FUJ00176540

Document Title: Audit Data Extraction Process

Document Type: Process

Release: Pre Bi3

Abstract: This document describes the process to be followed by Consignia Group Internal Audit (CGIA), and other groups external to Pathway as defined in Schedule A03, when requesting audit data extraction services from Pathway CS Security. It also describes those activities carried out within Pathway to handle the request, manage the data extraction and despatch the results to the original requester.

Document Status: APPROVED

Originator & Dept: Jane Bailey

Contributors: Jan Holmes / Anthony Brown / Richard Laking

Internal Distribution: Richard Laking; Graham Hooper; Jan Holmes; Chris Billings

External Distribution:

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

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

FUJ00176540

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	1/01/02	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	

0.2 Review Details

Review Comments by :	Date
Review Comments to :	Jane Bailey

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

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001	6.0	26/03/02	Fujitsu Services (Pathway) Ltd Document Template	PVCS
IA/MAN/005	1.0 22/12/	22/12/00	Horizon System Audit Manual	PVCS
IA/REQ/004	1.0 19/01	19/01/01	Audit Data Retrieval Requirements (CSR+)	PVCS
IA/SPE/008			Audit Data Catalogue	PVCS
IA/SPE/018			Audit Data Catalogue - ADC (Consignia SIS)	PVCS
IA/SPE/019			Audit Data Catalogue (Consignia AP Clients)	PVCS
IA/SPE/020			Audit Data Catalogue (System Management)	PVCS
IA/SPE/021			Audit Data Catalogue (Internal Audit)	PVCS
RS/MAN/010			SecureID Normal Token User Guide	PVCS
IA/REQ/005			Network Banking Internal Audit Requirements	PVCS

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
AS	Audit Server
AW	Audit Workstation
AWO	Audit Workstation Operator

FUJ00176540

CD-W	Writeable CD
DLT	Digital Linear Tape
FTMS	File Transfer Management System
OBCS	Order Book Control System
PA	Pathway Auditor
PIN	Personal Identification Number
PLUI	Pathway Legato User Interface
CGIA	Consignia Group Internal Audit
PWAY	Fujitsu Services (Pathway) Ltd
RFI	Request for Information
LUI	Standard Legato User Interface
TMS	Transaction Management System

0.5 Changes in this Version

Version	Changes
2.0	Distinction between requirements when using PLUI and standard LUI. Jan Holmes no longer an author. Audit Catalogues referenced. Change from OSD to ISD and ICL to Fujitsu Services. OCP process added. Section 9, Failed TMS tape procedure added.

0.6 Changes Expected

Changes
Post cloning tape recovery procedure shall be added to this document when it becomes available.
Bi3 Network Banking transaction will be incorporated in the audit extraction procedure

FUJ00176540

0.7 Table of Contents

FUJ00176540

FUJ00176540

1.0 Introduction

The Horizon system generates significant amounts of data that is of interest to 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 CGIA 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 from outside Pathway. Requests for audit data extraction from within Pathway will also be subject to this process although use of the Request For Information (RFI) form is optional.

FUJ00176540

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 DLT (tape) by the **Hoarder**. This value is recalculated by the **Retriever** and compared to the original value when first sealed. Used to ensure data integrity during storage on DLT.

Hoarder : The module responsible for writing audit data files onto DLT at pre-defined intervals.

Retriever : The module responsible for retrieving audit data from the buffer file where it is placed by Legato when requested by the Audit Workstation.

Extractor : **Retriever** brings back complete files or groups of files from the DLTs. Further work may be required to filter out unwanted information, especially true of the TMS files, using a number of tools available on the Audit Workstation.

Legato : Legato Networker is the storage management application selected by Pathway to store and manage audit data onto DLTs.

A more complete explanation of these modules can be found in [2].

FUJ00176540

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 Consignia Group Internal Audit that this integrity is maintained.

During audit data extractions the following controls apply:

- Extractions can only be made through the three 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 AW – where most extractions will take place – is located in a secure room subject to proximity pass access within a secured Fujitsu Services site.

- Logical access to the AW and its 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 RFIs, authorised by nominated persons within CGIA. This log can be scrutinised on the AW.

