

## Table of Contents

<b>SERVER SECURITY MANAGEMENT</b>	<b>3</b>
MYSQL SECURITY MANAGEMENT	4
<i>Privileges Provided by MySQL</i>	6
<i>MySQL User Designer</i>	7
Editing MySQL User General	8
Setting Advanced MySQL User Properties	9
Setting MySQL User Server Privileges	11
Setting MySQL User Object Privileges	12
ORACLE SECURITY MANAGEMENT	13
<i>Privileges Provided by Oracle</i>	17
<i>Oracle User Designer</i>	18
Editing Oracle User General	19
Setting Oracle User Roles	21
Setting Oracle User Quotas	22
Setting Oracle User System Privileges	23
Setting Oracle User Object Privileges	24
<i>Oracle Role Designer</i>	25
Editing Oracle Role General	26
Setting Oracle Role to Roles	27
Setting Oracle Role Members	28
Setting Oracle Role System Privileges	29
Setting Oracle Role Object Privileges	30
POSTGRESQL SECURITY MANAGEMENT	31
<i>Privileges Provided by PostgreSQL</i>	36
<i>Manage Users for PostgreSQL Server 7.3 to 8.0</i>	37
PostgreSQL User Designer	38
Editing PostgreSQL User General	39
Setting PostgreSQL User Membership	40
Setting PostgreSQL User Object Privileges	41
PostgreSQL Group Designer	42
Editing PostgreSQL Group General	43
Setting PostgreSQL Group Users	44
Setting PostgreSQL Group Object Privileges	45
<i>Manage Users for PostgreSQL Server 8.1 to 9.1</i>	46
PostgreSQL Role Designer	47
Editing PostgreSQL Role General	48
Setting PostgreSQL Role Membership	50

Setting PostgreSQL Role Members	51
Setting PostgreSQL Role Object Privileges	52
SQL SERVER SECURITY MANAGEMENT	53
<i>Privileges Provided by SQL Server</i>	61
<i>SQL Server Login Designer</i>	63
Editing SQL Server Login General	64
Setting SQL Server Login Roles	67
Setting SQL Server Login User Mapping	68
Setting SQL Server Login Server Permissions	69
Setting SQL Server Login Endpoint Permissions	70
Setting SQL Server Login Login Permissions	71
<i>SQL Server Server Role Designer</i>	72
Editing SQL Server Server Role Members	73
<i>SQL Server Database User Designer</i>	74
Editing SQL Server Database User General	75
Setting SQL Server Database User Roles	77
Setting SQL Server Database User Database Permissions	78
Setting SQL Server Database User Object Permissions	79
<i>SQL Server Database Role Designer</i>	80
Editing SQL Server Database Role General	81
Setting SQL Server Database Role Members	82
Setting SQL Server Database Role Membership	83
Setting SQL Server Database Role Database Permissions	84
Setting SQL Server Database Role Object Permissions	85
<i>SQL Server Application Role Designer</i>	86
Editing SQL Server Application Role General	87
Setting SQL Server Application Role Database Permissions	88
Setting SQL Server Application Role Object Permissions	89
PRIVILEGE MANAGER	90


## Server Security Management

Navicat provides server security management for MySQL, Oracle, PostgreSQL and SQL Server.

- [MySQL Security Management](#)
- [Oracle Security Management](#)
- [PostgreSQL Security Management](#)
- [SQL Server Security Management](#)
- [Privilege Manager](#)



## MySQL Security Management

Navicat provides **User** to add, duplicate, edit, delete users, grant/revoke server privileges and privileges on the selected databases, tables/views, fields and functions/procedures. The object pane displays all the users that exist in the **user** table.

Just simply click  to open an object pane for **User**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete users.


### Add User

To add a new user

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **User** showing the user list.
- Click the  from the object pane toolbar or control-click and select **New User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



### Duplicate User

To create a new user with modification as one of the existing users

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Control-click the user and select **Duplicate User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



### Edit User

To edit an existing user

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Design User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.

## Delete User

To delete a user

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **User** showing the user list.
- Select a user to delete in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Delete User** from the popup menu.
- Confirm deleting in the dialog window.

## Privilege Manager

To edit privilege according to the database objects by using Privilege Manager

- Select the connection you wish to set privileges in the navigation pane.
- Choose **Connection** -> **Set Privileges** or control-click the connection and select **Set Privileges** from the popup menu to open the **Privilege Manager** window and set privileges.

## Privileges Provided by MySQL

The primary function of the MySQL privilege system is to authenticate a user who connects from a given host and to associate that user with privileges on a database such as *SELECT*, *INSERT*, *UPDATE*, and *DELETE*.

Information about user privileges is stored in the **user**, **db**, **host**, **tables\_priv**, **columns\_priv**, and **procs\_priv** tables in the **mysql** database (that is, in the database named **mysql**). The MySQL server reads the contents of these tables when it starts.

MySQL access control involves two stages when you run a client program that connects to the server:

- Stage 1: The server checks whether it should allow you to connect.
- Stage 2: Assuming that you can connect, the server checks each statement you issue to determine whether you have sufficient privileges to perform it. For examples: Create table privilege, Drop table privilege or Alter table privilege.

The server uses the **user**, **db**, and **host** tables in the **mysql** database at both stages of access control.

## MySQL User Designer

The **User Designer** window allows you to set different properties and privileges for a MySQL user.

- [Editing User General](#)
- [Setting Advanced User Properties](#)
- [Setting Server Privileges](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing MySQL User General

The **General** tab allows you to set user properties which are **User name**, **Host** and **Password**.

