Installing and Administering the DateView, StratDB and DepIso databases and web interfaces

Bruce Eglington

Contents

Introduction

This document provides information for administrators and users needing to set up or use any of the databases and web-server interfaces for the DateView geochronology database, StratDB lithostratigraphy/deposit/LIP database and the DepIso deposit isotope database. Information is provided to allow administrators to deploy local copies of the databases and their user interfaces, including how to control user access permissions.

Anybody with questions about the databases or their interfaces is welcome to contact Bruce Eglington at bruce.eglington@usask.ca.

Overview of the database management software and physical databases

The physical database file system comprises several separate but programmatically interlinked databases:

- **UserControl.FDB**,
- **StratDB.FDB** and
- **DateView.FDB**
- **Replication.FDB**
- **DVRawData.FDB**

Slightly different versions of these filenames are used in practice, to facilitate recognition of different dates of release and version.

Users should be aware that multiple physical databases are used but do not need to concern themselves about how the process works, just that some information gets stored in one database and then gets automatically replicated (copied) to the other database after entry or modification.

UserControl.FDB stores all information for registered users, including access permissions granted by the System Administrator.

StratDB.FDB stores information for reference sources, lithostratigraphic units, deposits, large igneous provinces and structural domains.

DateView.FDB stores all geochronological and isotope geochemical data. It also contains duplicate copies of the information and fields required to maintain links to **StratDB.FDB** and master lookup values for reference sources, deposits, etc. Software interfaces to the database systems automatically replicate changes to 'master' values to other parts of the database system when changes are made although separate programs are also available to further manage and facilitate the process.

Replication.FDB stores information to facilitate forcing of replication for selected information from **StratDB.FDB** to *DateView.FDB*.

DVRawData.FDB is used for the offline compilation of 'raw' data, such as detrital zircon U-Pb and Lu-Hf analyses.

The relational database management system (RDBMS) used for all databases is Firebird, currently implemented using version 2.5. Further details of the open-source Firebird database are available from www.FirebirdSQL.org . Firebird is a completely free, open-source product derived from the commercial Interbase RDBMS and is actively maintained and developed. It has a small footprint and experience over 12 years has demonstrated that is extremely stable and requires little administrator effort other than to run regular backups.

Administrators should install GUI (graphical user interface) database management software to enable them to manage the databases. *IBExpert*, a commercial package from www.ibexpert.net is recommended for this purpose although other open-source packages, such as FlameRobin, are also available.

User access to the databases is provided by three separate web-server programs, *STRATDB.EXE*, *DVIW.EXE* and *DEPISO.EXE*. These programs act as independent web-servers (no web-server software like IIS, Microsoft's Internet Information Service, or Apache is needed), although they ought to be installed as service on their host Windows computers to ensure that they automatically restart in the event of power failures or system reboots. At this stage, these programs are 32-bit Windows programs which can run on either 32-bit or 64-bit Windows operating systems. It is not necessary to have Windows Server versions of the operating system, a standard Windows 7 or more recent OS release is fine.

The database server software (Firebird), databases (**UserControl.FDB**, **StratDB.FDB** and **DateView.FDB**), the web-server programs (*STRATDB.EXE*, *DVIW.EXE* and *DEPISO.EXE*) may be installed on the same computer although it is generally recommended to run the databases and database server software on a different computer to the web-server software. Database administration software may be installed on the database server but would more typically be installed on the work computer of whoever is designated to act as administrator.

Some of the additional programs provided to assist with deployment and administration of the database and the web server interfaces are:

- *Test.EXE* – facilitate tests that the web-server programs and folder structures are most likely correct
- *ConfigBME.EXE* – modify the configuration settings for replication between databases
- *ReplicateBME.EXE* – activate a specific replication cycle for one or more master databases
- *DVCheck.EXE* – perform a series of checks on the integrity of data records in the **DateView.FDB** database
- *DVRawData.EXE* – read 'raw', i.e. analytical data, from Excel spreadsheets and import into a temporary database (**DVRawData.FDB**) prior to final checking and pumping to the primary **DateView.FDB** database
- *IBPump.EXE* – free software, from Clever Components, used to pump data records from one database to another when needed

Software Installation and Administration

Installing Firebird

Latest download packages for installing Firebird are available from the www.firebirdsql.org . The current recommended version is 2.5. Firebird may be installed in one of three configurations (Classic, SuperClassic and SuperServer). The SuperServer configuration is recommended, following recommendations and settings documented at http://www.ibsurgeon.com/en/articles/firebird-hardware-guide/ . A number of other useful documents and software are also available from this IBSurgeon website, including software to control automated backups and restores if this is desired.

If the database server computer is Windows 64-bit, then ensure that the 64-bit version of Firebird is installed but note that a 32-bit version of the fbclient.dll file will need to be placed in the executable folder along with the web-server programs since these are currently all 32-bit programs.

Default installations of Firebird also include the GBAK.EXE program, which may be used for command-line backups and restores of the databases (see later).

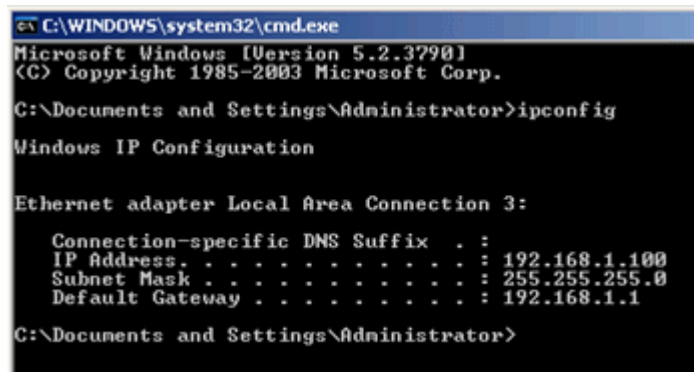## Enable firewall port for Firebird Server

It is important to remember that the Firebird database software responds via port 3050 for default setups. Windows firewalls need to have this port open for incoming traffic.

Ensure network uses TCPIP for communication between computers and server

· The server and networked computers will communicate via TCPIP. If your network is not yet configured, do so. If you are not experienced with this, please contact your local computer center.

· To confirm whether your network can communicate or not, determine the server's static internal IP address and ping from a local area networked computer

Open a command prompt on the server (Start -> Run -> type in cmd and click on OK) and type ipconfig in the DOS prompt

Figure 1. CMD window use of IPCONFIG to determine the IP address of a computer.

