DBARS

DBARSGUI
User's Guide

Version 4.4

www.sprdb2.com

Software Support: sup@sprdb2.com

1. Prerequisite

- DBARSGUI is a Java application.

  The workstation where DBARSGUI is invoked, should have Java Runtime Environment 1.8 or higher installed.

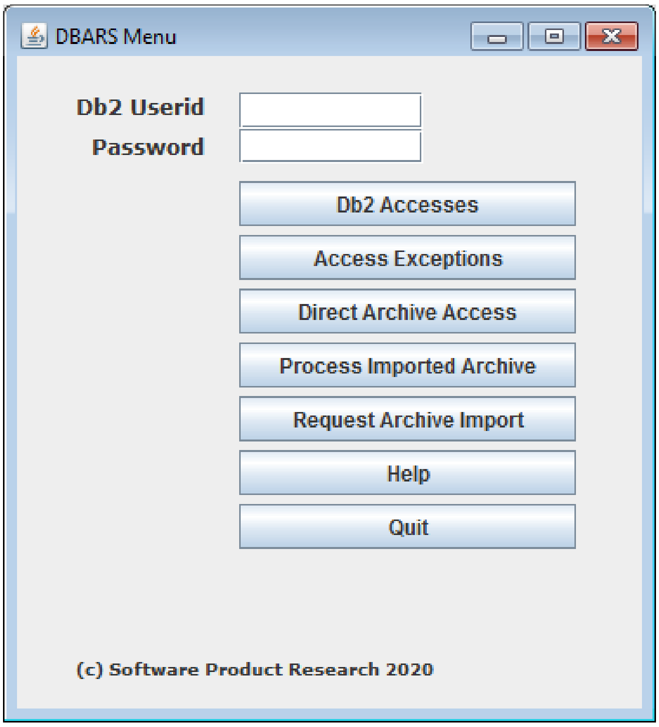
  To verify this, issue the command **java -version** on the Windows command prompt.

  The reply should look like this:

  ```
  java version "1.8.0_251"
  Java(TM) SE Runtime Environment (build 1.8.0_251-b08)
  ```

- On the Mainframe, the DBARSGUI process should have been started as well.

2. Logon



DBARS Menu

Db2 Userid

Password

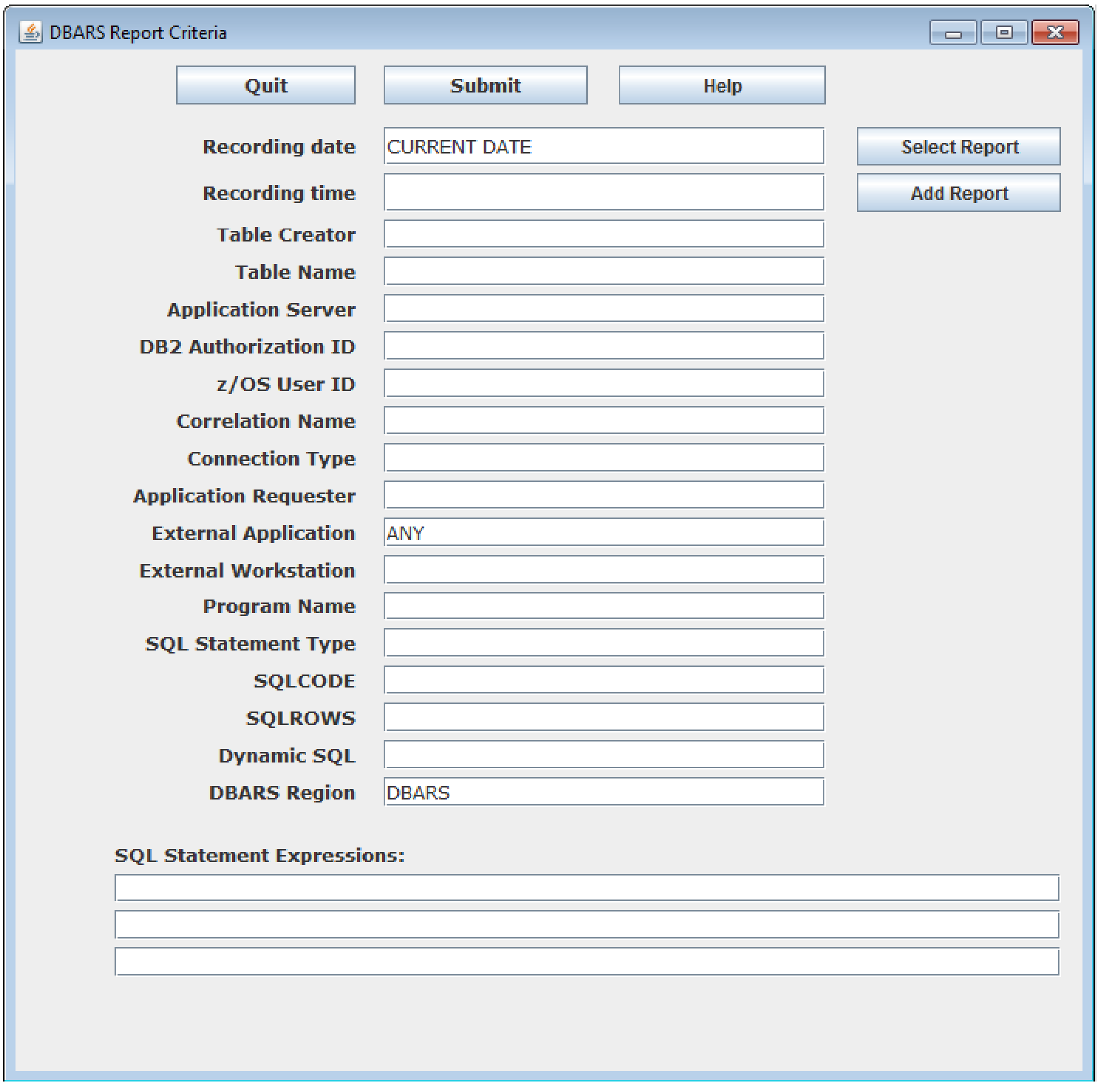
(c) Software Product Research 2020

Your system administrator has provided a DBARSGUI icon on your Windows desktop. Click that icon to start DBARSGUI.

