FUJ00176270

Document Title: Audit Data Extraction Process

Document Type: Process

Release: BI3

Abstract: This document establishes the process undertaken by Pathway CS Security Prosecution Support Section to locate, retrieve, extract, filter and prepare audit data for despatch to authorised requesters.

Document Status: APPROVED

Originator & Dept: Jane Bailey

Contributors: Jan Holmes / Richard Laking / Graham Hooper

Internal Distribution: Jan Holmes, Richard Laking, Graham Hooper

External Distribution: Jamie Henderson (POLIA) and Graham Ward (POL SI)

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Jan Holmes	Audit Manager		
Graham Hooper	CS Security Manager		

FUJ00176270

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	01/01/02	Initial draft based on CSR+ version IA/PRO/003	
0.2	15/04/02	Addition of comments and change to Fujitsu Services	
1.0	29/05/02	Approved	
1.1	17/01/03	Update to BI3 system and contractual changes	
2.0	27/01/03	Approved	

0.2 Review Details

Review Comments by :	
Review Comments to :	

Mandatory Review Authority	Name
Audit Manager	Jan Holmes*
CS Security Manager	Graham Hooper*
IPDU Audit	Richard Laking*
IPDU Audit	Bryan Muir*
Optional Review / Issued for Information	

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	8.0	19/12/02	Fujitsu Services Document Template	PVCS
IA/MAN/005			Horizon System Audit Manual	
IA/REQ/004			Audit Data Retrieval Requirements (CSR+)	
IA/SPE/008			Audit Data Catalogue	

FUJ00176270

IA/SPE/018			Audit Data Catalogue - ADC (Consignia SIS)	
IA/SPE/019			Audit Data Catalogue (Consignia AP Clients)	
IA/SPE/020			Audit Data Catalogue (System Management)	
IA/SPE/021			Audit Data Catalogue (Internal Audit)	
RS/MAN/010			SecureID Normal Token User Guide	
IA/REQ/005			Network Banking Internal Audit Requirements	
NB/PRO/003			Network Banking Management of Prosecution Support.	
NB/MAN/002			PSS Database Manual	
CS/SER/019			Service Description for Security Service Management	

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.4 Abbreviations/Definitions

Abbreviation	Definition
ARQ	Audit Record Query
AS	Audit Server
AW	Audit Workstation
CD-W	Writeable CD
OBCS	Order Book Control System
PIN	Personal Identification Number
PinICL	Problem Management System operated by Fujitsu Services
POLIA	Post Office Ltd, Internal Audit
PSS	Prosecution Support Section
RFI	Request For Information (RFI is synonymous with ARQ.)
TMS	Transaction Management System

FUJ00176270

0.5 Changes in this Version

Version	Changes
1.1	Updates to incorporate the Network Banking performance and update facilities.
2.0	Comments from review

0.6 Changes Expected

Changes
Reviewers comments. The term RFI will be replaced by ARQ in the Audit Extractor Client at Bi3 S30. Screen prints will be altered inline with these changes.

FUJ00176270

0.7 Table of Contents

FUJ00176270

FUJ00176270

1.0 Introduction

The Horizon system generates significant amounts of data that is of interest to Post Office Ltd Internal Audit and other groups. The Horizon System Audit Manual [2], and the supporting Audit Data Catalogues [4-8] provide further information on the structure, form and content of this data, referred to in this document as 'audit data'.

Subject to certain constraints the audit data must be made available to POLIA or other authorised groups within time scales established in the Audit Data Retrieval Requirements (CSR+) [3] and the Network Banking Internal Audit Requirements [10].

This document establishes the process for requesting audit data extractions and subsequent activities undertaken to locate, retrieve, extract & filter and prepare for despatch on behalf of authorised requesters.

2.0 Scope

Should future releases of Horizon bring about changes to the way that data is extracted this process will be updated to reflect those changes.

This process applies to ALL audit data extraction requests in respect of:

1. PSS ARQs
2. Other requests from POLIA
3. Internal Requests

Internal requests for audit data extraction will also be subject to this process. In these cases the use of an Audit Record Query (ARQ) form is optional but a PinICL must be raised to the data extraction stack.

FUJ00176270

3.0 Terminology

Within this process certain terms are used which have specific meaning within the Horizon Audit Solution. They are:

Gatherer : The module responsible for collecting the audit files from the hosts, agents, correspondence servers and interface mechanisms. This module is also responsible for the application of the audit file naming policy.

Sealer : The module responsible for calculating the checksum seal of each audit data file before it is written to audit archive. This value is recalculated after data is extracted by the **Retriever** and compared to the original value when first sealed. Used to ensure data integrity during storage on audit archive.

Hoarder : The module responsible Pre-Bi3 for writing audit data files onto DLT at pre defined intervals. From Bi3 sealer writes audit data to Centera cubes.

Retriever : The module responsible for moving audit data from the buffers where it is placed when retrieved by Legato (Pre Bi3) or Centera (Post Bi3) and making it available to Legato

Extractor : The Client/Server system responsible for retrieving data from Legato and Centera and managing Audit Data Extractions.

Legato: Legato Networker is the storage management application selected by Pathway to store and manage audit data onto DLTs Pre-Bi3. Post-Bi3 the data is migrated to Centera cubes.

Centera : Online mass disk storage unit selected by Pathway to store and manage audit data from Bi3.

A more complete explanation of these modules can be found in the Horizon System Audit Manual [2].

FUJ00176270

4.0 Audit Data Integrity

The integrity of audit data must be guaranteed at all times from its origination, storage and retrieval to subsequent despatch to the requester. Controls have been established to provide assurances to Post Office Internal Audit that this integrity is maintained.

During audit data extractions the following controls apply:

- Extractions can only be made through the Audit Workstations, which exist at Feltham and the 2 Data Centres. These are all subject to rigorous physical security controls appropriate to that location. Specifically, the Feltham AWs – where most extractions will take place – are located in secure rooms subject to proximity pass access within a secured Fujitsu Services site.

- Logical access to the AWs and their functionality is controlled by dedicated Logins, password control and utilises the NT and Pathway security features defined in the overall Horizon security policy.

- All extractions are logged on the Audit System and supported by documented ARQs, authorised by nominated persons within POLIA. This log can be scrutinised on the AWs.