## Setting Advanced MySQL User Properties

### Maximum Queries Per Hour, Maximum Updates Per Hour and Maximum Connections Per Hour

These options limit the number of queries, updates, and logins a user can perform during any given one-hour period. If they are set as 0 (the default), this means that there is no limitation for that user.

### Maximum User Connection

This option limits the maximum number of simultaneous connections that the account can make. If it is set as 0 (the default), the *max\_user\_connections* system variable determines the number of simultaneous connections for the account.

### Use OLD\_PASSWORD encryption

The password hashing mechanism was updated in MySQL 4.1 to provide better security and to reduce the risk of passwords being intercepted. However, this new mechanism is understood only by MySQL 4.1 (and newer) servers and clients, which can result in some compatibility problems. A 4.1 or newer client can connect to a pre-4.1 server, because the client understands both the old and new password hashing mechanisms. However, a pre-4.1 client that attempts to connect to a 4.1 or newer server may run into difficulties.

Enable this option if you wish to maintain backward compatibility with pre-4.1 clients under circumstances where the server would otherwise generate long password hashes. The option does not affect authentication (4.1 and later clients can still use accounts that have long password hashes), but it does prevent creation of a long password hash in the *user* table as the result of a password-changing operation.

### SSL

MySQL can check X509 certificate attributes in addition to the usual authentication that is based on the username and password. To specify SSL-related options for a MySQL account, use the *REQUIRE* clause of the *GRANT* statement.

### ANY

This option tells the server to allow only SSL-encrypted connections for the account.

Example:

```
GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost'  
IDENTIFIED BY 'goodsecret' REQUIRE SSL;
```

## **X509**

This means that the client must have a valid certificate but that the exact certificate, issuer, and subject do not matter. The only requirement is that it should be possible to verify its signature with one of the CA certificates.

Example:

```
GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost'  
IDENTIFIED BY 'goodsecret' REQUIRE SSL;
```

## **SPECIFIED**

Example:

```
GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost'  
IDENTIFIED BY 'goodsecret'  
REQUIRE SUBJECT '/C=EE/ST=Some-State/L=Tallinn/  
O=MySQL demo client certificate/  
CN=Tonu Samuel/Email=tonu@example.com'  
AND ISSUER '/C=FI/ST=Some-State/L=Helsinki/  
O=MySQL Finland AB/CN=Tonu Samuel/Email=tonu@example.com'  
AND CIPHER 'EDH-RSA-DES-CBC3-SHA';
```

### **Issuer**

This places the restriction on connection attempts that the client must present a valid X509 certificate issued by CA *issuer*. If the client presents a certificate that is valid but has a different issuer, the server rejects the connection. Use of X509 certificates always implies encryption, so the SSL option is unnecessary in this case.

### **Subject**

This places the restriction on connection attempts that the client must present a valid X509 certificate containing the subject *subject*. If the client presents a certificate that is valid but has a different subject, the server rejects the connection.

### **Cipher**


This is needed to ensure that ciphers and key lengths of sufficient strength are used. SSL itself can be weak if old algorithms using short encryption keys are used. Using this option, you can ask that a specific cipher method is used to allow a connection.

## Setting MySQL User Server Privileges

In the grid, check **Grant** option against the server privilege listed in **Privilege** to assign this user to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All** or **Revoke All** option.

## Setting MySQL User Object Privileges

To edit the specific object privileges of the user, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** option against the privilege listed in **Privilege** to assign this user to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.


## Oracle Security Management

Oracle manages database access permissions using users and roles. Users own schema objects (for example, tables, views) and can assign privileges on those objects to other users to control who has access to which objects.

Navicat provides **User** to add, duplicate, edit, delete users/roles, grant/revoke server privileges and privileges on the selected schema objects. The object pane displays all the users/roles that exist in the server.



In addition to the user accounts that you create, the database includes a number of user accounts that are automatically created upon installation. Administrative accounts: **SYS**, **SYSTEM**, **SYSMAN**, and **DBSNMP**. Administrative accounts are highly privileged accounts to perform administrative tasks such as starting and stopping the database, managing database memory and storage, creating and managing database users, and so on. Your database may also include sample schemas (**SCOTT**, **HR**, **OE**, **OC**, **PM**, **IX** and **SH**), which are a set of interlinked schemas that enable Oracle documentation and Oracle instructional materials to illustrate common database tasks.

### Manager User

Just simply click -> **User** to open an object pane for **User**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete users.


### Add User

To add a new user

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Click the  from the object pane toolbar or control-click and select **New User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



## Duplicate User

To create a new user with modification as one of the existing users

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Control-click the user and select **Duplicate User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



## Edit User

To edit an existing user


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Design User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.

## Delete User

To delete a user



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Select a user to delete in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Delete User** from the popup menu.
- Confirm deleting in the dialog window.

## Manage Role

Just simply click -> **Role** to open an object pane for **Role**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete roles.


## Add Role

To add a new role

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Role** to open the **Role** showing the role list.
- Click the  from the object pane toolbar or control-click and select **New Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.



## Duplicate Role

To create a new role with modification as one of the existing roles

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **Role** showing the role list.
- Select a role to edit in the object pane.
- Control-click the role and select **Duplicate Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.



## Edit Role

To edit an existing role

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Role** to open the **Role** showing the role list.
- Select a role to edit in the object pane.
- Click the  from the object pane toolbar or control-click the role and select **Design Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.

## Delete Role

To delete a role

- Select the connection you wish to set privileges in the navigation pane.
- Click  -> **Role** to open the **Role** showing the role list.
- Select a role to delete in the object pane.
- Click the  from the object pane toolbar or control-click the role and select **Delete Role** from the popup menu.
- Confirm deleting in the dialog window.