You should now logon to the DBARSGUI server, by entering your Db2 Userid and Password. Then:

- Click the **Db2 Accesses** button to view selected audit events on the online DBARS Recorder.
- Click the **Access Exceptions** button to view audit events that were alerted or blocked by DBARS.
- Click the **Direct Archive Access** button to directly access a DBARS Archive. For more information, refer to “Directly Processing a DBARS Archive”.
- Click the **Request Archive Import** button to request an import of a DBARS Archive. For more information, refer to “Request an import of a DBARS Archive”.
- Click the **Process Archive** button to process a previously imported DBARS Archive. For more information, refer to “Process an imported DBARS Archive.

3. Search Criteria



Recording date	CURRENT DATE
Recording time	
Table Creator	
Table Name	
Application Server	
DB2 Authorization ID	
z/OS User ID	
Correlation Name	
Connection Type	
Application Requester	
External Application	ANY
External Workstation	
Program Name	
SQL Statement Type	
SQLCODE	
SQLROWS	
Dynamic SQL	
DBARS Region	DBARS

SQL Statement Expressions:

If the options **Db2 Accesses**, **Access Exceptions** or **Process Archive** were chosen during logon, the next screen will request you to enter the Recorder Search Criteria.

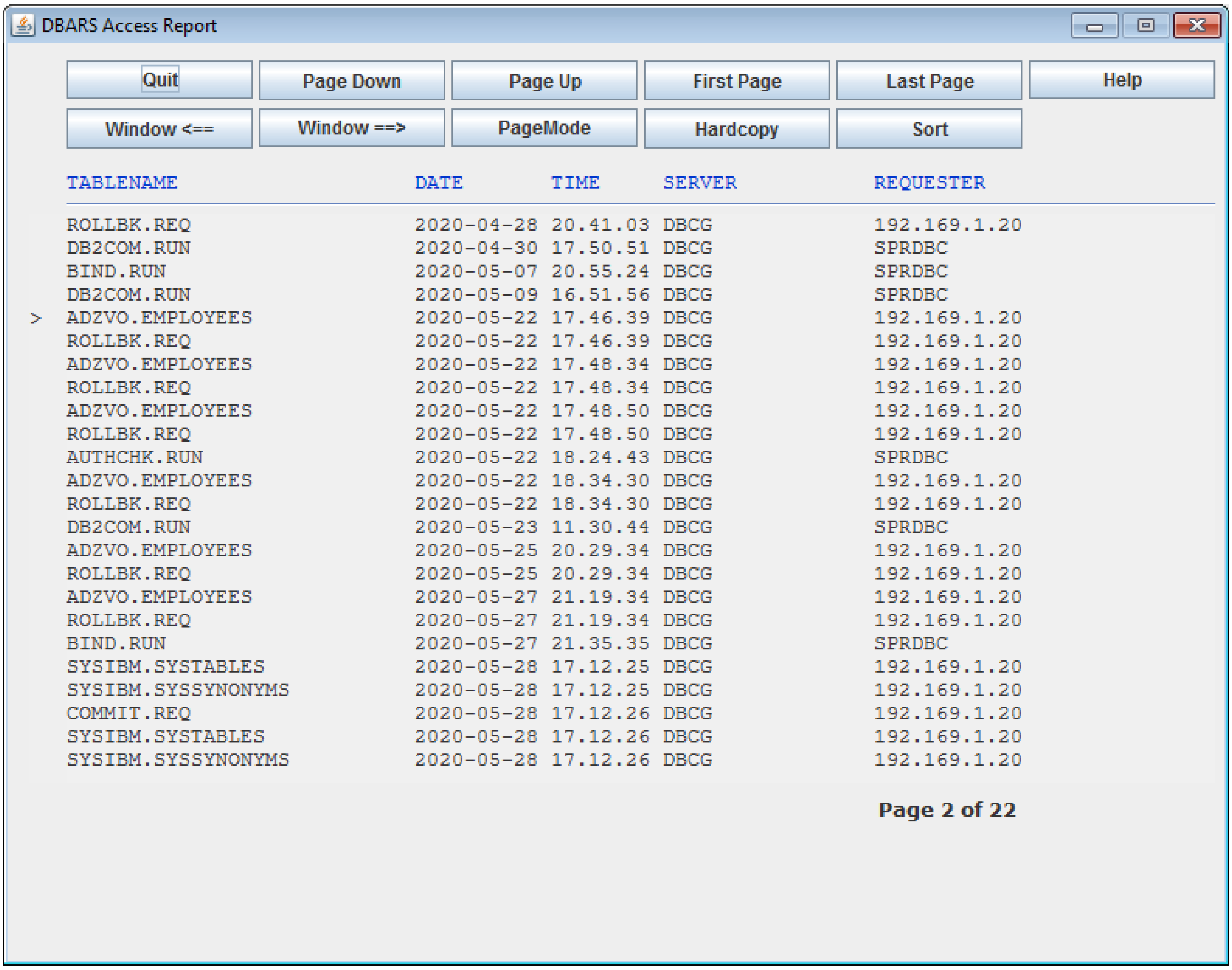
How to enter the criteria is described in section Entering Report Criteria of this manual. Alternatively, you can press the Help button for a description of the columns and buttons to be used. The Help file is an HTML document.

Also, when moving the mouse over a button or a criteria field, a short descriptive text is displayed for the item.