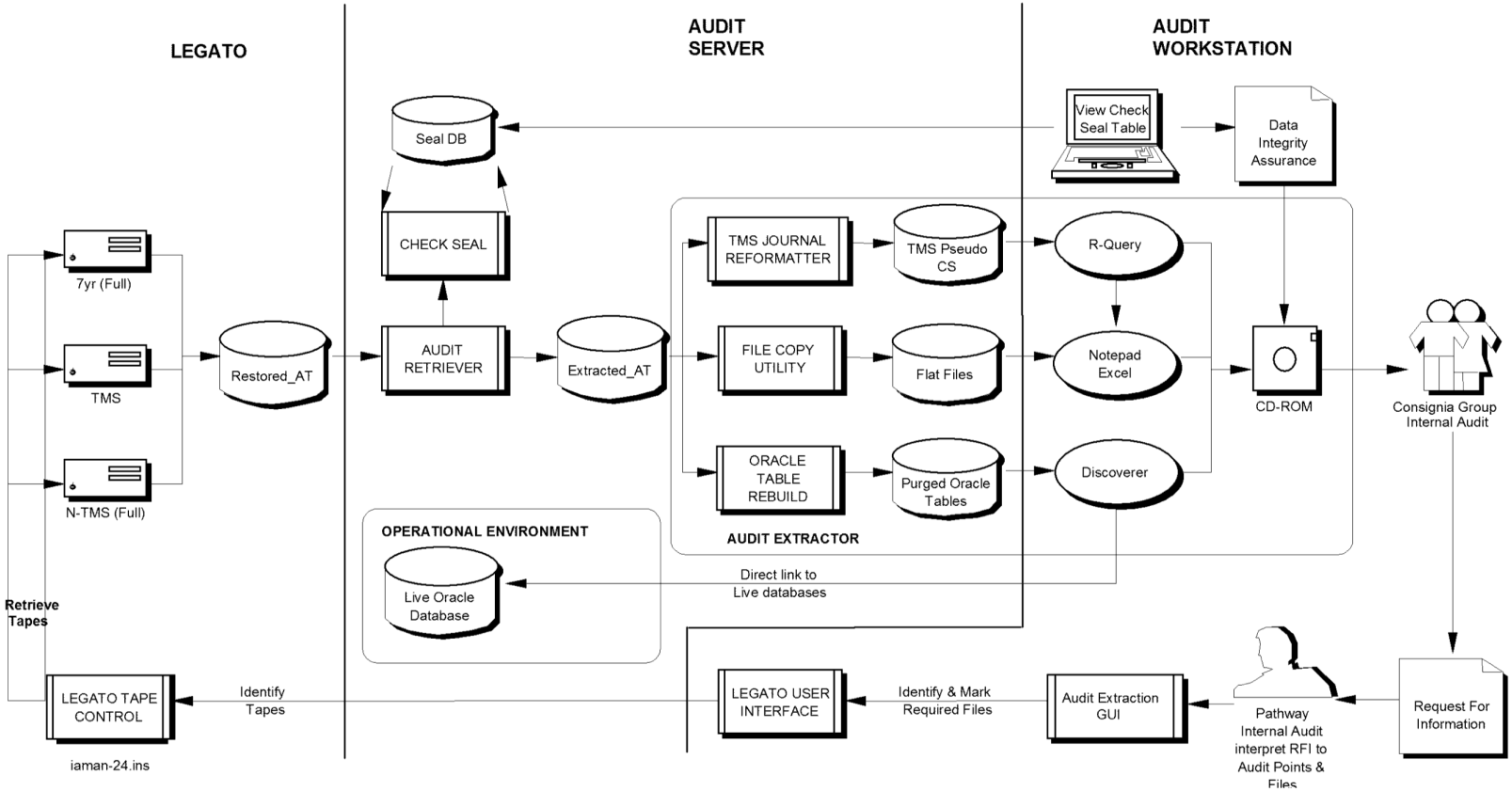
- Extractions will only be made by individuals previously notified to CGIA. Currently this is limited to Pathway Audit and Pathway CS Security personnel. Any additions will be notified to CGIA.

- Agreement has been reached with CGIA 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 DLT and re-calculated when the files are retrieved.

FUJ00176540

5.0 Retrieval Schematic



FUJ00176540

6.0 Overview

The process assumes that audit data has been Gathered, Sealed and Hoarded onto DLTs by the Audit Archive Server. The five main types of files are :

a. Flattened and compressed 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 and their associated FTMS control files.

d. AP Client Files

e. Tivoli Event files

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

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

The following paragraphs present an overview of each step in the extraction process and are ordered to reflect the actual processing of a Request For Information (RFI) by Pathway CS Security.

6.1 Request For Information

All CGIA requests for audit data must be made via the Request For Information form. This will contain a description, in business terms, of the times, outlets, events, items activities and required Excel reporting format that the Auditors are interested in. This request has to be interpreted by Pathway CS Security 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 this interpretation as many files of audit data that are needed to satisfy the request are 'marked' for retrieval. Legato is notified of these files and it in turn identifies the DLTs containing these files. Legato provides system prompts for Operators to load tapes and it copies the data into a local buffer area.

6.3 Audit Track Retriever

Polls the Legato buffer area and retrieves any data files found into temporary disk on the Archive Server prior to the extraction of relevant data for use by the auditors. The Retriever provides a second copy of the file which is input to the Check Seal function.

FUJ00176540

6.4 Audit Data Check Seal

To assure the integrity of the audit data while on the DLT 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 DLT. 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 RFI. It also places the information onto a CD-W, or other suitable media, for despatch to the RFI originator.

FUJ00176540

7.0 Retrieving & Extracting Audit Data

7.1 Receiving the RFI

a) All **CGIA requests** for audit data extractions must come to Pathway CS Security in the form of a Request For Information. An example of this form can be found at Annex A. The RFI may be mailed, faxed or e-mailed to Pathway.

