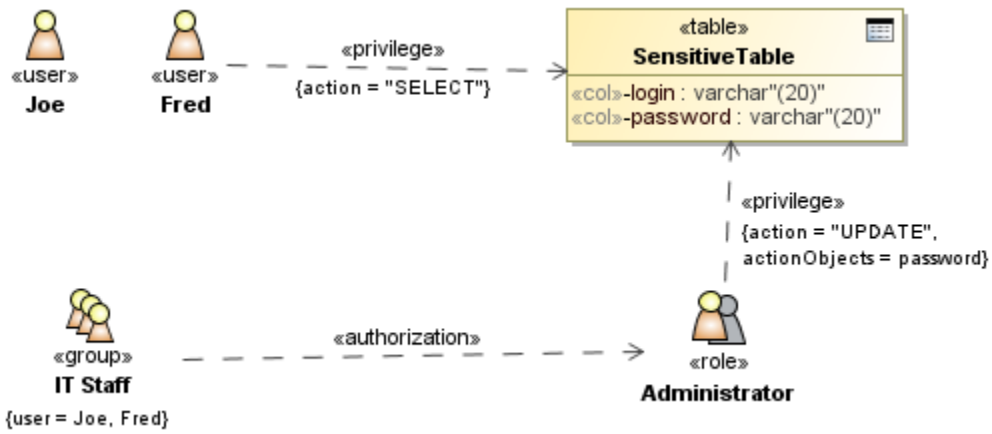
Access control

On this page



Access control example.

SQL has means to specify and control the rules of access to various data objects. This subset of SQL language is sometimes called Data Control Language. The relevant concepts are: User, Group, Role (3 different kinds of authorization subjects), Permission and Role Authorization (2 kinds of access control rules). Possible object types for access control varies depending on database flavor, but usually Tables, User-defined Types, Domains, Routines, Sequences can be specified as the target objects of access control.

User

> **Note**
> SQL User is modeled as UML Actor with the «User» stereotype applied.

User object represents the single user person in the system. User is subject to access control rules.

Besides the standard SQL element properties, user has the following properties available in the Specification window.

Property name	Description
Owned Schema	Schemas that are owned by this user.

Group

> **Note**
> SQL Group is modeled as UML Actor with the «Group» stereotype applied.

Group object represents a collection of Users. Group is subject to access control rules, and allows specifying access control rules on several users simultaneously.

Besides the standard SQL element properties, group has the following properties available in the Specification window.

Property name	Description
User	Collection of users the group is made of.
Owned Schema	Schemas that are owned by this group.

Role

> **Note**
> SQL Role is modeled as UML Actor with the «Role» stereotype applied.

Role object represents a specific role (typical activities) that can be played by users. Role is subject to access control rules, and allows specifying access control rules for all subjects, playing this role.

Besides the standard SQL element properties, role has the following properties available in the Specification window.

Property name	Description
Owned Schema	Schemas that are owned by this role.

Privilege

> **Note**
> SQL Privilege is modeled as UML Dependency with the «Privilege» stereotype applied.

Privilege relationship expresses the fact that the permission to perform specified action on specified object (relationship target) is granted to specified grantee (relationship source). Grantee can be any authorization subject - Use, Group or another Role. Object can by another SQL object (the precise list of object types, that can be targeted by privileges, varies by database type).

Privilege corresponds to SQL grant privilege statement as follows.

```
GRANT <action>[(<column list>)] ON <object> TO <grantee> [WITH HIERARCHY
OPTION][WITH GRANT OPTION]
```

Besides the standard SQL element properties, privilege has the following properties available in the Specification window.

Property name	Description
Action	Specifies action that is being granted (such as SELECT or UPDATE).
Action Objects	Specifies additional more narrow subobject lists, on which the specified action is permitted (usually column list for SELECT or UPDATE).
Grantable	Specifies that this privilege can be further re-granted to other subjects by the recipients. Corresponds to WITH GRANT OPTION part of GRANT statement.
With Hierarchy	Specifies that this privilege applies to subobjects (subtables). Corresponds to WITH HIERARCHY OPTION part of the GRANT statement.
Grantor	Subject, who grants this privilege to the grantees.

Role authorization

> **Note**
> SQL Role Authorization is modeled as UML Dependency with «RoleAuthorization» stereotype applied.

Role authorization relationship expresses the fact that the specified role (relationship target) is granted to specified grantee (relationship source). Grantee can be any authorization subject - Use, Group or another Role.

Role authorization corresponds to SQL grant role statement as follows.

```
GRANT <role> TO <grantee> [WITH ADMIN OPTION]
```

Besides the standard SQL element properties, role authorization has the following properties available in the Specification window.

Property name	Description
Grantable	Specifies that this role can be further re-granted to other subjects by the recipients. Corresponds to WITH ADMIN OPTION part of GRANT statement.
Grantor	Subject, who grants this role to the grantees.