Make a note of your server's IP Address

Confirm that network computers can "talk" to the server by opening a command prompt on a local area networked computer and typing ping xxx.xxx.xxx.xxx and the Enter key where xxx.xxx.xxx.xxx is the IP address of your server

For example, if your server's IP address is 192.168.1.15, you would type ping 192.168.1.15

If you get a timeout, there is an issue connecting via TCPIP. Please contact your local computer center to troubleshoot.

Check that Firebird is running

Reboot the computer and log in as the windows administrator

Confirm that the network Firebird server is running

·Open Control Panel -> Administrative Tools -> Services

·Confirm both the Firebird Guardian Service (if needed) and the Firebird Service are running, that the Firebird Guardian Service is set to Automatic and the Firebird Service is set to Manual as shown in screenshot below
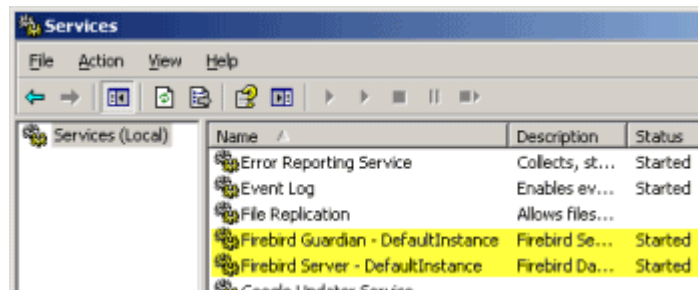
Figure 2. Services panel, illustrating that the Firebird Guardian and Firebird Server Control services are running.

·You will also note the Firebird Service Control in Control Panel if not using more recent versions of Windows OS. Double-click to open to confirm is running.
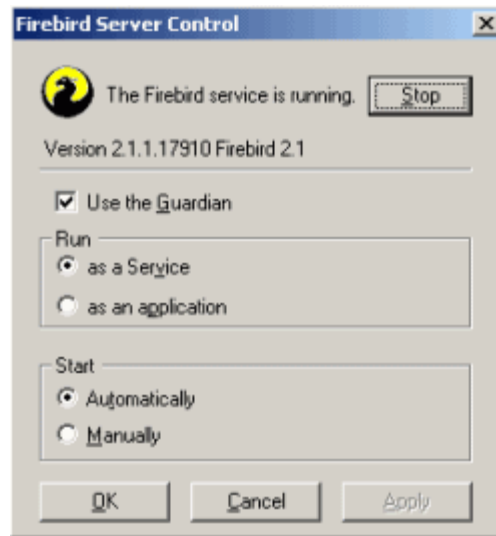
Figure 3. Firebird Server Control program settings.

Additional optional step i. As the network Firebird server uses a default password that is known by all, it is suggested that you change the default password.

Modify the Firebird system administrator password

The default userid after initial Firebird system installation is SYSDBA (not case sensitive) and the associated default password is "masterkey" (in fact only the first 8 characters apply so it is actually "masterke"). Note that the password is case sensitive. To ensure security, the password ought to be changed as described below:

·Open a command prompt (Start -> Run -> cmd)
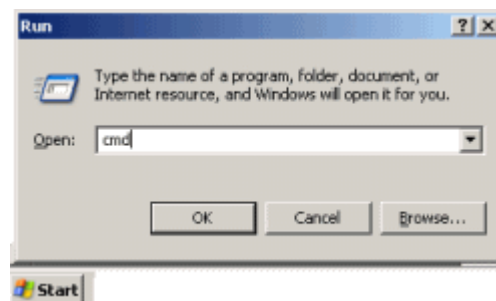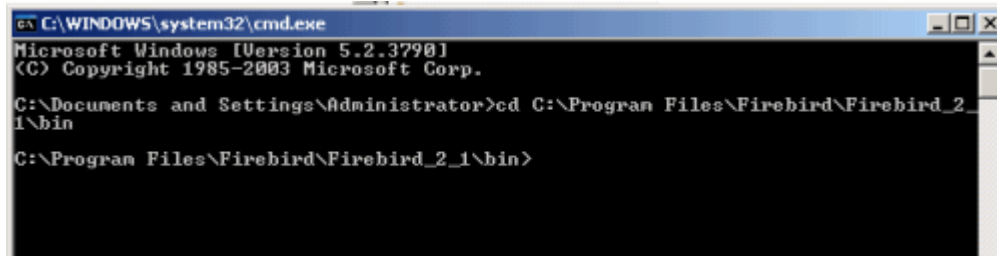
Figure 4. Starting the CMD application from the Windows command graphical user interface.

· Move to the C:\Program Files\Firebird\Firebird_2_1\bin directory by changing to that directory by typing

CD C:\Program Files\Firebird\Firebird_2_1\bin
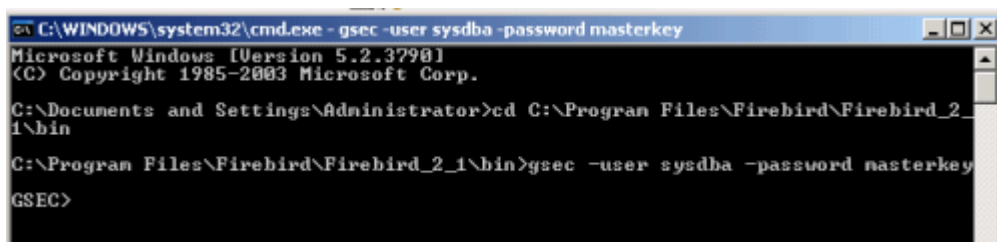
Figure 5. CMD prompt ready to enter the GSEC commands. Note that you need to be in the folder appropriate to the version of Firebird installed on the database server computer. The example provided had version 2.1 of Firebird installed at the time the image was captured.

· Type the following (do not copy as you will receive syntax error message if you attempt to do so)

gsec –user sysdba –password masterkey

· You will now see a shell prompt

GSEC>

Figure 6. CMD prompt ready to enter the statement to modify the SYSDBA password using GSEC.

