.
FORCE ANY TRANSACTION	Force the commit or rollback of any in-doubt distributed transaction in the local database. Induce the failure of a distributed transaction.
FORCE TRANSACTION	Force the commit or rollback of the grantee s in-doubt distributed transactions in the local database.
GRANT ANY OBJECT PRIVILEGE	Grant any object privilege that the object owner is permitted to to grant. Revoke any object privilege that was granted by the object owner or by some other user with the GRANT ANY OBJECT PRIVILEGE privilege.
GRANT ANY PRIVILEGE	Grant any system privilege.
RESUMABLE	Enable resumable space allocation.
SELECT ANY DICTIONARY	Query any data dictionary object in the SYS schema. This privilege lets you selectively override the default FALSE setting of the O7_DICTIONARY_ACCESSIBILITY initialization parameter.
SELECT ANY TRANSACTION	Query the contents of the FLASHBACK_TRANSACTION_QUERY view. **Caution:** This is a very powerful system privilege, as it lets the grantee view all data in the database, including past data. This privilege should be granted only to users who need to use the Oracle Flashback Transaction Query feature.

Table 18–1 (Cont.) System Privileges

System Privilege Name	Operations Authorized
SYSDBA	Perform STARTUP and SHUTDOWN operations. ALTER DATABASE: open, mount, back up, or change character set. CREATE DATABASE. ARCHIVELOG and RECOVERY. CREATE SPFILE. Includes the RESTRICTED SESSION privilege.
SYSOPER	Perform STARTUP and SHUTDOWN operations. ALTER DATABASE: open, mount, or back up. ARCHIVELOG and RECOVERY. CREATE SPFILE. Includes the RESTRICTED SESSION privilege.
CONNECT, RESOURCE, and DBA	These roles are provided for compatibility with previous versions of Oracle Database. You can determine the privileges encompassed by these roles by querying the DBA_SYS_PRIVS data dictionary view. **Note:** Oracle recommends that you design your own roles for database security rather than relying on these roles. These roles may not be created automatically by future versions of Oracle Database. **See Also:** *Oracle Database Reference* for a description of the DBA_SYS_PRIVS view
DELETE_CATALOG_ROLE EXECUTE_CATALOG_ROLE SELECT_CATALOG_ROLE	These roles are provided for accessing data dictionary views and packages. **See Also:** *Oracle Database Administrator's Guide* for more information on these roles
EXP_FULL_DATABASE IMP_FULL_DATABASE	These roles are provided for convenience in using the import and export utilities. **See Also:** *Oracle Database Utilities* for more information on these roles
AQ_USER_ROLE AQ_ADMINISTRATOR_ROLE	You need these roles to use Oracle Advanced Queuing. **See Also:** *Oracle Streams Advanced Queuing User's Guide and Reference* for more information on these roles
SNMPAGENT	This role is used by the Enterprise Manager Intelligent Agent. **See Also:** *Oracle Enterprise Manager Administrator's Guide*
RECOVERY_CATALOG_OWNER	You need this role to create a user who owns a recovery catalog. **See Also:** *Oracle Database Backup and Recovery Advanced User's Guide* for more information on recovery catalogs

Table 18–2 Oracle Database Predefined Roles

Predefined Role	Purpose
HS_ADMIN_ROLE	A DBA using Oracle Database heterogeneous services needs this role to access appropriate tables in the data dictionary. **See Also:** *Oracle Database Heterogeneous Connectivity Administrator's Guide* for more information
SCHEDULER_ADMIN	This role allows the grantee to execute the procedures of the DBMS_SCHEDULER package. It includes all of the job scheduler system privileges and is included in the DBA role. **See Also:** *Oracle Database Administrator's Guide* for more information on the DBMS_SCHEDULER package