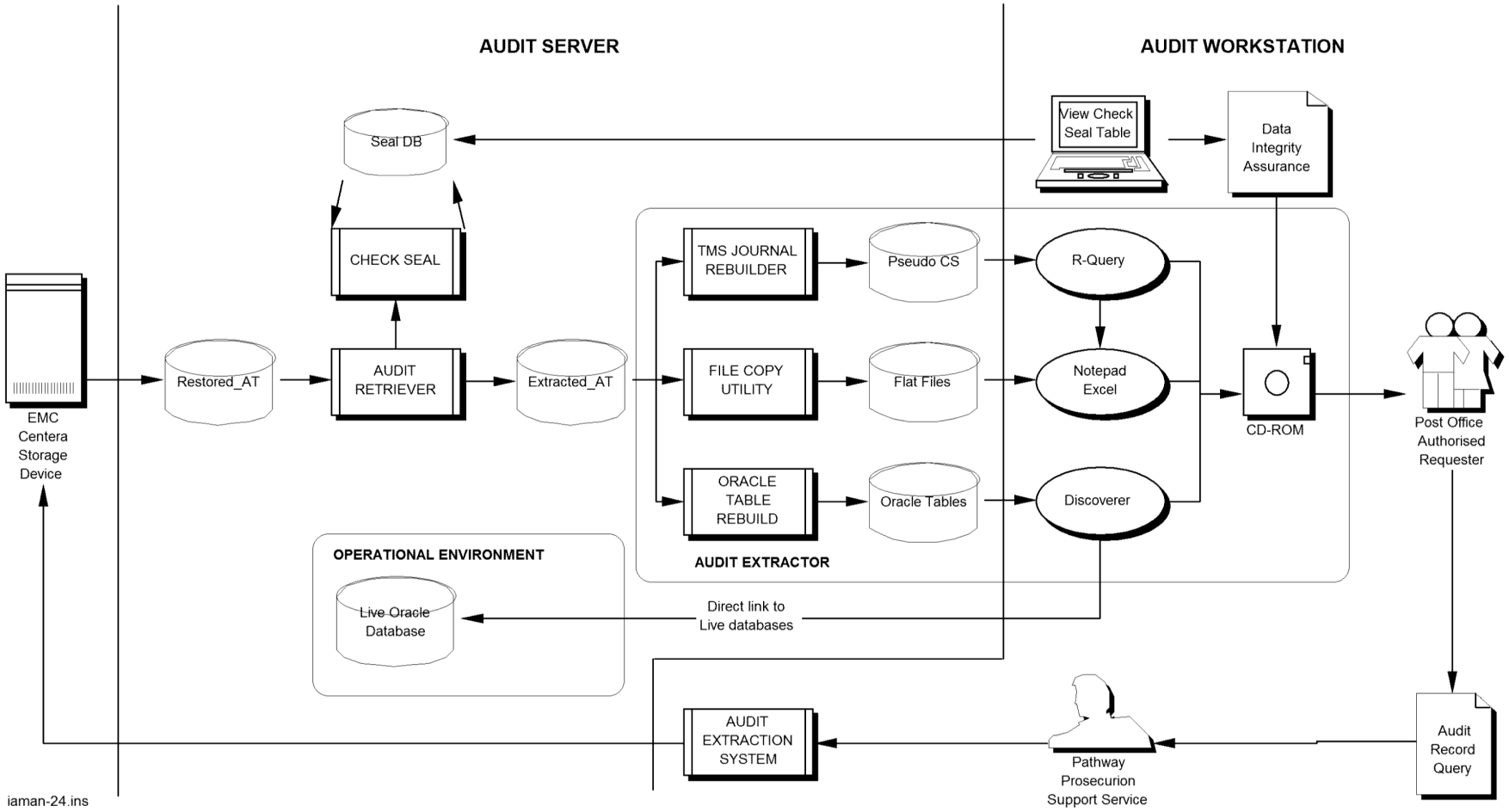
- Extractions will only be undertaken by individuals previously notified to POLIA. Currently this is limited to Pathway Audit and Pathway CS Security Prosecution Support personnel. Any additions will be notified to POLIA.

- Agreement has been reached with POLIA regarding their rights to witness extractions without warning or to request repeat extractions that they can witness.

- Checksum seals are calculated for audit data files when they are written to audit archive and re-calculated when the files are retrieved.

FUJ00176270

5.0 Retrieval Schematic



FUJ00176270

6.0 Overview

The process assumes that audit data has been Gathered, Sealed and written to audit archive. The five main types of files are :

a. TMS Journals from the Correspondence Servers.

b. Flattened Oracle tables output from regular OBCS database purging cycles.

c. Transaction files to and from PO systems

d. AP Client Files

e. Tivoli Event files

All file types are referenced in the audit data catalogues [4-8]

The process is invoked through the receipt of an ARQ into Pathway CS Security PSS. Expressed in business terms, the ARQ must be interpreted into its component Audit Points and Sub-points. This then enables specific files to be identified and retrieved by the Audit Retriever, formatted as appropriate and then further Extracted against the ARQ criteria. Depending on the extraction method the data can be extracted to standard MSExcel 95 before being placed onto CD-W or floppy disc for despatch to the ARQ originator.

The following paragraphs present an overview of each step in the extraction process and are ordered to reflect the actual processing of a Audit Record Query (ARQ) by Pathway CS Security PSS.

6.1 Audit Record Query

All POLIA requests for audit data must be made via the Audit Record Query form. This will contain a description, in business terms, of the times, outlets, events, items activities that the Auditors are interested in. This request has to be interpreted by Pathway CS Security PSS and mapped onto the Audit Points and Files described later in this document.

Internal requests (e.g. from Pathway investigations personnel) will typically be in the form of a PinICL on the 'Dataextraction' stack for CS Security.

6.2 Marking Files and Tapes

Based on the above interpretation of the ARQ, as many files of audit data that are needed to satisfy the request are 'marked' for retrieval.

6.3 Audit Track Retriever

Polls the user area buffers and makes them available to sealer for seal verification

FUJ00176270

6.4 Audit Data Check Seal

To assure the integrity of the audit data while on the audit archive the checksum seal for the file is re-calculated by the Audit Track Sealer and compared to the original value calculated when the file was originally written to the audit archive. The result is maintained in a Check Seal Table.

6.5 Audit Trail Extractor

This is a facility that uses various tools to extract or reform the retrieved audit data in accordance with the ARQ. It also places the information onto a CD-W, or other suitable media, for despatch to the ARQ originator.

FUJ00176270

7.0 Retrieving & Extracting Audit Data

7.1 Receiving the ARQ

a) **POLIA requests** for audit data extractions must come to Pathway CS Security PSS in the form of an Audit Record Query. An example of this form can be found at Annex A. The ARQ may be mailed, faxed or e-mailed to Pathway CS Security PSS.

ARQs will only be accepted from persons fulfilling the following role or their delegate :

POL Internal Audit. Casework Manager: Tel : GRO

Current names of persons fulfilling this role will be confirmed in writing by POLIA Internal Audit and held locally by PSS.

If other parts of the Post Office, or other organisations, require audit data extractions they must be channelled through POLIA to Pathway CS Security PSS.

Contractual limits and turnaround times for the provision of Audit Record Queries are detailed in the document Network Banking Management of Prosecution Support. [11]

b) **Internal requests** will be in the form of a PinICL, allowing the requestor's identity to be verified. Requestors should state what media is acceptable (e.g. CD-W, email of WinZipped file up to 500kB) The despatching of confidential data is bound by Fujitsu Services policy. For TMS files - also referred to as "message store" or "Correspondence Server"- they should also specify the output file format(s): text, MS-Excel or MS-Access. (See Section 8 for more information).

POLIA and Internal requests are recorded on the PSS Database (User Guide for Prosecution Support Database [12])**.** They should be logged to record the following information: Request id (e.g. ARQ no.), the date the request was received, the FAD and date range to search. Turnaround times are covered by contract as specified in the CCD CS/SER/016.

7.2 Interpreting the ARQ

It is necessary to interpret the ARQ by identifying the audit points and sub points that generated the records that are required and, through the Audit Data Catalogues [4-8], the files produced at those audit points and sub points.