Press the **Submit** button or the ENTER key to continue processing.

The **Select Report** and **Add Report** buttons are explained in the User Reports section.

4. List Mode Report

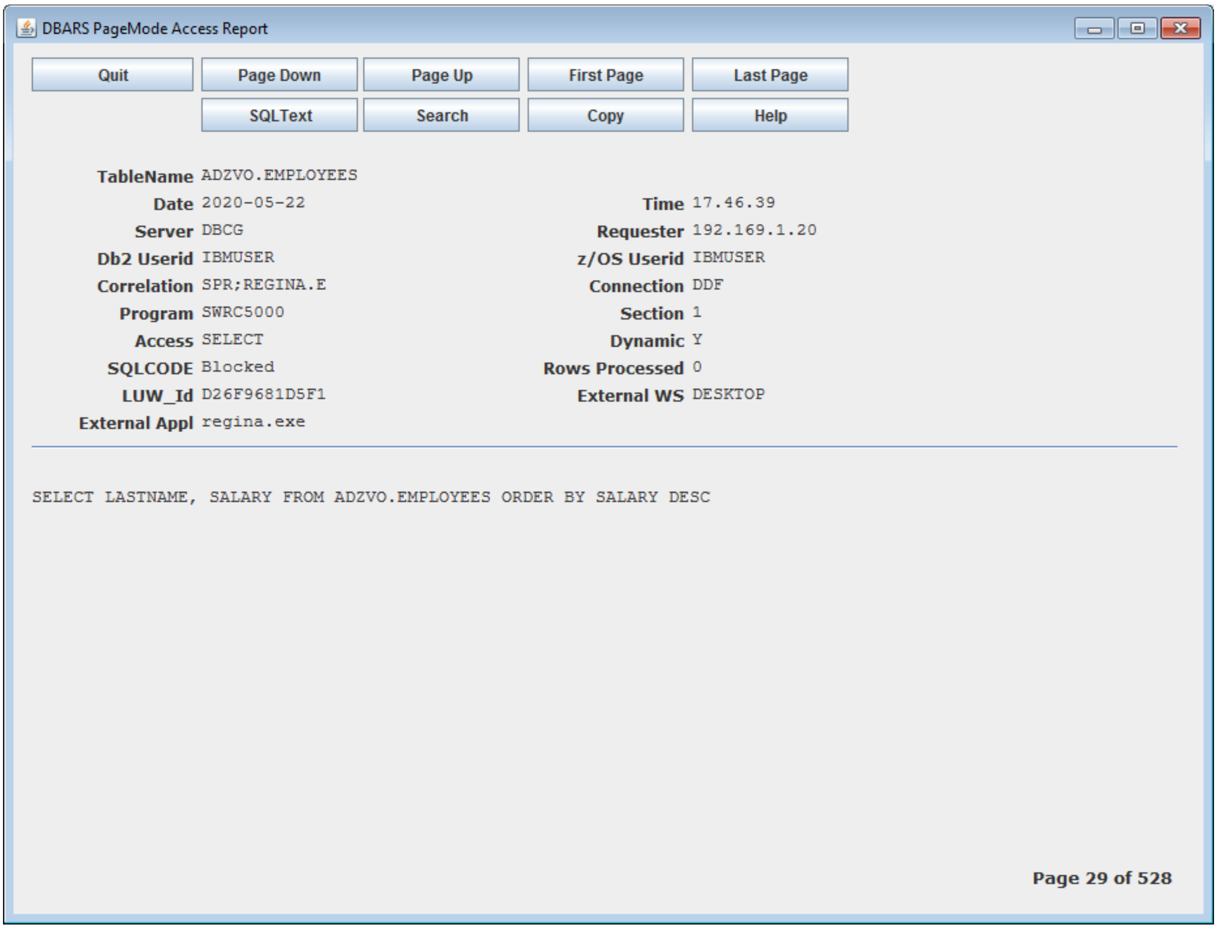


```
   TABLENAME                    DATE       TIME     SERVER           REQUESTER

   ROLLBK.REQ                   2020-04-28 20.41.03 DBCG             192.169.1.20
   DB2COM.RUN                   2020-04-30 17.50.51 DBCG             SPRDBC
   BIND.RUN                     2020-05-07 20.55.24 DBCG             SPRDBC
   DB2COM.RUN                   2020-05-09 16.51.56 DBCG             SPRDBC
>  ADZVO.EMPLOYEES              2020-05-22 17.46.39 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-22 17.46.39 DBCG             192.169.1.20
   ADZVO.EMPLOYEES              2020-05-22 17.48.34 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-22 17.48.34 DBCG             192.169.1.20
   ADZVO.EMPLOYEES              2020-05-22 17.48.50 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-22 17.48.50 DBCG             192.169.1.20
   AUTHCHK.RUN                  2020-05-22 18.24.43 DBCG             SPRDBC
   ADZVO.EMPLOYEES              2020-05-22 18.34.30 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-22 18.34.30 DBCG             192.169.1.20
   DB2COM.RUN                   2020-05-23 11.30.44 DBCG             SPRDBC
   ADZVO.EMPLOYEES              2020-05-25 20.29.34 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-25 20.29.34 DBCG             192.169.1.20
   ADZVO.EMPLOYEES              2020-05-27 21.19.34 DBCG             192.169.1.20
   ROLLBK.REQ                   2020-05-27 21.19.34 DBCG             192.169.1.20
   BIND.RUN                     2020-05-27 21.35.35 DBCG             SPRDBC
   SYSIBM.SYSTABLES             2020-05-28 17.12.25 DBCG             192.169.1.20
   SYSIBM.SYSSYNONYMS           2020-05-28 17.12.25 DBCG             192.169.1.20
   COMMIT.REQ                   2020-05-28 17.12.26 DBCG             192.169.1.20
   SYSIBM.SYSTABLES             2020-05-28 17.12.26 DBCG             192.169.1.20
   SYSIBM.SYSSYNONYMS           2020-05-28 17.12.26 DBCG             192.169.1.20

                                                                  Page 2 of 22
```

The initial result of the Recorder Scan is a ListMode report shown above. The report shows all Recorder rows that meet the supplied Search Criteria.