RFIs will only be accepted from the following named individual :

Graham Ward : CG Internal Audit : GRO

or one named delegate, to be confirmed in writing by CGIA Internal Audit.

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

Contractual turnaround times for the provision of data apply.

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).

CGIA and Internal requests are recorded on the Data Extraction Spreadsheet. They should be logged to record the following information: Request id (e.g. PINICL no. or RFI no.), the date the request was received, the urgency of the request, the FAD and date range to search. Turnaround times are agreed rather than covered by contract.

7.2 Interpreting the RFI

It is necessary to interpret the RFI 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.

FUJ00176540

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 [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.

7.4 Preliminary Housekeeping

It is highly likely that an average RFI 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 RFI :

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

7.5 Cluster Determinant

Note that this step is only required if (a) TMS files are involved and (b) the Legato User Interface is being used.

It is recommended that this step is carried out BEFORE entering the Retrieval GUI.

Access the Secure Id Admin workstation and use Tivoli Event Console which links in to the oracle database, to identify the cluster id of a particular FAD.

7.6 Targeting the Data Files

At this stage of the retrieval procedure the AWO can choose to use the Pathway Legato User Interface (Para 7.7), a Pathway developed intelligent front end, or the standard Legato User Interface (Para 7.8). While there are no hard and fast rule around which interface to use the PLUI has obvious benefits when attempting to identify and mark a large number of files for retrieval.

Note that if you are using the standard Legato User Interface it is still necessary to register the RFI on the RFI database.

FUJ00176540

7.7 Using the Pathway Legato User Interface

The Audit Data Retrieval Service utilises a complex Graphical User Interface (GUI) to help identify and mark files and also associate those files with the originating RFI.

The RFI must be registered on the RFI database before commencing the retrieval activity.

1. Select <Audit ExtractorClient.CMD> from the main program menu.
2. At dialogue SELECT DATA CENTRE select <Data Centre> required
3. At dialogue AUDIT EXTRACTOR select <Request> from title menu.
4. Select <New> if new RFI
5. Complete selection fields :

<Requester>	Mandatory	From drop down menu.
<Date Received>	Mandatory	Date RFI received in Pathway.
<Date Required>	Mandatory	Date data required by requester.
<Catalogue Entry>	Optional	Enter search criteria into Search Catalogue
<Receipt Reference>	Mandatory	Original RFI reference
<Access Reason>	Mandatory	Reason for running retrievals

6. Select <Specify Selection Criteria>.
7. Complete remaining selection fields :

Time Period required	<From date>	Mandatory	Start date of retrieval
	<To date>	Optional	End date of retrieval (assumes today)
File Source required			
	<Legato Server>		Select from drop down Wigan/Bootle
	<Tape Pool>	Optional	
	<Filename Template>	Optional	
<Update button>			
<Audit Point>		Optional	
<Audit S Point>		Optional	
<PO FAD>		Optional FAD code for retrieval	

FUJ00176540

8. Tick <Generate volume information with file list> if you wish to see the associated DLT names.

9. Select <Search for Files> or

<Save Selection Criteria> or

<Return to Menu>

10. A list of file names will be displayed in the response part of the dialogue

11. <Mark> the required files.

12. Select <Restore Selected Files>

It is highly unlikely that a single file will hold the information required by the RFI. Indeed, the broader the date spread or complexity of request the greater the number of files that will have to be retrieved from DLT.

7.8 Using the Standard Legato User Interface

The RFI must be registered on the RFI database before commencing the retrieval activity.

1. Select <Audit ExtractorClient.CMD> from the main program menu.

2. At dialogue SELECT DATA CENTRE select <Data Centre> required.

3. At dialogue AUDIT EXTRACTOR select <Request> from title menu.

4. Select <New> if new RFI

5. Complete selection fields :

<Requester>	Mandatory	From drop down menu.
<Date Received>	Mandatory	Date RFI received in Pathway.
<Date Required>	Mandatory	Date data required by requester.
<Catalogue Entry>	Optional	Enter search criteria into Search Catalogue
<Receipt Reference>	Mandatory	Original RFI reference
<Access Reason>	Mandatory	Reason for running retrievals

6. Select <Return to Menu>.

7. <Exit>

The default Legato approach, where the primary search index is the instance of a DLT hoard, does not allow for quick and easy identification of the required files. If files to be retrieved are spread across

FUJ00176540

more than 1 hoarding instance then they have to be retrieved on a hoard instance basis. For example, if 3 hoarding instances happened in a day and all 3 contained files of interest to a particular RFI there would have to be 3 separate retrieval runs.

1. Select <Legato_Client_Bootle.CMD> from main program menu
2. Select <Directed Recovery> from <Operations> drop down menu
3. Confirm <mboarc01> as Source Client in dialogue. <OK>
4. Confirm <mboarc01> as Destination Client dialogue. <OK>

Note that Bootle is assumed as the primary retrieval location. There is no difference in the audit data held at each Data Centre. If Wigan is selected then the <Legato Client Wigan CMD> should be selected and <mwiarc01> used to confirm Source and Destination dialogues.

