Permissions

This page explains the permissions required to use SQL Backup Pro.

Using SQL Backup Pro from the graphical user interface

Permissions required by the GUI user

The user connecting to the SQL Backup Pro GUI requires:

- Membership of the SQL Server *sysadmin* fixed server role, if connecting to the registered SQL Servers using Windows authentication. For information on how to connect using SQL Server authentication, see Adding SQL Server instances by name (step 4).
- *Execute* permissions on the SQL Backup Pro extended stored procedure, *sqlbackup*.
- For the compression analyzer, *execute* permissions on *sqbtest*, *sqbtestcancel* and *sqbteststatus* extended stored procedures.

Permissions required by the SQL Backup Agent service

The SQL Backup Agent service is a Windows service which SQL Backup Pro uses to perform backup and restore operations through the GUI. You specify the user account used to log on to the SQL Backup Agent service (the startup account) when you install the server components on a SQL Server instance.

The user account used to log on to the SQL Backup Agent service (the startup account) and connect to the SQL Server requires:

- "Log on as a service" rights in order to start the service.
- If using Windows authentication to connect to the SQL Server, membership of the SQL Server *sysadmin* fixed server role. If using SQL Server authentication, the SQL Server authenticated account must be a member of the SQL Server *sysadmin* fixed server role, but the startup account does not need to be. For information on changing the authentication mode the SQL Backup Agent service startup account uses to connect to the SQL Server instance, see Changing the authentication mode below.
- Access to any network locations that will be backed up or copied to, or restored from.
- Access to the following folders:
    - The SQL Backup Pro local data store. By default, this is installed in *%PROGRAMDATA%\Red Gate\SQL Backup\Data* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\SQL Backup\Data* (for Windows Server 2003 and Windows XP).
    - The SQL Backup Pro logs folder. By default this is *%PROGRAMDATA%\Red Gate\SQL Backup\Log* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\SQL Backup\Log* (for Windows Server 2003 and Windows XP).
    - The SQL Backup Pro backup settings registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Red Gate\SQL Backup\BackupSettings\<instance>*
    - The SQL Backup Pro backup settings global registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Red Gate\SQL Backup\BackupSettingsGlobal\<instance>*
    - The Red Gate licensing registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Red Gate\Licensing\SQL Backup* or *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Red Gate\Licensing\SQL Backup* (for 64-bit machines).
    - The Red Gate licenses folder *%PROGRAMDATA%\Red Gate\Licenses* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\Licenses* (for Windows Server 2003 and Windows XP).
    - The Microsoft MSSQLServer setup registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Setup* (read access only).

If you encounter errors related to permissions and access rights, ensure that the startup account for the SQL Backup Agent service application has been granted the necessary permissions.

Using SQL Backup Pro from the extended stored procedure

Permissions required by the extended stored procedure user

The user running the extended stored procedure requires:

- permission to back up, restore and drop databases
    - to back up databases, the user must be a member of the *db_backupoperator* fixed database role, or you can use the GRANT BACKUP DATABASE command to grant the permission
    - to restore or drop databases, the user must be a member of the *db_owner* fixed database role or the *dbcreator* fixed server role, or you can use the GRANT CREATE DATABASE command to grant the permission
- *execute* permissions on the SQL Backup Pro extended stored procedure, *sqlbackup*
- for the compression analyzer, *execute* permissions on *sqbtest*, *sqbtestcancel* and *sqbteststatus* extended stored procedures

Permissions required by the SQL Backup Agent service

The SQL Backup Agent service is a Windows service which SQL Backup Pro uses to perform backup and restore operations through the extended stored procedure. You specify the user account used to log on to the SQL Backup Agent service (the startup account) when you install the server components on a SQL Server instance.

The user account used to log on to the SQL Backup Agent service (the startup account) and connect to the SQL Server requires:

- "Log on as a service" rights in order to start the service.
- If using Windows authentication to connect to the SQL Server, membership of the SQL Server *sysadmin* fixed server role. If using SQL Server authentication, the SQL Server authenticated account must be a member of the SQL Server *sysadmin* fixed server role, but the startup account does not need to be. For information on changing the authentication mode the SQL Backup Agent service startup account uses to connect to the SQL Server instance, see Changing the authentication mode below.
- Access to any network locations that will be backed up or copied to, or restored from.
- Access to the following folders:
    - The SQL Backup Pro local data store *%PROGRAMDATA%\Red Gate\SQL Backup\Data* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\SQL Backup\Data* (for Windows Server 2003 and Windows XP).
    - The SQL Backup Pro logs folder *%PROGRAMDATA%\Red Gate\SQL Backup\Log* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\SQL Backup\Log* (for Windows Server 2003 and Windows XP).
    - The Red Gate licensing registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Red Gate\Licensing\SQL Backup* or *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Red Gate\Licensing\SQL Backup* (for 64-bit machines).
    - The Red Gate licenses folder *%PROGRAMDATA%\Red Gate\Licenses* (for Windows Server 2008, Windows Server 2008 R2, Windows Vista and Windows 7) or *%ALLUSERSPROFILE%\Application Data\Red Gate\Licenses* (for Windows Server 2003 and Windows XP).
    - The Microsoft MSSQLServer setup registry folder *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Setup* (read access only).