- The PageUp, PageDown, FirstPage and LastPage buttons browse the Access Report.
- The ListMode screen is too small to display all columns for a given Recorder row. The WindowLeft and WindowRight buttons will slide the screen window to the left or the right.
- The CopyList button writes the current list to the workstation file "My Documents"\DBARS\Hardcopy_<date>.html.
- The Sort button allows to sort the report on date, table name, username, program name or server name.
- The Help button displays the function help file.
- Moving the mouse over a button will show the action initiated by the button. Keyboard keys can also be used as a shortcut for the button. The PageDown and PageUp keyboard keys for instance are equivalent to the PrevPage and NextPage buttons.

5. Page Mode Report



TableName	ADZVO.EMPLOYEES		
Date	2020-05-22	Time	17.46.39
Server	DBCG	Requester	192.169.1.20
Db2 Userid	IBMUSER	z/OS Userid	IBMUSER
Correlation	SPR;REGINA.E	Connection	DDF
Program	SWRC5000	Section	1
Access	SELECT	Dynamic	Y
SQLCODE	Blocked	Rows Processed	0
LUW_Id	D26F9681D5F1	External WS	DESKTOP
External Appl	regina.exe		

```
SELECT LASTNAME, SALARY FROM ADZVO.EMPLOYEES ORDER BY SALARY DESC
```

Page 29 of 528

The PageMode Report shows all columns for a selected Recorder row on one screen. The PageMode report is invoked:

- By left clicking the mouse on a ListMode screenline.
- By selecting a line with the cursor up and down keys and pressing Enter or the PageMode button. (The “current report line” is indicated by a > sign at the begin of the line.)
- Use the NextPage, PrevPage, FirstPage and LastPage buttons to browse the Access Report in page mode.
- The SQLText button provides a formatted display of the current SQL statement.
- The Copy button writes the current screen to the workstation file “My Documents”\DBARS\Hardcopy_<date>.html.
- The Search key allows to search the current report. See section Access Report Search.

6. Access Report Search

Search is performed by supplying:

- the name of a Recorder column as it appears on the PageMode screen in **Search Column**
- the column value in **Search Value**
- The Search Up and Search Down radio buttons provide for forward and backward Report search.

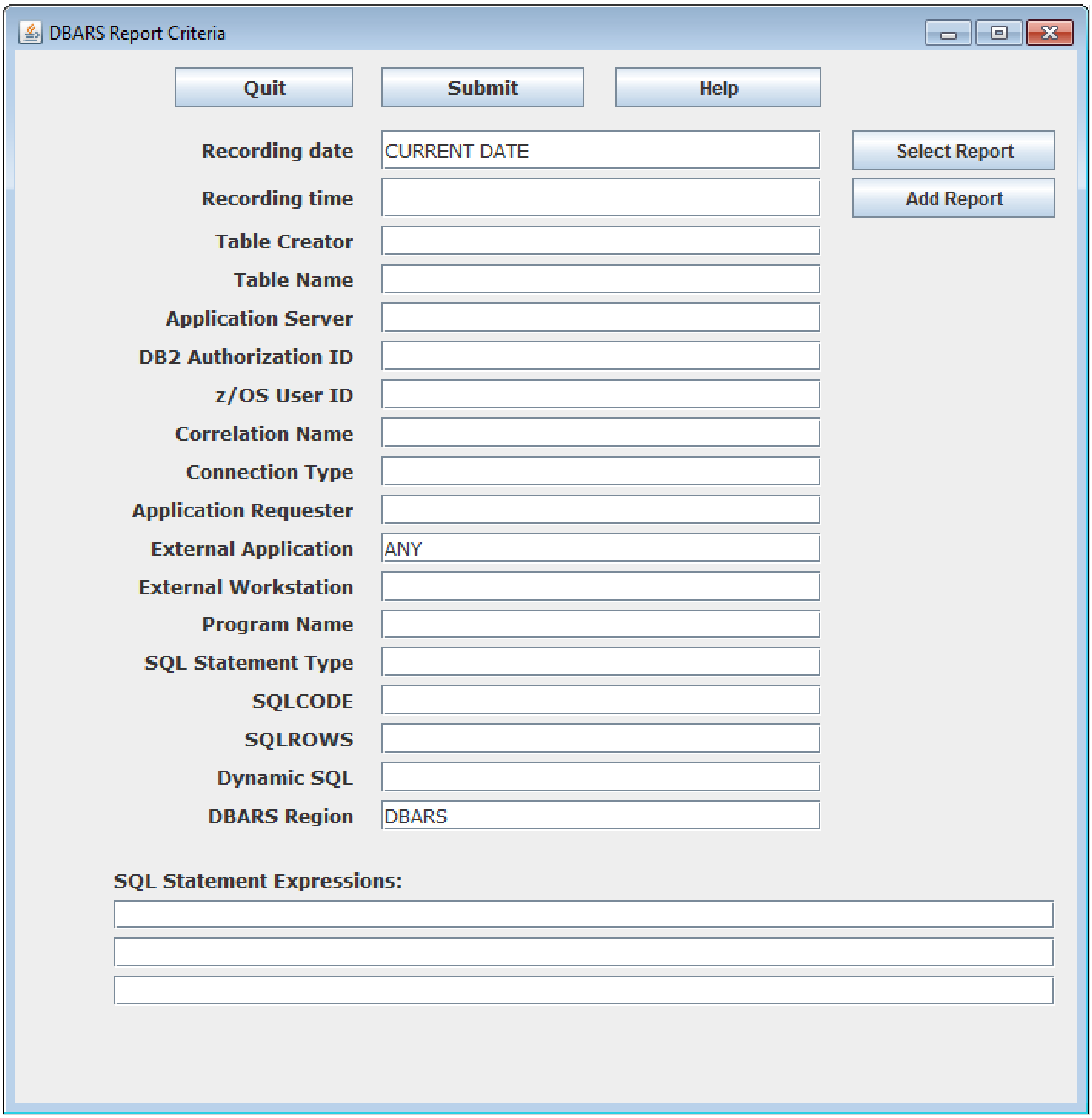
  Example:

Search Colum	PROGRAM
Search Value	USR01

  will show the next Recorder entry for program USR01.