FUJ00176270

7.3 Login Audit Workstation

Carry out following procedure to Login and obtain necessary shares

1. Login : *****##
2. Password : *********
3. Domain : PWYDCS

At this point the SecureID Authentication is invoked. See SecurID Normal Token User Guide [9].
Carry out the following procedure to authenticate yourself as an authorised user

1. Enter passcode : <personal 6 digit PIN and 6 digit SecureID token display>

The AW will present a blank desktop with a START icon in the bottom left of the screen. Using pull up <Programs> will reveal the extent of products available for any subsequent extraction work, as shown in Figure 1.

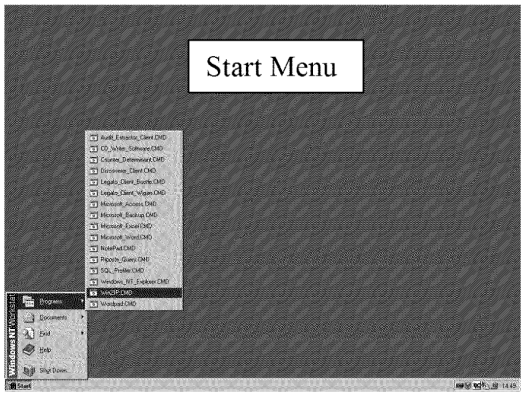


Figure 1

7.4 Preliminary Housekeeping

It is highly likely that an average ARQ will need a significant number of files to satisfy it. To avoid the AW filestore becoming clogged with hundreds of files it is strongly recommended that a working directory is established on the AW to hold all files relevant to a particular ARQ :

1. Select <Windows_NT_Explorer> from the drop down menu.
2. Set up <New Folder> as D:\audit data\ARQ Reference No.

7.5 Targeting the Data Files

At this stage of the retrieval procedure the Audit Extractor Client is used to identify and mark the files required for retrieval.

FUJ00176270

8.0 Using Audit workstations

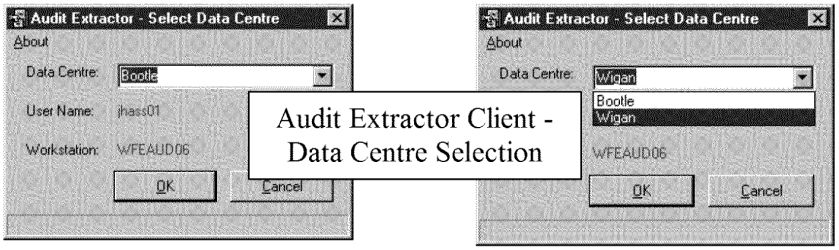
Each Audit Workstation is loaded with the following programs;

1. Audit Extractor Client
2. NT Explorer
3. RQuery
4. Roxio

An explanation of the functionality of each program is detailed in the following sections.

9.0 Extractor Client Functionality

The Audit Extractor Client is invoked from the start menu. The user will select the Data Centre they wish to work with as depicted in Figure 2. The Audit Extractor Client refers to RFI (Request For Information). RFI is synonymous with ARQ.



Audit Extractor Client - Data Centre Selection

Figure 2

The Audit Extractor Client (Figure 3) has three main options;

<New RFI> (Figure 4)

<Open RFI> (Figure 7)

<Close RFI> (Figure 9)

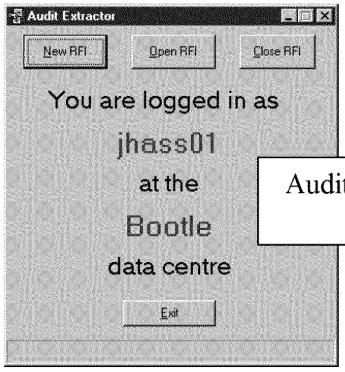


Figure 3

Audit Extractor Client - Main Screen

FUJ00176270

9.1 New RFI

This option is used to setup an audit trail for each request and to specify the search criteria identified from the ARQ form. See Figure 4.

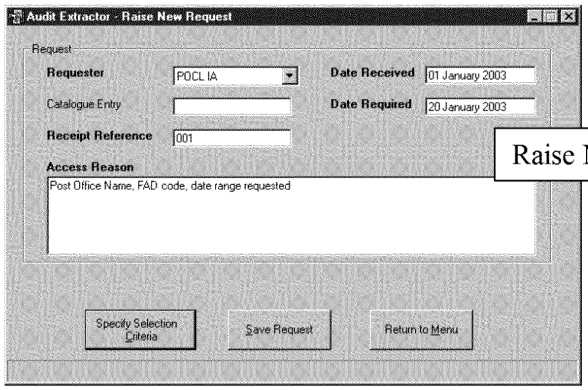


Figure 4

Raise New Request

Requester – Drop down list.

Other *3rd party*

Pathway IA (Post Office Internal Audit, ARQs are always POIA)

Pathway Other

Pathway SSC

POCL IA

POCL Other

POCL Security

Date Received – Date ARQ received, taken from ARQ form

Date Required – Date ARQ must be completed. Use SLA target times to calculate date to be completed by

Catalogue Entry - Blank

Receipt Reference – ARQ Number, taken from ARQ form

Access Reason – Post Office Name, FAD and dates specified on ARQ form

<Specify Selection Criteria> See Figure 5 below.

From Date – The first date requested on the ARQ

To Date – The last date requested on the ARQ + 3 days. This ensures if data hoarded late that all files are identified.

FUJ00176270

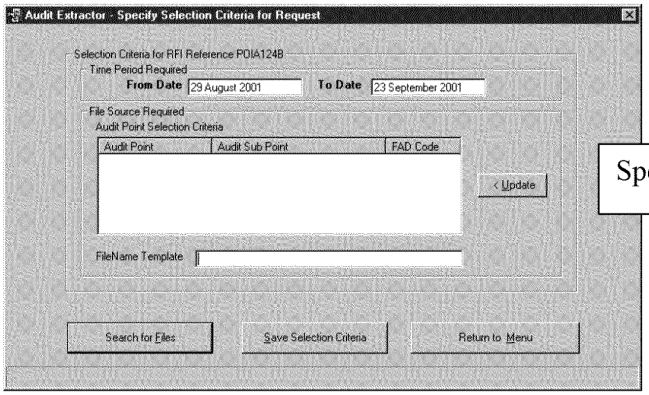


Figure 5

Specify Search Criteria

Search Criteria Audit Points

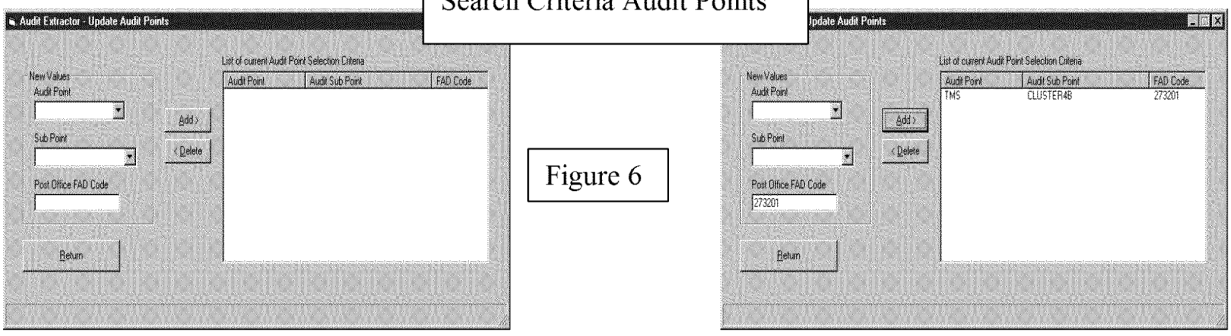


Figure 6

<Update> See Figure 6 above.

