Firebird's gsec User Management Utility

Norman Dunbar

Version 1.6, 24 February 2024

Table of Contents

Chapter 1. Introduction

Gsec is the security database manipulation utility. It allows the SYSDBA (or any privileged user) the ability to maintain user accounts for various Firebird databases. Using various options, users can be added, amended or deleted from the security database.

> A privileged user is an account on the database server which the Firebird engine considers to be privileged enough to automatically be given SYSDBA rights. At present there are four login names that are assumed to be privileged, these are:
>
> - root
> - firebird
> - interbase
> - interbas (without the 'e')

Normal users, ie all those accounts not listed above, can only see their own user details from version 2.0 of Firebird. They can, however, change their own passwords with the new version. Previously the SYSDBA had to make the changes on behalf of the users.

> It is possible on some operating systems that users will not be able to run gsec, even if they know the SYSDBA password. This is because those operating systems allow the system administrator to set file system permissions which prevent execution of certain programs and utilities for security reasons.

The Firebird database holds details of all users in a single security database. This is located on the server in a normal Firebird database named security.fdb for Firebird 1.5 or security2.fdb for Firebird 2.0 onwards. The default locations for this file are:

- C:\Program Files\Firebird\Firebird_1_5 for Windows (Change '1_5' to suit your Firebird version)

- /opt/firebird for Linux and other Unix systems.

The gsec utility manipulates data in the table(s) in the security database, and by doing so, allows users to be added, amended and deleted from the system.

Up until Firebird 2.0, it used to be possible to use isql to connect directly to the security database as the SYSDBA user. This is no longer possible, even if you have the SYSDBA username and password and/or are logged in as a privileged user.

Like most of the command line utilities supplied with Firebird, gsec can be run in interactive or batch mode and has a help screen showing all of the utility's options, we'll be seeing that a little later on.

In the remainder of this manual we shall discuss the following:

- Command line options for gsec.
- Gsec commands and their parameters.

- Running gsec in interactive or batch modes, both of which allow you to :

  - Display user details.

  - Amend user details.

  - Add new users.

  - Delete existing users.

- Using gsec to administer a remote security database.

- Some caveats, gotchas and foibles of gsec.

Chapter 2. Command Line Options

Regardless of the mode that `gsec` is run in, there are a number of options that can be supplied on the command line. These are:

`-user <username>`

Allows the username of the SYSDBA user to be specified if the database is to be modified, or a normal username if the database is to be displayed only. This need not be supplied if `ISC_USER` and `ISC_PASSWORD` environment variables exist and have the correct values.

`-password <password>`

Supplies the password for the username specified above. This need not be supplied if `ISC_USER` and `ISC_PASSWORD` environment variables exist and have the correct values.

`-fe[tch_password] <password file name> | stdin | /dev/tty`

This switch causes the password for the appropriate user to be read from a file as opposed to being specified on the command line. The file name supplied is *not* in quotes and must be readable by the user running `gsec`. If the file name is specified as `stdin`, then the user will be prompted for a password. On POSIX systems, the file name `/dev/tty` will also result in a prompt for the password.

> Firebird 2.5 onwards.

`-role <SQL role name>`

Allows the specification of the role to be used by the connecting user.

`-database <server:security database name>`

You can specify the full pathname of a security database to `gsec` and this will allow you to remotely administer the users for that server. The whole parameter should be enclosed in quotes if there are any spaces in the path to the security database.

`-z`

Displays the version number of the `gsec` utility.

`-help` **or** `-?`

Help displays the following screen of information:

```
gsec utility - maintains user password database

   command line usage:
     gsec [ <options> ... ] <command> [ <parameter> ... ]

   interactive usage:
     gsec [ <options> ... ]
     GSEC>
     <command> [ <parameter> ... ]
```

```
available options:
  -user <database administrator name>
  -password <database administrator password>
  -fetch_password <file to fetch password from>
  -role <database administrator SQL role name>
  -trusted (use trusted authentication)
  -database <database to manage>
  -z

available commands:
  adding a new user:
    add <name> [ <parameter> ... ]
  deleting a current user:
    delete <name>
  displaying all users:
    display
  displaying one user:
    display <name>
  modifying a user's parameters:
    modify <name> <parameter> [ <parameter> ... ]
  changing admins mapping to RDB$ADMIN role in security database:
    mapping {set|drop}
  help:
    ? (interactive only)
    help
  displaying version number:
    z (interactive only)
  quit interactive session:
    quit (interactive only)

available parameters:
  -pw <password>
  -uid <uid>
  -gid <uid>
  -fname <firstname>
  -mname <middlename>
  -lname <lastname>
  -admin {yes|no}
```

