

JD Edwards World
Database Audit Manager
Release A9.4
E58806-01

April 2015

Describes how to use the Database Audit Manager tool to set up an audit process on demand and enable selective historical database transaction logging.

JD Edwards World Database Audit Manager, Release A9.4

E58806-01

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

| | |
|---|------|
| Preface | v |
| Audience | v |
| Documentation Accessibility | v |
| Related Information | v |
| Conventions | v |
| | |
| 1 Overview to Database Audit Manager | |
| 1.1 System Requirements | 1-1 |
| | |
| 2 Menus and Screens | |
| 2.1 Overview | 2-1 |
| 2.2 Audit Configuration Defaults (P98201) | 2-3 |
| 2.3 Audit Manager Workbench (P98200) | 2-5 |
| 2.4 Change Audit Definition (P98200W) | 2-6 |
| 2.5 File List (P98200X) | 2-7 |
| 2.6 Audit Definition Parameters (P98202) | 2-8 |
| 2.7 Field Selection List (P98203) | 2-11 |
| 2.8 Save Changes (P00CFMCHG) | 2-13 |
| 2.9 Confirm Deletion (P00CFMDLT) | 2-13 |
| 2.10 Database File Triggers (P98211W) | 2-14 |
| 2.11 Reason Code Maintenance (P98204) | 2-15 |
| 2.12 Inactive Reason Codes (P98204I) | 2-17 |
| 2.13 Electronic Signature (P98208) | 2-18 |
| 2.14 Associated Text Search (P98209) | 2-19 |
| 2.15 Associated Text Properties (P98209H) | 2-20 |
| 2.16 Associated Text (P98209D) | 2-21 |
| 2.17 Selection List (P98209X) | 2-22 |
| | |
| 3 Tasks | |
| 3.1 Setting Up an Audit Process | 3-1 |
| 3.1.1 Before You Begin | 3-1 |
| 3.1.2 Place the triggers on the file | 3-6 |
| 3.2 Editing an Audit File | 3-6 |
| 3.3 Deleting an Audit Process from a File | 3-11 |
| 3.4 Displaying Triggers for a File | 3-14 |

| | | |
|-----|--------------------------------------|------|
| 3.5 | Maintaining Reason Codes..... | 3-16 |
| 3.6 | Changing Configuration Defaults..... | 3-20 |

4 Tips and Techniques

| | | |
|-----|-----------------------------------|-----|
| 4.1 | Sleeper | 4-1 |
| 4.2 | Issues and Assumptions | 4-1 |
| 4.3 | Impact on Other Applications..... | 4-1 |
| 4.4 | Coexistence | 4-2 |
| 4.5 | Performance Impact..... | 4-2 |
| 4.6 | Reporting..... | 4-2 |

A Electronic Signatures

| | | |
|-------|--|-----|
| A.1 | Overview | A-1 |
| A.2 | Definitions..... | A-1 |
| A.3 | Implementation..... | A-2 |
| A.4 | Two Levels of Signatures..... | A-2 |
| A.4.1 | Record Level Authorizations | A-2 |
| A.4.2 | Transaction Level Authorizations | A-2 |
| A.5 | Signature Servers | A-3 |
| A.5.1 | P98208 Transaction Level Authentication Server | A-3 |
| A.5.2 | P00CKPWD Transaction Level Authentication Server (External)..... | A-4 |
| A.6 | Application Program Code Samples..... | A-5 |
| A.6.1 | P4108 - Single record update..... | A-5 |
| A.6.2 | P41080 - Transaction processor..... | A-5 |
| A.6.3 | Example of Single Record Update..... | A-6 |
| A.6.4 | Transaction Level Interfaces - Copy Modules | A-6 |

Index

Preface

Welcome to the JD Edwards World Database Audit Manager Guide.

Audience

This guide is intended for implementers and end users of JD Edwards World Database Audit Manager.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Information

For additional information about JD Edwards World applications, features, content, and training, visit the JD Edwards World pages on the JD Edwards Resource Library located at:

<http://learnjde.com>

Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|-----------------|--|
| boldface | Indicates cautionary information or terms defined in the glossary. |
| <i>italic</i> | Indicates book titles or emphasis. |

Overview to Database Audit Manager

This chapter contains the topic:

- [Section 1.1, "System Requirements."](#)

New federal regulations necessitate a flexible auditing tool that can be reconfigured quickly. The Database Audit Manager provides that tool. The Database Audit Manager enables selective historical database transaction logging. Support for electronic signature verification, enforcement, and capture, is embedded within Audit Manager. Be aware that enforcement of electronic signatures requires changes to JD Edwards World application programs.

The Food and Drug Administration (FDA) requires that companies be able to set up an audit process on demand. These audits need to track changes to any field in any file.

To set up an audit process, first identify the library that contains the file to be configured for audit. Select the file from the library. Define the audit program, define a target file to store the audit information, and determine the type of audit to occur. Select the data fields to trigger an audit or to be copied into the audit target file for informational purposes only. Finally, attach reason codes to the audit actions.

For example, if the FDA requires tracking address changes, set up an audit to record changes to the address data field of the Address Book Master file (F0101). First, find out which library contains the Address Book Master File. After selecting the Address Book Master File from the library, define an audit program (P0101AUD) and a target file (F0101AUD). Then select the address data field to trigger the audit program. Finally, attach reason codes to the actions.

The Database Audit Manager (G946) allows selecting a file and the fields in the file to be tracked. In addition, it allows the following:

- Add a new audit process
- Build an audit
- Activate and deactivate audit triggers
- Maintain reason code
- Set the default library names used throughout the system

1.1 System Requirements

The minimum requirements for running Database Audit Manager are as follows:

- JD Edwards World
- Source Code for Database Audit Manager must be loaded at the time of install for the product to work properly

- IBM V5R1 or above
- All JDESRC code does not need to be installed. DBAM only requires the source code member XBASETTRG - this is the trigger template source member and its location must be specified in the library/file on the Configuration Defaults Panel
- DB2 Query Manager and SQL Development Kit program product.5722-ST1 is no longer required
- SQL is no longer a requirement.

Menus and Screens

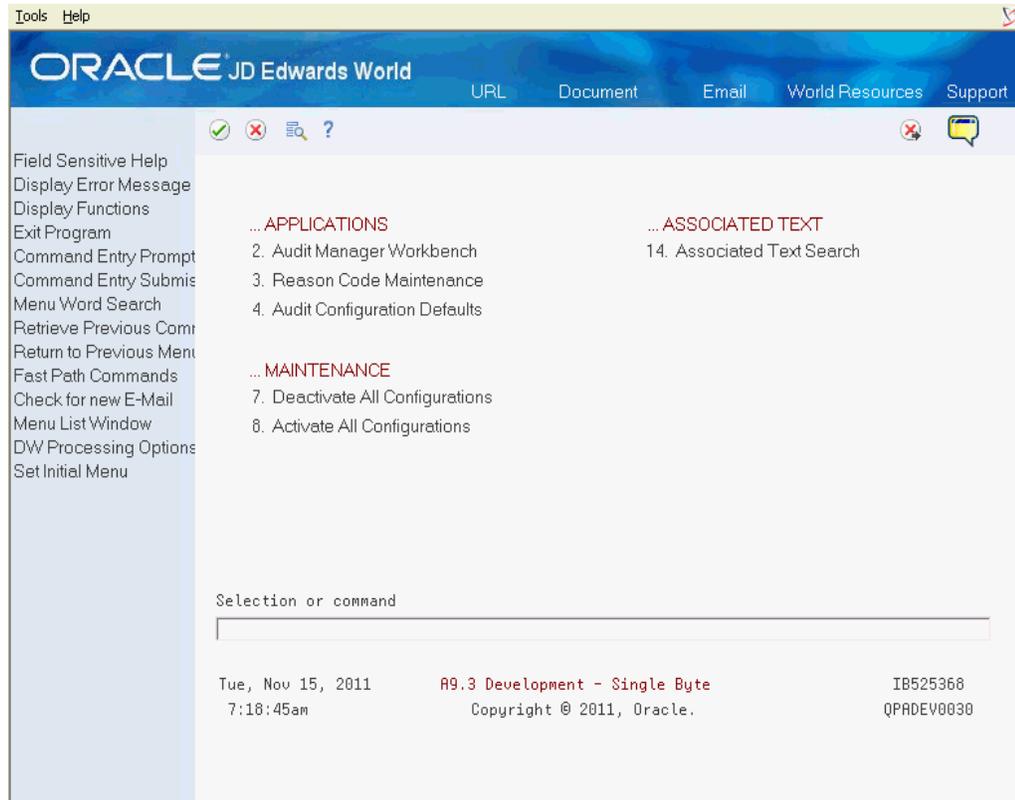
This chapter contains these topics:

- Section 2.1, "Overview,"
- Section 2.2, "Audit Configuration Defaults (P98201),"
- Section 2.3, "Audit Manager Workbench (P98200),"
- Section 2.4, "Change Audit Definition (P98200W),"
- Section 2.5, "File List (P98200X),"
- Section 2.6, "Audit Definition Parameters (P98202),"
- Section 2.7, "Field Selection List (P98203),"
- Section 2.8, "Save Changes (P00CFMCHG),"
- Section 2.9, "Confirm Deletion (P00CFMDLT),"
- Section 2.10, "Database File Triggers (P98211W),"
- Section 2.11, "Reason Code Maintenance (P98204),"
- Section 2.12, "Inactive Reason Codes (P98204I),"
- Section 2.13, "Electronic Signature (P98208),"
- Section 2.14, "Associated Text Search (P98209),"
- Section 2.15, "Associated Text Properties (P98209H),"
- Section 2.16, "Associated Text (P98209D),"
- Section 2.17, "Selection List (P98209X)."