Audit points – Used to select AP Client files and Tivoli events, etc

Subpoints – Used to narrow audit point selection

FAD code – FAD code from ARQ

<Add> - input above value and click add to enter the details

<Delete> - Select any values in List of current Audit points and click delete to remove them

<Return> - Click to return to Search Criteria Screen (Figure 5)

<Search files> – when file search completes, the 'Retriever' screen opens, see Figure 10.

<Save selection> - saves the selection criteria

<Return to menu> – returns to main screen (Figure 3)

<Save request> - saves the request

<Return to menu> – returns to main screen (Figure 3)

FUJ00176270

9.2 Open RFI

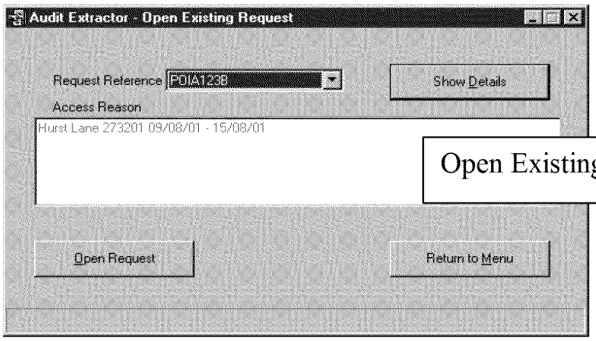


Figure 7

Open Existing Request

Select the 'Request Reference' from the drop down list i.e. POIA001B

<Show Details> - Figure 8 below.

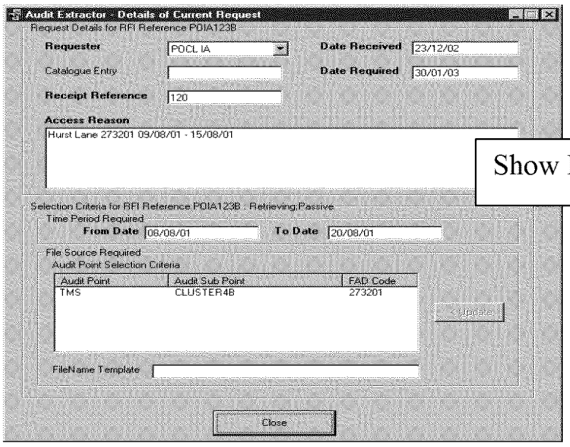


Figure 8

Show Details

This lists the details of the request as inputted in Figure 4, New RFI. The user can not add or update any fields.

Requester Details

- Requester
- Date Received
- Date Required
- Catalogue Entry
- Receipt Reference
- Access Reason

Selection Criteria

- From Date
- To Date

FUJ00176270

File Source Requirement

- Audit Points
- Sub Points
- FAD Code
- File Name Template

<Close> Closes 'Details' screen and returns to 'Open RFI' screen

<Open Request> Displays Figure 10

<Return To Menu> Returns to Figure 4

9.3 Close RFI

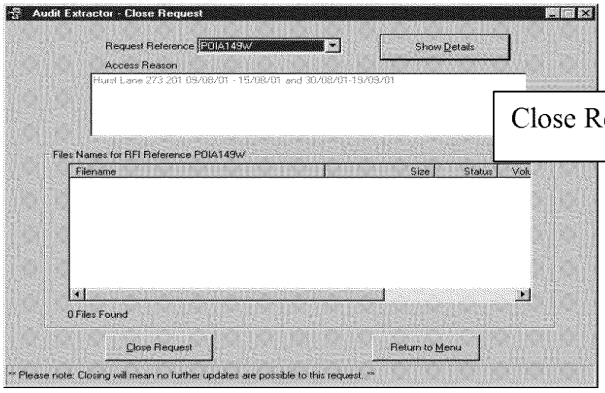


Figure 9

Close Request

When all work has been completed the ARQ must be closed on the Audit Extractor Client.

Request Ref - Select reference from drop down list (ref POIA***)

Access Reason

Filenames for RFI reference POIA**

<Close Request> - once the request is closed the audit log is written to the request directory on the Audit Server, Figure 13. A copy of an example audit log can be viewed in appendix 2.

<Return To menu> - returns to Figure 4

<Show details> – Figure 8 this function displays the ARQ details as in 'Show Details' from 'Open RFI' screen

9.4 Audit Extractor Client – Retriever Screen

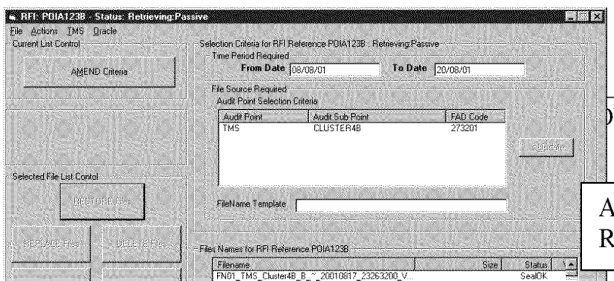


Figure 10

Audit Extractor Client – Retriever Screen

FUJ00176270

Selection Criteria

These fields are as entered on the 'New RFI' screen, Figure 4.

Time Period Required

From Date

To Date

File Source Required

Audit Point Selection Criteria

- Audit Points
- Audit Subpoints
- FAD Code

Filename Template

File Names for RFI Reference POIA***

The Audit Extractor Client retrieves the following information using the search criteria inputted in the 'New RFI' screen, Figure 4

- Filename
- Size
- Status
- Volume
- Barcode
- On-Line

Current List Control

<Amend Criteria> - If the original search criteria is too narrow, select this button to re-input the search criteria and re-search for the required files. This facility is not available once files have started to restore.

FUJ00176270

Selected File List Control

<Restore Files> - Mark the files required by either holding the <CTRL> key and marking the individual files spaced throughout the range listed or select the first file in a group, hold the <SHIFT> key and select the last file to mark a consecutive group of files. Once all the required files are marked click the 'Restore Files' button to restore the files from archive.

<Replace Files> - Mark the required files, select 'Replace Files' and the files not selected will be removed.

<Volume Status> - Again select the files required and click the 'Volume Status' button to initiate a search for TMS Numbers and corresponding barcode reference for any audit tapes required. This only applies to Pre Bi3 files stored in legato, not files held in Centera.

<Delete Files> - Similar to 'Replace Files' except the marked files are removed from the list.

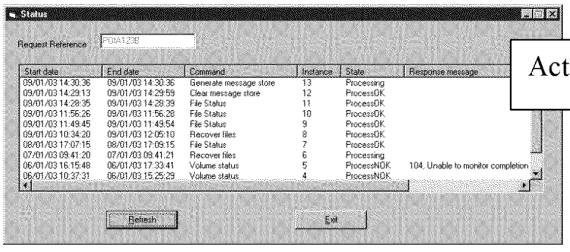
<File Status> - this function updates the status of a set of selected files so that the user can identify progress and seal validity.
<List Update> - this function updates the audit workstation in line with the audit server

<File Sizes> - This button will update file sizes for Legato based files, in the 'Files Names for RFI Reference POIA****' section for the marked files. The user will need to select 'List Update' to view this on the audit workstation. Centera file sizes are shown in the original selection list.