5. Select <Change Browse Time> from View drop down menu
6. Select appropriate date button
7. Select appropriate Hoard time (note 7:30p)
8. Locate files through Legato directory structure and naming convention [3]
9. <Mark> files using <✓> button on toolbar
10. Select <Recover Options> from Options drop down menu
11. Enter d:\Archiveserver\INTERFACES\RESTORED_AT into dialogue box
12. Select <traffic lights> button on toolbar

Note: The 'View Versions' facility on the Legato User Interface can be used to identify when hoardings took place.

7.9 Targeting the DLTs

Most Retrievals will be made from the TMS18Mnth, NonTMS18Mnth and NON TMS7Yr tape pools.

In order to achieve next day loading ISD must be notified before 1200hrs, using the OCP form. See annexe 2 for a template OCP form. The following fields must be filled in and then emailed to ISD;

1. Requested by – requesters name
2. Date raised – today's date
3. System id – mwiarc01/mboarc01
4. Requested tape serial number – must be TMS number followed by tape serial number.
5. Date required –

FUJ00176540

6. Required until – (this is not mandatory)

7. The reason for tape load – to satisfy Pathway internal audit (PO/*RFI*#/00)

Note: The 'View Versions' facility on the Legato User Interface can be used to identify whether the DLTs containing the data are in place.

For example, following the directory tree down as far as the 'TMS Pool' branch will show an entry 'TMS'. Highlighting this enables 'View Versions' to be used.

7.10 Reformatting Retrieved Data

Before detailed extractions can take place using R-Query, Wordpad, Discoverer or other appropriate tools it is necessary to 're-format' the retrieved data into a format suitable for access. There are three options :

a. TMS Re-formatter to rebuild a pseudo Correspondence Server.

b. Winzip for flat files that were zipped prior to Hoarding.

c. Oracle Table Re-formatter to rebuild Oracle tables.

7.10.1 Reformatting TMS Journals

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

The utility is evoked with the use of the Pathway Audit Extractor GUI

1. Select <Audit Extractor Client> from the programs menu

2. Select <Message store>, <Reset Message Store>

When it has reset successfully

3. Select <Message store>, <Generate Message Store>

4. Enter start date for messages

End date for messages

PO FAD

5. Generate Message Store

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%.

1. Select <Winzip.CMD> from main program Menu.

2. Select <Open> and identify zipped file through dialogue screen.

FUJ00176540

3. Select <Extract> and establish a new 'Unzipped' directory for unzipped datafiles.
4. Unzipped file will be placed into new Directory
5. Open unzipped files using the <Wordpad.CMD> utility from main program menu

7.10.2 Oracle Archive Tables

These are stored in text format.

FUJ00176540

7.11 Checking the Seals

This step is only required if the Legato User Interface is being used. There is a File Status button on the Pathway Legato User Interface

When using the Legato user interface to recover a file from DLT a copy is made and subjected to a re-calculation of the integrity seal. This value is compared to the original value on the Seal Database and an entry made in the Check Seal table of MatchOK, MatchNOTOK or MatchFAIL. This activity carries on independently of any further extraction or filtering activity on the part of the AW Operator.

1. Select <Microsoft_Access.CMD> from main program menu.

2. Using **File/Open Database…** open the share'd 'Audit_Seal_DB.mdb' database that exists on the mapped drive 'AS_db on 'mboarc01' or mwiarc01'

3. A list of 4 database 'tables' will be displayed.

4. Position the mouse cursor on the **<QUERIES>** tab and click.

5. A list of 2 database 'queries' will be displayed.

6. Double click on the <Seals Match Check – Normal> icon.

7. You will obtain an extract of the data that is in the <Check Seal Table> of the database.

(Note: only 5 of the available fields from this table, will be displayed. These are:
Request ID Audit Track Match? On At

8. From this point on, all of the 'Access' facilities to: sort, filter, export to spread sheet etc. are available.

9. Should you need to examine the records in the 'No Initial track table' i.e. the exceptions, then you will have to double click on the 'Seals Match Check – Exceptions' icon

10. You will obtain an extract of the data that is in the 'No Initial Track Table' of the database.

(Note: as above, only 5 of the available fields from this table, will be displayed. These are:
Request ID Audit Track Match? On At

11. From this point on, all of the 'Access' facilities to: sort, filter, export to spread sheet etc. are available

When using the PLGUI the operator shall use the 'file status' button to check the value of the seal status.

7.12 Despatch of Audit Data

Despatch of the extract data is by the most appropriate means depending on the nature and volume of the extracted data, and subject to any special requests made on the RFI.

The Audit Data Extraction Spreadsheet must be updated to record the date that the extraction activity was completed.

FUJ00176540

1. Select <CD_Writer_Software.CMD> from main program menu
2. Maximise dialogue box
3. Select files required in top dialogue box
4. Drag & drop to bottom dialogue box
5. When complete select **RED** dot <Red>
6. Create 'Closed' CD
7. Save layout as RFI_id

The media is despatched to the CGIA contact using Royal Mail Special Delivery. This ensures that a receipt is provided to Pathway confirming delivery.