## Privilege Manager

To edit privilege according to the database objects by using Privilege Manager

- Select the connection you wish to set privileges in the navigation pane.
- Choose **Connection** -> **Set Privileges** or control-click the connection and select **Set Privileges** from the popup menu to open the **Privilege Manager** window and set privileges.

## Privileges Provided by Oracle

In Oracle, a set of access privileges and restrictions exist for each applicable database object.

When you create a database object, you become its owner. By default, only the owner of an object can do anything with the object. In order to allow other users to use it, privileges must be granted. (However, users that have the superuser attribute can always access any object.)

Ordinarily, only the object's owner (or a superuser) can grant or revoke privileges on an object. However, it is possible to grant a privilege **Admin Option/Grant Option**, which gives the recipient the right to grant it in turn to others. If the grant option is subsequently revoked then all who received the privilege from that recipient (directly or through a chain of grants) will lose the privilege.

**Note:** The special name **PUBLIC** is accessible to every database user, all privileges and roles granted to **PUBLIC** are accessible to every database user.

## Oracle User Designer

The **User Designer** window allows you to set different properties and privileges for a Oracle user.

- [Editing User General](#)
- [Setting User Roles](#)
- [Setting User Quotas](#)
- [Setting System Privileges](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing Oracle User General

The **General** tab allows you to set user properties which are:

### User name

Set name of the user.

### Authentication

Choose to use either Password, External or Global as authentication method.

#### Password

A local user must specify password to log on to the database.

##### Password

Set user's password.

##### Confirm Password

Re-type the user's password here.

##### Expire Password

Expire the user's password. This setting forces the user or the DBA to change the password before the user can log in to the database.

#### External

An external user must be authenticated by an external service, such as an operating system or a third-party service.

#### Global

A global user must be authorized by the enterprise directory service (Oracle Internet Directory).

#### X.500 Distinguished Name

Enter the X.509 name at the enterprise directory service that identifies this user.

#### Default Tablespace

Choose the default tablespace for objects that the user creates.

#### Temporary Tablespace

Choose the tablespace or tablespace group for the user's temporary segments.

## Profile

Choose the profile that assign to the user.

### **Locked account**

Lock the user's account and disable access.

## Setting Oracle User Roles

In the grid, check **Granted**, **Admin Option** or **Default** option against the role listed in **Role Name** to assign this user to be a member of selected role. Multiple roles can be granted.

## Setting Oracle User Quotas


In the grid, specify the maximum amount of space the user can allocate in the tablespaces. Enter the **Quota** and choose the **Unit** of the **Tablespace**. **Unlimited** lets the user allocate space in the tablespace without bound. Multiple tablespaces can be set.

## Setting Oracle User System Privileges

In the grid, check **Grant** or **Admin Option** option against the system privilege listed in **Privilege** to assign this user to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All with Grant Option** or **Revoke All** option.

## Setting Oracle User Object Privileges

To edit the specific object privileges of the user, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** or **Grant Option** option against the privilege listed in **Privilege** to assign this user to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All with Grant Option** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## Oracle Role Designer

The **Role Designer** window allows you to set different properties and privileges for a Oracle role.

- [Editing Role General](#)
- [Setting Role to Roles](#)
- [Setting Role Members](#)
- [Setting System Privileges](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing Oracle Role General

The **General** tab allows you to set role properties which are:

### **Role name**

Set name of the role.

### **Authentication**

Choose to use either Password, External or Global Authentication method.

#### **Not Identified**

The role is authorized by the database and that no password is required to enable the role.

#### **Password**

User must specify the password to the database when enabling the role.

##### **Password**

Set role's password.

##### **Confirm Password**

Re-type the role's password here.

#### **External**

An external user must be authorized by an external service, such as an operating system or third-party service, before enabling the role.

#### **Global**

A global user must be authorized to use the role by the enterprise directory service before the role is enabled at login.

## Setting Oracle Role to Roles

In the grid, check **Granted** or **Admin Option** option against the role listed in **Role Name** to assign this role to be a member of selected role. Multiple roles can be granted.

## Setting Oracle Role Members


In the grid, check **Granted** or **Admin Option** option against user listed in **Name** to assign the selected user to be a member of this role. Multiple users can be granted.

## Setting Oracle Role System Privileges

In the grid, check **Grant** or **Admin Option** option against the system privilege listed in **Privilege** to assign this role to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All with Grant Option** or **Revoke All** option.

## Setting Oracle Role Object Privileges

To edit the specific object privileges of the role, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** or **Grant Option** option against the privilege listed in **Privilege** to assign this role to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All With Grant Option** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## PostgreSQL Security Management

PostgreSQL manages database access permissions using users and groups. Users own database objects (for example, tables) and can assign privileges on those objects to other users to control who has access to which objects.

**Note:** Starting from PostgreSQL version 8.1, users and groups were no longer distinct kinds of entities, now there are only roles. Any role can act as a user, a group, or both. The concept of roles subsumes the concepts of users and groups.


Navicat provides **User** to add, duplicate, edit, delete users/groups/roles, grant/revoke server privileges and privileges on the selected database objects. The object pane displays all the users/groups/roles that exist in the server.

Only a superuser (a user who is allowed all rights) can add/delete users. PostgreSQL installs a single superuser by default named **postgres**. All other users must be added by this user, or by another subsequently added superuser.

The **User** for PostgreSQL Server 7.3 to 8.0 and PostgreSQL Server 8.1 to 9.1 are different.



### PostgreSQL Server 7.3 to 8.0

#### Manage User

Just simply click -> **User** to open an object pane for **User**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete users.