Main Menu

File / Close – This exits the 'Retriever' screen

Actions / Check Actions – Actions allow the user to view the status of each function/facility as detailed throughout section 9.0 of this document, thus allowing the user to identify when each process completes and if it completes successfully.



Actions Screen

Figure 11

TMS

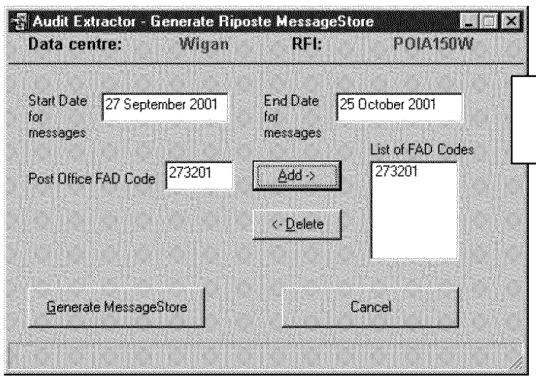
Once the TMS Archive files have been deposited in EXTRACTED_AT they must be 'built' into a pseudo Correspondence Server for R-Query to access. Further filtering is

FUJ00176270

available to restrict the number of Outlet records that are included in the re-build activity based on the original ARQ.

Clear MessageStore – This clears the current messagestore on the audit workstation

Generate MessageStore – enter the date parameters and FAD code, as depicted below in Figure 12 and then 'Generate MessageStore' to generate the message store on the audit workstation.



Generate Message Store Screen

Figure 12

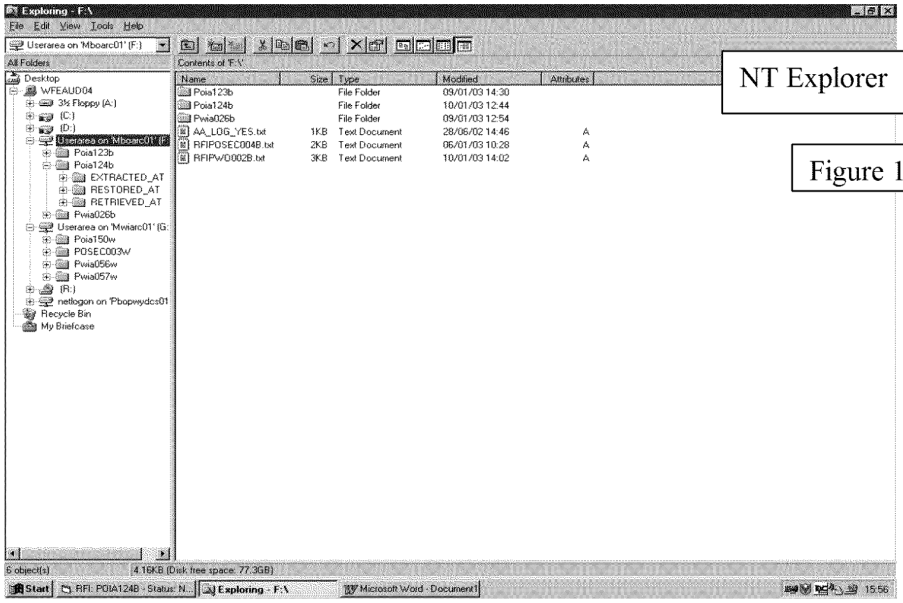
Server MS Build – Used to generate a messagestore on the audit server. Only one workstation at a time can generate a messagestore on the audit server. This shall only be used as a last resort.

Oracle / Build Table – Allows the user to rebuild Oracle back up files in the Oracle format.

Unzipping Zipped Flat Files - It is strongly recommended that files to be unzipped are transferred from the AS to the AW in their zipped state and unzipped on the AW. This can produce space savings of the order of 90%.

FUJ00176270

10.0 NT Explorer



NT Explorer

Figure 13

NT Explorer is used as a tool for viewing files associated with an ARQ. As each new request is logged on the Audit Extractor Client using 'New RFI' a directory will be created on the audit server for which the request was initiated from. Each directory takes the Audit Extractor Client RFI Reference i.e. POIA****. This main directory holds the sub directories; Extracted_at, Restore_at and Retrieved_at. The main directory includes a txt file named using the Audit Extractor Client RFI reference. This files contains details of each process initiated through the Audit Extractor Client. NT Explorer allows a window to view these files and directories.

FUJ00176270

11.0 Introduction to R-Query

R-Query is an interrogation tool used to extract data from a Correspondence Server. It has powerful SQL type features, which are used to define the extraction scenarios and the ability to output the results to standard MS-Office utilities.

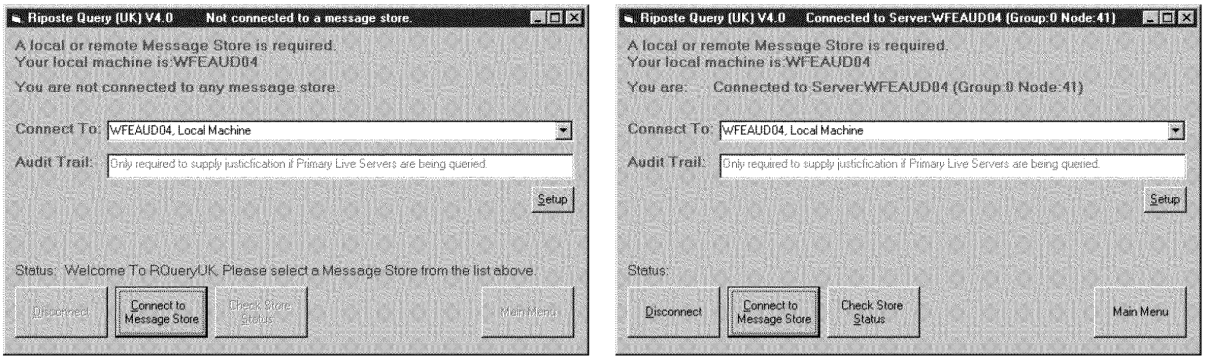
It is a vital element in the Audit Workstation tool set and requires that a Correspondence Server exists on one of the Audit Workstations or Servers. Details on how to achieve this pre-requisite can be found earlier in this procedure.

11.1 Invoking R-Query and Connecting to a Correspondence Server.

The Riposte Query initial screen is invoked from the start menu.

Figure 14

Riposte Query Initial Screen



Connect to – The user selects the workstation/server for which the message store exists

Audit Trail – User is only required to justify use of servers

<Set up> - Development only

<Disconnect> - disconnects any connection from current workstation to messagestore

<Connect to MessageStore> - 'connect to' and 'audit Trail' are to be specified before connecting

<Check Store Status> - details of message ranges in the rebuilt message store.

<Main Menu> - Connects to the main RQuery Screens as detailed in the following sections.

FUJ00176270

11.2 RQuery Main Screen.

This consists of 7 tabs.

Select Cols – Used to select attributes required for output to excel etc.