2.1 Overview

This section describes the menus and screens that comprise the Database Audit Manager (DBAM). The menu for the Database Audit Manager is G946, shown below. From the menu you can select a file and the fields you want tracked. You can also add a new audit process, build an audit, activate and deactivate audit triggers, maintain reason codes and set the default library names used throughout the system.

Figure 2–1 Database Audit Manager Menu screen



The selections on the Database Audit Manager menu are described briefly below.

| Menu Selection | Description |
|--|---|
| Audit Manager Workbench | Displays the primary application screen, Audit Management Workbench. It allows you to add new audit process, build audit, turn audit triggers on or off, and delete the audit configuration for a file. |
| Reason Code Maintenance | Opens the Reason Code Maintenance screen that displays reasons to be associated with events. On this screen, you can add, change, and display inactive reasons. |
| Audit Configuration Defaults | This screen contains the default library names that will be used throughout the system. Audit defaults must be set up in an environment where the audit process will be active. |
| Deactivate All Configurations Activate All Configurations | These two menu selections are bulk operations will turn on or off all current Database Audit Manager configured audits. These utilities are provided specifically to facilitate the operations which are needed before applying software upgrades (Releases, Cumes, or PcCpys) and resuming audit functions after upgrades. These bulk trigger activation and deactivation processes should be used only by personnel knowledgeable about JD Edwards World software applications, and with the proper system authorities to add or remove database triggers from production files. Manipulating these configurations requires exclusive object allocation of the database file. Therefore, these operations may need to be performed when no users are accessing the software. |

| Menu Selection | Description |
|------------------------|--|
| Associated Text Search | Use this screen to access the associated text attached to a specific audit action. Associated text can be changed but never deleted. |

2.2 Audit Configuration Defaults (P98201)

Audit Configuration Defaults allows you to add, view, or change the default values used when you add a new file. Select Audit Configuration Defaults (P98201) directly from the menu or press F8 on the Audit Manager Workbench (P98200).

Figure 2–2 Audit Configuration Details screen

The screenshot shows the Oracle JD Edwards World interface for the Audit Configuration Defaults (P98201) screen. The title bar includes 'Tools Help' and 'ORACLE JD Edwards World'. The main content area is titled 'Audit Configuration Defaults' and displays the following fields:

- Library Locations:**
 - Database Files: PGFDTA93
 - Audit Log Files: JDFAUDIT
 - Trigger Programs: JDFAUDIT
- Output Trigger Source:**
 - Library: JDFAUDIT
 - Source File: JDESRC
- Trigger Source Template:**
 - Library: JDFSRC93
 - Source File: JDESRC
 - Member: WBASETRG

Additional elements include a left-hand menu with options like 'Field Sensitive Help', 'Display Error Message', 'Display Functions', and 'Exit Program'. A status bar at the bottom indicates 'F3=Exit'.

The Audit Configuration Defaults (P98201) screen has the following fields:

| Field | Explanation |
|--------------------|--|
| Library Locations: | |
| Database Files | The library that is used to generate the initial database selection list when a new configuration is being created. This should be your production database library. |
| Audit Log Files | The library into which the Audit Manager will create the audit log files. This library does not need to be in user library lists. The generated auditing trigger programs are able to access the log files without the library appearing in users library lists. |
| Trigger Programs | The library into which the Audit Manager will create the auditing trigger programs. This library does not need to be in user library lists. The generated auditing trigger programs are able to access the log files without the library appearing in users library lists. |

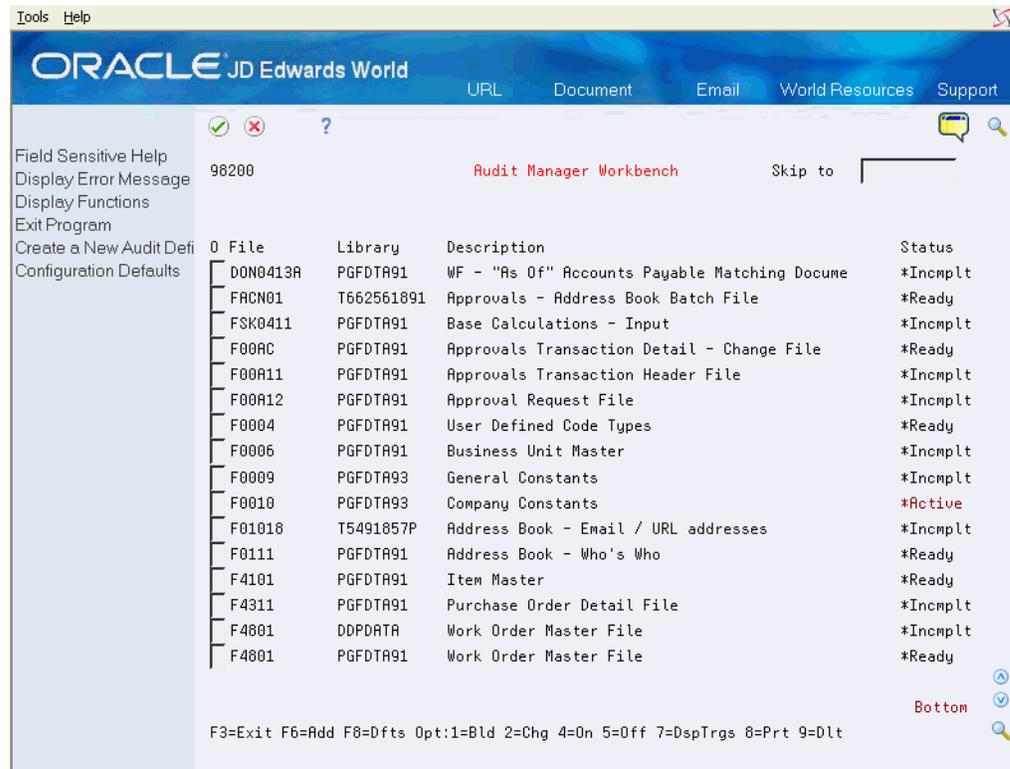
| Field | Explanation |
|--------------------------|--|
| Output Trigger Source: | Specify the library and source file location into which the Audit Manager is to place the generated source code for the auditing trigger program. This source file location does not need to be the standard JD Edwards source file (JDESRC) where production source code resides. This library does not need to be in user library lists to generate audit configurations. Object generation is qualified to this location. The only requirement is that this be a standard IBM source file. |
| Library | Defines the source code library. |
| Source File | Defines the source physical file that is in the output trigger source library. This can be any client designated library name. |
| Trigger Source Template: | Specify the library, source file, and member name of the audit trigger template program that the Audit Manager uses to generate the necessary audit objects. Note: The JD Edwards supplied audit trigger template source code contains substitution markers that the build process uses to insert information specific to the defined audit configuration. Each configuration is specific to the database file being audited. It is advised that modifications to this template not be performed, or if required by your installation, they be performed by highly qualified engineers only. |
| Library | Defines the library that contains the source code that JD Edwards World delivers. This library name was determined at the time of install. |
| Source File | Defines the source physical file that is in the library. |
| Member | Defines the template program that is shipped from JD Edwards World to be used with the Database Audit Manager system. |

The Audit Configuration Defaults (P98201) screen has one function key exit.

| Function Key | Task |
|-------------------|---|
| Exit Program (F3) | Returns the Audit Manager Workbench (P98200). |

2.3 Audit Manager Workbench (P98200)

Figure 2–3 Audit Manager Workbench screen



The Audit Manager Workbench (P98200) is the primary application screen of the Database Audit Manager. It lists files that have been selected for auditing and the stage of that audit process. The screen provides the following information on each file:

| Field | Explanation |
|-------------|--|
| File | Identifies the data file containing the fields tracked by the audit. |
| Library | Identifies the library that contains the data file. |
| Description | Describes the file containing the fields tracked by the audit process. |
| Status | Indicates if the audit is active (built and turned on), ready (built but not turned on), or incomplete (not built or setup is not complete). |

By entering an option number in the Option field for a displayed file, you can perform the following tasks:

| Option | Task |
|--------|--|
| 1 | Executes the build process that creates or changes the audit file. Creates and compiles the trigger program that is used to audit the data file. |
| 2 | Accesses the setup files. |

| Option | Task |
|--------|--|
| 4 | Places the triggers on the file. |
| 5 | Removes the triggers from the file. |
| 7 | Displays triggers for a file. |
| 9 | Deletes the audit program and setup records. It does not delete the audit file or the SVR record created for the audit file. |

In addition to the options, there are function key exits that allow the user to add new files for auditing and configure defaults used by the system. The following table describes the function key exits:

| Function Key | Task |
|------------------------------------|---|
| Exit Program (F3) | Returns the Database Audit Manager (G946). |
| Create a New Audit Definition (F6) | Displays the File List screen, which allows you to select a new data file to audit. |
| Configuration Defaults (F8) | Display Audit Configuration Defaults screen, which allows you to change the environment default values. |

2.4 Change Audit Definition (P98200W)

The Change Audit Definition (P98200W) screen displays when you select a file with an option 2 on the Audit Manager Workbench.