Table 18–3 Object Privileges Available for Particular Objects

Object Privilege	Table	View	Sequence	Procedure, Function, Package (Note 1)	Material-ized View	Directory	Library	User-defined Type	Operator	Indextype
ALTER (Note 2)	X	--	X	--	--	--	--	--	--	--
DELETE	X	X	--	--	X (Note 3)	--	--	--	--	--
EXECUTE	--	--	--	X (Note 2)	--	--	X (Note 2)	X (Note 2)	X (Note 2)	X (Note 2)
DEBUG	X	X	--	X	--	--	--	X	--	--
FLASHBACK	X	X	--	--	X	--	--	--	--	--
INDEX	X	--	--	--	--	--	--	--	--	--
INSERT	X	X	--	--	X (Note 3)	--	--	--	--	--
ON COMMIT REFRESH	X	--	--	--	--	--	--	--	--	--
QUERY REWRITE	X	--	--	--	--	--	--	--	--	--
READ	--	--	--	--	--	X	--	--	--	--
REFERENCES	X	X	--	--	--	--	--	--	--	--
SELECT	X	X	X	--	X	--	--	--	--	--
UNDER	--	X	--	--	--	--	--	X	--	--
UPDATE	X	X	--	--	X (Note 3)	--	--	--	--	--
WRITE	--	--	--	--	--	X	--	--	--	--

Note 1: Oracle Database treats a Java class, source, or resource as if it were a procedure for purposes of granting object privileges.

Note 2: Job scheduler objects are created using the DBMS_SCHEDULER package. After these objects are created, you can grant the EXECUTE object privilege on job scheduler classes and programs. You can grant ALTER privilege on job scheduler jobs, programs, and schedules.

Note 3: The DELETE, INSERT, and UPDATE privileges can be granted only to updatable materialized views.

Table 18–4 Object Privileges and the Operations They Authorize

Object Privilege	Operations Authorized
TABLE PRIVILEGES	The following **table privileges** authorize operations on a table. Any one of following object privileges allows the grantee to lock the table in any lock mode with the LOCK TABLE statement. **Note:** For external tables, the only valid object privileges are ALTER and SELECT.
ALTER	Change the table definition with the ALTER TABLE statement.
DELETE	Remove rows from the table with the DELETE statement. **Note:** You must grant the SELECT privilege on the table along with the DELETE privilege if the table is on a remote database.
DEBUG	Access, through a debugger: ■ PL/ SQL code in the body of any triggers defined on the table ■ Information on SQL statements that reference the table directly
INDEX	Create an index on the table with the CREATE INDEX statement.
INSERT	Add new rows to the table with the INSERT statement.
REFERENCES	Create a constraint that refers to the table. You cannot grant this privilege to a role.
SELECT	Query the table with the SELECT statement.
UPDATE	Change data in the table with the UPDATE statement. **Note:** You must grant the SELECT privilege on the table along with the UPDATE privilege if the table is on a remote database.
VIEW PRIVILEGES	The following **view privileges** authorize operations on a view. Any one of the following object privileges allows the grantee to lock the view in any lock mode with the LOCK TABLE statement. To grant a privilege on a view, you must have that privilege with the GRANT OPTION on all of the base tables of the view.
DEBUG	Access, through a debugger: ■ PL/ SQL code in the body of any triggers defined on the view ■ Information on SQL statements that reference the view directly
DELETE	Remove rows from the view with the DELETE statement.
INSERT	Add new rows to the view with the INSERT statement.
REFERENCES	Define foreign key constraints on the view.
SELECT	Query the view with the SELECT statement.
UNDER	Create a subview under this view. You can grant this object privilege only if you have the UNDER ANY VIEW privilege WITH GRANT OPTION on the immediate superview of this view.
UPDATE	Change data in the view with the UPDATE statement.
SEQUENCE PRIVILEGES	The following **sequence privileges** authorize operations on a sequence.
ALTER	Change the sequence definition with the ALTER SEQUENCE statement.
SELECT	Examine and increment values of the sequence with the CURRVAL and NEXTVAL pseudocolumns.
PROCEDURE, FUNCTION, PACKAGE PRIVILEGES	The following **procedure, function, and package privileges** authorize operations on procedures, functions, and packages. These privileges also apply to **Java sources, classes, and resources**, which Oracle Database treats as though they were procedures for purposes of granting object privileges.