Chapter 3. Gsec Commands

After the assorted options, comes the command that you wish to run. The following commands are available in both batch and interactive modes, but for interactive mode the leading minus sign is not required.

`-add <name> [ <parameter> ⋯ ]`

This command adds a new user to the database. You may optionally add other details such as first, middle and last names plus a password for the new user, all in the same `add` command. Alternatively, you may add a user then `modify` it to fill in the missing details.

`-delete <name>`

This command removes the named user from the database. All details of the user are removed and cannot be undone unless you add the user back again.

`-display [ <name> ]`

This command displays the details of a single named user, or all users in the database. The password is never displayed.

`-modify <name> <parameter> [ <parameter> ⋯ ]`

The *name* option is how you wish the user to be known when connecting to Firebird databases.

Some of the above commands take parameters and these are one, or more, of the following:

`-pw <password>`

This parameter lets you supply a new password for the user. If you omit the password, the current one will be removed and the user will be unable to login to any Firebird databases at all. The password can be up to 8 characters long, but when supplying one to `gsec`, or logging into databases, the characters after the eighth are simply ignored.

`-uid <uid>, -gid <gid>`

`-uid` and `-gid` are used on some POSIX systems to enter the Unix userid and groupid as found in `/etc/passwd` and `/etc/group` configuration files. If not supplied, these default to zero.

`-fname [ <first name> ]`

This parameter allows you to store the user's first name in the database. This helps when identifying users from their login name — which may be abbreviated. You can delete a first name by not supplying a name.

`-mname [ <middle name> ]`

This parameter allows you to store the user's middle name in the database. This helps when identifying users from their login name — which may be abbreviated. You can delete a middle name by not supplying a name.

`-lname [ <lastname> ]`

This parameter allows you to store the user's last name in the database. This helps when identifying users from their login name — which may be abbreviated. You can delete a last name by not supplying a name.

`-admin yes | no`

> This parameter allows you to specify whether or not the user will be granted the RDB$ADMIN role.
>
> | | Firebird 2.5 onwards. |

Chapter 4. Interactive Mode

To run gsec in interactive mode, start the utility using the command line:

```
C:\>gsec -user sysdba -password masterkey
GSEC>
```

The GSEC> prompt shows that the utility is waiting for a command. The -user and -password options are those of the user who wishes to manipulate the security database. Obviously, the username supplied must be a valid SYSDBA user if updates are to be carried out. Normal users may only read the database.

> ℹ️ With Firebird 1.5 and Windows Vista this may not work correctly and an 'unavailable database' error will be displayed. The problem is caused by trying to use the IPCServer transport implemented in Firebird 1.5 which doesn't work on Vista. The solution is to use TCP local loopback.
>
> - Put an alias in aliases.conf for the path to your security.fdb, e.g. sec = C:\Program Files\Firebird\Firebird_1_5\security.fdb.
>
> - Call gsec using gsec -database localhost:sec -user SYSDBA -password masterkey
>
> As localhost may not be available on some Vista workstations you may have to change localhost in the command above to use the actual host name or the IP address of the Vista computer.

To exit gsec in interactive mode, the quit command is used:

```
GSEC> quit
C:\>
```

The following sections show how to carry out various commands in interactive mode. It is assumed that you are already running the utility as a SYSDBA user.

4.1. Displaying User Details

> ℹ️ From Firebird 2.5 onwards, the display command shows an additional column named admin. This shows the text admin where a user has been granted the RDB$ADMIN role either within the database, or by using gsec. In the following examples, where it is necessary to show this detail, it will be shown, otherwise, all output examples are as per Firebird 2.0.