· Now you will type in to modify the Firebird Server's sysdba's password to something other than the default. In the example below, we have entered "newpwd". You can and should of course have your sysdba password set to something different

modify sysdba –pw newpwd
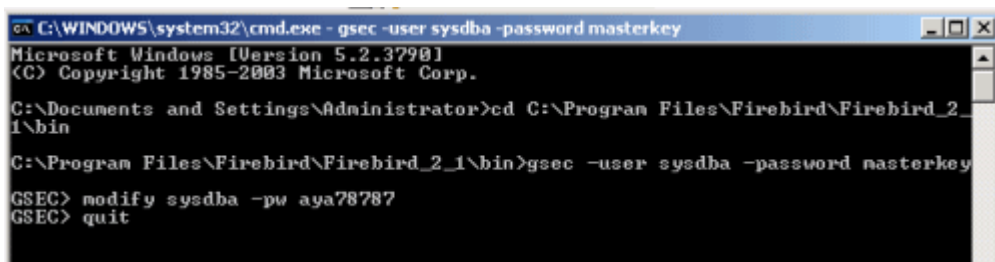
Figure 7. CMD prompt in which the SYSDBA password is changed to a different value, in this case to aya78787.

· Make a note of the password you have chosen exactly as typed as you will need it when you edit the various .INI files for the web-server programs and for any other programs that connect to the Firebird database server.

· Type the following at the prompt which will close out of the gsec utility.

Quit

Figure 8. CMD prompt to quit from the GSEC interface.

· Exit out of the command prompt window

Copy the various Firebird databases to the data folder
Using Windows Explorer, create a folder on the database server in which the networked databases will be located - for example: C:\Data\Firebird\

 NOTE: Never ever move or edit or copy the database files once network Firebird is installed and running unless:

· every user is out of the database and of the web-server programs

· any additional database-related programs are shut down

· and you have stopped the Firebird service by opening Control Panel -> Firebird Server Manager -> select Stop

· Moving, editing or copying a live database file will cause database problems – even corruption

Installing the Web-server Programs

The recommended folder structure for installation on MS Windows computers is to create a separate folder on drive C:. The default used for this purpose is C:\EXE32. This folder, rather than a subfolder under \PROGRAM FILES, has been chosen to facilitate easy changes to various files in the folder. Typical computer access permissions for \PROGRAM FILES make it rather difficult to make changes. A number of sub-folders with various files need to be present in this folder:

C:\EXE32\WWWROOT
C:\EXE32\WWWROOT\FILES
C:\EXE32\WWWROOT\FILES\FLEXCELL
C:\EXE32\WWWROOT\FILES\MAPS

The \FLEXCELL subfolder contains Excel spreadsheet template files used by the web-server programs for exporting data selected in various queries. Aspects of these templates, in particular headings and layout, may be changed if necessary. If changes are required, please contact the software developer (Bruce Eglington) before doing so to ensure that changes are compatible with program requirements.

The \MAPS folder contains shape files appropriate for use by DVIW.EXE for some of its graphical output.

The C:\EXE32 folder needs to contain the following files for the database interfaces to work correctly:

DVIW.EXE
STRATDB.EXE
DEPISO.EXE
FBCLIENT.DLL
DBEXPIDA40.DLL

The *TEST.EXE* web-server program executable (see details later) should also be placed in this folder and installed as a service, similar to the other programs.

All web-server programs used for database access should be installed as Windows services. The web service aspect of each program responds to calls to unique ports which would be implemented via URL hot links on a separate web page served from a company's web site. Thus, the URL to run DVIW.EXE would be something like
        http://mywebserver.usask.ca:8085/
where the web-server programs are hosted on a computer named "mywebserver.usask.ca" and responding to port 8085. Port numbers for each of the web-server programs are as follows:

STRATDB.EXE	-	8091
DVIW.EXE	-	8085
DEPISO.EXE	-	8092
TEST.EXE	-	8087

The computer hosting these web-server programs needs to have its firewall opened for incoming and outgoing traffic utilising these ports.

DVIW.EXE, *STRATDB.*EXE and *DEPISO.EXE* expect .INI files with various software configuration details. The .INI files need to available in a \EGGSOFT subfolder of the computer's 'Public path folder'. For most

Windows 7 and more recent operating systems this path is C:\PROGRAMDATA\EGGSOFT. The INI files are read the first time the program service is started and allow easy changes to software paths for where the databases are physically located and to changes in database setup without the need to hard-code these in versions of program file for different user environments. It also means that it is easy to run personal versions of the software and databases while testing or while travelling away from internet access.

Typical file contents for the INI files are as follows:

StratDB INI file
[URLBase]
URLBase=/
[Paths]
Usercontrol path = dataserver.usask.ca:d:/Data/Firebird/UserControl2015v25.fdb
StratDB path = dataserver.usask.ca:d:/Data/Firebird/StratDB2015v25.fdb
DateView path = dataserver.usask.ca:d:/Data/Firebird/DateView2015v25.fdb
[Monitor]
DBMonitor = InActive
[Debug]
Buttons = InActive
DelayConnections = true
 [Parameters]
DriverName=DevartInterBase
RoleName=
User_Name=SYSDBA
Password=masterkey
SQLDialect=3
BlobSize=-1
ErrorResourceFile=
LocaleCode=0000
DevartInterBase TransIsolation=ReadCommitted
WaitOnLocks=True
Charset=ASCII
CharLength=1
EnableBCD=True
OptimizedNumerics=True
LongStrings=True
UseQuoteChar=False
FetchAll=False
UseUnicode=False

DateView INI file
[URLBase]
URLBase=/
[Paths]
Usercontrol path = dataserver.usask.ca:d:/Data/Firebird/UserControl2015v25.fdb
StratDB path = dataserver.usask.ca:d:/Data/Firebird/StratDB2015v25.fdb
DateView path = dataserver.ca:d:/Data/Firebird/DateView2015v25.fdb
[Monitor]
DBMonitor = InActive
[Debug]

```
Buttons = InActive
DelayConnections = true
 [Parameters]
DriverName=DevartInterBase
RoleName=
User_Name=SYSDBA
Password=masterkey
SQLDialect=3
BlobSize=-1
ErrorResourceFile=
LocaleCode=0000
DevartInterBase TransIsolation=ReadCommitted
WaitOnLocks=True
Charset=ASCII
CharLength=1
EnableBCD=True
OptimizedNumerics=True
LongStrings=True
UseQuoteChar=False
FetchAll=False
UseUnicode=False
```

