

# Whitepaper

**Product: combit Relationship Manager / Report Server**

**Windows Authentication with PostgreSQL**

## **Content**

<b>Requirements</b>	<b>3</b>
<b>Necessary steps</b>	<b>3</b>
<b>Additional information: User Name Maps</b>	<b>5</b>

## Requirements

To use Windows authentication with combit Relationship Manager / Report Server and PostgreSQL the following requirements have to be met:

- combit Relationship Manager from version 7.004 upwards or combit Report Server
- PostgreSQL server from version 9.1 upwards
- Domain environment

## Necessary steps

These steps need to be taken in order to being able to connect to a PostgreSQL server via Windows authentication from combit Relationship Manager / Report Server:

1. A domain user, which the PostgreSQL services later uses to log on, has to exist or be created.
2. The ownership of the folder "[PostgreSQL installation path]\PostgreSQL\9.x\data" and all its child objects has to be changed to the user from step 1 and be granted full control.
3. Stop the PostgreSQL service and change the log on credentials (right click > 'Properties' on the service) in the 'Log On' tab to the user from step 1. Start the service again.

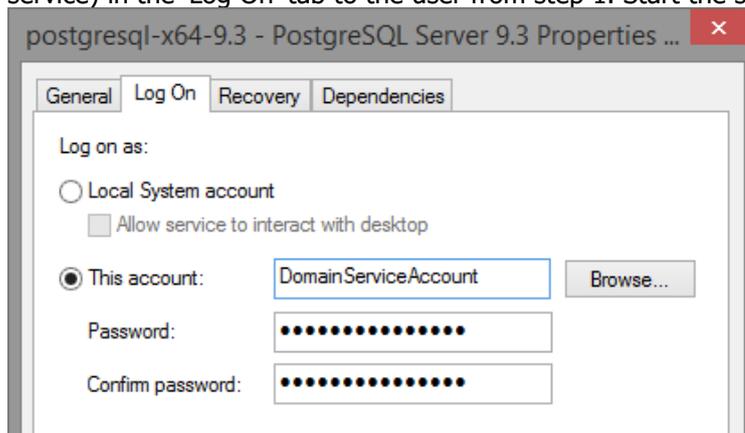


Image 1: Log on properties of the PostgreSQL service

4. Now you have to tell the ActiveDirectory that your user account from step 1 is running the database. For that, you add a Service Principle Name (SPN) to your service account. Run the following command on the windows command line:

```
setspn -S POSTGRES/[fully.qualified.domain.name] DOMAIN\[service_account_name]
```

This step can also be directly done in the Microsoft management console snap-in "Users and Computers" or similar tools which can edit either the ActiveDirectory or the property "servicePrincipalName" of a domain user.

5. You have to create a server login role for each domain user who should be able to use Windows authentication to log in to combit Relationship Manager / Report Server. In the PostgreSQL admin tool ("[PostgreSQL installation path]\PostgreSQL\9.x\bin\pgAdmin3.exe") right click 'Login Roles' in the object browser and choose 'New Login Role...'

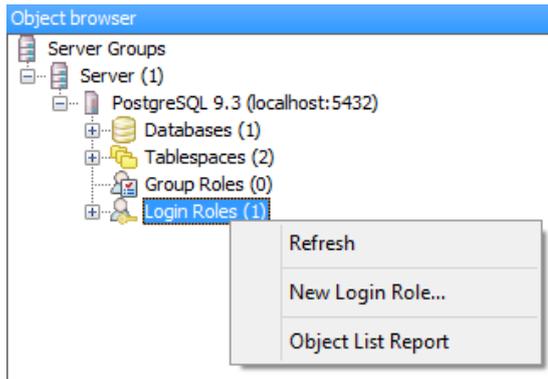


Image 2: PostgreSQL admin tool 'pgAdmin3' object browser

Please note that the role name has to be exactly the same as the domain user account (you can find a workaround for this in the chapter Additional information: User Name Maps) and that the role needs full role privileges in order to use all available features of combit Relationship Manager / Report Server.

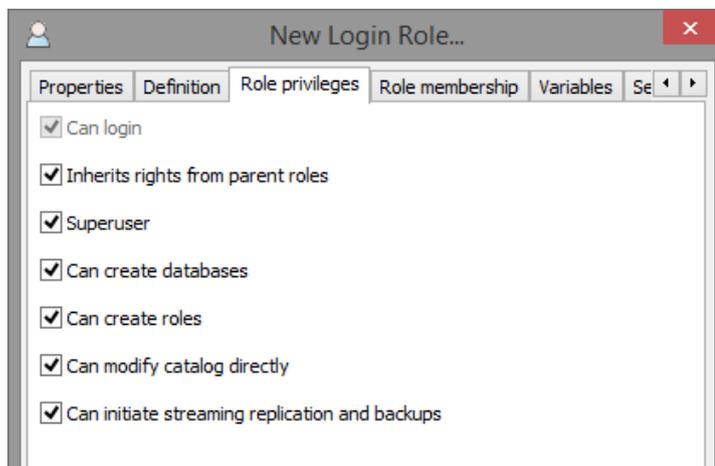


Image 3: Role privileges of a PostgreSQL login role

- The login method in the file "[PostgreSQL installation path]\PostgreSQL\9.x\data\pg\_hba.conf" for the role from step 5 has to be changed / created.

TYPE	DATABASE	USER	ADDRESS	METHOD
host	all	domain-user / login-role	127.0.0.1/32	sspi

Table 1: Configuration of PostgreSQL login methods

If you want to use Windows authentication for all users the entry for the column 'USER' can be changed to 'all'.

- You can now change the login method in combit Relationship Manager / Report Server to Windows authentication.

For further information about connection / login problems there are log files in the directory "[PostgreSQL installation path]\PostgreSQL\9.x\data\pg\_log\".

## Additional information: User Name Maps

In certain circumstances it could be desired to not have the domain user account match the PostgreSQL login role. As PostgreSQL, when using Windows Authentication, compares these two user names before granting access to the database, you have to create a mapping between the domain user account and the PostgreSQL login role if they differ.

This mapping can be configured with the steps below:

1. A map name with the format "map=[map name]" has to be added after the authentication method ("sspi" in the case of Windows Authentication) in the file "[PostgreSQL installation path]\PostgreSQL\9.x\data\pg\_hba.conf". An entry to this file could look like this:

TYPE	DATABASE	USER	ADDRESS	METHOD
host	all	domain-user / login-role	127.0.0.1/32	sspi map=[map name]

Table 2: Example of an entry in the `pg_hba.conf` file with a mapping name

2. The mapping itself has to be added to the file "[PostgreSQL installation path]\PostgreSQL\9.x\data\pg\_ident.conf"

MAPNAME	SYSTEM-USERNAME	PG-USERNAME
[map name]	domain-/system-user	PostgreSQL login-role

Table 3: Example of an entry in the `pg_ident.conf` file

It is possible to specify more than one domain-user for a single map name on multiple lines. Additionally, you can use a slash ("/") as the first character of the SYSTEM-USERNAME column to have the rest of the column be interpreted as a regular expression.

Further information about User Name Maps can be found in the PostgreSQL documentation:  
<https://www.postgresql.org/docs/current/static/auth-username-maps.html>

The information stated above is for purely informative purposes and does not stand under guarantee. Although our goal is to give you the best information we can, errors and mistakes may occur. In some cases the information has been given in order to help you with a special task, even though the product wasn't necessarily meant for that specific purpose. This information does not have an effect on your product guarantee.