Where – Used to enter search criteria i.e. date range and FAD code

Order By – Used to specify sort criteria when output to excel

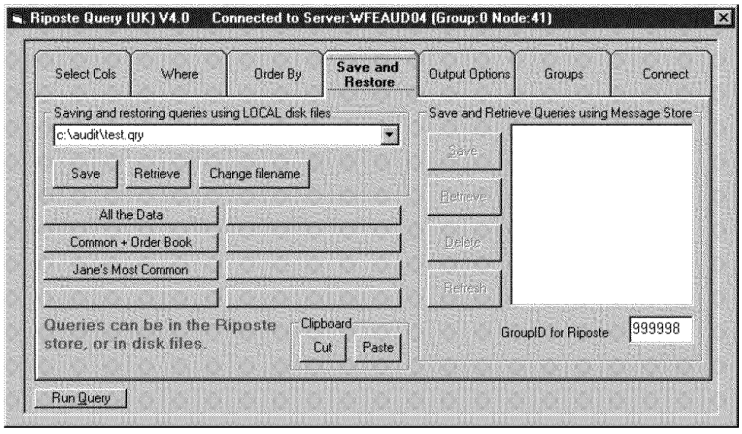
Save and Restore – Used to load and save Query

Output Options – Used to specify file and MS product to export data to.

Groups - Used to specify PAN or STAN identifier

Connect – Used to connect to Messagestore.

11.2.1 Save and Restore - Restoring Retrieval Scenarios



Save and Restore

Figure 15

The <Save and Restore> dialogue provides the opportunity to restore scenarios that have already been scripted for further use.

SCENARIOS FOR RE-USE EXIST AT TWO LEVELS:

Those that are associated with the current Correspondence Server.

Those that have been saved to an external file or Catalogue.

Scenarios associated with the Correspondence Server exist only while that particular CS exists. If the user believe that an extraction scenario is likely to be re-usable it's as well to remember that unless the scenario is saved to an external file it will not be available if a new CS is built for another retrieval exercise.

Use these steps to re-use scenarios associated with current Correspondence Server.

Go to 'Save and Retrieve Queries using Message Store' window.

Select <Refresh> to list all scenarios associated with the current Correspondence Server.

Highlight the required scenario and select <Retrieve>.

FUJ00176270

OR

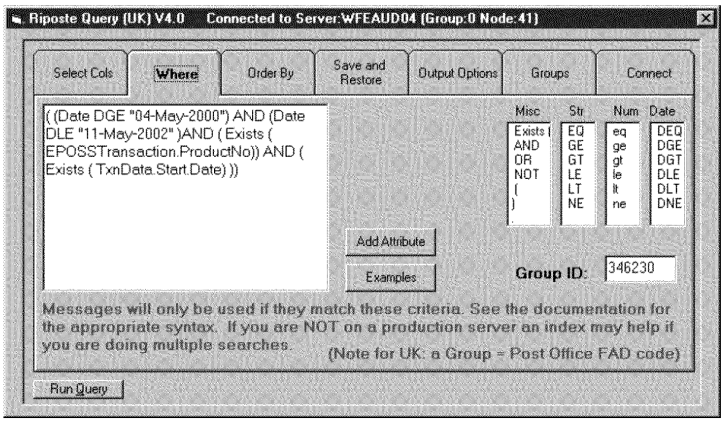
Use this step if retrieving scenarios from the Catalogue.

Locate stored scenario from the Catalogue via <Change filename> button to browse as required.

At this stage the user will have retrieved the scenario complete with the parameter setting used on the last retrieval activity. If the user want to change any of the parameters they will need to go to the <Where> tab.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown.

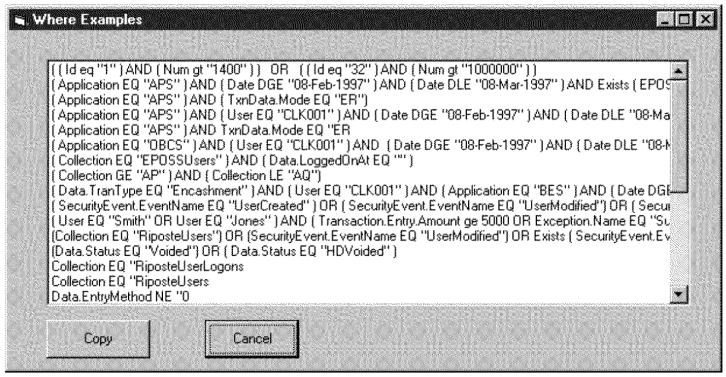
11.2.2 Where - Changing Retrieval Parameters



Where Screen

Figure 16

Note that the current version provides significant amounts of assistance with regard to the structure of the query statement. An 'Examples' button (see Figure 17) allows search parameters to be retrieved and tailored (e.g.):



Where Example Screen

Figure 17

(Date DGE "29-May-2000") AND (Date DLE "01-Jun-2000")

for all dates between 29 May-1 June 2000.

Date DEQ "31-May-2000"

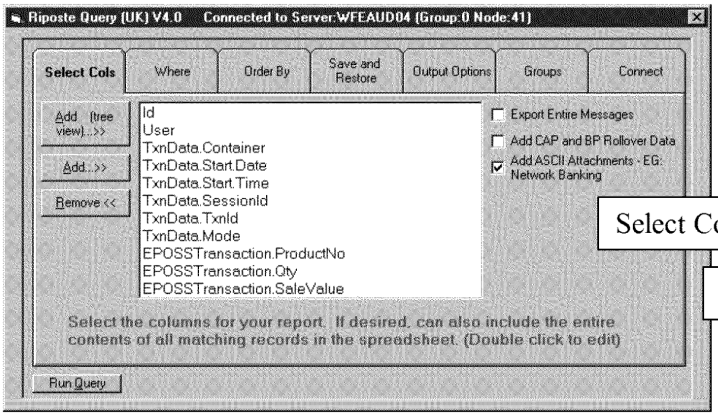
FUJ00176270

for this day only.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown. If the user want to change the TMS fields that will be visible following the retrieval they will need to go to the <Select Cols> Tab.

Note: Riposte Query can only work with one FAD code (GroupID) at a time. It will need to be run separately for each Post Office, remembering that by default it may delete the previous output file

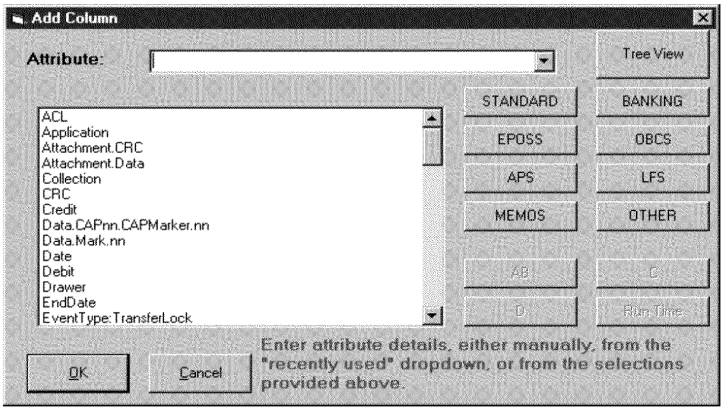
11.2.3 Select Cols - Selecting TMS Fields for Display



Select Cols Screen

Figure 18

Note that the current version provides lists of available fields per Horizon application which can be selected by highlighting and pressing <Add> or <Add (tree view)>. See Figure 19 below. Alternatively to reduce the numbers of fields displayed highlight the field in the window and press <Remove>.