#### Add User

To add a new user

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Click the  from the object pane toolbar or control-click and select **New User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



## Duplicate User

To create a new user with modification as one of the existing users

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Control-click the user and select **Duplicate User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.



## Edit User

To edit an existing user


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Select a user to edit in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Design User** from the popup menu.
- Edit user properties and privileges on the appropriate tabs of the User Designer.

## Delete User

To delete a user



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **User** to open the **User** showing the user list.
- Select a user to delete in the object pane.
- Click the  from the object pane toolbar or control-click the user and select **Delete User** from the popup menu.
- Confirm deleting in the dialog window.

## Manage Group

Just simply click -> **Group** to open an object pane for **Group**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete groups.


## Add Group

To add a new group

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Group** to open the **Group** showing the group list.
- Click the  from the object pane toolbar or control-click and select **New Group** from the popup menu.
- Edit group properties and privileges on the appropriate tabs of the Group Designer.



## Duplicate Group

To create a new group with modification as one of the existing groups

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Group** to open the **Group** showing the group list.
- Select a group to edit in the object pane.
- control-click the group and select **Duplicate Group** from the popup menu.
- Edit group properties and privileges on the appropriate tabs of the Group Designer.



## Edit Group

To edit an existing group


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Group** to open the **Group** showing the group list.
- Select a group to edit in the object pane.
- Click the  from the object pane toolbar or control-click the group and select **Design Group** from the popup menu.
- Edit group properties and privileges on the appropriate tabs of the Group Designer.

## Delete Group

To delete a group



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Group** to open the **Group** showing the group list.
- Select a group to delete in the object pane.
- Click the  from the object pane toolbar or control-click the group and select **Delete Group** from the popup menu.
- Confirm deleting in the dialog window.

## PostgreSQL Server 8.1 to 9.1

Just simply click  to open an object pane for **Role**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete roles.


## Add Role

To add a new role

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **Role** showing the role list.
- Click the  from the object pane toolbar or control-click and select **New Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.



## Duplicate Role

To create a new role with modification as one of the existing roles

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **Role** showing the role list.
- Select a role to edit in the object pane.
- control-click the role and select **Duplicate Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.



## Edit Role

To edit an existing role

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **Role** showing the role list.
- Select a role to edit in the object pane.
- Click the  from the object pane toolbar or control-click the role and select **Design Role** from the popup menu.
- Edit role properties and privileges on the appropriate tabs of the Role Designer.

## Delete Role

To delete a role

- Select the connection you wish to set privileges in the navigation pane.
- Click  to open the **Role** showing the role list.
- Select a role to delete in the object pane.
- Click the  from the object pane toolbar or control-click the role and select **Delete Role** from the popup menu.
- Confirm deleting in the dialog window.

## Privilege Manager

To edit privilege according to the database objects by using Privilege Manager

- Select the connection you wish to set privileges in the navigation pane.
- Choose **Connection** -> **Set Privileges** or control-click the connection and select **Set Privileges** from the popup menu to open the **Privilege Manager** window and set privileges.

## Privileges Provided by PostgreSQL

In PostgreSQL, a set of access privileges and restrictions exist for each applicable database object.

When you create a database object, you become its owner. By default, only the owner of an object can do anything with the object. In order to allow other users to use it, privileges must be granted. (However, users that have the superuser attribute can always access any object.)

Different privileges: *SELECT, INSERT, UPDATE, DELETE, REFERENCES, TRIGGER, CREATE, CONNECT, TEMPORARY, EXECUTE, and USAGE*. The privileges applicable to a particular object vary depending on the object's type (table, function, etc).

Ordinarily, only the object's owner (or a superuser) can grant or revoke privileges on an object. However, it is possible to grant a privilege **Grant Option**, which gives the recipient the right to grant it in turn to others. If the grant option is subsequently revoked then all who received the privilege from that recipient (directly or through a chain of grants) will lose the privilege.

**Note:** The special name **public** can be used to grant a privilege to every role (user/group) on the system.

## Manage Users for PostgreSQL Server 7.3 to 8.0

PostgreSQL version 7.3 to 8.0 manages database access permissions using users and groups.

- [User Designer](#)
- [Group Designer](#)

## PostgreSQL User Designer

The **User Designer** window allows you to set different properties and privileges for a PostgreSQL user.

- [Editing User General](#)
- [Setting User Membership](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing PostgreSQL User General

The **General** tab allows you to set user properties which are:

### User Name

Set name of the user.

### User ID

Specify an ID for the user. This is normally not necessary, but may be useful if you need to recreate the owner of an orphaned object. If this is not specified, the highest assigned user ID plus one (with a minimum of 100) will be used as default.

### Password

Set user's password.

**Note:** If you do not plan to use password authentication you can omit this option, but then the user will not be able to connect if you decide to switch to password authentication.

### Confirm Password

Re-type the password here.

### Password Encryption

This option control whether the password is stored **ENCRYPTED** or **UNENCRYPTED** in the system catalogs. (If neither is specified, the default behavior is determined by the configuration parameter *password\_encryption*.)

### Expiry Date

Set a date and time after which the user's password is no longer valid. If this clause is omitted the password will be valid for all time.

### Can create databases

Check this option to define the user to be allowed to create databases.


### Superuser

Check this option to define the user as a superuser.

## Setting PostgreSQL User Membership

In the grid, check **Granted** option against the group listed in **Group Name** to assign this user to be a member of selected group. Multiple groups can be granted.

## Setting PostgreSQL User Object Privileges

To edit the specific object privileges of the user, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** or **Grant Option** option against the privilege listed in **Privilege** to assign this user to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All with Grant Option** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## PostgreSQL Group Designer

The **Group Designer** window allows you to set different properties and privileges for a PostgreSQL group.