7. User Reports

7.1 Adding a User Report



Recording date: CURRENT DATE

Recording time:

Table Creator:

Table Name:

Application Server:

DB2 Authorization ID:

z/OS User ID:

Correlation Name:

Connection Type:

Application Requester:

External Application: ANY

External Workstation:

Program Name:

SQL Statement Type:

SQLCODE:

SQLROWS:

Dynamic SQL:

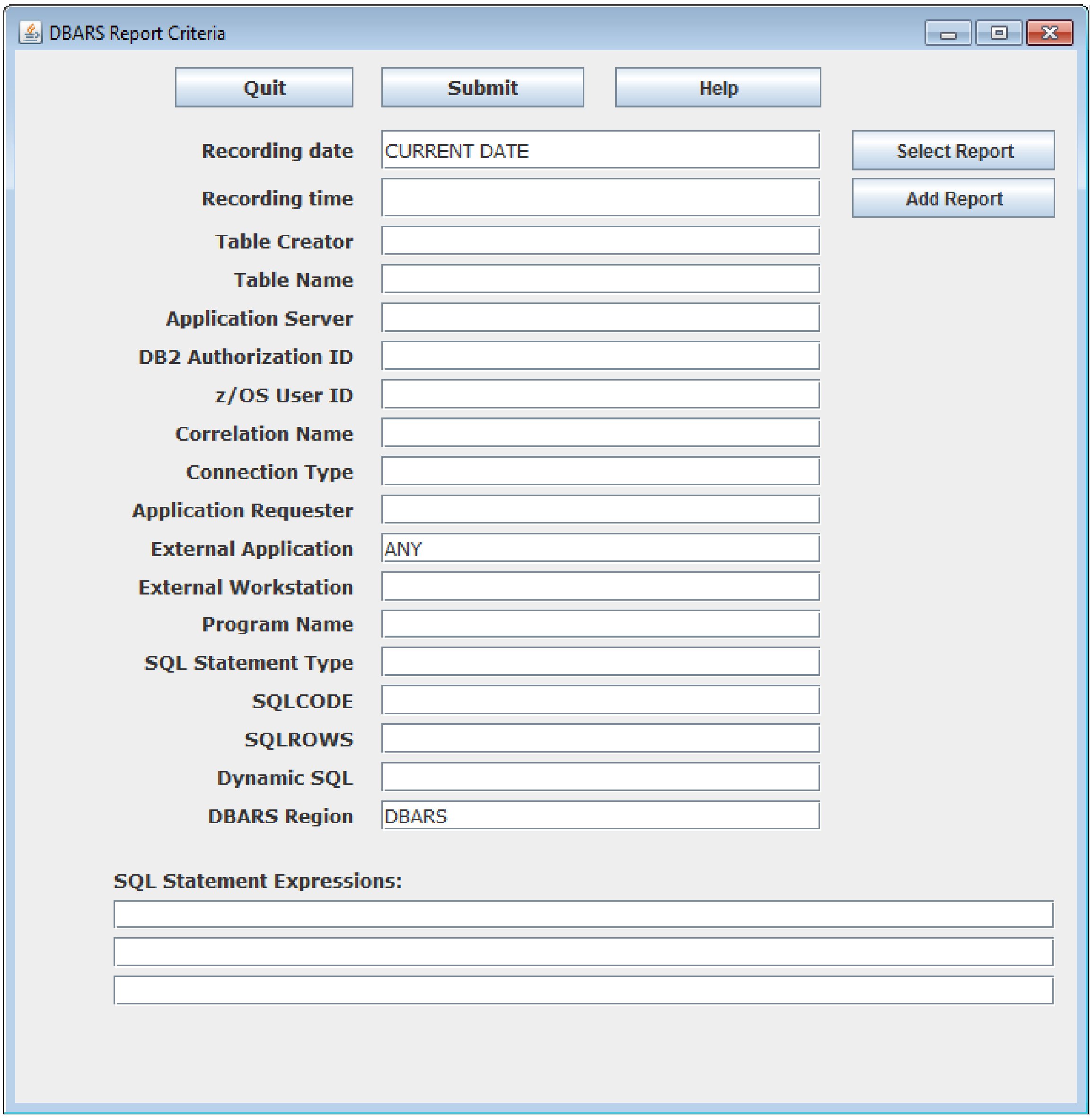
DBARS Region: DBARS

SQL Statement Expressions:

On the initial Report Criteria press the **Add Report** button to save the selection criteria currently on the screen.

The criteria are saved to a set named by you in the "My Documents" folder of your Windows system.