For **internal requests**, it will usually be convenient to email the extracted data file to the recipient, although in the case of large files (>100kB) this is ideally done at the end of the working day. The alternative is to arrange despatch/collection with the recipient.

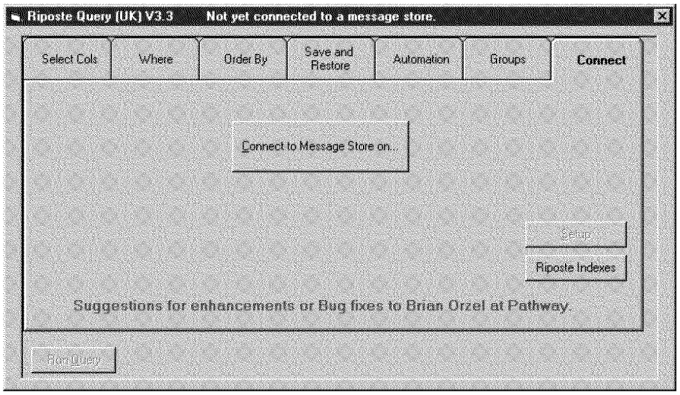
8.0 Introduction to R-Query

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 Servers. Details on how to achieve this pre-requisite can be found earlier in this procedure.

8.1 Invoking R-Query and Connecting to a Correspondence Server

1. Select <Riposte-Query.CMD> from main program menu



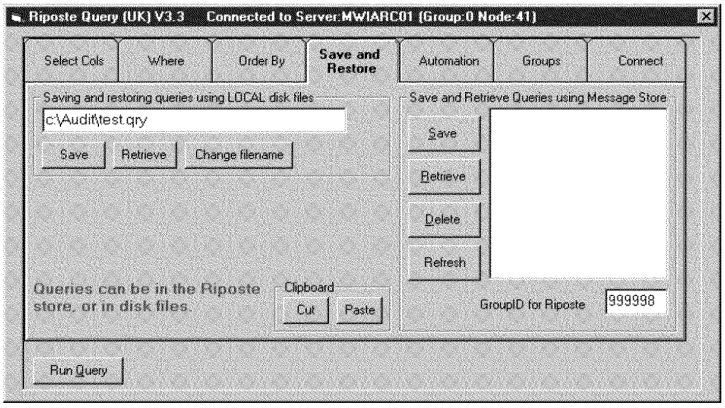
FUJ00176540

1. Select <Connect to Message Store on>
2. When asked type <mboarc01> if connecting to Bootle AS or
3. <mwiarc01> if connecting to Wigan AS.
4. When asked to justify the usage of the system type <RFI Reference> See [1].
5. You will be automatically transferred to the <Save and Restore> Tab

FUJ00176540

8.2 Restoring Retrieval Scenarios

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 you 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.

1. Go to <Message Store> window.
2. Select <Refresh> to list all scenarios associated with the current Correspondence Server.
3. Highlight the required scenario and select <Retrieve Query>.

OR

Use this step if retrieving scenarios from the Catalogue.

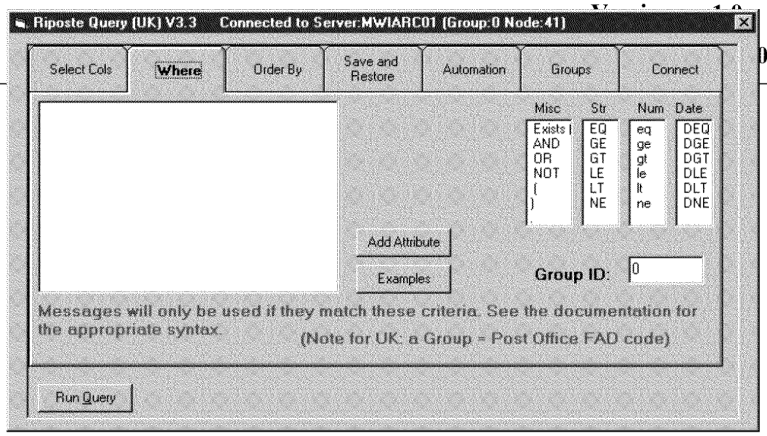
1. Locate stored scenario from the Catalogue via the <Retrieve Query from File> button using the <Change filename> to browse as required.

At this stage you will have retrieved the scenario complete with the parameter setting used on the last retrieval activity. If you want to change any of the parameters you 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.

8.3 Changing Retrieval Parameters

FUJ00176540



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

(Date DGE "29-May-2000") AND (Date DLE "01-Jun-2000")
for all dates between 29 May-1 June 2000.

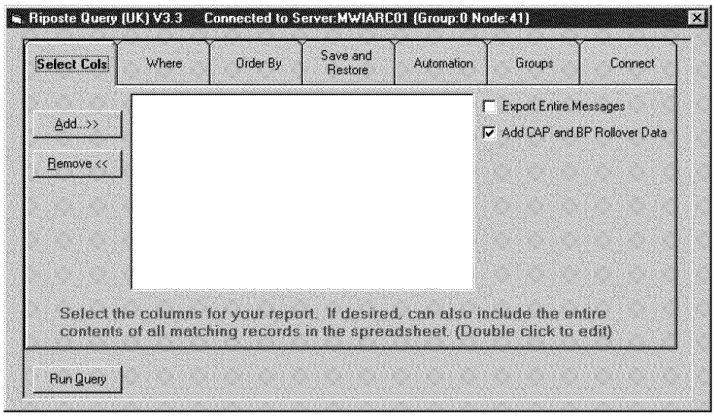
Date DEQ "31-May-2000"
for this day only.