To display all users in the security database the command, and it's output are:

```
GSEC> display
    user name                        uid    gid     full name
```

```
--------------------------------------------------------------------
SYSDBA                              0     0
NORMAN                              0     0      Norman  Dunbar
EPOCMAN                             0     0      Benoit Gilles Mascia
GSEC>
```

To display details of a single user, pass the username as a parameter to the `display` command.

```
GSEC> display epocman
     user name                     uid   gid     full name
--------------------------------------------------------------------
EPOCMAN                             0     0      Benoit Gilles Mascia
GSEC>
```

If you enter the name of a non-existent user as a parameter of the `display` command, nothing is displayed and gsec remains in interactive mode.

```
GSEC> display alison
GSEC>
```

4.2. Adding New Users

When adding a new user in interactive mode, nothing is displayed to confirm that the user was indeed added. You need to use the `display` or `display <name>` commands to make sure that the user was added successfully.

```
GSEC> add newuser -pw newuser -fname New -lname User
GSEC>
```

```
GSEC> display newuser
     user name                     uid   gid     full name
--------------------------------------------------------------------
NEWUSER                             0     0      New  User
GSEC>
```

From Firebird 2.5 onwards, a new role — RDB$ADMIN — has been added to the security database. Gsec allows you to indicate whether new users are assigned this role. The display command has also been modified to show whether a user had this role or not.

```
GSEC> add newadmin -pw secret -fname New -mname admin -lname User -admin yes
GSEC>
```

```
GSEC> display newadmin
```

```
    user name                      uid   gid admin     full name
--------------------------------------------------------------------------------
----------
NEWADMIN                            0     0 admin      New admin User
GSEC>
```

4.3. Deleting Existing Users

When deleting a user in interactive mode, there is no confirmation that the user has been deleted. You should use the `display` or `display <name>` command to check.

```
GSEC> delete newuser
GSEC>
```

```
GSEC> display
    user name                      uid   gid       full name
-----------------------------------------------------------------
SYSDBA                             0     0
NORMAN                             0     0         Norman  Dunbar
EPOCMAN                            0     0         Benoit Gilles Mascia
GSEC>
```

If, on the other hand, you try to delete a non-existing user, `gsec` will display an error message, and exit.

```
GSEC> delete newuser
record not found for user: NEWUSER

C:\>
```

4.4. Amending Existing Users

Existing users can have one or more of their password, first name, middle name or lastname amended. There is no confirmation that your modification has worked, so you must use one of the `display` commands to determine how well it worked.

```
GSEC> modify norman -pw newpassword
GSEC>
```

```
GSEC> modify norman -mname MiddleName -fname Fred
GSEC>
```

```
GSEC> display norman
     user name                        uid   gid     full name
---------------------------------------------------------------
NORMAN                               0     0       Fred MiddleName Dunbar
GSEC>
```

If you wish to remove one or more of a user's attributes, don't pass a (new) value for that attribute.

```
GSEC> modify norman -mname -fname -lname
```

```
GSEC> display norman
     user name                        uid   gid     full name
---------------------------------------------------------------
NORMAN                               0     0
GSEC>
```

Now I can be known as 'the man with no name', just like Clint Eastwood !

From Firebird 2.5 onwards, a user's admin rights can be modified using this command:

```
GSEC> modify norman -admin yes
```

```
GSEC> display norman
     user name                        uid   gid admin     full name
------------------------------------------------------------------------------------
----------
NORMAN                               0     0 admin     New admin User
GSEC>
```

4.5. OS Admin Mapping

Firebird 2.5.

Since Firebird 2.1, Windows domain administrators have had *full* access to the user management functions. This meant that when an admin user connected to the server and then used gsec, they had the ability to modify *any* user account in the security database.