Add Columns

Figure 19

If the user want to retrieve the entire message for a given selection parameters <Remove> all entries in the window and put an 'x' in the <Export Entire Messages> field.

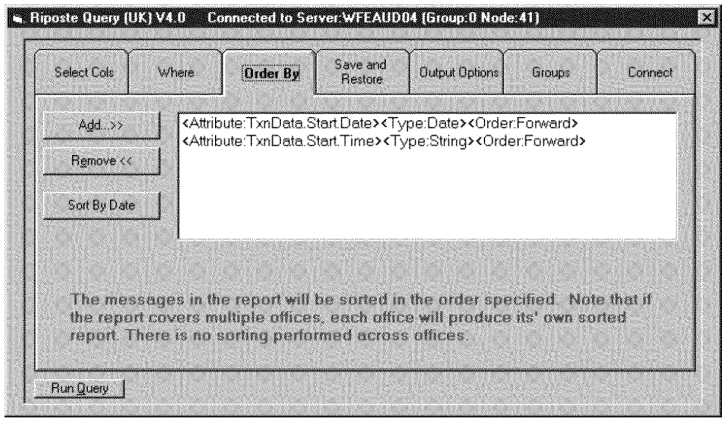
Optionally a field "Add CAP and BP rollover data" or "Add ASCII Attachments – EG; Network Banking" can also be checked.

FUJ00176270

The user may now want to choose how the results of the retrieval will be presented. To do this go to the <Output Options> Tab.

Note: For TMS extractions, "Export Entire Messages" will normally be checked; the field "GroupID" is typically the only one selected via the "Add" button, ensuring that all rows are linked to a FAD code in the output file.

11.2.4 Order By Tab

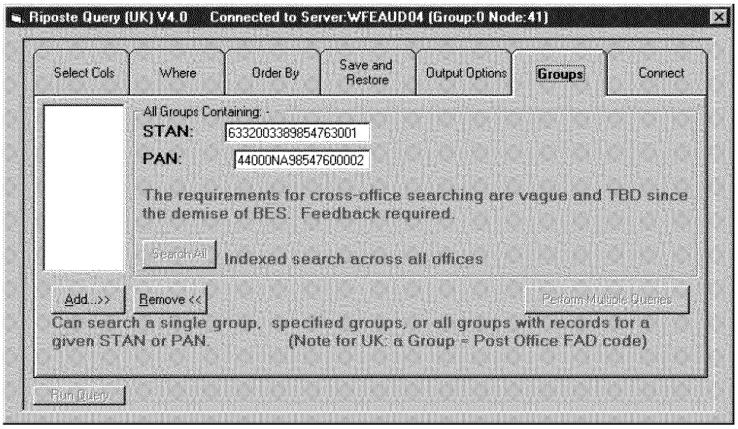


Order By

Figure 20

Selecting the parameter "Sort By Date" is recommended to ensure ascending time sequence (where appropriate).

11.2.5 Groups Tab



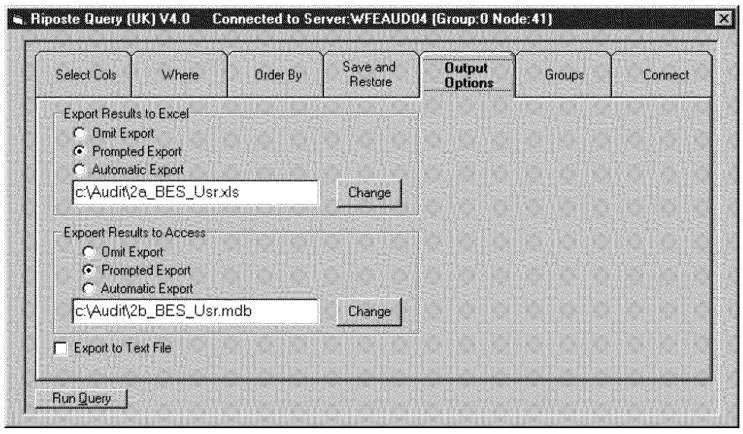
Groups

Figure 21

The Groups tab on the R-Query tool is used to specify PAN search criteria.

FUJ00176270

11.2.6 Output Options



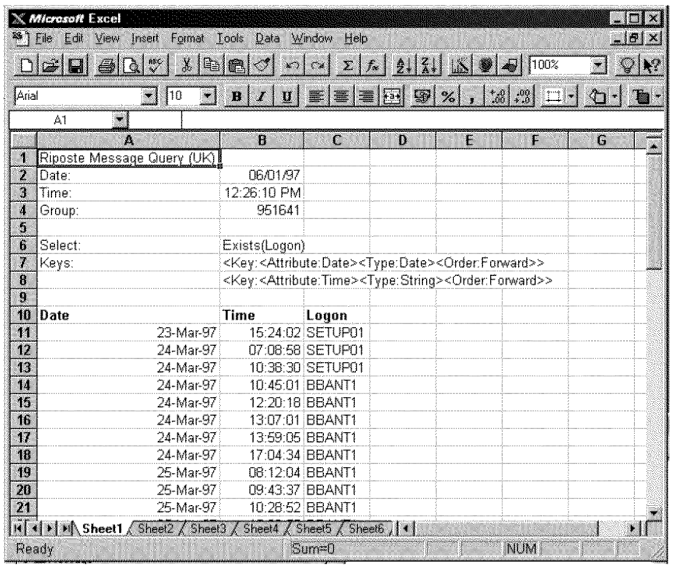
Output Options

Figure 22

By default an Excel spreadsheet is created (default name when selected: C:\Audit\2a_BES_Usr.xls). In the current version there is also an option to export to an MS-Access database (default name when selected: C:\Audit\2b_BES_Usr.mdb) and a text output file.

If the user want to export the retrieved message to either an Excel spreadsheet or an Access database then enter 'x' in the "Export Results to Excel/Access, Prompt Export" field.

Using the template.qry file found in d:\audit data gives the report format as shown below



Excel Output

Figure 23

Details of the query statement used will appear on the spreadsheet and this provides the evidence to POLIA of the search criteria used, in other words, how their ARQ has been interpreted.

FUJ00176270

11.3 Running the Query

Normally the user would not actually execute the retrieval scenario until such time as they had built the query statement (the Where tab), selected the fields (Select Cols) and chosen the output medium (Output Options). However, at any time in this sequence they can run the query statement by selecting <Run Query> using the button on the "Save and Restore" tab.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown.

Once this has been done an intermediate screen will be displayed, allowing the file format to be confirmed – select the <Excel> or <Access> buttons or the "text" icon, as appropriate to commence loading the package and complete the data transfer. This will also allow the data format to be checked on-screen.

Note: In the case of very large Correspondence Server files spanning a number of days, an error may be generated on trying to save an Excel file. This will be because the maximum number of rows (records) has been exceeded. Should this occur, the range of dates should be covered, say one or two days at a time, and a number of output files generated.