Figure 2-4 Change Audit Definition Window



From the Change Audit Definition (P98200W) screen, select any or all of the following:

- Audit Definition Parameters (P98202)

- Field Selection List (P98203)
- Add/Change Reason Codes (P98204)

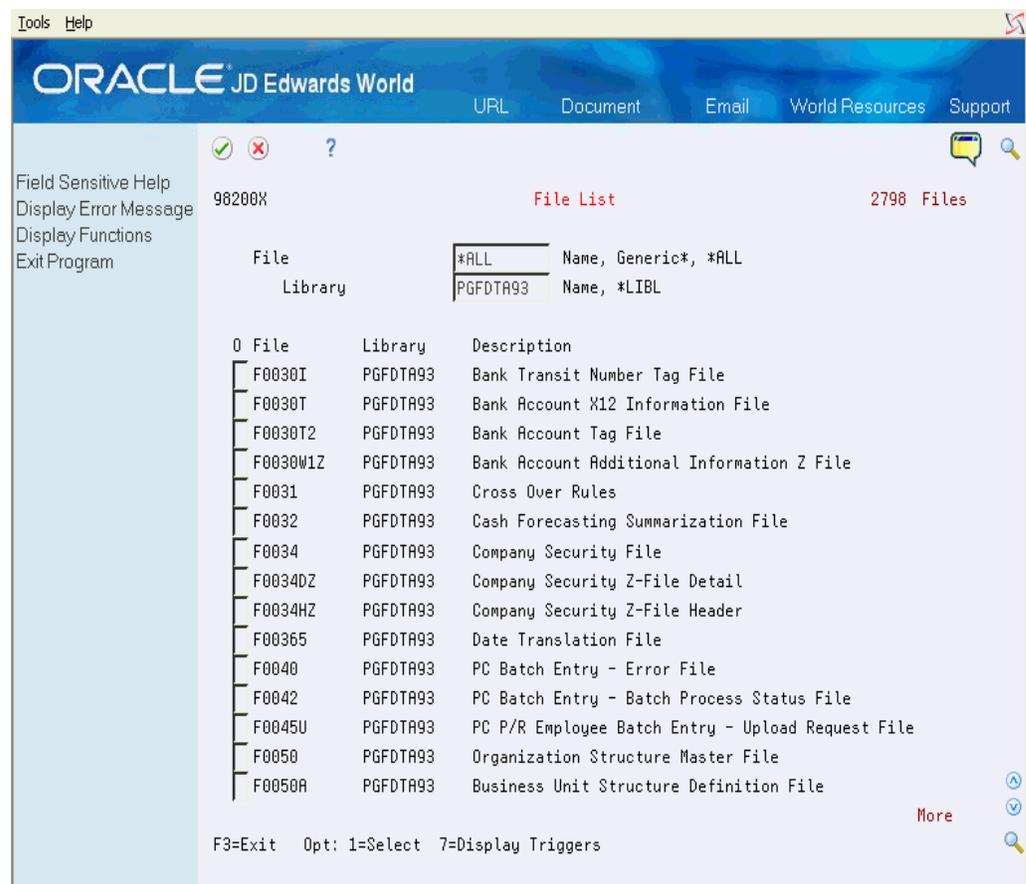
The Change Audit Definition (P98200W) screen has one function key exit.

| Function Key | Task |
|-------------------|--|
| Exit Program (F3) | Returns the Database Audit Workbench (P98200). |

2.5 File List (P98200X)

The File List (P98200X) screen displays when you press F6 from the Audit Manager Workbench (P98200) screen. It lists the files in a selected library.

Figure 2-5 File List screen



Note: The description comes from the object itself. No description on the object means none will show on the display. Files highlighted are not selectable as they are already files with audit configurations. (Depending on the number of files in the library, the response may take several seconds to display the list of files. The message Retrieve Database File List appears at the bottom of the screen.)

The File List screen provides the following information for each file listed.

| Field | Explanation |
|-------------|-------------------------------------|
| File | The production data file. |
| Library | The library that contains the file. |
| Description | A description of the file. |

By entering an option number in the Option field for a displayed file, you can perform the following tasks:

| Option | Task |
|--------|---|
| 1 | Selects a file for auditing. |
| 7 | Displays the triggers currently defined for the file. |

In addition to the options, there is one function key exit.

| Function Key | Task |
|-------------------|--|
| Exit Program (F3) | Returns the Database Audit Workbench (P98200). |

2.6 Audit Definition Parameters (P98202)

The Audit Definition Parameters (P98202) screen displays if a file is selected from the File List (P98200X) screen or the Detail Parameters is selected from the Change Configuration (P98200W) screen. Specify the audit file and trigger program that will be used to audit actions made to the file.

The Audit Definition Parameters (P98202) screen pulls the default values for its fields from the Configuration Defaults (P98201) screen.

Figure 2-6 Audit Definition Parameters screen

Tools Help

ORACLE JD Edwards World

URL Document Email World Resources Support

98202 Audit Definition Parameters

Field Sensitive Help
Display Error Message
Display Functions
Exit Program

Database File

File Name F0111
Library PGFDTA93
Description Address Book - Who's Who

Audit Log File

File Name
Library JDFAUDIT

Trigger Program

Program Name
Library JDFAUDIT

Electronic Signature

Require Signature Blank=None,1=Transactional,2=Record Lvl

Trigger Activation Mode. I=Interactive,B=Batch

F3=Exit

The Audit File Details (P98202) screen has the following fields:

| Field | Explanation |
|-----------------|---|
| Database File: | |
| File Name | The build process does not generate DDS, rather SQL DDL (data definition language - "Create Table") is used to create audit log files. After creation, SVR (F9801/F9802) records are created but there is no source code for an audit file. |
| Library | The library that contains the file to be audited. |
| Description | The description of the file to be audited. |
| Audit Log File: | |
| | Specify the name to give the audit log file and the library in which to create it. The library name defaults from the location specified in the Audit Configuration Defaults panel. The name of the audit log file must be unique and not already exist in the audit log library, and it must not currently exist in the Software Versions Repository. When the configuration is built and the audit log file is created, an entry will be added to the Software Versions Repository. |

| Field | Explanation |
|-----------------------|--|
| File Name | The audit file that records the audit. This file name needs to be a unique file name derived by the user. For example if you are planning to audit the F0101 file, you might name the audit file F0101A or F0101AUD. The Audit file name must follow the JD Edwards World standards and begin with an 'F'. The build process will create the data description specifications (DDS) and physical file. |
| Library | The library where the audit file will be created. |
| Trigger Program: | Specify the name to give the audit trigger program and the library in which to create it. The library name defaults from the location specified in the Audit Configuration Defaults panel. The name of the audit trigger program must be unique and not already exist in the audit log library, and it must not currently exist in the Software Versions Repository. When the configuration is built and the audit trigger program is created, an entry will be added to the Software Versions Repository. |
| Program Name | The program that triggers the audit. This needs to be a unique program name derived by the user. For example, if you are planning to audit the F0101 file you might name the trigger program P0101A or P0101AUD. The program name must follow JD Edwards World standards and begin with a "P". The build process will create the source code and compile the program to the library. To avoid overlaying source code the system will require the name be unique across all libraries. |
| Library | The library that contains the trigger program object. |
| Electronic Signature: | |
| Require Signature | <p>* – Blank - No electronic signature is required for any action on the audited database file. Triggers are attached to the audit file as *AFTER triggers, and the fields configured for the audit log file are recorded after the database processes the action on the audited database file.</p> <p>1 – Transaction level signature required - An electronic signature will be expected on all transactions to the audited database file. Transaction authorization is defined and prompted for by the application program invoking the authorization server (P98208) to acquire and establish the electronic signature. Audit trigger programs are attached to the database file as *AFTER triggers. The electronic signature is recorded along with the fields configured in the audit log file.</p> <p>2 – Record level signature required - An electronic signature is required for all transactions to the audited database file. Record level authorization is prompted for by the audit trigger program. Valid authorization must be provided for the database action to continue. Triggers are attached to the audit file as *BEFORE triggers and failing valid authorization, the database action is terminated and an I/O error is returned to the program initiating the database action. Application program must monitor and be able to handle the I/O error returned by the database trigger program.</p> |

| Field | Explanation |
|-------------------------|--|
| Trigger Activation Mode | <p>Indicates the type of processing to be used when executing the build, activate, or deactivate functions.</p> <p>B – Batch - The functions such as the build, adding or removing triggers will be submitted to a JOBQ and run in batch mode. This may need to be used when files are open and locks could prevent triggers from being applied.</p> <p>I – Interactive - he functions such as the build, adding or removing triggers will execute immediately and run interactively.</p> <p>Note: Adding and removing triggers from database files can only be done when there are no locks on the file. That is, when nobody is using or accessing the database file. The batch option may be used along with hidden selection 82 (and Sleeper) to schedule the activation or deactivation of audit triggers configured for control files, or other files that would normally be open during the times when users are accessing the database files.</p> |

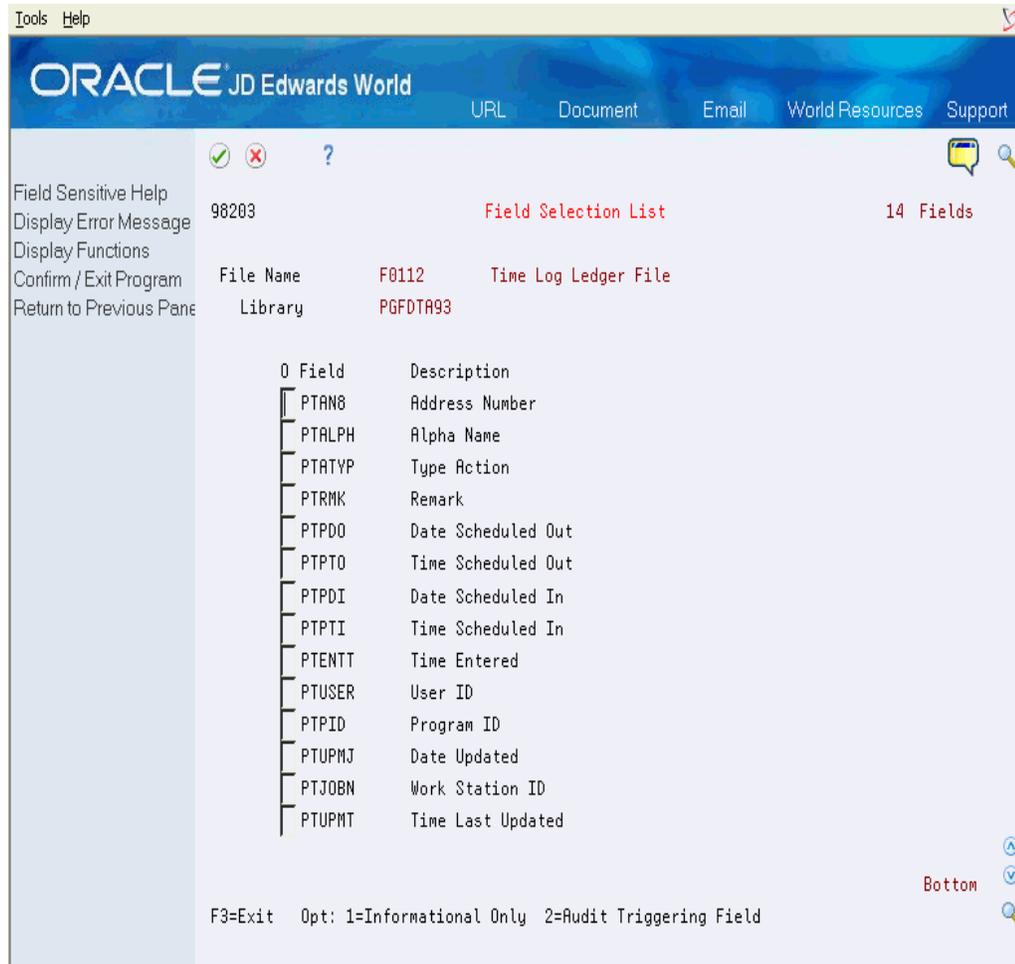
The Audit File Details (P98202) screen has one function key exit.