From Firebird 2.5 they do *not* get these privileges automatically unless the DBA has configured the security database to make it happen automatically. This is done either in isql as follows:

```
SQL> SQL> alter role rdb$admin set auto admin mapping;
SQL> commit;
```

The command above will cause all Windows Administrator accounts to automatically have full access to the user management functions. The automatic mapping can be revoked as follows:

```
SQL> SQL> alter role rdb$admin drop auto admin mapping;
SQL> commit;
```

The functionality of the above `isql` commands can also be set using `gsec`, as follows, by using the `-mapping` command. The command takes a parameter of `set` or `drop` accordingly.

```
GSEC> mapping set
```

or:

```
GSEC> mapping drop
```

4.6. Help

The `help` command, in interactive mode, displays the same help screen as shown above. From Firebird 2.5, this can be abbreviated to a single question mark.

4.7. Version Information

The version of `gsec` can be obtained using the `z` command.

```
GSEC> z
gsec version  WI-V1.5.0.4306 Firebird 1.5
GSEC>
```

Or, in `gsec` from Firebird 2.5:

```
GSEC> z
gsec version LI-V2.5.0.26074 Firebird 2.5
GSEC>
```

Chapter 5. Batch Mode

In the following descriptions of batch mode operations, assume that I have set the `ISC_USER` and `ISC_PASSWORD` environment variables. This allows `gsec` to be run without always having to specify the `-user` and `-password` switches. This in turn reduces the amount of code on the command line, which means that when this XML file is rendered into pdf, all the command line will fit on the width of an A4 page.

It is not secure to have these variables set all the time, so don't do it !

If you are using `gsec` from Firebird version 1.5 (and possibly version 1.0 as well) then when you are running in batch mode, you may think that you can check the result of an operation by checking `%ERRORLEVEL%` in Windows, or `$?` in various flavours of Unix. This doesn't work. The result is always zero.

In `gsec` from Firebird version 2.0 onwards, this problem is fixed and the exit code will be zero for everything was ok, or a non-zero value for error conditions.

In batch mode, the command line to run `gsec` is as follows :

```
gsec [ <options> ... ] <command> [ <parameter> ... ]
```

5.1. Displaying User Details

To display all users in the security database the command, and its output are:

```
C:\>gsec -display
    user name                     uid   gid     full name
--------------------------------------------------------------------
SYSDBA                            0     0
NORMAN                            0     0       Norman  Dunbar
EPOCMAN                           0     0       Benoit Gilles Mascia
```

To display details of a single user, pass the username as a parameter to the `display` command.

```
C:\>gsec -display epocman
    user name                     uid   gid     full name
--------------------------------------------------------------------
EPOCMAN                           0     0       Benoit Gilles Mascia
```

5.2. Adding New Users

When adding a user in batch mode, there is no confirmation that the user has been added. You

should use the `-display` or `-display <name>` command to check.

```
C:\>gsec -add newuser -pw newuser -fname New -lname User
```

```
C:\>gsec -display
    user name                    uid   gid     full name
------------------------------------------------------------------
SYSDBA                            0     0
NORMAN                            0     0       Norman  Dunbar
NEWUSER                           0     0       New  User
EPOCMAN                           0     0       Benoit Gilles Mascia
```

Under Firebird 2.5, the `-admin` parameter may be specified:

```
C:\>gsec -add newadmin -pw ignoreit -fname New -mname Admin -lname User -admin yes
```

```
c:\>gsec -display newadmin
    user name                    uid   gid admin     full name
--------------------------------------------------------------------------------
----------
NEWADMIN                          0     0             New Admin User
```

5.3. Deleting Existing Users

When deleting a user in batch mode, there is no confirmation that the user has been deleted. You should use the `-display` or `-display <name>` command to check.

```
C:\>gsec -delete newuser
```

```
C:\>gsec -display
    user name                    uid   gid     full name
------------------------------------------------------------------
SYSDBA                            0     0
NORMAN                            0     0       Norman  Dunbar
EPOCMAN                           0     0       Benoit Gilles Mascia
```

5.4. Amending Existing Users

Existing users can have one or more of their password, first name, middle name, lastname or admin rights amended.

```
C:\>gsec -modify norman -pw newpassword
```

```
C:\>gsec -modify norman -mname MiddleName -fname Fred
```

```
C:\>gsec -display
     user name                    uid   gid     full name
------------------------------------------------------------------
SYSDBA                            0     0
NORMAN                            0     0       Fred MiddleName Dunbar
EPOCMAN                           0     0       Benoit Gilles Mascia
```