Enter the required Post Office (FAD) code into the <Group ID:> field if it is not shown. If you want to change the TMS fields that will be visible following the retrieval you 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 (see Section 8.7).

FUJ00176540

8.4 Selecting TMS Fields for Display



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

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

Optionally a field "Add CAP and BP rollover data" can also be checked.

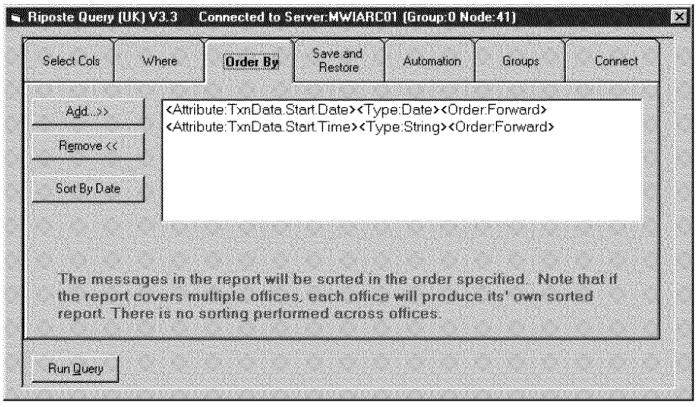
You may now want to choose how the results of the retrieval will be presented. To do this go to the <Automation> Tab.

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.

FUJ00176540

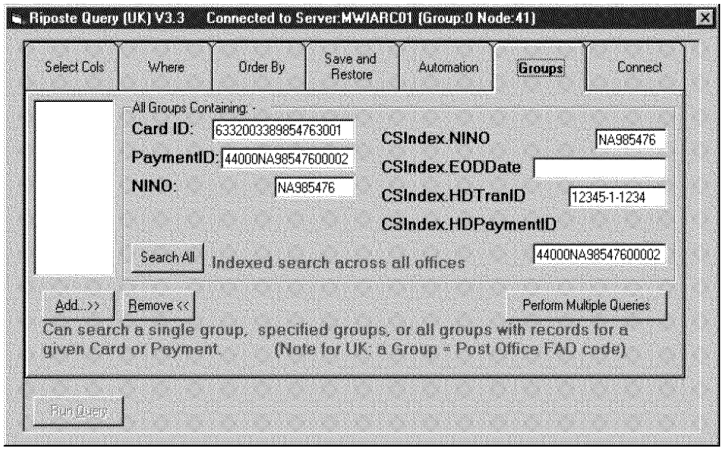
8.5 Order By Tab

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



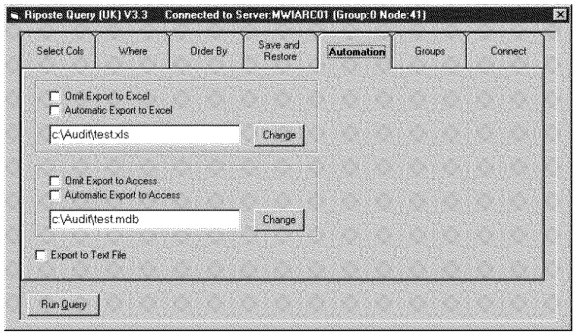
8.6 Groups Tab

The Groups tab on the R-Query tool is a remnant from the aborted Benefit Payment Card system. All of the fields should be blanked.



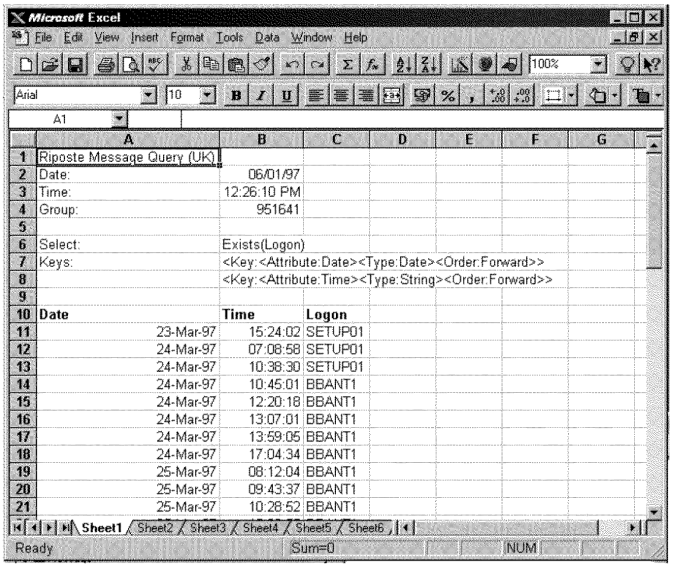
FUJ00176540

8.7 Select Output Medium



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

If you want to export the retrieved message to either an Excel spreadsheet or an Access database the enter 'x' in the <Automatic Export to Excel> or <Automatic Export to Access> field. Using the template.qry file found in d:\audit data gives the following report format:



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

8.8 Running the Query

Normally you would not actually execute the retrieval scenario until such time as you had built the query statement (Section 8.3), selected the fields (Section 8.4) and chosen the output medium (Section 8.7). However, at any time in this sequence you can run the query statement by selecting <Run Query> using the button on the "Connection" tab screen.

