

# GRANT and REVOKE

## GRANTED BY

Available in: [DSQL](#)

Added in: 2.5

### Description

When a privilege is granted, it is normally stored in the database with the current user as the grantor. With the **GRANTED BY** clause, the user who grants the privilege can have someone else registered as the grantor. When **GRANTED BY** is used with **REVOKE**, the privilege (registered as) granted by the named user will be removed. To make migration from certain other RDBMSes easier, the non-standard **AS** is supported as a synonym of **GRANTED BY**.

Access: Use of the **GRANTED BY** clause is reserved to:

- The database owner;
- SYSDBA;
- anybody who has the [RDB\\$ADMIN role](#) in the database and specified it while connecting;
- if [AUTO ADMIN MAPPING](#) is on for the database: any Windows administrator who connected to the database using trusted authentication without specifying a role.

Even the owner of the role can't use **GRANTED BY** if he isn't in the above list.

### Syntax

```
GRANT
  {<privileges> ON <object> | role}
  TO <grantees>
  [WITH {GRANT|ADMIN} OPTION]
  [{GRANTED BY | AS} [USER] grantor]
```

```
REVOKE
  [{GRANT|ADMIN} OPTION FOR]
  {<privileges> ON <object> | role}
  FROM <grantees>
  [{GRANTED BY | AS} [USER] grantor]
```

(These are not the complete **GRANT** and **REVOKE** syntaxes, but they are complete as far as **GRANTED BY** is concerned.)

### Example

1. - connected as database owner BOB:

```
create role digger;
```

```
grant digger to francis;
grant digger to fred;
grant digger to frank with admin option granted by fritz;
commit;

revoke digger from fred;
-- OK
revoke admin option for digger from frank;
-- error: "BOB is not grantor of Role on DIGGER to FRANK."
revoke admin option for digger from frank granted by fritz;
-- OK
revoke digger from frank
-- error: "BOB is not grantor of Role on DIGGER to FRANK."
commit;

-- exit BOB, enter FRITZ:

revoke digger from frank;
-- OK
revoke digger from francis;
-- error: "FRITZ is not grantor of Role on DIGGER to FRANCIS."
revoke digger from francis granted by bob;
-- error: "Only SYSDBA or database owner can use GRANTED BY clause"
commit;
```

*Note:* Please notice that a **GRANT** or **ADMIN** option is just a flag in the privilege record; it does not have a separate grantor. So this line:

```
grant digger to frank with admin option granted by fritz
```

does not mean *Grant digger to Frank*, and *grant the admin option in Fritz's name*, but *Grant digger to Frank with admin option – all in Fritz's name*.

[back to top of page](#)

## REVOKE ALL ON ALL

Available in: [DSQL](#)

Added in: 2.5

### Description

Revokes all privileges (including role memberships) on all objects from one or more users and/or roles. This is a quick way to “clean up” when a user has left the system or must be locked out of the database.

### Syntax

```
REVOKE ALL ON ALL FROM <grantee> [, <grantee> ...]  
  
<grantee> ::= [USER] username | [ROLE] rolename
```

### Example

```
revoke all on all from buddy, peggy, sue
```

#### Notes:

- When invoked by a privileged user (the database owner, `SYSDBA` or anyone whose `CURRENT_ROLE` is `RDB$ADMIN`), all privileges are removed regardless of the grantor. Otherwise, only those privileges granted by the current user are removed.
- The `GRANTED BY` clause is not supported.
- This statement cannot be used to revoke privileges from stored procedure, trigger or view grantees. (Privileges ON such objects are removed, of course.)

[back to top of page](#)

## REVOKE ADMIN OPTION

Available in: [DSQL](#)

Added in: 2.0

### Description

Revokes a previously granted admin option (the right to pass on a granted role to others) from the grantee, without revoking the role itself. Multiple roles and/or multiple grantees can be handled in one statement.

### Syntax

```
REVOKE ADMIN OPTION FOR <role-list> FROM <grantee-list>  
  
<role-list> ::= role [, role ...]  
<grantee-list> ::= [USER] <grantee> [, [USER] <grantee> ...]  
<grantee> ::= username | PUBLIC
```

#### Example

```
revoke admin option for manager from john, paul, george, ringo
```

If a user has received the admin option from several grantors, each of those grantors must revoke it or the user will still be able to grant the role(s) in question to others.

From:  
<http://ibexpert.com/docu/> - **IBExpert**

Permanent link:  
<http://ibexpert.com/docu/doku.php?id=01-documentation:01-09-sql-language-references:firebird2.5-language-reference-update:security-and-access-control:grant-and-revoke>

Last update: **2023/08/04 06:44**