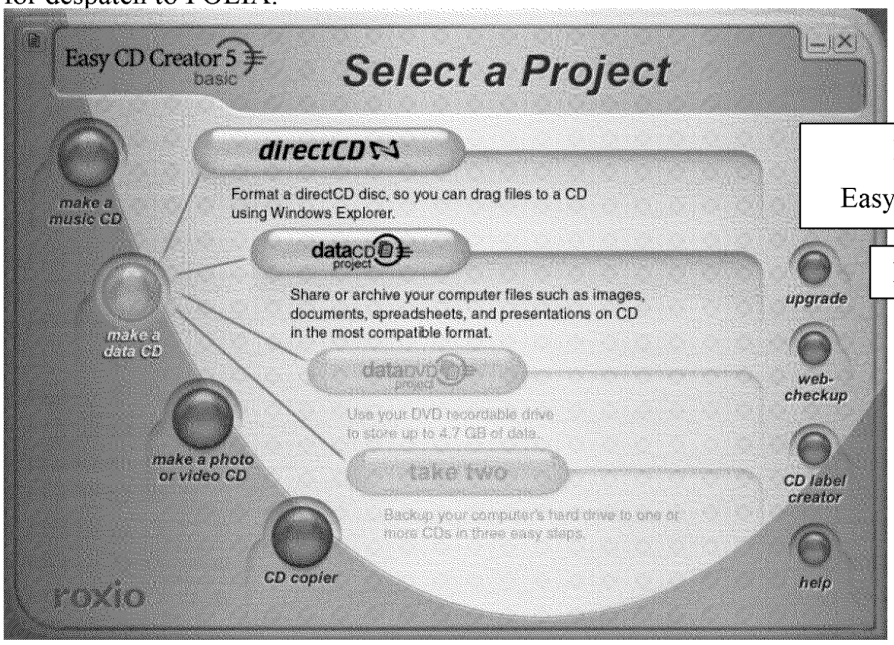
In rare cases it will theoretically be possible to produce a text output file that is too big to be read by Wordpad. Should this occur, a possible response is to produce output files for a smaller range of dates, or to initially create data as an Excel working file which can be 'Save As' "Text, OS/2 or MS-DOS".

It is good practice to check that all output files can be opened before they are copied to floppy disk or CD-W for onward transmission.

FUJ00176270

12.0 Creating CDs

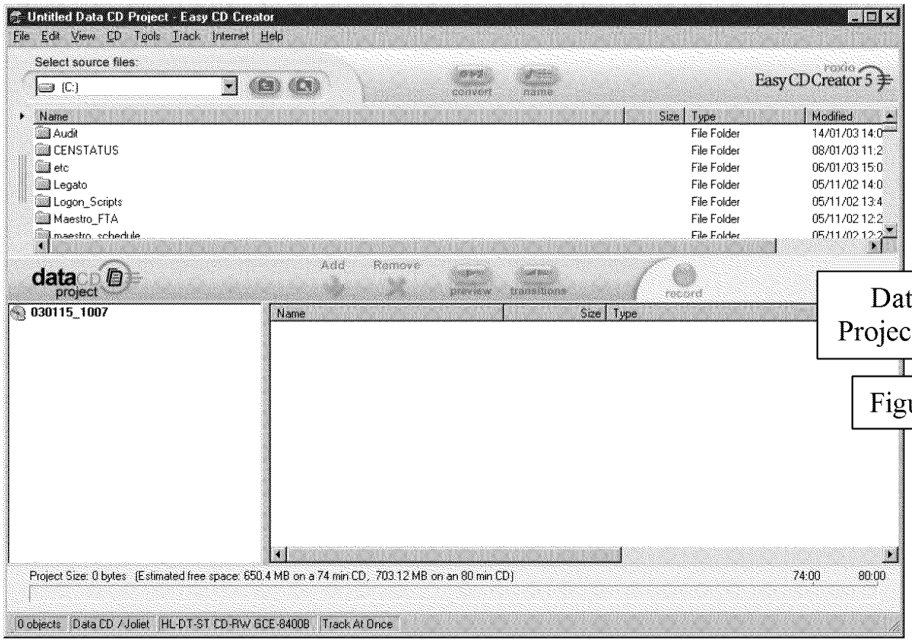
Roxio Easy CD Creater is used to copy the ARQ requested information on to CD-R, for despatch to POLIA.



Roxio – Easy CD Creator

Figure 24

To launch CD Creator inserts a new CD-R in to the CD writer. This will launch the main screen (Figure 24) The user selects "Make a Data CD", then "Data CD Project" this initiates the Data CD – Easy CD Creator Screen Figure 25.



Data CD Project Screen

Figure 25

FUJ00176270

From here the user selects the source file from the drop down box. The source file should be held on the D:\ under Auditdata\ARQ***. The files will appear in the top window, the user will then drag and drop the required files to the lower window. All CD's will be recorded as 'Closed' to prevent any further data being added to the CD.

13.0 Despatch of Audit Data

The audit data is despatched to POLIA contact using Royal Mail Special Delivery. This ensures that a receipt is provided to Pathway confirming delivery.

The Prosecution Support Database must be updated to record the date that the extraction activity was started, completed and posted.

FUJ00176270

14.0 Appendix

Appendix 1 ARQ Form

Appendix 2 Example audit log

FUJ00176270

Appendix 1

AUDIT RECORD QUERY

Originator:	Post Office Ltd Casework Manager The 4th Floor, Impact House, Edridge Road, Croydon CR9 1PJ	**Date:**	dd/mm/ccyy
Telephone:	GRO		

Witness Statement (delete as applicable)	YES/NO	**REF NO.**	ARQ ####/00

Information Requested			
Date range:		**Post Office**	Name and FAD
GENERAL DESCRIPTION / FORMAT REQUIREMENTS:			
Specific Details:	(PAN or equivalent identifier)		
Signed		**Date**	**dd/mm/ccyy**

FUJ00176270

Appendix 2

Log for closed RFI: POIA149W

==========

RFI created by: jhass01

RFI Closed: 09/01/03 15:01:44

Actions:

Instance: 5

CommandUsed: Get cluster ID

ErrorCode: -12

Error message: Failed to open the CLUSTER ID file.

StateID: ProcessNOK

Started At: 06/01/03 16:07:54

Ended At: 06/01/03 16:08:41

Generated by: rlaki01

Instance: 4

CommandUsed: Get cluster ID

ErrorCode: -12

Error message: Failed to open the CLUSTER ID file.

StateID: ProcessNOK

Started At: 06/01/03 10:27:07

Ended At: 06/01/03 10:27:23

Generated by: jhass01

Instance: 2

CommandUsed: Get cluster ID

ErrorCode: -12

Error message: Failed to open the CLUSTER ID file.

StateID: ProcessNOK

Started At: 06/01/03 09:55:49

FUJ00176270

Ended At: 06/01/03 09:56:04
Generated by: jhass01

Instance: 1
CommandUsed: Get cluster ID
ErrorCode: -12
Error message: Failed to open the CLUSTER ID file.
StateID: ProcessNOK
Started At: 06/01/03 09:49:37
Ended At: 06/01/03 09:50:23
Generated by: jhass01

Instance: 0
CommandUsed: Create directory structure
ErrorCode: 0
Error message: No error message held.
StateID: ProcessOK
Started At: 06/01/03 09:48:48
Ended At: 06/01/03 09:48:59
Generated by: jhass01

Files and status of files used by: POIA149W
==========
This RFI did not utilise any files.
Total number of files utilised: 0
==========

End of log for RFI: POIA149W