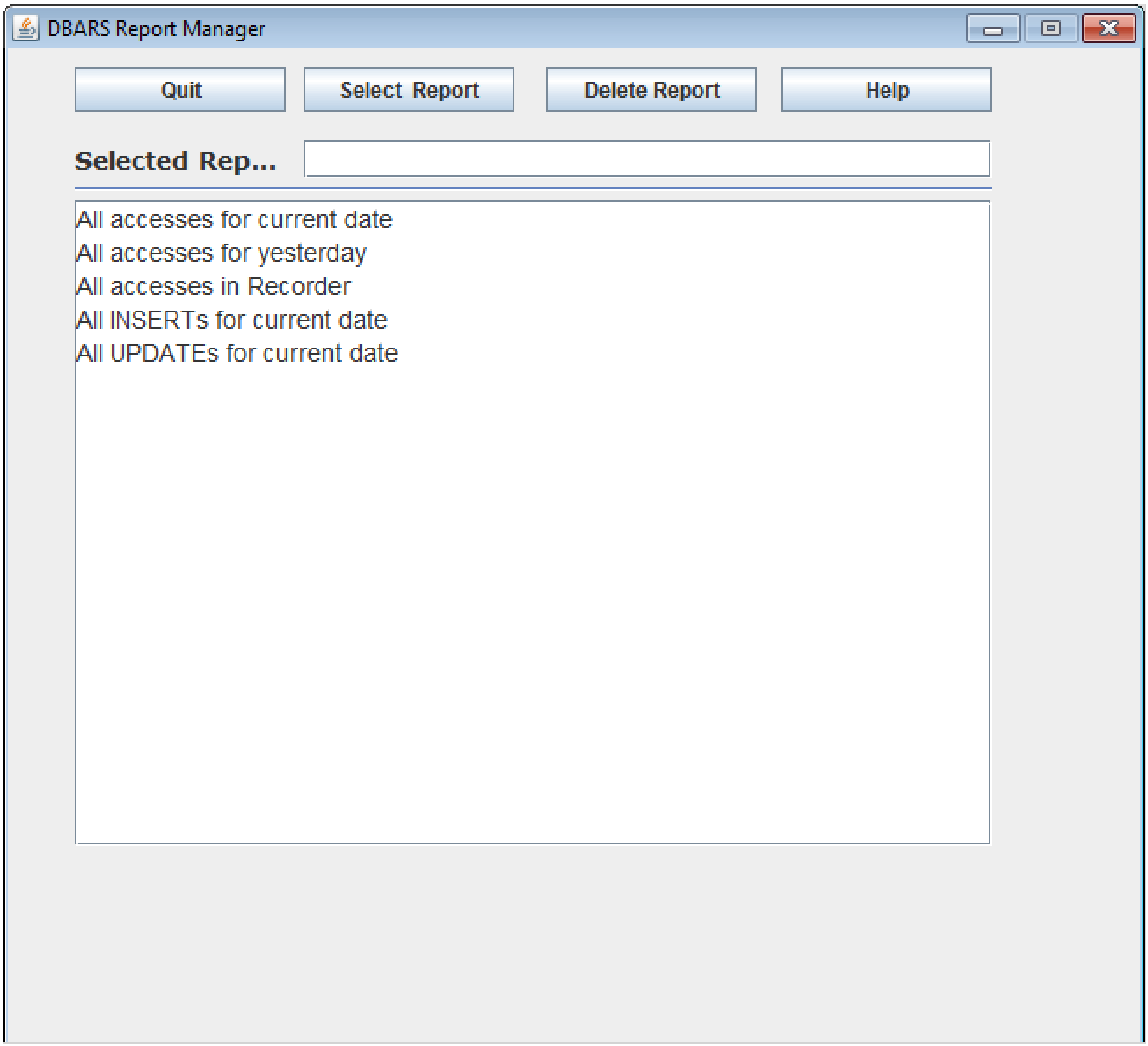
7.2 Selecting a saved User Report



Recording date	CURRENT DATE
Recording time	
Table Creator	
Table Name	
Application Server	
DB2 Authorization ID	
z/OS User ID	
Correlation Name	
Connection Type	
Application Requester	
External Application	ANY
External Workstation	
Program Name	
SQL Statement Type	
SQLCODE	
SQLROWS	
Dynamic SQL	
DBARS Region	DBARS

SQL Statement Expressions:

Pressing **Select Report** on the criteria screen will show the Report Manager panel. It will show the list of report sets, previously saved.



All accesses for current date
All accesses for yesterday
All accesses in Recorder
All INSERTs for current date
All UPDATEs for current date

Select a report set from the list by mouse click.

- Hit the **Delete Report** button to remove the report.
- Use the **Select Report** button to activate the set. The selection criteria previously saved, are returned to the Report Criteria screen. Pressing ENTER then will generate the desired report.

8. Entering Report Criteria

Report criteria can be entered for the columns of the Recorder table and for expressions in the recorded SQL statement text.

8.1. Recorder Table Column Criteria

Enter selection values for one or more of the following Recorder columns:

Recording date Date of the recorded access, as yyyy-mm-dd or as a valid Db2 date expression

Recording time Time of the access, as hh:mm:ss or as a valid Db2 time expression

Table creator Creator of the table accessed

Table name Name of the table accessed

Appl server Name of the Db2 system where the SQL statement was executed

Db2 authid Db2 userid issuing the recorded SQL statement

z/OS userid z/OS userid issuing the recorded SQL statement

Correlation name Name of the process issuing the recorded SQL statement (for example the z/OS job name)

Connection type Type of the users Db2 connection ('BATCH', 'TSO', CICS etc.)