| Function Key | Task |
|-------------------|--|
| Exit Program (F3) | Returns the Database Audit Workbench (P98200). |

2.7 Field Selection List (P98203)

The Field Selection List (P98203) screen lists the data fields in a file. Data fields selected from this screen will be used to trigger the audit process and are recorded for informational reasons. Changes to informational only fields will not cause an audit file record to be written (the trigger programs always fire).

Figure 2-7 Field Selection List screen



The File Field List (P98203) screen contains the following fields for each listed data field:

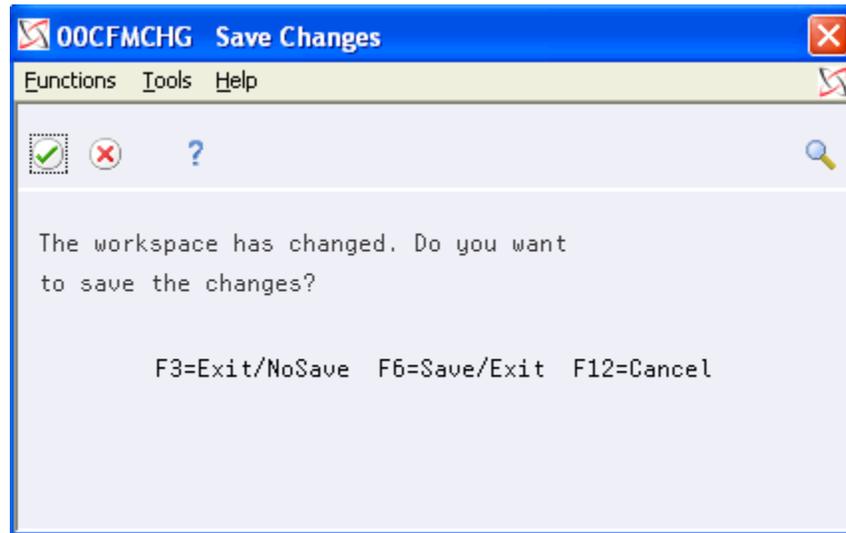
| Field | Explanation |
|-------------|---|
| Option | <p>2 – Specifies this field as a triggering field. Triggering fields appear in the audit log file record format and are the fields that determine when a change record is written to the audit log file.</p> <p>1 – Include the field in the audit log file as an informational only field. That is, the field will appear in the audit log file record format.</p> <p>Note: When auditing mode is on a database file, a corresponding record is written to the audit log file every time a record is added to or deleted from the database file. For database file changes, corresponding records are written to the audit log file only when a designated triggering field changes in value.</p> |
| Field | Provides the name of the data field. |
| Description | Provides a description of the data field. |

The File Field List (P98203) screen has one function key exit.

| Function Key | Task |
|--------------|--|
| F3 | Returns the Database Audit Workbench (P98200). |

2.8 Save Changes (P00CFMCHG)

Figure 2–8 Save Changes Window

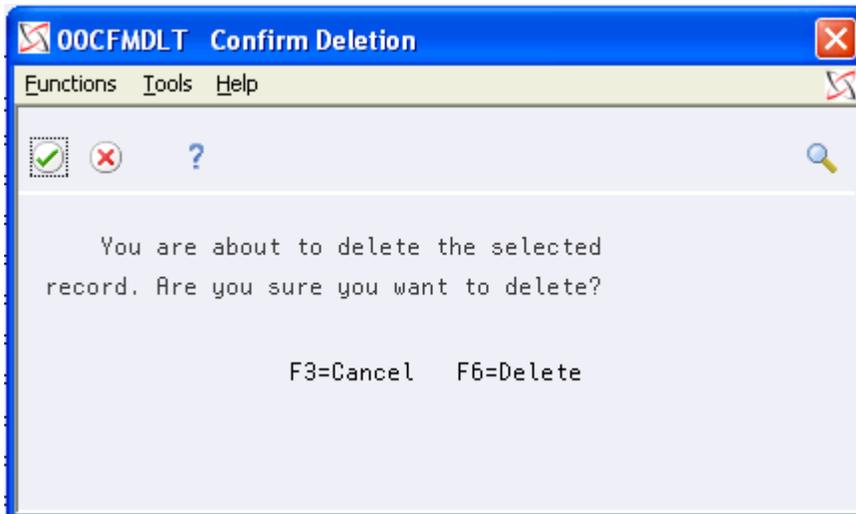


The Save Changes (P00CFMCHG) screen displays upon updating and exiting the Field Selection List (P98203) screen. The following are the valid function keys for this screen:

| Function Key | Task |
|-------------------|---|
| Exit Program (F3) | Exit without saving any changes. |
| Save/Exit (F6) | Exit and save your changes. |
| Cancel (F12) | Return to the File Selection List (P98203). |

2.9 Confirm Deletion (P00CFMDLT)

The Confirm Deletion (P00CFMDLT) screen allows you to confirm the intent to delete an audit configuration. Deleting removes the program and setup, but does not delete the audit file or the audit file SVR record. The audit file and SVR record must be deleted manually.

Figure 2–9 Confirm Deletion Window

The Confirm Deletion (P00CFMDLT) screen has two function key exits.

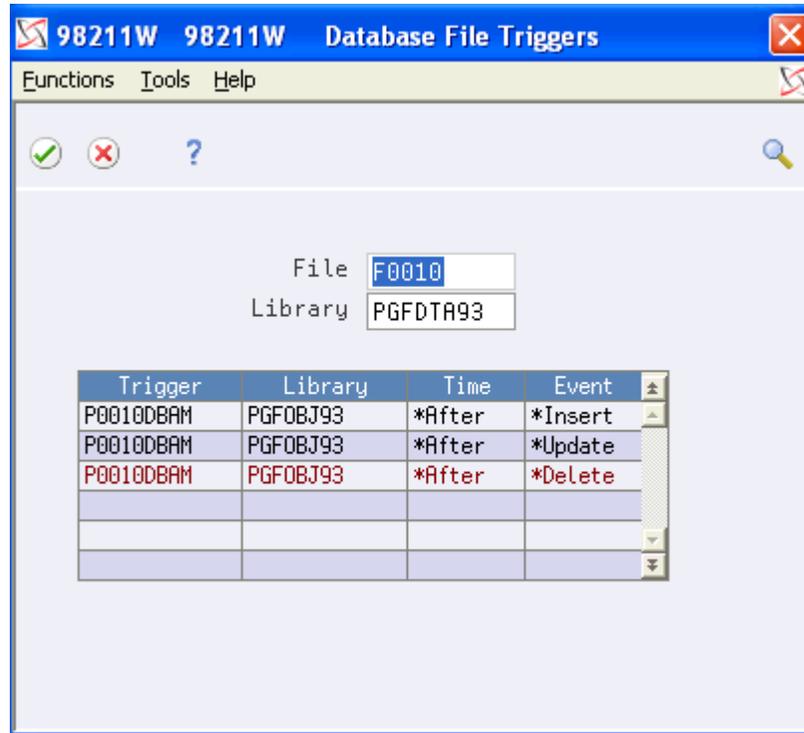
| Function Key | Task |
|-------------------|----------------------|
| Exit Program (F3) | Cancel the deletion. |
| Delete (F6) | Perform the delete. |

2.10 Database File Triggers (P98211W)

The Database File Triggers (P98211W) screen displays when you select option 7 from the workbench (P98200). This screen automatically displays when adding a new file to the audit process if the file already contains triggers.

Prior to V5R1, the maximum triggers on a file was six; One for each event (action) Add/Change/Delete, and one for each time *BEFORE/*AFTER the file was updated. As of V5R1, the number of triggers has been increased to 300 per file.

Pre-existing triggers may be replaced with new audit triggers during the audit process if the IBM release is prior to V5R1.

Figure 2–10 Database File Triggers Window

For each trigger, the Active DBF Triggers (P98211W) screen displays the following information:

| Field | Explanation |
|---------|--|
| Trigger | The name of the trigger program. |
| Library | The library that contains the trigger program. |
| Time | A flag indicating when the program runs, before or after the target file is updated. |
| Event | The event that triggers the program. |

The Database File Triggers (P98211W) screen has one function key exit.

| Function Key | Task |
|-------------------|--|
| Exit Program (F3) | Returns the Database Audit Workbench (P98200). |

2.11 Reason Code Maintenance (P98204)

The Reason Code Maintenance (P98204) screen allows you to set up and maintain reason codes. Reason codes indicate what action was made to a file and why. For example, set up an audit to track changes to employee records, and associate the reasons "New Hire", "Employee Relocation", and "Employee Terminated" with the addition, change, or deletion of employee records, respectively.