FUJ00176540

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 you can '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.

FUJ00176540

9.0 Failed TMS Tape Procedure Pre Cloning

This section specifies the action to be taken in the event of a TMS Audit Trail tape becoming unreadable. Prior to the commencement of the retention of a clone copy at each site in October 2001.

The process will ensure that the TMS audit trail at the alternate site to that of the failing tape has a resilient copy taken in order to maintain two copies of the Audit Trail.

9.1 Step 1 – Create a new document to record details

This initial step handles the creation of a Word document to record the details of the failing tape, and later capture details of the Cloning required.

Create a new Word document from the template TMS tape fail. See Annexe C.

Record the tape details in Table 1

9.2 Step 2 – Record data content of the failing tape.

This step records the details of the savesets held on the failing tape and thus identifies the data that cannot be accessed.

From Networker Administrator select the Volumes Tab and locate the failed tape.

Double-click on the failed tape and record the details in Table 2

Note: record the date in American format as held by Legato

Do not record savesets marked as RECYC

9.3 Step 3 – Record savesets encompassing period at alternate site

This step records details from the audit archive at the ALTERNATE site to the failing tape of savesets which span the period of data held on the failing tape.

From Networker Administrator select the alternate Audit server from the Indexes tab

Select the Index for the server (i.e. server name) double click. Takes a few mins.

From the index list select D:\Archiveserver\Hoarded_AT\TapepoolBackup\TMS_Pool and press the <Details> button.

From the list of savesets record those required which cover the period with an overlap of one day each side. in columns 1-4 of Table 3

9.4 Step 4 – Record Volume Details for the savesets

This step records volume details for the savesets identified in the previous step.

FUJ00176540

From Networker Administrator select the volumes Tab and search through the volumes for the savesets recorded in table 3.

Care must be taken where the flag is 'h' as there will be a continuation volume to be found

9.5 Step 5 –Determine clone tapes required & Volumes to be loaded

This step calculates the data volume which requires cloning and thus gives the new volumes required to hold the cloned data. It also provides a tape loading list.

Total the data sizes in Table 3 (in Gigabytes) and divide by 70 to determine the number of Clone tapes that will be required.

Complete Table 4 with the details, and record the TMS Volumes / barcodes for loading to complete the cloning operation. The barcode details can be obtained from the Volumes tab in Networker Administrator

9.6 Step 6 – Complete a Clone list by Volume

This step records details of the savesets to be cloned BY VOLUME as this will be required when producing the OCP.

From table 3 create entries in Table 5 which detail the savesets required for each volume (which will then be used to construct the OCP)

9.7 Step 7 – Validate Clone list

This step validates that the correct data has been identified and that there are no 'GAPS'.

For each of the volumes in table 5 check that the savesets are correctly identified

Select Operations / Clone savesets

On the Clone Saveset screen

Set Volume to *{volume name}*
Clear field Start date
Clear field End date
Set Maximum level 'radio button' to Full

Press **Query**…..

On the returned Clone Saveset Query screen

Check that the Saveset date/times listed in table 5 for the volume are present and contiguous

9.8 Step 8 – Raise OCP

This step raises the OCP required for ISD NT to perform the Cloning work.

FUJ00176540

Using the template TMS Clone OCP template fill in the required cloning details from tables 4 & 5 and submit to Pathway SM ISD

For template TMS Clone OCP see Annexe D

9.9 Step 9 – File details

This step provides a record of the work undertaken to preserve the resilient audit data copy.

Print a copy of the failed TMS tape details document and the OCP and file in the audit problems archive

FUJ00176540

10.0 Annexes

A Example RFI form – for CGIA contact use

B Example OCP form – tape reload request (page for data extraction user to complete)

C Example of TMS tape fail template

D Example of TMS Clone OCP template

(unnumbered pages follow)

FUJ00176540

A. Example (RFI) REQUEST FOR INFORMATION form

Originator:	Internal Crime Policy & Standards Manager Post Office Counters Ltd. 4th Floor, Impact House 2 Edridge Road CROYDON CR9 1PJ	**Date:**	DD/MM/CCYY
Telephone:	GRO	**Ref No. (originator)**	##/01
Priority:	Urgent Routine x Other	**Ref No. (Pathway)**	
Information Requested			
Date range:		**Post Office ids**	FAD ***/*** Name of PO
General Description/ Format requirements:	A report of all transactions and events for the office for the relevant days, including remittances received, transfers between stock units and error notices. We would like the following format for logs (in Excel format with each category in a separate column): Balancing Period; Cash Accounting Period; Session Type - i.e. Serve Customer, Reversal. Rem In etc. Transaction No; Session Indicator; Date; Time; Stock; User ID; Transaction Type; Amount £p Session Indicator is whatever way the system has of indicating that individual transactions are linked		
Specific Details:	Sorted by time within days		
Signed		**Date**	**DD/MM/YY**