Appl requester Name of the Db2 system sending the SQL statement

Ext_application Name of the external application issuing the SQL statement (distributed data access only)

Ext_workstation Name of the workstation issuing the SQL statement (distributed data access only)

Program name Name of the program containing the recorded SQL statement

Statement type Type of the recorded SQL statement as SELECT, INSERT, DELETE or UPDATE

SQLCODE SQLCODE resulting from statement execution

SQLROWS Number of rows modified by the statement

Location Name of the Db2 subsystem where the recorded statement was executed

Dynamic SQL Y reports SQL statements executed in dynamic mode

N will report SQL statements executed in static mode

blank will report both static and dynamic statements

8.2. Criteria syntax rules

- Criteria can be entered as a simple value, for example:

  TABLE NAME **CUSTOMER**

  A generic value may be supplied using a trailing % sign, for example: PROGRAM NAME **DSQ%**

- Selection criteria may be entered as a Db2 expression, for example:

  STATEMENT TYPE **<> 'SELECT'**

  or

  RECORDING DATE **> CURRENT DATE - 2 MONTHS**

- Db2 expressions on the DBARS Recorder columns are executed using Db2 calls. Therefore, these expressions must obey Db2 syntax rules. All columns of the Recorder, except SQLCODE and SQLROWS, have the CHARACTER format. Search values entered for CHARACTER columns must be enclosed in quotes.

- When multiple selection values are entered, the Recorder rows must satisfy all criteria for being selected.

8.3. ORDER BY column-names or column-numbers

Column-nr	Column-name
1	ACCESS_STAMP
2	DATE(ACCESS_STAMP)
3	TIME(ACCESS_STAMP)
4	LOCATION
5	DB2_ID
6	MVS_ID
7	CORRELATION
10	TCREATOR
11	TNAME
12	PROGRAM
13	STMNTNR
14	SQLCODE
15	SQLROWS
16	OPCODE
17	DYNAMIC
18	CONNECT_ID
19	LUWID
20	EXT_SERVER
21	EXT_APPL
22	EXT_STATION

8.4 SQL text expressions

Recorded accesses may be selected by examining the text of the recorded SQL statement.

An SQL text expression consists of a **column_name** with an optional **column_value**. When a column_value is supplied, it is connected to the column_name by an **operator**.

When a column_name is specified alone, recorded statements will be reported as soon as they contain a reference to the column_name.

When a column_name with an operator and a column_value is specified, recorded statements are reported when they reference the column_name with the specified value.

The supplied expression is checked against:

- the INSERT VALUES clause
- the UPDATE SET clause
- the WHERE clause when present

Expression Syntax Rules

- The column expression has the format:

  column_name operator column_value

- The operator should be entered as:

  = to test equal

  < to test lower than

  > to test higher than

  <= to test lower or equal than

  >= to test higher or equal than

  <> to test not equal

  LIKE to perform a generic test using a trailing % sign

- Column_values may, but need not, be enclosed in quotes.

- Leading zeroes need not be supplied for a column that is logically numerical, even if it has been defined as character to Db2.

- The elements of the expression may, but need not, be separated by one or more blanks.

- Up to 3 column expressions can be specified on the criteria panel.

- When multiple column expressions are specified, a recorded statement will be reported only when it satisfies all the expressions.

Examples

(1) Table-Name EMP_MED_HIST

Statement-Type SELECT

Text-expression-1 EMPNO = 100

Reports all recorded SELECT's on the medical history of employee 100.

(2) Table-Name EMPLOYEE

Statement-Type UPDATE

Text-expression-1 EMPNO = 100

Text-expression-2 SALARY

Reports all recorded UPDATE's on the SALARY of employee number 100.