Reason codes are associated with serial numbers. If a reason code is associated with the audit program and an audit event has been triggered, the serial number is placed in the audit file to provide more information on the triggering event.

Figure 2–11 Reason Code Maintenance screen

The screenshot shows the 'Reason Code Maintenance' screen in Oracle JD Edwards World. The interface includes a menu on the left with options like 'Field Sensitive Help', 'Display Error Message', 'Display Functions', and 'Exit Program'. The main area displays a table with the following columns: Program, User, Event, and Reason Description. The table contains several rows of data, including entries for *DFT, P000909, and P9801. The status bar at the bottom indicates 'F3=Exit Opt: 1=Display Inactive 2=Add/Chg/Dlt'.

| Program | User | Event | Reason Description |
|---------|-----------|-------|--|
| *DFT | *DFT | A | Default Add |
| | | C | Default Change |
| | | D | Default Delete |
| P000909 | *ALL | A | add |
| | | C | Multi-Currency Conversion switch changed |
| | | D | delete |
| P9801 | SA5491857 | A | Add |
| | | C | Change |
| | | D | Delete |
| | | A | |
| | | C | |
| | | D | |
| | | A | |
| | | C | |
| | | D | |
| | | A | |
| | | C | |
| | | D | |

The Reason Code Maintenance screen lists programs with reason codes defined. Each record listed has the following fields.

| Field | Explanation |
|---------|--|
| Program | The name of the update program with which the reason codes are associated. |
| User | The name of the user that would be updating the data file. |
| Event | A – Add C – Change D – Delete |
| Reason | Description - Information about the events being audited. |

By entering an option number in the Option field for a displayed file, you can perform the following tasks:

| Option | Task |
|--------|---------------------------------------|
| 1 | Display inactive reason codes. |
| 2 | Edit or delete existing reason codes. |

In addition to the options, there is one function key exit:

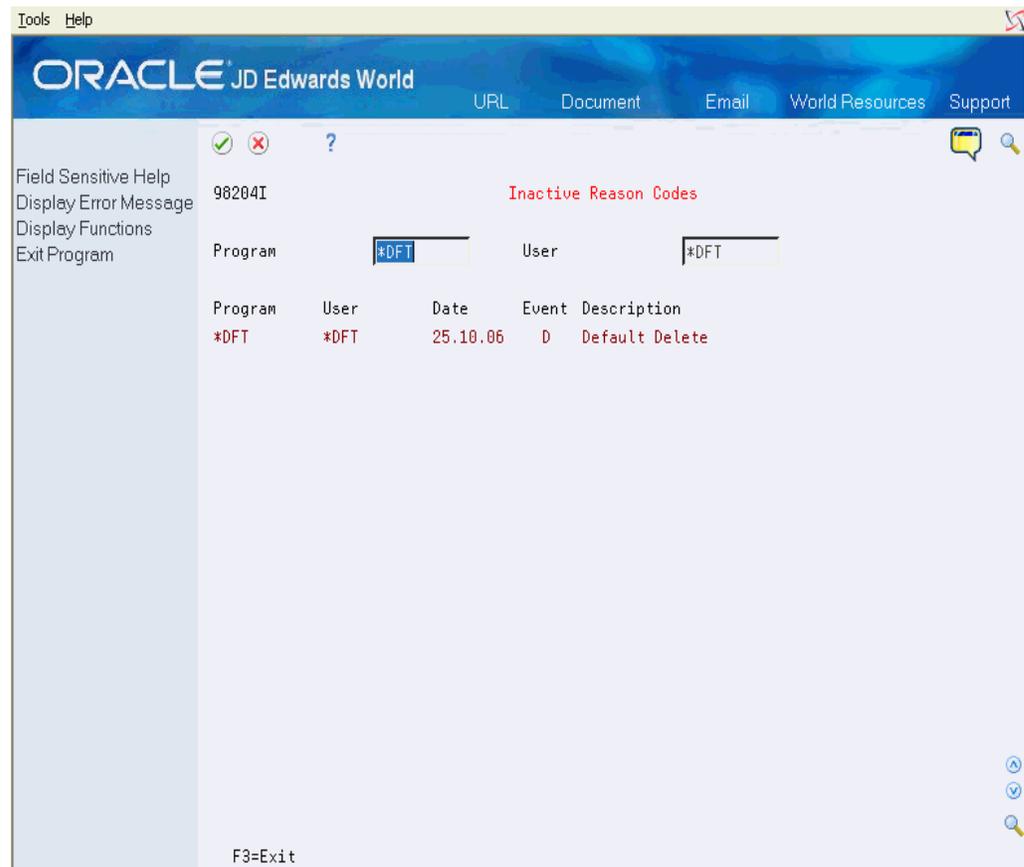
| Function Key | Task |
|-------------------|--|
| Exit Program (F3) | Returns the Reason Code Maintenance (P90204) |

2.12 Inactive Reason Codes (P98204I)

The Inactive Reason Codes (P98204I) screen lists reason codes that are no longer associated with an update program. Reason codes are codes that associate reasons with events recorded in the audit file.

Display Inactive Reason Codes (P98204I) screen by entering 1 in the option field of a program listed on the Reason Code Maintenance (P98204) screen.

Figure 2–12 Inactive Reason Codes screen



The Inactive Reason Codes (P98204I) screen provides the following information for each inactive reason code listed.

| Field | Explanation |
|---------|--------------------------------------|
| Program | The program if the reason code. |
| User | The user. |
| Date | The date the reason became inactive. |

| Field | Explanation |
|-------------|-------------------------------------|
| Event | A – Add C – Change D – Delete |
| Description | A description of the reason code. |

In addition to the options, there is one function key exit:

| Function Key | Task |
|-------------------|---|
| Exit Program (F3) | Returns to the Database Audit Manager (G946). |

2.13 Electronic Signature (P98208)

An electronic signature is validation of the user credentials, a confirmation that the user identity is known and has been established. The electronic signature is carried along with the transaction for auditing trail and logging purposes.

You are prompted for credential validation before continuing with this database transaction because the Database Audit Manager is monitoring the file and transactions to this file require an electronic signature.

Figure 2–13 Credential Validation Window

The screenshot shows a window titled 'Functions Tools Help'. The main content area has a light blue background. In the top right corner, the text 'P01051' and 'Deletion' is displayed in red. Below this, there are two input fields: 'User' with the value 'LS5697353' and 'Password' which is empty. Underneath the password field is a table with three columns: 'Transaction', 'Description', and 'Note'. The first row of the table contains the value '1' in the 'Transaction' column, 'delete' in the 'Description' column, and an empty text box in the 'Note' column.

The Electronic Signature (P98208) screen has the following fields:

| Field | Explanation |
|------------------------------|--|
| User | The User ID. |
| Password | The password for the User ID. |
| Transaction Description Note | The text provided for the transaction performed. |

The Electronic Signature (P98208) screen has the following function key:

| Function Key | Task |
|-----------------------|--|
| Exit Program (F3) | Returns to calling program. |
| Associated Text (F14) | Displays the Associated Text (P98209D) screen, allowing additional text to be attached to the audit file record. |

2.14 Associated Text Search (P98209)

The Associated Text Search display is used to access associated text. Various search criteria can be specified to zero in on specific items.

Figure 2–14 Associated Text Search screen

The screenshot shows the Oracle JD Edwards World interface for the Associated Text Search screen (P98209). The title bar includes 'Tools Help' and 'ORACLE JD Edwards World'. The main window has a blue header with navigation links: 'URL', 'Document', 'Email', 'World Resources', and 'Support'. Below the header, there are icons for search and help. The screen is divided into several sections:

- Left Panel:** A vertical menu with options: 'Field Sensitive Help', 'Display Error Message', 'Display Functions', 'Exit Program', and 'Add New Text'.
- Search Criteria Section:** Fields for 'Subject', 'Category', 'From Date', and 'Through Date'. There are also fields for 'Audit Log File' and 'Audit Log Lib'.
- Results Table:** A table with columns: 'Title', 'Author', 'Created On', and 'Chg Date'. The table contains 15 rows of test data.
- Footer:** 'F3=Exit Opt: 1=Header 2=Text' and a 'Bottom' button.

| Title | Author | Created On | Chg Date |
|------------------------------|-----------|------------|------------|
| T08-S08-C08-H08-AUD08-@TEST2 | GB284234A | 11.01.2006 | 24.01.2006 |
| T09-S09-C09-H09-AUD09-@TEST | GB284234B | 10.01.2006 | 07.02.2008 |
| T10-S10-C10-H10-AUD10-@TEST2 | GB284234 | 09.01.2006 | |
| T11-S11-C11-H11-AUD11-@TEST | GB284234A | 08.01.2006 | |
| T12-S12-C12-H12-AUD12-@TEST2 | GB284234B | 07.01.2006 | |
| T13-S13-C13-H13-AUD13-@TEST | GB284234 | 06.01.2006 | |
| T14-S14-C14-H14-AUD14-@TEST2 | GB284234A | 05.01.2006 | |
| T15-S15-C15-H15-AUD15-@TEST | GB284234B | 04.01.2006 | |

The Associated Text Search (P98209) screen has the following fields:

| Field | Explanation |
|----------------|---|
| Author | The IBM-defined user profile. |
| Subject | Displays the Selection List (P98209X) screen. |
| Category | Displays the Selection List (P98209X) screen. |
| From Date | Displays the Calendar. |
| Audit Log File | Displays the Selection List (P98209X) screen. |
| Through Date | Displays the Calendar. |
| Audit Log Lib | Displays the Selection List (P98209X) screen. |