DepIso INI file

```
[URLBase]
URLBase=/
[Paths]
Usercontrol path = dataserver.usask.ca:d:/Data/Firebird/UserControl2015v25.fdb
StratDB path = dataserver.usask.ca:d:/Data/Firebird/StratDB2015v25.fdb
DateView path = dataserver.usask.ca:d:/Data/Firebird/DateView2015v25.fdb
[Monitor]
DBMonitor = InActive
[Debug]
Buttons = InActive
DelayConnections = true
 [Parameters]
DriverName=DevartInterBase
RoleName=
User_Name=SYSDBA
Password=masterkey
SQLDialect=3
BlobSize=-1
ErrorResourceFile=
LocaleCode=0000
DevartInterBase TransIsolation=ReadCommitted
WaitOnLocks=True
Charset=ASCII
CharLength=1
EnableBCD=True
OptimizedNumerics=True
LongStrings=True
UseQuoteChar=False
FetchAll=False
```

UseUnicode=False

Test web-server INI file

[URLBase]
URLBase=/
[Paths]
Usercontrol path = dataserver.usask.ca:d:/Data/Firebird/UserControl2015v25.fdb
StratDB path = dataserver.usask.ca:d:/Data/Firebird/StratDB2015v25.fdb
DateView path = dataserver.usask.ca:d:/Data/Firebird/DateView2015v25.fdb
 [Monitor]
DBMonitor = InActive
[Debug]
Buttons = InActive
DelayConnections = true
 [Parameters]
DriverName=DevartInterBase
RoleName=
User_Name=SYSDBA
Password=masterkey
SQLDialect=3
BlobSize=-1
ErrorResourceFile=
LocaleCode=0000
DevartInterBase TransIsolation=ReadCommitted
WaitOnLocks=True
Charset=ASCII
CharLength=1
EnableBCD=True
OptimizedNumerics=True
LongStrings=True
UseQuoteChar=False
FetchAll=False
UseUnicode=False

The [URLBase] aspect of each INI file contains details for use with future reverse proxy definitions so as to enable reverse proxy servers to associate standard HTTP protocols and calling on port 80 with the web-server port numbers. This has not yet been tested and implemented but the software vendor for the web interface component used during program coding has indicated that new versions of their components will be able to use this capability.

The [Paths] section of each INI file provides the path URL for each of the physical databases required by that program.

The DBMonitor field of the [Monitor] section is usually set to InActive but may be set to Active when testing database interfaces with a Devart© database monitor program which allows one to see all SQL calls to the databases.

The Buttons field of the [Debug] section is usually set to InActive but may be set to Active when testing database interfaces. It makes two buttons visible on the main window interface so that a user may check what permissions have been granted and also some of what is read in from the INI file.

The DelayConnections field of the [Debug] section is usually set to true which ensures that database connections are only attempted once a user has logged in. This is a useful setting to check that a web-server program is running before connecting to any database.

The [Parameters] section holds definitions appropriate to the Firebird 2.5 database installation used. Of particular note at this stage is that all databases expect only ANSI ASCII characters. Unicode strings and character sets are not supported with the current database designs.

Note that, for the *TEST.EXE* web-server program, paths and connection details are listed for various databases, even though this program does not actually connect to any database. This is to permit one to check that the program is correctly reading the values provided.

Firewall Settings for Firebird and the Web-server Programs
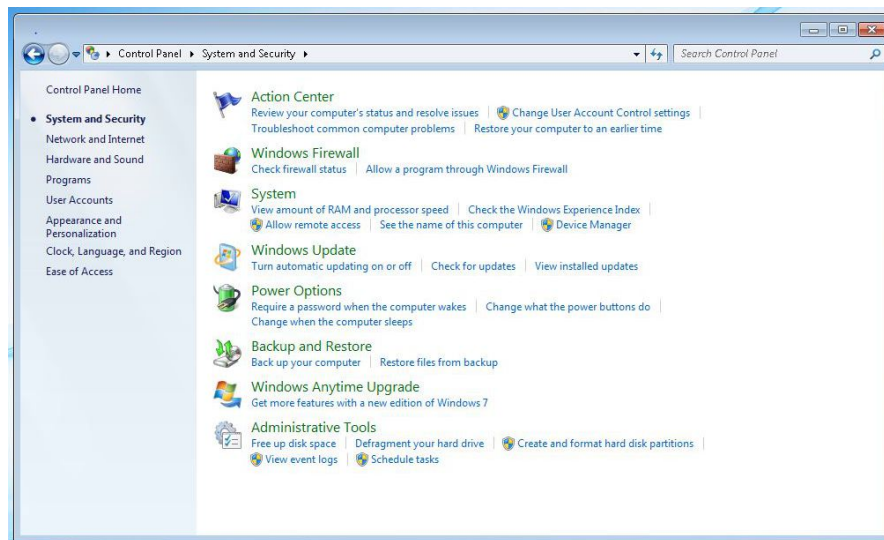
Figure 9. Windows interface to modify firewall settings.

The Windows firewall needs to be open for communications between the web-server applications and the Firebird database management system.

Backing up and Restoring Firebird Databases

Commercial software, such as FBDataGuard, may be purchased to facilitate automated backup and restore of the databases, although this is not necessary. Both can also be run from IBExpert, although not for remote databases. It is easy to run backups for both local and remote databases manually using

appropriate .BAT batch files which call the GBAK.EXE program installed with Firebird. Documentation on GBAK is readily available from the internet. A typical batch file or command line statement to backup a database would be:

```
echo on
cd c:\program files\firebird\firebird_2_5\bin
pause
gbak -B -V  dataserver.usask.ca:d:/data/firebird/usercontrol2015v25.FDB
c:\data\firebird_backups\usercontrol_20151203.fbk -USER SYSDBA -PASS masterkey
pause
```

This batch file changes active directory to the path where the GBAK.EXE file is located (c:\program files\firebird\firebird_2_5\bin in this case), then backs up (-B option) the file usercontrol2015v25.FDB from path dataserver.usask.ca:d:/data/firebird/ to a file c:\data\firebird_backups\usercontrol_20151203.fbk on the local computer. User ID and password are Firebird's default values, SYSDBA and masterkey, respectively. The –V option provides verbose output on-screen so that one sees all stages of the process. Note the convention that Firebird database files have a .FDB extension whereas backup files have a .FBK extension.

The backup process cleans a database file by doing a sweep and removing all cases of multiple information since the database stores copies of all changes, which would lead to degradation of database processing speeds over time.

Restores, if needed, may be performed in a similar manner. Although possible, one should never overwrite an existing database. Rather, restore to a new database file, test that this works without errors and then replace the original version with the new one. Even if one does not replace an old database file with a new one, one should always check that the backup process has worked correctly. It is no use having a backup of a corrupted database! This is one of the advantages of the FirebirdDataGuard software as this entire process may be automated.