Table 18–4 (Cont.) Object Privileges and the Operations They Authorize

Object Privilege	Operations Authorized
DEBUG	Access, through a debugger, all public and nonpublic variables, methods, and types defined on the object. Place a breakpoint or stop at a line or instruction boundary within the procedure, function, or package. This privilege grants access to the declarations in the method or package specification and body.
EXECUTE	Execute the procedure or function directly, or access any program object declared in the specification of a package, or compile the object implicitly during a call to a currently invalid or uncompiled function or procedure. This privilege does not allow the grantee to explicitly compile using ALTER PROCEDURE or ALTER FUNCTION. For explicit compilation you need the appropriate ALTER system privilege. Access, through a debugger, public variables, types, and methods defined on the procedure, function, or package. This privilege grants access to the declarations in the method or package specification only. **Note:** Users do not need this privilege to execute a procedure, function, or package indirectly. **See Also:** *Oracle Database Concepts* and *Oracle Database Application Developer's Guide - Fundamentals*
MATERIALIZED VIEW PRIVILEGES	The following **materialized view privileges** authorize operations on a materialized view.
ON COMMIT REFRESH	Create a refresh-on-commit materialized view on the specified table.
QUERY REWRITE	Create a materialized view for query rewrite using the specified table.
SELECT	Query the materialized view with the SELECT statement.
SYNONYM PRIVILEGES	**Synonym privileges** are the same as the privileges for the base object. Granting a privilege on a synonym is equivalent to granting the privilege on the base object. Similarly, granting a privilege on a base object is equivalent to granting the privilege on all synonyms for the object. If you grant to a user a privilege on a synonym, then the user can use either the synonym name or the base object name in the SQL statement that exercises the privilege.
DIRECTORY PRIVILEGES	The following **directory privileges** provide secured access to the files stored in the operating system directory to which the directory object serves as a pointer. The directory object contains the full path name of the operating system directory where the files reside. Because the files are actually stored outside the database, Oracle Database server processes also need to have appropriate file permissions on the file system server. Granting object privileges on the directory database object to individual database users, rather than on the operating system, allows the database to enforce security during file operations.
READ	Read files in the directory.
WRITE	Write files in the directory. This privilege is useful only in connection with external tables. It allows the grantee to determine whether the external table agent can write a log file or a bad file to the directory. **Restriction:** This privilege does not allow the grantee to write to a BFILE.
LIBRARY PRIVILEGE	The following **library privilege** authorizes operations on a library.
EXECUTE	Use and reference the specified object and invoke its methods.
OBJECT TYPE PRIVILEGES	The following **object type privileges** authorize operations on a database object type.

Table 18–4 (Cont.) Object Privileges and the Operations They Authorize

Object Privilege	Operations Authorized
DEBUG	Access, through a debugger, all public and nonpublic variables, methods, and types defined on the object type. Place a breakpoint or stop at a line or instruction boundary within the type body.
EXECUTE	Use and reference the specified object and invoke its methods. Access, through a debugger, public variables, types, and methods defined on the object type.
UNDER	Create a subtype under this type. You can grant this object privilege only if you have the UNDER ANY TYPE privilege WITH GRANT OPTION on the immediate supertype of this type.
INDEXTYPE PRIVILEGE	The following **indextype privilege** authorizes operations on indextypes.
EXECUTE	Reference an indextype.
OPERATOR PRIVILEGE	The following **operator privilege** authorizes operations on user-defined operators.
EXECUTE	Reference an operator.