- [Editing Group General](#)
- [Setting Group Users](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing PostgreSQL Group General

The **General** tab allows you to set group properties which are:

### **Group name**

Set name of the group.


### **Group ID**

Specify an ID for the group. This is normally not necessary, but may be useful if you need to recreate a group referenced in the permissions of some object. If this is not specified, the highest assigned group ID plus one (with a minimum of 100) will be used as default.

## Setting PostgreSQL Group Users

In the grid, check **Granted** option against the user listed in **User Name** to assign selected user to be a member of this group. Multiple users can be granted.

## Setting PostgreSQL Group Object Privileges

To edit the specific object privileges of the group, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** option against the privilege listed in **Privilege** to assign this group to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## Manage Users for PostgreSQL Server 8.1 to 9.1

Starting from PostgreSQL version 8.1, users and groups were no longer distinct kinds of entities, now there are only roles. Any role can act as a user, a group, or both. The concept of roles subsumes the concepts of users and groups.

- [Role Designer](#)

## PostgreSQL Role Designer

The **Role Designer** window allows you to set different properties and privileges for a PostgreSQL role.

- [Editing Role General](#)
- [Setting Role Membership](#)
- [Setting Role Members](#)
- [Setting Object Privileges](#)
- SQL Preview

## Editing PostgreSQL Role General

The **General** tab allows you to set role properties which are:

### Role Name

Set name of the role.

### Role ID

Specify an ID for the role. This is normally not necessary, but may be useful if you need to recreate the owner of an orphaned object. If this is not specified, the highest assigned role ID plus one (with a minimum of 100) will be used as default.

**Note:** In PostgreSQL versions 8.1 or above, the specified ID will be ignored, but is accepted for backwards compatibility.

### Can login

Check this option to create a role that allow to login. A role having this option can be thought of as a user. Roles without this attribute are useful for managing database privileges, but are not users in the usual sense of the word.

### Password

Set role's password.

**Note:** If you do not plan to use password authentication you can omit this option, but then the role will not be able to connect if you decide to switch to password authentication.

### Confirm Password

Re-type the password here.

### Password Encryption

This option control whether the password is stored **ENCRYPTED** or **UNENCRYPTED** in the system catalogs. (If neither is specified, the default behavior is determined by the configuration parameter *password\_encryption*.)

### Connection Limit

If role can log in, this specifies how many concurrent connections the role can make. -1 (the default) means no limit.

## **Expiry Date**

Set a date and time after which the role's password is no longer valid. If this clause is omitted the password will be valid for all time.

## **Can create databases**

Check this option to define a role's ability to create databases.

## **Superuser**

Check this option to determine the new role is a superuser, who can override all access restrictions within the database.

## **Can modify catalog directly**

Check this option to allow a role's ability to update system catalog.

## **Inherit rights from parent roles**

Check this option to determine whether a role inherits the privileges from its parent.

## **Can create roles**

Check this option to allow creating roles.


## Setting PostgreSQL Role Membership

In the grid, check **Granted** or **Admin Option** option against the role listed in **Role Name** to assign this role to be a member of selected role. Multiple roles can be granted.

## Setting PostgreSQL Role Members

In the grid, check **Granted** or **Admin Option** option against the role listed in **Role Name** to assign the selected role to be a member of this role. Multiple roles can be granted.

## Setting PostgreSQL Role Object Privileges

To edit the specific object privileges of the role, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant** or **Grant Option** option against the privilege listed in **Privilege** to assign this role to have that privilege. Multiple privileges can be granted.

To grant (select) or revoke (unselect) all privileges, control-click the grid and select **Grant All**, **Grant All with Grant Option** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.


## SQL Server Security Management

Navicat provides **Server User** to add, duplicate, edit, delete users/roles, grant/revoke server permissions and permissions on the selected database objects. The object pane displays all the users/roles that exist in the server.

The SQL Server **sa** log in is a server-level principal. By default, it is created when an instance is installed. In SQL Server 2005 or above, the default database of **sa** is **master**. This is a change of behavior from earlier versions of SQL Server.



By default, the database includes a **guest** user when a database is created. Permissions granted to the **guest** user are inherited by users who do not have a user account in the database. The **guest** user cannot be dropped, but it can be disabled by revoking its CONNECT permission. The CONNECT permission can be revoked by executing REVOKE CONNECT FROM GUEST within any database other than **master** or **tempdb**.

### Manage Login

Just simply click -> **Server Login** to open an object pane for **Server Login**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete login.


### Add Server Login

To add a new login

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Server Login** to open the **Server Login** showing the login list.
- Click the  from the object pane toolbar or control-click and select **New Server Login** from the popup menu.
- Edit login properties and permissions on the appropriate tabs of the Server Login Designer.



## Duplicate Server Login

To create a new login with modification as one of the existing logins

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Server Login** to open the **Server Login** showing the login list.
- Select a login to edit in the object pane.
- control-click the login and select **Duplicate Server Login** from the popup menu.
- Edit login properties and privileges on the appropriate tabs of the Server Login Designer.



## Edit Server Login

To edit an existing login

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Server Login** to open the **Server Login** showing the login list.
- Select a login to edit in the object pane.
- Click the  from the object pane toolbar or control-click the login and select **Design Server Login** from the popup menu.
- Edit login properties and permissions on the appropriate tabs of the Server Login Designer.