Troubleshooting Connection Problems

Several problems may be encountered when installing and running database servers, databases, web-servers, etc; especially in situations where organisations implement additional levels of security. In general, the problems may be classified as one or more of the following:

- Related to the web-server programs themselves and unrelated to the databases or database server
- Incorrect path addresses for individual databases
- Database server issues

These need to be investigated systematically to ensure that one is certain of the cause.

Step 1 - Testing that the web interfaces work

The web-server programs each require that both the web server and the database server work correctly and that connections between them are appropriate. The first stage that needs to be tested with new deployments is that the web-server interface is operating correctly, independent of any associated database requirements. A small web-server program, named *TEST.EXE* has been provided for this purpose. You may either install this program as a service in the same way as detailed for *STRATDB.EXE*, *DVIW.EXE* and *DEPISO.EXE* (see above) or you just create a shortcut to the program on the desktop. Both situations require a .INI file, as described earlier. If you start the program from the desktop (i.e. not as a service), then the first window seen will look something like the image in Figure 10.
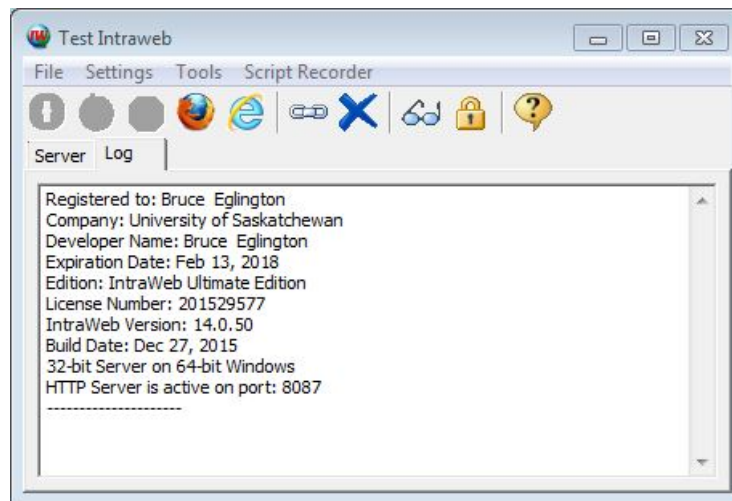
Figure 10. Start window for TEST.EXE web-server program when run as a standalone program, not a service.

In this case, two types of internet browser are available on the host computer, as indicated by the Mozilla Firefox and Microsoft Internet Explorer icons. Click on the icon for the browser you wish to use

The program should display an interface similar to the image in Figure 11.
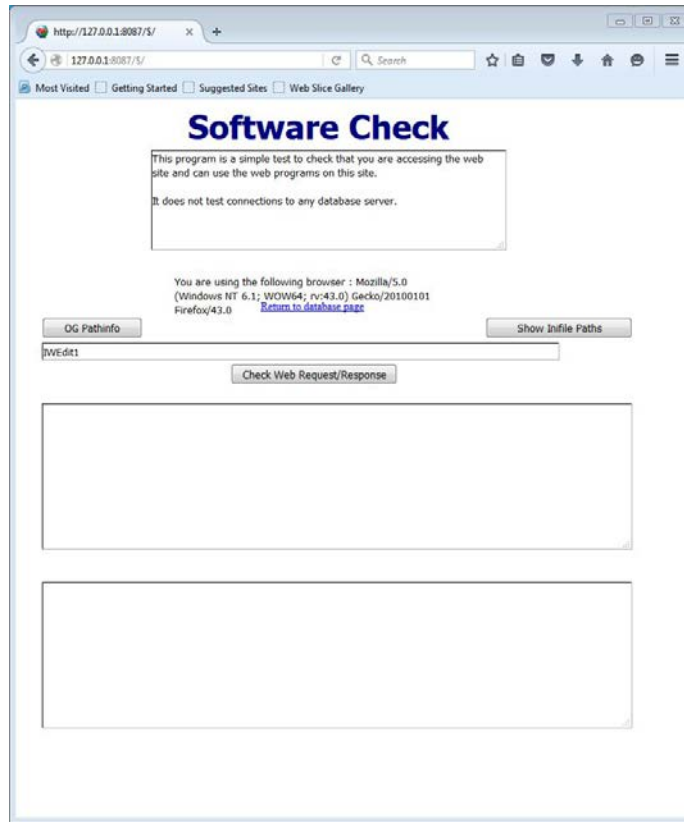
Figure 11. Program interface to check that web-server instances and basic file paths are correct.

Clicking on the various buttons should provide text in some of the fields or a series of messages which may be compared with values known to be in the INI file. As long as these INI file values are correct and the program is responding then the web-server interface has been correctly deployed and one may assume that the other web-server programs are also correct. If these other web-server programs don't work, then it is likely that either the database server is not correctly deployed, there are problems with the connections to the database server or that a firewall is limiting access to the databases .

Step 2 - Testing that the databases, database server and firewall ports are correctly configured

If you have completed the steps in the Firebird guide (available from www.firebirdsql.org) and are experiencing problems connecting to the database, please follow the troubleshooting steps below:

Connection Error	Potential Causes	Resolution
Unable to complete network request to host [hostname].	1. The server name or IP Address could not be found.	Step 1: Click the "Ping" button. If the result is: "Ping Failed", then the problem is Cause #1 to the left.