Examples

Granting a System Privilege to a User: Example To grant the CREATE SESSION system privilege to the sample user hr, allowing hr to log on to Oracle Database, issue the following statement:

```
GRANT CREATE SESSION
   TO hr;
```

Granting System Privileges to a Role: Example The following statement grants appropriate system privileges to a data warehouse manager role, which was created in the "Creating a Role: Example" on page 15-65:

```
GRANT
     CREATE ANY MATERIALIZED VIEW
   , ALTER ANY MATERIALIZED VIEW
   , DROP ANY MATERIALIZED VIEW
   , QUERY REWRITE
   , GLOBAL QUERY REWRITE
   TO dw_manager
   WITH ADMIN OPTION;
```

The dw_manager privilege domain now contains the system privileges related to materialized views.

Granting a Role with the Admin Option: Example To grant the dw_manager role with the ADMIN OPTION to the sample user sh, issue the following statement:

```
GRANT dw_manager
   TO sh
   WITH ADMIN OPTION;
```

User sh can now perform the following operations with the dw_manager role:

- Enable the role and exercise any privileges in the privilege domain of the role, including the CREATE MATERIALIZED VIEW system privilege
- Grant and revoke the role to and from other users

- Drop the role

Granting Object Privileges to a Role: Example The following example grants the SELECT object privileges to a data warehouse user role, which was created in the "Creating a Role: Example" on page 15-65:

```
GRANT SELECT ON sh.sales TO warehouse_user;
```

Granting a Role to a Role: Example The following statement grants the warehouse_user role to the dw_manager role. Both roles were created in the "Creating a Role: Example" on page 15-65:

```
GRANT warehouse_user TO dw_manager;
```

The dw_manager role now contains all of the privileges in the domain of the warehouse_user role.

Granting an Object Privilege on a Directory: Example To grant READ on directory bfile_dir to user hr, with the GRANT OPTION, issue the following statement:

```
GRANT READ ON DIRECTORY bfile_dir TO hr
   WITH GRANT OPTION;
```

Granting Object Privileges on a Table to a User: Example To grant all privileges on the table oe.bonuses, which was created in "Merging into a Table: Example" on page 18-74, to the user hr with the GRANT OPTION, issue the following statement:

```
GRANT ALL ON bonuses TO hr
   WITH GRANT OPTION;
```

The user hr can subsequently perform the following operations:

- Exercise any privilege on the bonuses table
- Grant any privilege on the bonuses table to another user or role

Granting Object Privileges on a View: Example To grant SELECT and UPDATE privileges on the view emp_view, which was created in "Creating a View: Example" on page 17-39, to all users, issue the following statement:

```
GRANT SELECT, UPDATE
   ON emp_view TO PUBLIC;
```

All users can subsequently query and update the view of employee details.

Granting Object Privileges to a Sequence in Another Schema: Example To grant SELECT privilege on the customers_seq sequence in the schema oe to the user hr, issue the following statement:

```
GRANT SELECT
   ON oe.customers_seq TO hr;
```

The user hr can subsequently generate the next value of the sequence with the following statement:

```
SELECT oe.customers_seq.NEXTVAL
   FROM DUAL;
```

Granting Multiple Object Privileges on Individual Columns: Example To grant to user oe the REFERENCES privilege on the employee_id column and the UPDATE

privilege on the employee_id, salary, and commission_pct columns of the employees table in the schema hr, issue the following statement:

```
GRANT REFERENCES (employee_id),
      UPDATE (employee_id, salary, commission_pct)
   ON hr employees
   TO oe;
```

The user oe can subsequently update values of the employee_id, salary, and commission_pct columns. User oe can also define referential integrity constraints that refer to the employee_id column. However, because the GRANT statement lists only these columns, oe cannot perform operations on any of the other columns of the employees table.

For example, oe can create a table with a constraint:

```
CREATE TABLE dependent
    (dependno   NUMBER,
    dependname VARCHAR2 10),
    employee   NUMBER
   CONSTRAINT in_emp REFERENCES hr employees employee_id) );
```

The constraint in_emp ensures that all dependents in the dependent table correspond to an employee in the employees table in the schema hr.