## Delete Server Login

To delete a login


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Server Login** to open the **Server Login** showing the login list.
- Select a login to delete in the object pane.
- Click the  from the object pane toolbar or control-click the login and select **Delete Server Login** from the popup menu.
- Confirm deleting in the dialog window.

## Manage Server Role

To edit an existing server role



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Server Role** to open the **Server Role** showing the server role list.
- Select a server role to edit in the object pane.
- Click the  from the object pane toolbar or control-click the server role and select **Design Server Role** from the popup menu.
- Edit server role properties and permissions on the appropriate tabs of the Server Role Designer.

## Manage Database User

Just simply click -> **Database User** to open an object pane for **Database User**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete database users.


## Add Database User

To add a new database user

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database User** to open the **Database User** showing the database user list.
- Click the  from the object pane toolbar or control-click and select **New Database User** from the popup menu.
- Edit database user properties and permissions on the appropriate tabs of the Database User Designer.



## Duplicate Database User

To create a new database user with modification as one of the existing database users

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database User** to open the **Database User** showing the database user list.
- Select a database user to edit in the object pane.
- Control-click the database user and select **Duplicate Database User** from the popup menu.
- Edit database user properties and privileges on the appropriate tabs of the Database User Designer.



## Edit Database User

To edit an existing database user


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database User** to open the **Database User** showing the database user list.
- Select a database user to edit in the object pane.
- Click the  from the object pane toolbar or control-click the database user and select **Design Database User** from the popup menu.
- Edit database user properties and permissions on the appropriate tabs of the Database User Designer.

## Delete Database User

To delete a database user



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database User** to open the **Database User** showing the database user list.
- Select a database user to delete in the object pane.
- Click the  from the object pane toolbar or control-click the database user and select **Delete Database User** from the popup menu.
- Confirm deleting in the dialog window.

## Manage Database Role

Just simply click -> **Database Role** to open an object pane for **Database Role**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete database roles.


## Add Database Role

To add a new database role

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database Role** to open the **Database Role** showing the database role list.
- Click the  from the object pane toolbar or control-click and select **New Database Role** from the popup menu.
- Edit database role properties and permissions on the appropriate tabs of the Database Role Designer.



## Duplicate Database Role(Available only in Full Version)

To create a new database role with modification as one of the existing database roles

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database Role** to open the **Database Role** showing the database role list.
- Select a database role to edit in the object pane.
- Control-click the database role and select **Duplicate Database Role** from the popup menu.
- Edit database role properties and privileges on the appropriate tabs of the Database Role Designer.



## Edit Database Role

To edit an existing database role


- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database Role** to open the **Database Role** showing the database role list.
- Select a database role to edit in the object pane.
- Click the  from the object pane toolbar or control-click the database role and select **Design Database Role** from the popup menu.
- Edit database role properties and permissions on the appropriate tabs of the Database Role Designer.

## Delete Database Role

To delete a Database Role



- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Database Role** to open the **Database Role** showing the database role list.
- Select a database role to delete in the object pane.
- Click the  from the object pane toolbar or control-click the database role and select **Delete Database Role** from the popup menu.
- Confirm deleting in the dialog window.

## Manage Application Role

Just simply click -> **Application Role** to open an object pane for **Application Role**. A control-click displays the popup menu or use the object pane toolbar, allowing you to add, edit and delete application roles.


## Add Application Role

To add a new application role

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Application Role** to open the **Application Role** showing the application role list.
- Click the  from the object pane toolbar or control-click and select **New Application Role** from the popup menu.
- Edit application role properties and permissions on the appropriate tabs of the Application Role Designer.



## Duplicate Application Role

To create a new application role with modification as one of the existing application roles

- Select the connection you wish to set privileges in the navigation pane.
- Click -> **Application Role** to open the **Application Role** showing the application role list.
- Select an application role to edit in the object pane.
- Control-click the application role and select **Duplicate Application Role** from the popup menu.
- Edit application role properties and privileges on the appropriate tabs of the Application Role Designer.



## Edit Application Role

To edit an existing application role

- Select the connection you wish to set privileges in the navigation pane.
- Click  -> **Application Role** to open the **Application Role** showing the application role list.
- Select an application role to edit in the object pane.
- Click the  from the object pane toolbar or control-click the application role and select **Design Application Role** from the popup menu.
- Edit application role properties and permissions on the appropriate tabs of the Application Role Designer.

## Delete Application Role

To delete an application role

- Select the connection you wish to set privileges in the navigation pane.
- Click  -> **Application Role** to open the **Application Role** showing the application role list.
- Select an application role to delete in the object pane.
- Click the  from the object pane toolbar or control-click the application role and select **Delete Application Role** from the popup menu.
- Confirm deleting in the dialog window.

## Privilege Manager

To edit privilege according to the database objects by using Privilege Manager

- Select the connection you wish to set privileges in the navigation pane.
- Choose **Connection** -> **Set Privileges** or control-click the connection and select **Set Privileges** from the popup menu to open the **Privilege Manager** window and set privileges.

## Privileges Provided by SQL Server

In SQL Server, the concept for permissions is using principals and securables. Principals are the individuals, groups, and processes granted access to SQL Server. Securables are the server, database, and objects the database contains. Principals can be arranged in a hierarchy. To easily manage the permissions in your databases, SQL Server provides several roles which are security principals that group other principals. Database-level roles are database-wide in their permissions scope.

### Windows-level principals

- Windows Domain Login
- Windows Local Login

### SQL Server-level principal

- SQL Server Login

### Database-level principals

- Database User
- Database Role
- Application Role

## Login

SQL Server uses two ways to validate connections to SQL Server databases: Windows Authentication and SQL Server Authentication. SQL Server Authentication uses login records to validate the connection. A Login object exposes a SQL Server login record.