	2. The Firebird service is not running on the server. 3. A firewall is blocking access to the port. 4. The port that the web-server programs are configured for is not the same one that Firebird is listening on.	Verify the server name or IP Address with your server administrator, and confirm that it is accessible on the network. Step 2: Check Windows Task manager to ensure that Firebird is running. If not, then the problem is Cause #2 to the left. Skip the remainder of this section and follow the steps listed for the error message in the next row below. Fr all other failed connection attempts, then the problem is Cause #3, or 4 to the left. Use the troubleshooting steps listed below this table for the specified cause to resolve the problem.
No connection could be made because the target machine actively refused it.	The Firebird service is not running on the server.	Start the Firebird service in Windows Control Panel --> Administrative Tools --> Services. If the Firebird service is not listed there, install the latest Firebird package. If you have run the Firebird database server installer, but the service is not displayed or will not run, an anti-virus software may have interfered with the installation. Temporarily disable any anti-virus software and re-install Firebird again.
Your user name and password are not defined. Ask your database administrator to set up a Firebird login.	The value entered in the SYSDBA password field does not match the SYSDBA password on the Firebird server. Note: The SYSDBA password is used by the database server. It is not the same as the application passwords that have been set up for personnel to login to the client software. Leave the setting as the default value	If the Firebird administrator has changed the SYSDBA password for the Firebird database, request the password or have the administrator enter the password for you in the SYSDBA Password field of the web-server program's .INI file. If the SYSDBA password has not been changed, there may be another instance of Firebird running on the server with a different

	unless it has been changed on the server.	SYSDBA password. See the multi-instance configuration instructions in the Firebird user guides.
Unsuccessful execution caused by a system error that precludes successful execution of subsequent statements. I/O error for file ".....\security2.fdb". Error while trying to open file. The system cannot find the path specified.	This message may appear when attempting to use the database from a file share. A database being accessed through a file share is subject to data corruption. Firebird is designed to run in client-server configuration for multiple users.	Do not use a file share.
Any other error message not listed above.	Unknown	Check each of the items listed below and then try again. If the problem continues, contact the software developer.

Check the Windows firewall:
The Windows firewall is a frequent cause for not being able to connect to the server. Make sure port 3050 is available for Inbound TCP connections on the server. Here are the steps:

For Windows 2008 and later:
Open the Windows Firewall With Advanced Security: Start --> Search --> enter "firewall", and select the program "Windows Firewall With Advanced Security".
Select "Inbound Rules" in the left pane.
Click "New Rule" in the Actions pane on the right, and create a rule with the following settings:
Rule Type: Port
Protocol: TCP
Specific Port: 3050
Action: Allow the connection.
Profile: As required.
Name: Firebird

Check the Firebird database process:
If you have already configured the firewall and are still unable to connect, please check to see if the Firebird database process is running on your server.

1. Open the Windows Task Manager: Start --> Run --> enter "taskmgr", and then click the Ok button.
2. Go to the processes tab, and make sure the checkbox for show processes for all users is checked.
3. Sort the processes by clicking on the Image Name column header and look for a process named fb_inet_server.exe.
4. If the process is not there, please install the Firebird Server.

Confirm the database connection setting:
If you have configured the Firewall and the database process is running, confirm that the database connection settings in the .INI file for the web-server program is correct.

If the problem continues, there may be an anti-virus or other security software blocking the process on the server.

Check the firebird.log file for errors:
Log in to the server, and check the firebird.log file in the Program Files\Firebird directory for errors.

You may see an error such as the following: "INET/inet_error: select in packet_receive errno = 10038" --> This error indicates that the Firebird server process cannot operate correctly due to network interference which may be caused by an anti-virus or other security software blocking it. Check your security software and exclude the Firebird process or temporarily disable the security to test the connection again.

inet server err: setting KEEPALIVE socket option or inet server err: setting NODELAY socket option --> This error may indicate that you need to use the "SuperServer" version of Firebird instead of the "Classic" or "SuperClassic" versions. Re-install Firebird and choose the "SuperServer" option when prompted.

Installing Programs as Services in Windows 7

It is possible to run each web-server application program by manually starting it when necessary but, for use by multiple users in a server type environment it makes more sense to install and run the programs as Windows services. This allows the application to automatically run at boot time without the need for a user to be logged into the system in order for the application to start and operate. While built-in mechanisms such as Task Scheduler exist to help facilitate this, the ability to run an application as a service has certain advantages, notably the ability to prescribe certain actions be taken should the service fail, for instance in cases where an application is listening for incoming IP connections. Being able to automatically restart the service without user intervention is desirable in order to avoid loss of service.

This documentation describes how to use the Microsoft utilities *instrsrv.exe* and *srvany.exe* to install a Windows application as a service. *instrsrv.exe* is used to install the service while *srvany.exe* acts as a wrapper around the application and handles the service events. Both utilities are available as part of Microsoft's Windows Server 2003 Resource Kit Tools and both run under Windows 7.

IMPORTANT: This documentation contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information on how to do this, view the "Restoring the Registry" or the "Restoring a Registry Key" online Help topics in Registry Editor.

1. Download the Windows Server 2003 Resource Kit from Microsoft's web site and install so as to have access to the *instrsrv.exe* and *srvany.exe* files.

2. Copy *instrsrv.exe* and *srvany.exe* to the **C:\Windows** directory.

3. It is assumed that all user application software will be installed in the folder **C:\EXE32**. Create this folder if necessary and copy the programs to it.

4. Open a command prompt window as administrator.

5. In the command prompt window go to the **C:\EXE32** directory.

6. Type: **instsrv.exe <application.ext> srvany.exe** and press the **Enter** key (where **<application.ext>** is the program to be installed as a service e.g. *STRATDB.EXE*).

7. Run Registry Editor (**regedit.exe**) and locate the following subkey: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<application.ext>** (where **<application.ext>** is the program to be installed as a service e.g. *STRATDB.EXE*).

8. In Registry Editor select the menu item **Edit>New>Key**.   The key name will appear highlighted for editing. Type **Parameters** and press the **Enter** key.

9. Select the **Parameters** key.

10. In Registry Editor select the menu item **Edit>New>String Value**.   The value name will appear highlighted for editing. Type **Application** and press the **Enter** key.

11. Right click **Application** and select **Modify…** In the box labelled **Value data:** type **<path>\<application.ext>** (where **<path>\<application.ext>** is the drive and full path to the application executable including the extension e.g. **C:\EXE32** *STRATDB.EXE*) and press the **OK** button.

12. Close Registry Editor.

13. Reboot the computer.

14. Run the **Services** program and verify that the Programs that were just installed are running as services.

Controlling and Administering User Access and Permissions

Introduction

All users need to login to be able to access data from the various databases. This permits control of user access to various software capabilities and ensures that only those users with appropriate permissions are able to modify existing records or insert new records. The default permissions provided for new users is quite restrictive to ensure that new users can read public data in the system but are not able to make changes, nor download much. In general, only the database administrator has delete privileges for information in the system.

User login and permissions also allow one to implement data management in which individual users or specified groups of users may access particular records which are not available for 'public' consumption. Typical examples may be personal, unpublished data or company-specific data. User access also provides a way to limit the maximum number of records that may be downloaded by individual users, which is particularly useful in cases where internet connection speeds are slower.