If you wish to remove one or more of a user's attributes, don't pass a (new) value for that attribute.

```
C:\>gsec -modify norman -mname -fname -lname
```

```
C:\>gsec -display
     user name                    uid   gid     full name
------------------------------------------------------------------
SYSDBA                            0     0
NORMAN                            0     0
EPOCMAN                           0     0       Benoit Gilles Mascia
```

Now nobody knows who I am :o)

5.5. Version Information

The version of gsec can be obtained using the -z command. However, note that it leaves you in interactive mode on completion. It doesn't exit like the other batch mode commands do, so you have to use the interactive quit command to exit. There is a way around this problem as shown in the following. The first part shows the problem — which still exists in Firebird 2.5.

```
C:\>gsec -z
gsec version  WI-V1.5.0.4306 Firebird 1.5
GSEC>
```

The solution is to have a small file containing the command quit and force gsec to read this file when it needs user input, as follows.

```
C:\>copy con fred
quit
^Z
```

```
        1 file(s) copied.
```

```
C:\>gsec -z <fred
gsec version  WI-V1.5.0.4306 Firebird 1.5
GSEC>
C:\>
```

This could be a good idea for any of the commands which leave you 'stuck' in the interactive mode when you thought you were running in batch mode. By redirecting input from a command file, gsec will read a line of text from that file any time it requires user input. By forcing it to read the `quit` command, you make it exit.

> The `-z` command doesn't need a `-user` and `-password`, it will display the version details and then tell you that you don't have a username/password — but you can safely ignore this message.

5.6. OS Admin Mapping

> Firebird 2.5.

Since Firebird 2.1, Windows domain administrators have had *full* access to the user management functions. This meant that when an admin user connected to the server and then used gsec, they had the ability to modify any user account in the security database.

The functionality that allows Windows domain administrators to have *full* access to the user management functions of the Firebird's security database, can also be set using `gsec` on the command line as follows, by using the `-mapping` command. The command takes a parameter of `set` or `drop` accordingly.

```
C:/> gsec -mapping set
```

or:

```
C:/> gsec -mapping drop
```

Chapter 6. Running Gsec Remotely

Gsec can be used to administer the security database on a remote server. To do this you must supply the remote security database name on the command line as shown in the following example which connects my Windows XP client version of gsec to my Linux server named ganymede and allows me to manage the users on my Linux server.

```
C:\>gsec -database ganymede:/opt/firebird/security2.fdb
         -user sysdba -password masterkey
GSEC>
```

> In the above example, I have split the full command line over two lines. This is to prevent it 'falling off' the right side of the page when this manual is rendered as a PDF document. The whole command should, indeed must, be typed on a single line.
>
> Also note that if there are spaces in the database path, you must enclose the whole parameter in double quotes.

Once connected to the remote security database, you can manipulate users in the normal manner in either interactive or batch modes as described above.

The version of gsec provided in Firebird 2.0 can be used to maintain the security database on previous versions of Firebird and it is hoped, Interbase from version 6.0 upwards. However, from version 2.0 of Firebird, the format of the security database changed and because of this, gsec from an older version cannot be used to maintain the security database for Firebird 2.0 onwards.

Chapter 7. Gsec caveats

The following is a brief list of gotchas and funnies that I have detected in my own use of gsec. Some of these are mentioned above, others may not be. By collecting them all here in one place, you should be able to find out what's happening if you have problems.

7.1. Normal Versus Privileged Users

Only a privileged user can update the security database. Normal users can run the gsec utility, but can only list the contents under Firebird 1.5. The following shows what happens when trying to update the database when running gsec as a normal user.

```
C:\>gsec -user norman -password norman
GSEC> add myuser -pw mypassword
add record error
no permission for insert/write access to TABLE USERS
```

A normal users can only display details from the security database.

```
C:\>gsec -user norman -password norman -display
     user name                      uid   gid     full name
-------------------------------------------------------------------
SYSDBA                              0     0
NORMAN                              0     0       Norman  Dunbar
EPOCMAN                             0     0       Benoit Gilles Mascia
```

> From Firebird version 2 onwards, there are slight changes to the above. Normal users are now able to change their own passwords and can no longer display details of other users that may be present in the security database.