The Associated Text Search (P98209) screen has the following options:

| Option | Task |
|--------|----------------------------|
| 1 | Work With Text Header. |
| 2 | Work With Associated Text. |

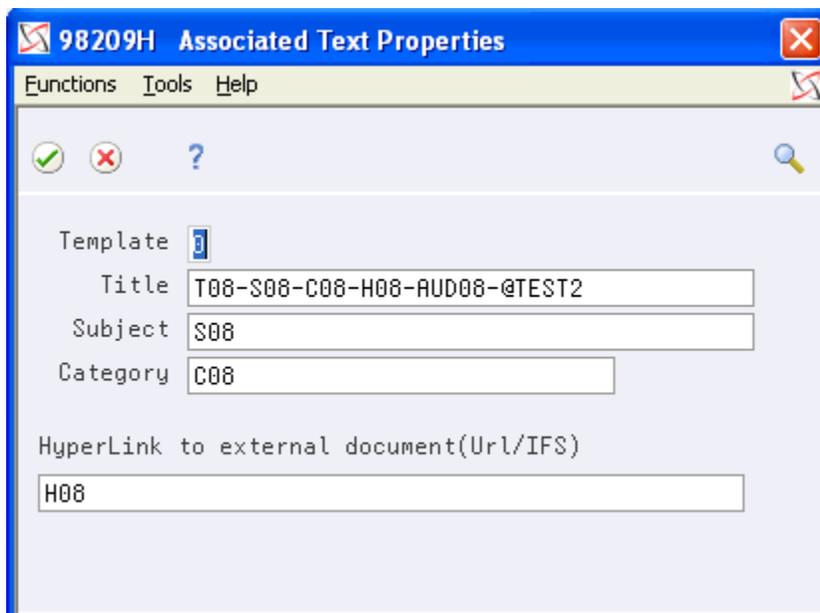
The Associated Text Search (P98209) screen has the following function key exits:

| Function Key | Task |
|-------------------|-----------------------------|
| Exit Program (F3) | Returns to calling program. |

2.15 Associated Text Properties (P98209H)

The Associated Text Properties panel is used to label text with a title, subject, and category, and also associate the text with a document connected by a URL. The URL can be a hotlink to an IFS directory or a server accessible through your web browser.

Figure 2–15 Associated Text Properties Window



The Associated Text Properties (P98209H) screen has the following fields:

| Field | Explanation |
|--|---|
| Template | Identifies the group of text as a template. |
| Title | Title name given to a group of text. |
| Subject | Displays the Selection List (P98209X) screen. |
| Category | Displays the Selection List (P98209X) screen. |
| Hyperlink to external document (URL/IFS) | Hyperlink to a document that is associated with this group of text. |

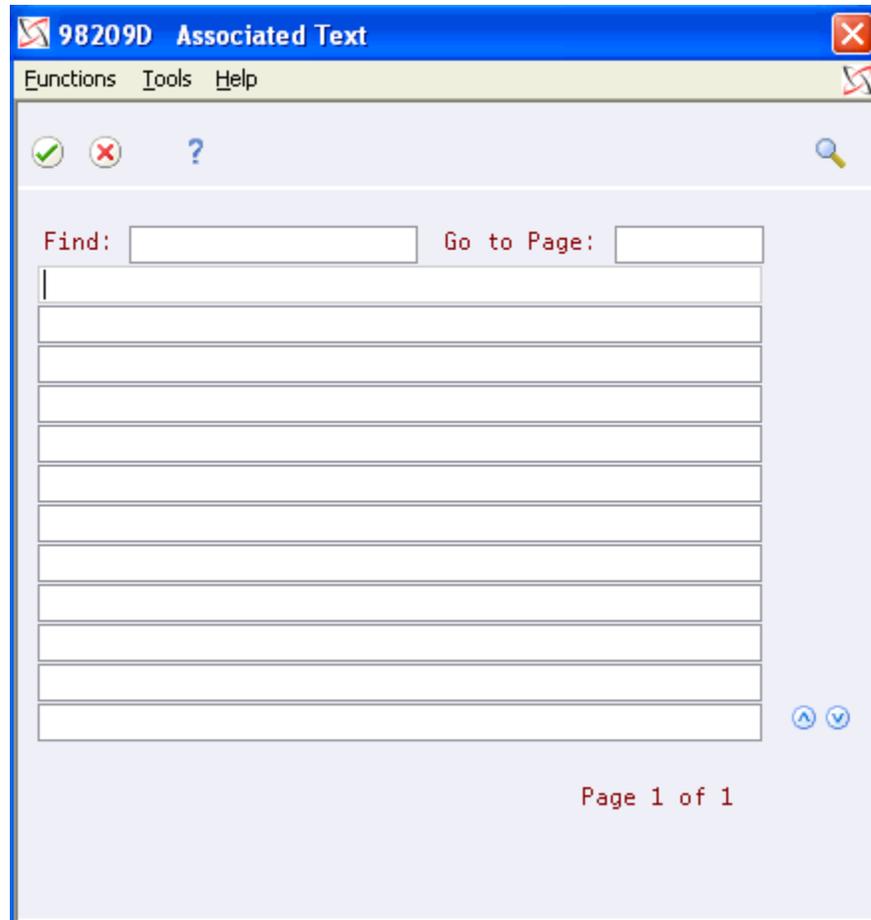
The Associated Text Properties (P98209H) screen has the following function key exit:

| Function Key | Task |
|-------------------|-----------------------------|
| Exit Program (F3) | Returns to calling program. |

2.16 Associated Text (P98209D)

The associated text editor enables free form text entry. Editing functions and capabilities are more robust than the Generic Text editor. Work is saved in a temporary workspace then applied to the production file upon exiting the editor.

Figure 2–16 Associated Text Window



The Associated Text (P98209D) screen has the following fields:

| Field | Explanation |
|------------|--|
| Find | Search criteria you need to find. |
| Go To Page | The system takes you to the page number you typed, if it is available. |
| Editor | Free form text entry. |

The Associated Text (P98209D) screen has the following function key exits:

| Function Key | Task |
|---|--|
| Exit Program (F3) | Returns to calling program. |
| Position Cursor to Command Line (F10) | Position Cursor to Command Line. |
| Position Cursor to Page Number (F11) | Position Cursor to Page Number. |
| Toggle Command Line Display (F13) | Toggle Command Line Display. |
| Insert Line at Cursor Position (F14) | Insert Line at Cursor Position. |
| Split Text Line at Cursor Position (F15) | Split Text Line at Cursor Position. |
| Scan Forward for Text from Cursor (F16) | Scan Forward for Text from Cursor. |
| Scan Backwards for Text from Cursor (F17) | Scan Backwards for Text from Cursor. |
| Copy Text Line at Cursor Position (F18) | Copy Text Line at Cursor Position. |
| Merge Text Line Below up to Cursor Line (F19) | Merge Text Line Below up to Cursor Line. |
| Display Text Properties (F20) | Display Text Properties. |
| Delete Line at Cursor Position (F23) | Delete Line at Cursor Position. |

2.17 Selection List (P98209X)

The Associated Text Search Selection List (P98209X) is the cursor help program for the Associated Text Search program. Since the descriptive columns such as subject, category, etc. are free form entry fields, this window will dynamically build the query list to display all values for the requested column you selected.

Figure 2-17 Selection List Window



The Selection List (P98209X) screen has the following fields:

| Field | Explanation |
|-------------|--|
| Description | A description of the available selections. |

The Selection List (P98209X) screen has the following function key exit:

| Function Key | Task |
|-------------------|-----------------------------|
| Exit Program (F3) | Returns to calling program. |

This chapter contains these topics:

- [Section 3.1, "Setting Up an Audit Process,"](#)
- [Section 3.2, "Editing an Audit File,"](#)
- [Section 3.3, "Deleting an Audit Process from a File,"](#)
- [Section 3.4, "Displaying Triggers for a File,"](#)
- [Section 3.5, "Maintaining Reason Codes,"](#)
- [Section 3.6, "Changing Configuration Defaults."](#)

3.1 Setting Up an Audit Process

This chapter provides instructions for the most frequent tasks performed with the Database Audit Manager (G946).