All user control data are stored in the **UserControl.FDB** database, which can only be edited manually by the database administrator using software such as the IBExpert package referred to earlier or for a limited number of fields by the end user through the registration interfaces provided by *DVIW.EXE*, *STRATDB.EXE* and *DEPISO.EXE*. When new users register online to use any of the databases, their basic supplied information is stored in this database and they are able change this information or ask for an email to be sent to their registered email address if they forget their passwords.

Access-permission Keywords

Access permissions are controlled by a number of program-specific keywords and by membership of administrator-specified user groups. By default, all users belong to the "PUBL" group i.e. they have access to published or public-domain data. Currently permissible user-access keywords for the different web-server programs and databases are provided in Table 1.

Table 1. User-access and permission keywords.

	StratDB	DateView	DepIso
Allowed to view data.	ViewStrat	ViewDateView	ViewDepIso
Allowed to modify existing records in the database.	ModifyStrat	ModifyDateView	ModifyDepIso
May insert new records into the database.	InsertStrat	InsertDateView	InsertDepIso
May delete records in the database. This is EXTREMELY dangerous and should only be available to the database administrator or very	DeleteStrat	DeleteDateView	DeleteDepIso

experienced senior administrators who know the database structure and design and understand the consequences of deleting specific entries.			
User has agreed to play the additional role of moderator or adjudicator for information in a database. Different users may play different roles in the same database and this is not distinguished. This capability is implemented programmatically but appropriate users have not yet been appointed.	ValidateStrat	ValidateDateView	ValidateDepIso
May export data from searches. The maximum number of records which may be exported is specified in a separate table (USERMAXOUTPUTRECORDS) in the UserControl.FDB database.	ExportStrat	ExportDateView	ExportDepIso
Additional permission level for viewing data. Principally implemented to facilitate testing of new capabilities by limited groups of individuals.	ViewStratPlus	ViewDateViewPlus	ViewDepIsoPlus
Additional permission level for modifying. Principally implemented to facilitate testing of new capabilities by limited groups of individuals.	ModifyStratPlus	ModifyDateViewPlus	ModifyDepIsoPlus

These keywords are concatenated but separated by semi-colons and a space in a BLOB field for each registered user in the WEBUSERS table in the **UserControl.FDB** database. For convenience of reading, they are separated by a heading which indicates to which database they apply. An example is shown below:

Table 2. Example extract of user-access permission keywords from the WEBUSERS table.

```
[StratDB]
ViewStrat; ModifyStrat; ValidateStrat; DeleteStrat; ViewStratPlus;
ModifyStratPlus; InsertStrat; ExportStrat;

[DateView database]
ViewDateView;ModifyDateView;InsertDateView;DeleteDateView;ValidateDateView;
ExportDateView;ViewDateViewPlus;ModifyDateViewPlus;

[DepIso]
```

ViewDepIso; ModifyDepIso; InsertDepIso; DeleteDepIso; ValidateDepIso;
ExportDepIso; ViewDepIsoPlus; ModifyDepIsoPlus;

Specifying Maximum Download Limits for a Session

The number of records (rows) which may be downloaded by users is specified in the
USERMAXOUTPUTRECORDS table. The default value is 20 for each type of download but may be set at
any integer value. Lots of users simultaneously downloading many records could impact server
performance considerably.

Once users have registered and connected to specific database interfaces, they need to contact the
appropriate database administrators to organise for greater permission levels or for greater download
limits. Changes to values in these table have to be made manually by the database adminstrators.

User Groups

In addition to the 'PUBL' user group which all users belong to by default, users may also organise to
belong to additional groups which may be created by the database administrator. An abbreviation and
name for each group first needs to be defined in the FORLIST table in the **StratDB.FDB** database by the
administrator using a program like IBExpert. Then the individual users belonging to the group need to be
specified in table USERSWHOFOR, also in the **StratDB.FDB** database. At the next replication cycle, these
entries will be replicated to other appropriate nodes in the database hierarchy. Replication may be
forced by running program ReplicateBME.EXE once it has been correctly set up.

Default Starting ID Numbers

In cases where additional databases; separate from the master versions of StratDB and DateView,
hosted at the University of Saskatchewan and administered by Dr Bruce Eglington; exist, it is important
to ensure that unique ID values in various tables do not conflict with ones in the master databases.
Some of these potential conflicts can be guarded against by changing the default increment starting
values in the non-master systems and by changing some values for GENERATORS for the databases.

The alternative is to always add new records in the master database and then have them replicated to
non-master systems. This approach is not feasible, however, in cases where non-master databases have
been established for organisations requiring separate, secure systems.

Prior to adding new records and values to 'lookup' tables, database administrators for non-master
database implementations should discuss and agree on changes with the master system database
administrator (currently Bruce Eglington) to minimise the chance of future conflicts. Specific tables and
fields which are definite likely causes of conflict and which MUST be considered prior to deployment as
non-master versions are:

StratDB

Table	Field	Default values and comments
COUNTRIES	STARTINGVALUE	Default values for the first record in each country are provided in this field. Values for all countries in non-master databases should have values in excess of 200,000,000 to avoid conflict with the master databases when merging records. Specific excess range values will need to be agreed prior to implementation of specific non-master databases.
DEPOSITS	SDBDEPOSITID	Default values are generally associated with specific DATABASEID values (foreign key to records in table OTHERDATABASES. Non-master systems should establish different, new DATABASEID values for their new compilations of deposits.
DOMAINS	DOMAINID	DOMAINID values in non-master databases should be in excess of 100,000 to avoid conflict with the master databases when merging records. Specific excess range values will need to be agreed prior to implementation of specific non-master databases.
LIPS	LIPID	Values for all LIP's in non-master databases should have values in excess of 100,000 to avoid conflict with the master databases when merging records. Specific excess range values will need to be agreed prior to implementation of specific non-master databases.
SOURCELIST	SOURCENUM	Values for all LIP's in non-master databases should have values in excess of 100,000 to avoid conflict with the master databases when merging records. Specific excess range values will need to be agreed prior to implementation of specific non-master databases.
STRATUNITS	UNITID	See discussion above for default values per country in situations where no records already exist in the database for the country concerned. UNITID values for all countries in non-master databases should be in excess of 200,000,000

		to avoid conflict with the master databases when merging records. Specific excess range values will need to be agreed prior to implementation of specific non-master databases and need to be compatible with STARTINGVALUE numbers in the COUNTRIES table (see above).