FUJ00176540

B. Example OCP form

PATHWAY TAPE LOADING REQUEST : TLNRnnnnn ***Requested By: **** ****** (CS Security / Audit)***		
Date Raised: *dd/mm/yy*	***System Id:*** **m**arc01**	
REQUESTED TAPE SERIAL No(s): **Tape serial nos. are:** **TMS 000 (AO0000),TMS 000 (AO0000), TMS 000 (AO0000), TMS 000 (AO0000), TMS 000 (AO0000)**		
Date Required: *dd/mm/yy*	***Required Until:*** ***(if known) dd/mm/yy provisionally***	
Reason for tape load request: ***To satisfy Pathway Internal Audit (PO**/00).***		
To be Implemented by: ISD		
Technical Support Completion Agreed	***DATE***	***Signature***
ISD Service Management Completion Agreed:		

FUJ00176540

C. Example Failed TMS Tape Details

Failed TMS Tape Details

Table 1 – Failing Tape Details

Site	
Tape Name	
Barcode	

Table 2 – Failing tape saveset contents

Date (mm/dd/yy)	Time	Data Size	SSID

Table 3 – Alternate Site savesets covering period

SSID	Data size (Gb)	Date (mm/dd/yy)	Time	Volume	Con flag	Cont.Vol

FUJ00176540

Table 4 – Volume Loading table

	Volume / Quantity	Barcode
Clone tapes required		
TMS Volumes		

Table 5 – Required Savesets by Volume

Volume	Saveset Date (mm/dd/yy)	Time

FUJ00176540

D. Example TMS Clone OCP form

OCP	**REQUIRED IMPLEMENTATION: ASAP**

Summary: Take a copy of TMS Audit data volumes to provide resilience for the period where a volume has become defective .

RAISED BY: ***Richard Laking***	**Approving Team :-**	**Electronic Signature**
CHANGE AT (LOCATION): {Enter site}	ISD UNIX SUPPORT TEAM	
TYPE OF CHANGE ***Media Copy***	ISD NT SUPPORT TEAM	
MACHINE ID {Enter machine}	ISD NETWORK TEAM	
SERVICE ID:	ISD STANDBY SUPPORT TEAM	
SCHEDULED DURATION:	ISD SMG TEAM	
SERVICE AFFECTING (Y/N): N	**ISD SMC TEAM**	
PRIORITY: (H / M / L) ***H***	ISD SERVICE MANAGEMENT	
RISK: (H / M / L) ***L***	PATHWAY SERVICE MANAGEMENT	
SYSTEM BUILD AFFECTED (Y/N): ***N***	*PATHWAY SSC SUPPORT TEAM*	
REQUIRED ON LST RIGS (Y/N). ***N***	PATHWAY DEVELOPMENT TEAM	
CALL REF No N/a	PATHWAY SECURITY	
ORIGINATORS REF No	***OTHERS***	

DETAILS AND PURPOSE OF CHANGE :

The purpose of the change is to provide some resilience for failed TMS Audit tape *{Enter failed tape Name and site}*.
This will be achieved by Cloning savesets at the alternate site which cover the same period so as to provide a 'second' Audit trail copy

1 Introduce {NO of Clone tapes from table 4} new volumes to the Default Clone Pool and label them

2. Load Volumes {Enter ALL TMS Volumes / barcodes from Table 4} READ ONLY

3.Start a Networker Administrator Session

FUJ00176540

4. Clone tapes

Select Operations / Clone savesets
On the Clone Saveset screen
Set Volume to {1st volume in table 5}
Clear field Start date
Clear field End date
Set Maximum level 'radio button' to Full
Press Query…..
On the returned Clone Saveset Query screen
Select entries {record each date/time pair for volume} **by using CTRL and clicking on each**
Set the Clone Pool field to default clone
Press Clone button

{repeat above block for each additional volume entry in table 5}

5. On completion unload the TMS volumes and replace on the rack and the Default Clone volumes and store safely .

TEAM TO BE ACTIONED BY : ***ISD NT***		
REGRESSION ACTION : ***None required***		
DATE SENT TO CUSTOMER :	*DATE AGREEMENT RETURNED*	*DATE COMPLETION NOTIFIED :*
SERVICE MANAGEMENT GO AHEAD AGREED:	*DATE*	*ELECTRONIC SIGNATURE*
VARIANCE AND OTHER NOTES ON IMPLEMENTATION		
TECHNICAL SUPPORT COMPLETION AGREED	*DATE*	*ELECTRONIC SIGNATURE*
SERVICE MANAGEMENT COMPLETION AGREED	*DATE*	*ELECTRONIC SIGNATURE*