Navigation

From Advanced and Technical Operations (G9), choose Security Officer

From Security Officer (G94), choose Database Audit Manager

From Database Audit Manager (G946), choose Audit Manager Workbench

Use the Audit Manager Workbench (P98200) to set up new or change existing audit configurations. Setting up an audit consists of the following tasks:

- Adding a data file
- Executing the build process
- Activating the audit

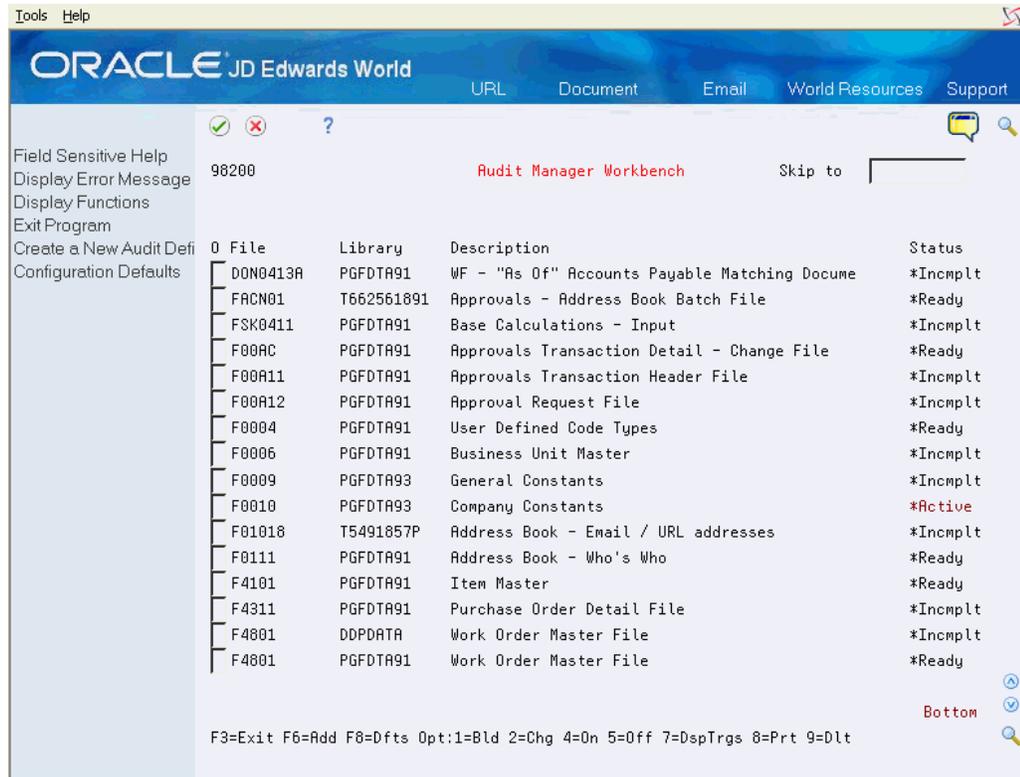
3.1.1 Before You Begin

- Know the library that contains the file to audit
- Default must be set up using the Audit Configuration Defaults (P98201)
- Default must be set up using the Reason Code Maintenance (P98204)

To add a data file

On Audit Manager Workbench (P98200)

Figure 3–1 Audit Manager Workbench screen



1. Choose Add (F6). The File List (P98200X) screen displays a list of the database files in a selected library. Highlighted files are currently being audited. (Depending on the number of files in the library, the response may take several seconds to display the list of files.)
2. Type 1 in the O (Option) field to select a file. Choose Enter to display the Audit Definition Parameters (P98202) screen.

Figure 3–2 Audit Definition Parameter screen

Tools Help

ORACLE JD Edwards World URL Document Email World Resources Support

Field Sensitive Help 98202 Audit Definition Parameters
 Display Error Message
 Display Functions
 Exit Program

Database File
 File Name F0030I
 Library PGFDTA93
 Description Bank Transit Number Tag File

Audit Log File
 File Name
 Library JDFAUDIT

Trigger Program
 Program Name
 Library JDFAUDIT

Electronic Signature
 Require Signature Blank=None,1=Transactional,2=Record Lvl

Trigger Activation Mode. I=Interactive,B=Batch

F3=Exit

3. Complete the following fields:

- File Name
- Program Name
- Electronic Signature
- Trigger Activation Mode

Note: If you select the trigger activation mode B, for Batch, you can use Sleeper to schedule field selection changes without interrupting users.

4. The Field Selection List (P98203) screen displays.

Figure 3-3 Field Selection List screen

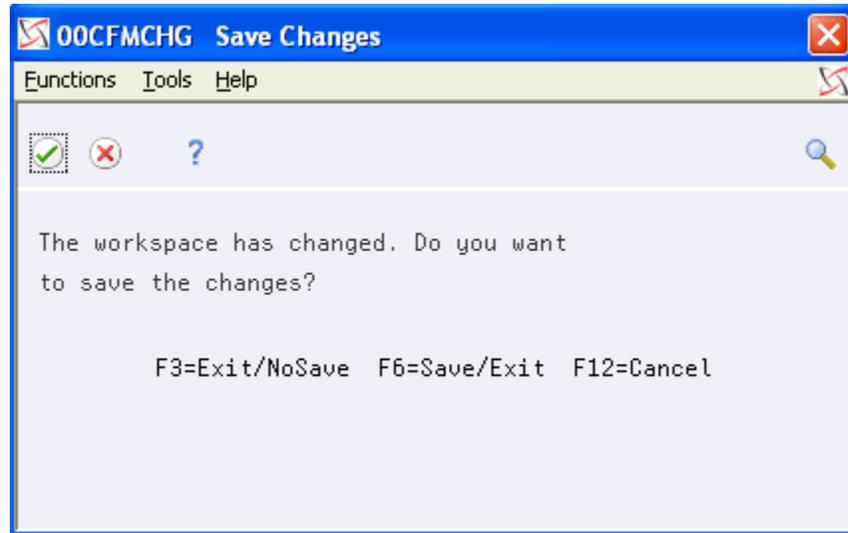


5. Type 1 in the O (Option) to select the data fields that will be recorded in the audit file for informational purposes only.
6. Type 2 in the O (Option) field of the data fields that will trigger the audit program when an action on the file occurs.

Note: Record adds and deletions are always written to the audit log file. Changes to the selected fields will trigger those changes to be recorded to the audit log file. Selecting fields with a 2 slows system performance. Limit the use of 2 to fields that must be audited. At least one field must contain a 2.

7. Choose Enter to accept the entry.
8. Choose Exit (F3). The Save Changes (P00CFMCHG) screen displays.

Figure 3-4 Save Changes Window

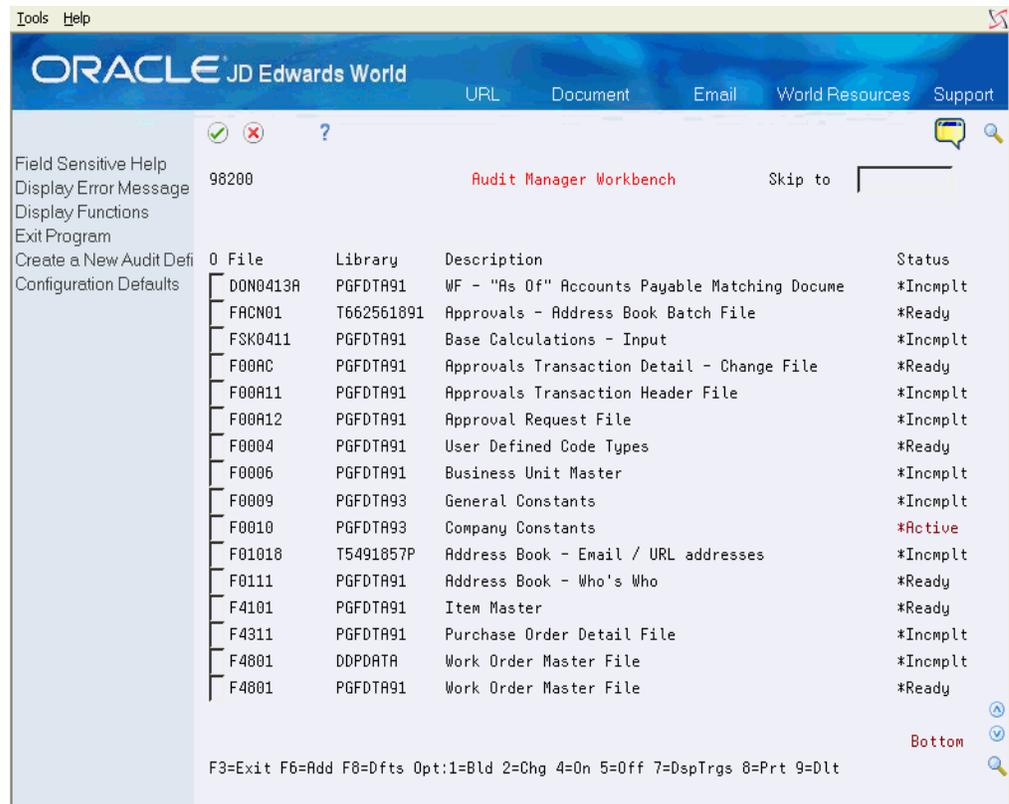


9. Choose Enter to confirm the fields selected. The Audit Manager Workbench (P98200) screen, displays with the status of *Incmlpt. This indicates that changes can still be made to the fields selected.

To build the audit

On Audit Manager Workbench (P98200)

Figure 3-5 Audit Manager Workbench screen



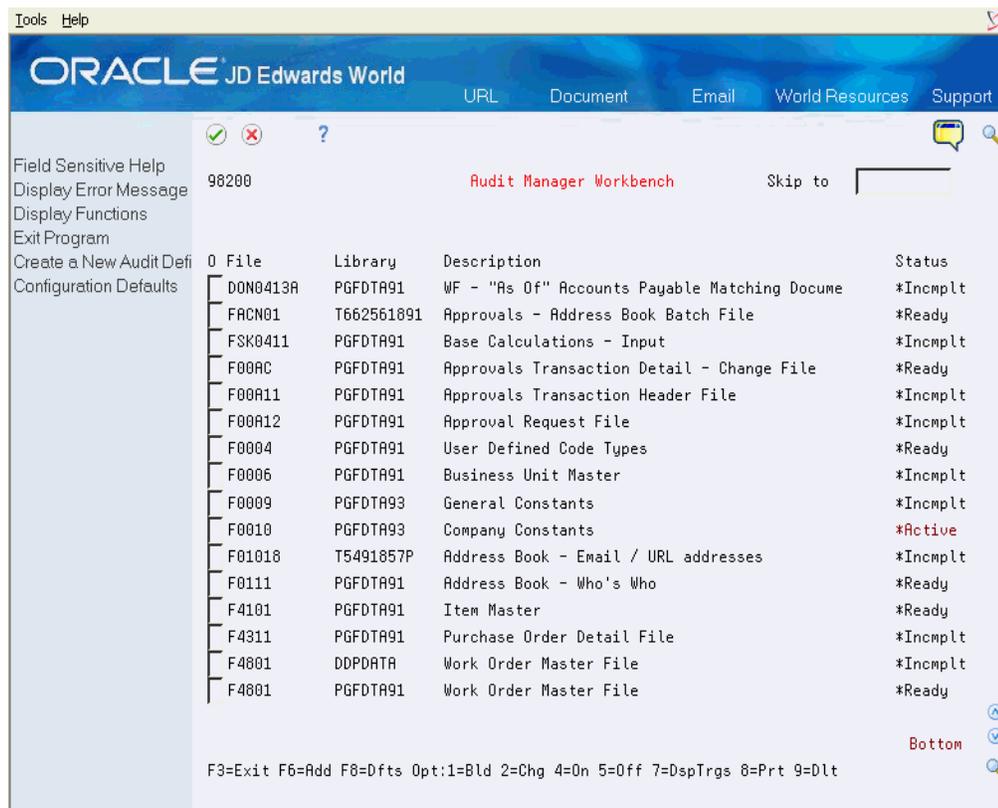
1. Enter 1 in the O (Option) field to select the file you wish to build.
2. Choose Enter. When the build is complete, the status changes to *Ready. This indicates that fields may not be changed or added without rerunning the build process.