Generator	Default values	Comments
GEN_CHARTS2_I	20001	
GEN_DEPOSITCLANS_ID	2001	Should rather be updated and drawn from the master system
GEN_DEPOSITS_ID		Value set to work with new "OtherDatabase" ID's
GEN_DOMAINS_ID	200001	
GEN_LIPS_ID	200001	
GEN_OROGENIES_ID	200001	Should rather be updated and drawn from the master system
GEN_OTHERDATABASES_ID	20001	
GEN_SOURCELIST_ID	200001	
GEN_SPECIALFEATURES_ID	2001	Should rather be updated and drawn from the master system
GEN_USERPROJECTS_ID	200001	

DateView

Table	Field	Default values and comments
DEPOSITS	SDBDEPOSITID	All values and records in this table come from the StratDB database. No new values should be directly entered in DateView.
DOMAINS	DOMAINID	All values and records in this table come from the StratDB database. No new values should be directly entered in DateView.
FORLIST	WHOFORID	All values and records in this table come from the StratDB database. No new values should be directly entered in DateView.
LIPS	LIPID	All values and records in this table come from the StratDB database. No new values should be directly entered in DateView.

LITHOL	LITHOLOGY	Manual compatibility with the master database needs to be maintained.
SOURCELIST	SOURCENUM	All values and records in this table come from the StratDB database. No new values should be directly entered in DateView.
VARVAR	VARIABLEID	Manual compatibility with the master database needs to be maintained.

Generator	Default values	Comments
GEN_SUITE_ID	200001	

General Program and Database Information on the Initial Access Windows

Each web-server program interface displays the title of the database/interface, the display name of the users once they have logged in and some information which the database administrator wishes to provide.

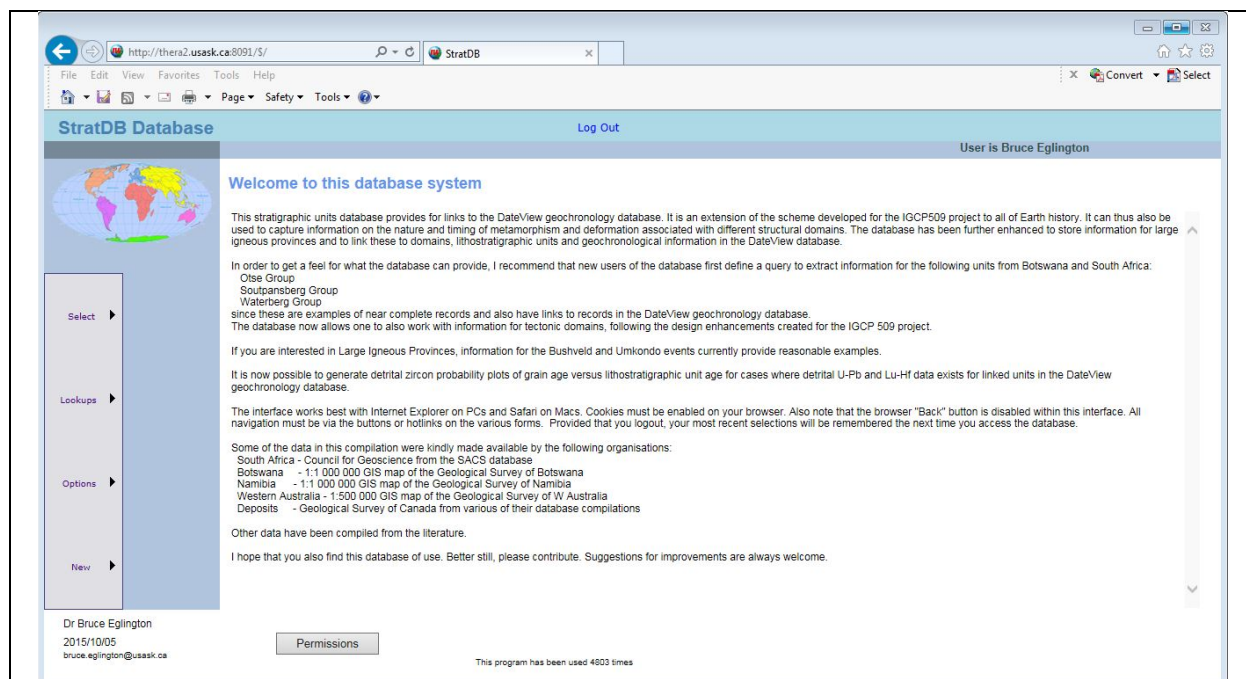An example window, in this case for the **StratDB.FDB** database, is provided in Figure 12.

Figure 12. Main window for the StratDB interface shown after a user has logged in.

Text for these fields are extracted from the PROGRESS table in the **UserControl.FDB** database. Database administrators may choose to modify the values in this table to better represent their specific implementations of the databases and interfaces.

When users logout from a particular web-server interface, their browser pages will be redirected to the URL specified in the URLOnTerminate field of table PROGRAMS. Database administrators need to specify URL values appropriate to their specific websites.

All users should be aware that the 'Back' button, a common feature of most web browsers, will not work in these web-server programs. This is by-design since the ability to modify and insert records into databases requires that the web-server interfaces keep track of 'state' i.e. they need to know what previous web requests have been issued by a user and responded to by the server. Standard web browser interfaces, which only serve existing data, do not have this requirement so they can use the back button to rerun preceding queries without confusing the system. All navigation in these *DVIW.EXE*, *STRATDB.EXE* and *DEPISO.EXE* web-server interface must be via specific buttons or 'hot-links' on the web pages and never via the 'Back' button..

Users are encouraged to logout of an interface when they finish a session, i.e. not to just click on the close X for a page. If this is done, then the details of the last query they ran will be stored for the next time they login to the system.

Merging or Copying Records Between Databases

Sometimes it is necessary to copy records between database tables, implementations of different databases or from a local compilation in Microsoft Access to Firebird. A number of methods are available for various of these situations, including importing data from Excel and desktop databases in IBExpert or by pumping data using software packages such as IBPump.

IBPump is a free utility program provided by Clever Components (http://www.clevercomponents.com) and is particularly useful for transferring records from Microsoft Access databases to Firebird or Interbase databases or from one Firebird or Interbase database to another one. Commercial versions of the code and methodology by behind IBPump are also available from Clever Components.

Documentation on how to use IBPump is available online from http://www.clevercomponents.com/products/datapump/dp-tour.asp