## Server Role

Server-level roles are also named fixed server roles because you cannot create new server-level roles and the permissions of fixed server roles cannot be changed. You can add SQL Server logins, Windows accounts, and Windows groups into server-level roles. Each member of a fixed server role can add other logins to that same role.

## Database User

To gain access to a database, a login must be identified as a database user. The database user is usually known by the same name as the login, but you can create a database user (for a login) with a different name.

## **Database Role**

Fixed database roles are defined at the database level and exist in each database. You can add any database account and other SQL Server roles into database-level roles. Each member of a fixed database role can add other logins to that same role.

## **Application Role**

An application role is a database principal that enables an application to run with its own, user-like permissions. You can use application roles to enable access to specific data to only those users who connect through a particular application. Unlike database roles, application roles contain no members and are inactive by default.

## SQL Server Login Designer

The **Login Designer** window allows you to set different properties and privileges for a SQL Server login.

- [Editing Login General](#)
- [Setting Roles](#)
- [Setting User Mapping](#)
- [Setting Server Permissions](#)
- [Setting Endpoint Permissions](#)
- [Setting Login Permissions](#)
- SQL Preview

## Editing SQL Server Login General

### Options for SQL Server

#### Login Name

Set name of the login.

#### Authentication Type

Select the authentication type.

#### SQL Server Authentication

Selects to use the SQL Server login for authentication.

#### Password

A login must specify password to log on to the database.

#### Confirm Password

Re-type the login's password here.

#### Specify Old Password

Check this option to enter the old password used by this account.

#### Enforce Password Policy

You can check this option to force password to follow password policy of SQL Server.

**Note:** Support from SQL Server 2005 or later.

#### Enforce Password Expiration

You can check this option to force password to have expiry date.

**Note:** Support from SQL Server 2005 or later.

#### User Must Change Password at Next Login

You can check this option to force user to change password everytime when login.

**Note:** Support from SQL Server 2005 or later.

#### Windows Authentication

Selects to use the Windows login for authentication.

## **Mapped to Certificate**

You can select to use certificate for authentication.

SQL Server contains features that enable you to create and manage certificates and keys for use with the server and database. You can use externally generated certificates or SQL Server can generate certificates.

**Note:** Support from SQL Server 2005 or later.

### **Certificate Name**

Select the certificate name.

## **Mapped to Asymmetric Key**

You can select to use asymmetric key for authentication.

**Note:** Support from SQL Server 2005 or later.

### **Asymmetric Key Name**

Selects the asymmetric key name.

**Note:** Certificates and asymmetric keys are both ways to use asymmetric encryption. There is no difference between the two mechanisms for the cryptographic algorithm, and no difference in strength given the same key length.

## **Default Database**

Selects the default database when login.

## **Default Language**

Selects the default display language when login.

## **Credential**

You can add credential on specific role for this login. A credential is a record that contains the authentication information (credentials) required to connect to a resource outside SQL Server. This information is used internally by SQL Server.

**Note:** Support from SQL Server 2005 or later.

### **Enabled**

Checks to enable the login.

**Note:** Support from SQL Server 2005 or later.

## Options for SQL Azure

### **Login Name**

Set name of the login.

### **Password**

A login must specify password to log on to the database.

### **Confirm Password**

Re-type the login's password here.

### **Enabled**

Checks to enable the login.

## Setting SQL Server Login Roles

In the grid, check **Granted** against the server role listed in **Role Name** to assign this server login to be a member of selected server role. Multiple roles can be granted.

**Note:** Every SQL Server login belongs to the **public** server role. When a server principal has not been granted or denied specific permissions on a securable object, the user inherits the permissions granted to **public** on that object. Only assign **public** permissions on any object when you want the object to be available to all users.

**Note:** SQL Azure does not support.

## Setting SQL Server Login User Mapping

In the Grid, check the **Database** and enter the **User** and **Default Schema** to create user for login the database and specify the first schema will be searched by the server.

## Setting SQL Server Login Server Permissions

You can check **Grant**, **Grant Option** or **Deny** against the server permissions listed in **Permission** to assign this login to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** Support from SQL Server 2005 or later.

## Setting SQL Server Login Endpoint Permissions

You can check **Alter**, **Connect**, **Control**, **Take Ownership** or **View Definition** against the endpoint listed in **Endpoint** to assign this login to have that endpoint permission. Multiple permissions can be granted. You can click on the checkbox to have more choices on the permission setting.

To set all permissions for an endpoint, control-click the endpoint and select **Grant Selected**, **Grant Selected With Grant Option**, **Deny Selected** or **Revoke Selected** option.

**Note:** Support from SQL Server 2005 or later.

## Setting SQL Server Login Login Permissions

You can check **Alter**, **Control**, **Impersonate** or **View Definition** against the server login listed in **Login** to assign this server login to have that login permission. Multiple permissions can be granted. You can click on the checkbox to have more choices on the permission setting.

To set all permissions for a login, control-click the login and select **Grant Selected**, **Grant Selected With Grant Option**, **Deny Selected** or **Revoke Selected** option.

**Note:** Support from SQL Server 2005 or later.

## SQL Server Server Role Designer

The **Server Role Designer** window allows you to edit server role for the SQL Server.

**Note:** SQL Azure does not support.

- [Editing Server Role Members](#)
- SQL Preview

## Editing SQL Server Server Role Members

In the grid, check **Member** against the server role listed in **Name** to assign the selected server role to be a member of this server role. Multiple roles can be granted.

## SQL Server Database User Designer

The **Database User Designer** window allows you to set different properties and permissions for a SQL Server database user.