(3) Table-Name CUSTOMERS

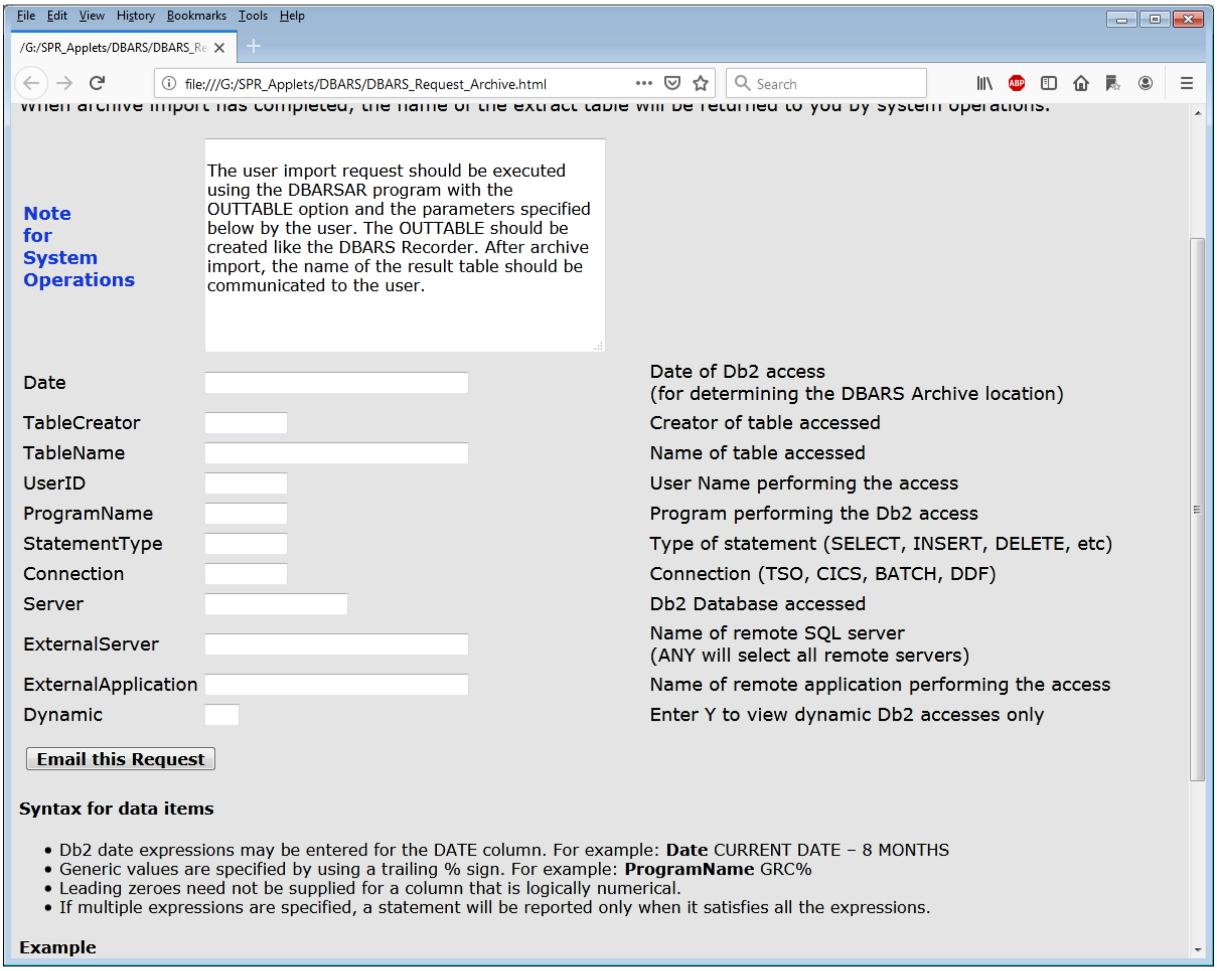
Text expression-1 CUSTNAME LIKE FREI%

Reports all recorded accesses to customer names matching the generic specification.

9. Processing a DBARS Archive

9.1. Request an import of a DBARS Archive

When the Db2 access data required are no longer on the online DBARS Recorder, they should be imported from a DBARS archive into an imported archive. Since the archives reside on offline media, not directly accessible from DBARSGUI, the import operation must be requested from system operations personnel.



File Edit View History Bookmarks Tools Help
/G:/SPR_Applets/DBARS/DBARS_Re
file:///G:/SPR_Applets/DBARS/DBARS_Request_Archive.html
Search

When archive import has completed, the name of the extract table will be returned to you by system operations.

Note for System Operations

The user import request should be executed using the DBARSAR program with the OUTTABLE option and the parameters specified below by the user. The OUTTABLE should be created like the DBARS Recorder. After archive import, the name of the result table should be communicated to the user.

Date		Date of Db2 access (for determining the DBARS Archive location)
TableCreator		Creator of table accessed
TableName		Name of table accessed
UserID		User Name performing the access
ProgramName		Program performing the Db2 access
StatementType		Type of statement (SELECT, INSERT, DELETE, etc)
Connection		Connection (TSO, CICS, BATCH, DDF)
Server		Db2 Database accessed
ExternalServer		Name of remote SQL server (ANY will select all remote servers)
ExternalApplication		Name of remote application performing the access
Dynamic		Enter Y to view dynamic Db2 accesses only

Syntax for data items

- Db2 date expressions may be entered for the DATE column. For example: **Date** CURRENT DATE – 8 MONTHS
- Generic values are specified by using a trailing % sign. For example: **ProgramName** GRC%
- Leading zeroes need not be supplied for a column that is logically numerical.
- If multiple expressions are specified, a statement will be reported only when it satisfies all the expressions.

Example

With the above form you can communicate the data items to be used by System Operations when creating the imported archive. The form also allows to send the request by email, but any other means may be used to transfer the request.

When archive import has completed, the name of the imported archive will be returned to you by system operations.

Example

To retrieve from a DBARS Archive, all UPDATEs on the CUSTOMERS table done from a remote SQL server in January 2018, following selection data should be entered:

Date	2018-01%
TableName	CUSTOMERS
StatementType	UPDATE
ExternalServer	ANY

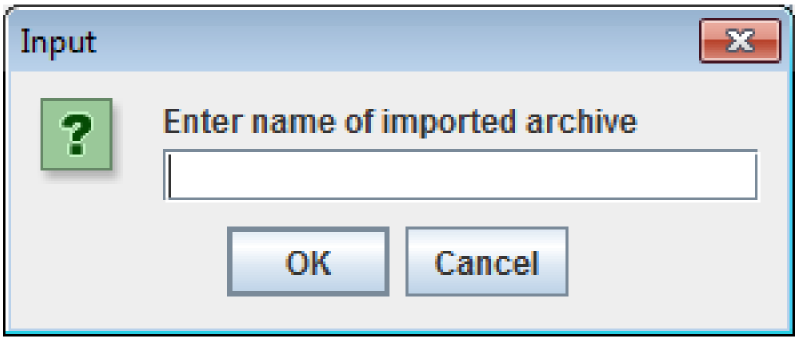
Syntax of the data items

Db2 date expressions may be entered for the DATE column. For example: **Date** CURRENT DATE – 8 MONTHS

Generic values are specified by using a trailing % sign. For example: **ProgramName** GRC%

If multiple expressions are specified, a statement will be reported only when it satisfies all the expressions.

9.2. Process an imported DBARS Archive


Input

Enter name of imported archive

When the “Process Archive” button is clicked, you are requested to enter the name of the imported archive. When Archive import has completed, the name of the imported archive will be communicated by z/OS System Operations.

After entering the name of the imported archive, processing continues as for the online DBARS Recorder. At this point, search criteria for the archive can be entered, as show earlier in section “**Search Criteria**”.

9.3. Directly Processing a DBARS Archive

If mainframe system administration has given you privileges to directly access the DBARS Archive datasets, proceed as follows:

- After clicking the “Direct Archive Access” button, the standard DBARSGUI selection screen is displayed.

- Enter the date range on the DBARS archive that should be inspected.

  For example, when archived audit data are needed for September 2019, type 2019-09-* in the Recording Date field. This date specification will be used to locate the DBARS archive volume containing the required audit data.

- Additional selection criteria (such as a userid) may be entered as filters to obtain the required audit data.

Note

DBARS archives are stored on off-line volumes such as (virtual) tapes. Mounting an off-line volume may require some time.