If you encounter errors related to permissions and access rights, ensure that the startup account for the SQL Backup Agent service application has been granted the necessary permissions.

Using SQL Backup Pro from the command line

The SQL Backup Pro command line program communicates with SQL Server directly; it does not use the SQL Backup Agent service application. To run *SQLBackupC.exe*, the user must have the SQL Server *sysadmin* fixed server role. For more information, see Using the command line.

Changing the SQL Backup Agent service credentials

When you install the SQL Backup Pro server components, you specify:

- the user the SQL Backup Agent service logs on as, and
- the authentication mode the SQL Backup Agent service uses to connect to the SQL Server instance.

You can change the credentials used by the SQL Backup Agent service at any time, as described below.

Changing the SQL Backup Agent service startup account

> You will need to restart the SQL Backup Agent service for the change to take effect.

To change the account the SQL Backup Agent service logs on as, use the Windows Services snap-in:

1. From the Windows Control Panel, select **Administrative Tools** > **Services**, or run *services.msc*.
2. Select the SQL Backup Agent service for the SQL Server instance: *SQL Backup Agent - <instance name>*.
   Note: The SQL Backup Agent service for the local instance is called just *SQL Backup Agent*.
3. Right-click the service and select **Properties**.
4. On the **Log On** tab, specify the account you want the service to log on as. The account must have the permissions listed above.
5. Click **OK** to close.
6. Right-click the service and select **Restart** to restart the service and apply your changes.

Changing the authentication mode for the SQL Backup Agent service

To change the authentication mode the SQL Backup Agent service startup account uses to connect to the SQL Server instance, use the *sqbsetlogin* extended stored procedure:

1. Add the *sqbsetlogin* stored procedure from the SQL Backup Pro extended stored procedure dynamic link library (*xp_sqlbackup.dll*).
2. Provide the user name and password to specify SQL Server authentication.
3. Remove the *sqbsetlogin* extended stored procedure when you have finished using it. (This step is optional but recommended.)

For example:

```
EXECUTE master..sp_addextendedproc sqbsetlogin, 'xp_sqlbackup.dll'

EXECUTE master..sqbsetlogin 'sa', 'sqbpassword'

EXECUTE master..sp_dropextendedproc sqbsetlogin
```

To revert to Windows authentication, call *sqbsetlogin* with blank values:

```
EXECUTE master..sqbsetlogin '', ''
```

If you are using SQL Server authentication and you change the account password, you must also apply the change to the SQL Backup Agent service, otherwise backups and restores may fail. This can be done using the *sqbsetlogin* stored procedure as above, but specifying the new account credentials on step 2.

Using a different security model

You may want to use a different security model, for example if you want to back up locally but copy the backup to a locked down network share. The following procedure assumes that you are working in a single domain.

1. Create a domain account with minimal permissions. Add the domain account to a security group on the Windows server on which the SQL Server is installed; the security group must have sufficient permissions to run as a service.
2. Create a SQL Server authenticated account that has the ability to back up and restore databases.To do this, add the account to the *sysadmin* or *db_backupoperator* fixed role, or if you are using SQL Server 2005, 2008 or 2012, you can use the GRANT BACKUP command.
3. When you install the SQL Backup Pro server components on the SQL Server:
    - For the SQL Backup Agent service credentials, select **Specific account** and enter the domain account you created in step 1.
    - For the SQL Server credentials, select **SQL Server authentication**, and specify the credentials for the SQL Server authenticated account you created in step 2.
4. Create the folder on the local server in which you want to create the backups, and a folder on a network share to which you want to copy the backup files.
5. Confirm that the permissions on both folders are set such that the domain user you created in step 1 can access and write to them.

To check that all the accounts have the appropriate permissions, use the Back Up wizard to create a backup in a local folder and copy it to a network share.

Alternatively, run the following query to ensure that the domain account has sufficient permissions on the network share:

```
EXECUTE master..sqbutility 999, 'RWE', '<network location>'
```

If this is successful and the SQL Backup Agent service has read (R), write (W), and execute (E) permissions, the query will return:

```
<SQBUTILITYRESULT>:1:
```

If there is a problem, the query will return a value of *0*, followed by a message, for example:

```
<SQBUTILITYRESULT>:0:Folder does not exist :
<network location>
```

Working with servers on different Windows domains

If you are working with servers which do not participate in the same Windows domain, you can still use SQL Backup Pro to work with them as usual by setting up "matching accounts". This will be necessary if you want to copy backups to a locked down network share on a different Windows domain, or set up log shipping between servers on different domains.

1. Create accounts on each machine with identical user names and passwords.
2. Set the SQL Backup Agent service to log in to the SQL Server using the account created in step 1, using the *sqbsetlogin* extended stored procedure. For more information, see Changing the authentication mode above.
   When log shipping, the SQL Backup Agent on *both* SQL Servers must log in using the matched account.
3. Give the account on the other domain access permissions to the relevant locations.