- [Editing Database User General](#)
- [Setting Roles](#)
- [Setting Database Permissions](#)
- [Setting Object Permissions](#)
- Editing Database User Comment (SQL Azure does not support)
- SQL Preview

## Editing SQL Server Database User General

### Options for SQL Server 2000

#### User Name

Set name of the database user.

#### Login Name

Assign SQL Server login that this database user uses. When this SQL Server login enters the database, it will retrieve the information of this database user.

### Options for SQL Server 2005 or later and SQL Azure

#### User Name

Set name of the database user.

#### Authentication Type

Select the type for this database user.

#### Login

Specifies the SQL Server login for which the database user is being created.

#### Login Name

Assign SQL Server login that this database user uses. When this SQL Server login enters the database, it will retrieve the information of this database user.

#### Default Schema

You can specify the first schema that will be searched by the server for this database user.

**Note:** SQL Azure does not support.

#### Certificate

Specifies the certificate for which the database user is being created.

**Note:** SQL Azure does not support.

#### Certificate Name

Specify the certificate for this database user.

## **Asymmetric Key**

Specifies the asymmetric key for which the database user is being created.

**Note:** SQL Azure does not support.

## **Asymmetric Key Name**

Specify the asymmetric key for this database user.

## **Without Login**

Specifies this database user not be mapped to an existing login.

## **Default Schema**

You can specify the first schema that will be searched by the server for this database user.

**Note:** SQL Azure does not support.

## Setting SQL Server Database User Roles

In the grid, check **Granted** against the database role listed in **Role Name** to assign this database user to be a member of selected database role. Multiple roles can be granted.


Every database user belongs to the **public** database role. When a user has not been granted or denied specific permissions on a securable, the user inherits the permissions granted to **public** on that securable.

## Setting SQL Server Database User Database Permissions

In the grid, check **Grant**, **Grant Option** or **Deny** against the permission listed in **Permission** to assign this database user to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

## Setting SQL Server Database User Object Permissions

To edit the specific object permission of this database user, click  **Add Permission** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant**, **Grant Option** or **Deny** option against the permission listed in **Permission** to assign this database user to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## SQL Server Database Role Designer

The **Database Role Designer** window allows you to set different properties and permissions for a SQL Server database role.

- [Editing Database Role General](#)
- [Setting Database Role Members](#)
- [Setting Database Role Membership](#)
- [Setting Database Permissions](#)
- [Setting Object Permissions](#)
- Editing Database Role Comment (Support from SQL Server 2005 or later)
- SQL Preview

## Editing SQL Server Database Role General

The **General** tab allows you to set database role properties which are:

### **Role name**

Set name of the database role.

### **Owner**

Enter the owner for this database role. This owner can be a database user or database role. If the owner is not specify, this database role will be owned by the user who executes the CREATE ROLE command.

## Setting SQL Server Database Role Members

In the grid, check **Member** against the database user/role listed in **Name** to assign the selected database user/role to be a member of this database role. Multiple roles can be granted.

## Setting SQL Server Database Role Membership

In the grid, check **Member of** against the database role/application role listed in **Name** to assign this database role to be a member of the selected database role/application role. Multiple roles can be granted.


## Setting SQL Server Database Role Database Permissions

In the grid, check **Grant**, **Grant Option** or **Deny** against the permission listed in **Permission** to assign this database role to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** SQL Server 2000 does not have Grant Option column.

## Setting SQL Server Database Role Object Permissions

To edit the specific object permission of this database role, click  **Add Permission** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant**, **Grant Option** or **Deny** against the permission listed in **Permission** to assign this database role to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.

## SQL Server Application Role Designer

The **Application Role Designer** window allows you to set different properties and permissions for a SQL Server application role.

**Note:** SQL Azure does not support.

- [Editing Application Role General](#)
- [Setting Database Permissions](#)
- [Setting Object Permissions](#)
- Editing Application Role Comment (Support from SQL Server 2005 or later)
- SQL Preview

## Editing SQL Server Application Role General

The **General** tab allows you to set application role properties which are:

### **Role name**

Set name of the application role.

### **Password**

Set role's password.

### **Confirm Password**

Re-type the password here.

### **Default Schema**

You can specify the first schema that will be searched by the server for this application role.

**Note:** Support from SQL Server 2005 or later.


## Setting SQL Server Application Role Database Permissions

In the grid, check **Grant**, **Grant Option** or **Deny** against the permission listed in **Permission** to assign this application role to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** SQL Server 2000 does not have Grant Option column.

## Setting SQL Server Application Role Object Permissions

To edit the specific object permission of this application role, click  **Add Permission** to open the window and follow the steps below:


- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check **Grant**, **Grant Option** or **Deny** against the permission listed in **Permission** to assign this application role to have that permission. Multiple permissions can be granted.

To grant (select) or revoke (unselect) all permissions, control-click the grid and select **Grant All**, **Grant All With Grant Option**, **Deny All** or **Revoke All** option.

**Note:** Click **Add** to apply permission settings.


## Privilege Manager

The **Privilege Manager** provides another view on privileges in server and its database objects.

To add privilege, click  **Add Privilege** to open the window and follow the steps below:

- (1) Expand the node in the tree view until reaching to the target object.
- (2) Check the object to show the grid on the right panel.
- (3) In the grid, check the relevant privilege against the user/role listed in **Name** to assign the selected user/role to have that object privilege. Multiple privileges can be granted. You can click on the checkbox to have more choices on the permission setting.

**Note:** Click **Save** to apply any changes you have made.

To view specific permissions, you can click  **Filter Privilege** button to open the window and select the type and permissions to list on the right panel.