The above user, running under Firebird 2.0 would see the following:

```
C:\>gsec -user norman -password norman -display
     user name                      uid   gid     full name
-------------------------------------------------------------------
NORMAN                              0     0       Norman  Dunbar
```

7.2. Differences Between Batch And Interactive Mode

The gsec commands apply to both modes of operation, however, when running in batch mode, you must prefix the command name with a minus sign (-) or you will get an error message similar to the following:

```
C:\>gsec -user sysdba -password masterkey display
```

```
invalid parameter, no switch defined
error in switch specifications
GSEC>
```

Note also that you will be left in interactive mode when an error occurs. The correct command line should have a minus in front of the `display` command, as follows:

```
C:\>gsec -user sysdba -password masterkey -display
     user name                      uid   gid     full name
--------------------------------------------------------------------
SYSDBA                              0     0
NORMAN                              0     0       Norman  Dunbar
EPOCMAN                             0     0       Benoit Gilles Mascia
```

This time, `gsec` performed its duties, displayed all known users and quit from the utility.

> If environment variables `ISC_USER` and `ISC_PASSWORD` have been defined, and this isn't a very good idea for security reasons, `gsec` can be run without passing the `-user` or `-password` options.

> As with all of the command line utilities, it is best to use the version of the `gsec` utility that was supplied with your database.

7.3. Batch Mode Exit Codes

When running `gsec` under windows, you can trap the exit code in `%ERRORLEVEL%` and check it to determine the success or failure of the last command executed.

When your operating system is Unix — whatever flavour — the exit code is to be found in the $? variable.

Unfortunately, using the version of `gsec` supplied with Firebird 1.5, it appears that `gsec` always exits with a zero and this makes it quite unsuitable to build into a properly error trapped batch script on either system. Sad but true.

> From version 2.0 of Firebird, this has been corrected and an exit code of zero indicates success while non-zero values indicate failures.

7.4. Errors In Batch Mode Swap To Interactive Mode

Sometimes, when running in batch mode, an error condition in gsec will result in gsec switching over to interactive mode. This is not very useful if you started gsec in batch mode from a script, because your script will just sit there waiting on something to be typed.

7.5. Potential Security Problems

Up until Firebird 2.0, running *any* of the Firebird utilities with a password supplied on the command line meant that anyone logged on to the same server could call `ps -efx|grep -i pass` (or similar) and be able to see the SYSDBA or other passwords. From Firebird 2.0 this is no longer possible as Firebird now replaces the supplied password with spaces.

Appendix A: Document history

The exact file history is recorded in the firebird-documentation git repository; see https://github.com/FirebirdSQL/firebird-documentation

Revision History

1.0	9 Nov 2004	ND	Created as a chapter in the Command Line Utilities manual.
1.1	19 Nov 2004	ND	Updated for Firebird 2.0.
1.2	20 Oct 2009	ND	More minor updates and converted to a stand alone manual.
1.3	05 Jan 2010	ND	Updated with details of Firebird 1.5 and Windows Vista not working when using IPCServer protocol. Thanks to Helen Borrie for the fix information.
1.4	11 Oct 2011	ND	Updated for Firebird 2.5. Spelling errors corrected.
1.5	18 Jun 2020	MR	Conversion to AsciiDoc, minor copy-editing
1.6	24 Feb 2024	MR	Change title to "Firebird's gsec User Management Utility", making it the same as on https://firebirdsql.org/en/reference-manuals/

Appendix B: License notice

The contents of this Documentation are subject to the Public Documentation License Version 1.0 (the "License"); you may only use this Documentation if you comply with the terms of this License. Copies of the License are available at https://www.firebirdsql.org/pdfmanual/pdl.pdf (PDF) and https://www.firebirdsql.org/manual/pdl.html (HTML).

The Original Documentation is titled *Firebird Password File Utility*.

The Initial Writer of the Original Documentation is: Norman Dunbar.

Copyright © 2004–2011. All Rights Reserved. Initial Writer contact: NormanDunbar at users dot sourceforge dot net.