Note: If the build errors, you will need to edit the setup information.

3.1.2 Place the triggers on the file

On Audit Manager Workbench (P98200)

Figure 3-6 Audit Manager Workbench screen



1. To start the audit process, type 4 in the O (Option) field to select the file.
2. Choose Enter. The status of the file becomes *Active.

Note: To add the trigger to the file requires an exclusive file allocation thus no users may be accessing the file when triggers are activated. Use sleeper to schedule activation at a time when the file will be available.

3.2 Editing an Audit File

Navigation

From Advanced and Technical Operations (G9), choose Security Officer

From Security Officer (G94), choose Database Audit Manager

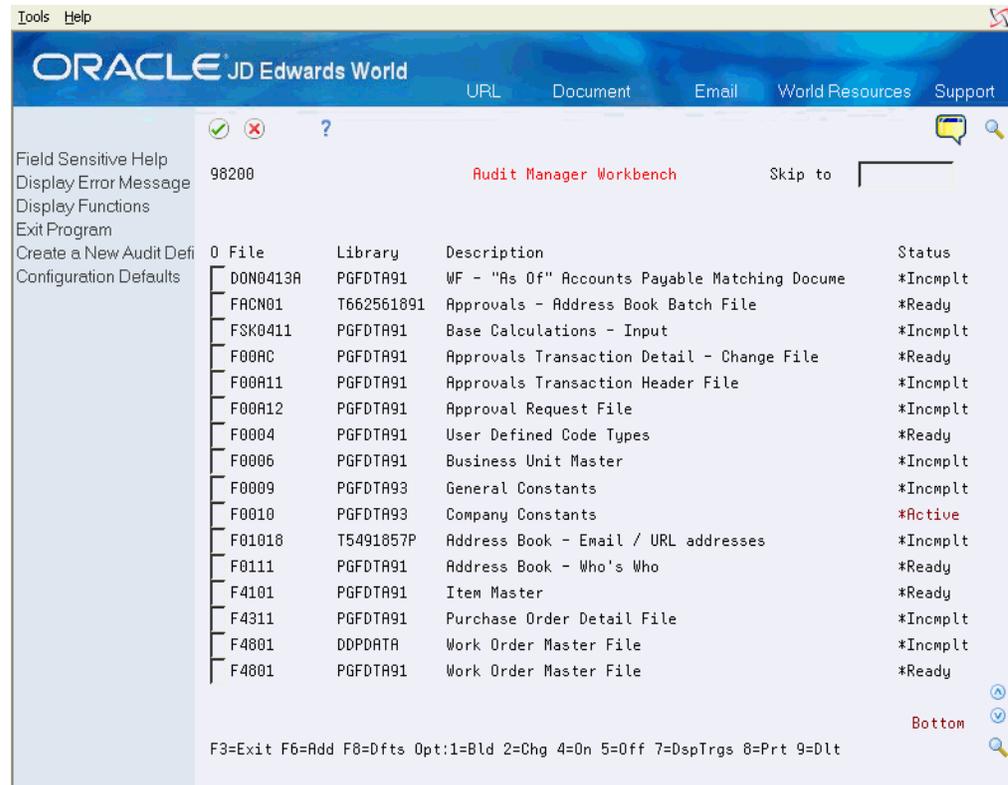
From Database Audit Manager (G946), choose Audit Manager Workbench

It is possible that a file already defined for audit requires changes. However, different steps may need to be performed based on the status of the audit. Once a file has been set up and is active, fields may no longer be removed from the process.

To change audit file setup

On Audit Manager Workbench (P98200)

Figure 3–7 Audit Manager Workbench screen



1. Type 2 in the O (Option) field to select the file to be changed. Choose Enter to display the Change Audit Definition (P98200W) screen.

Figure 3-8 Change Audit Definition Window



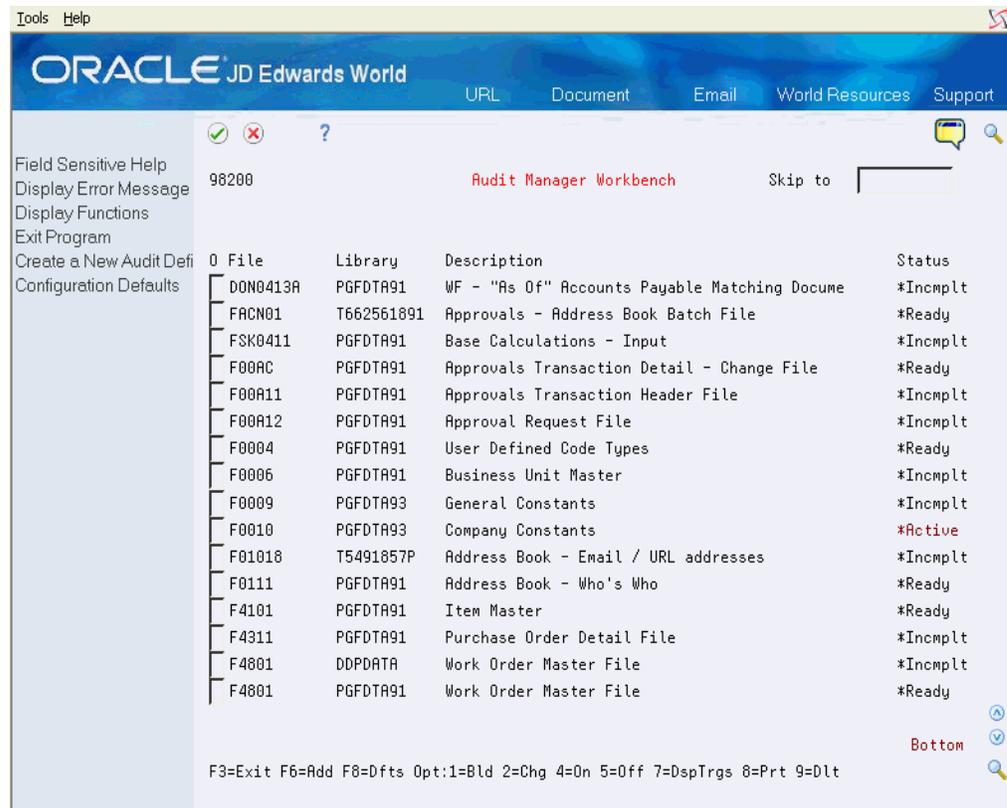
2. Type 1 in the Sel (Selection) field of the line indicating the type of information you need to change. Select any or all of the following:
 - Audit Definition Parameters (P98202)
 - Field Selection List (P98203)
 - Add/Change Reason Codes (P98204)

The selected screen displays.

3. Overtyping the information on the screen with your changes. Some information is protected when the status is *Active and cannot be changed.
4. Choose Enter.

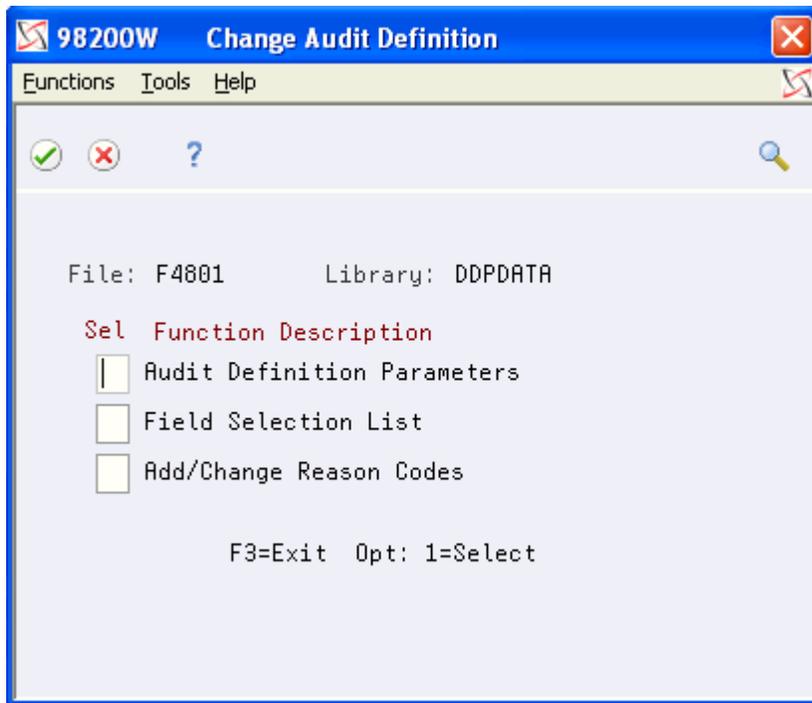
To add a field to an existing audit file where the status is *Active
 On Audit Manager Workbench (P98200)

Figure 3–9 Audit Manager Workbench screen



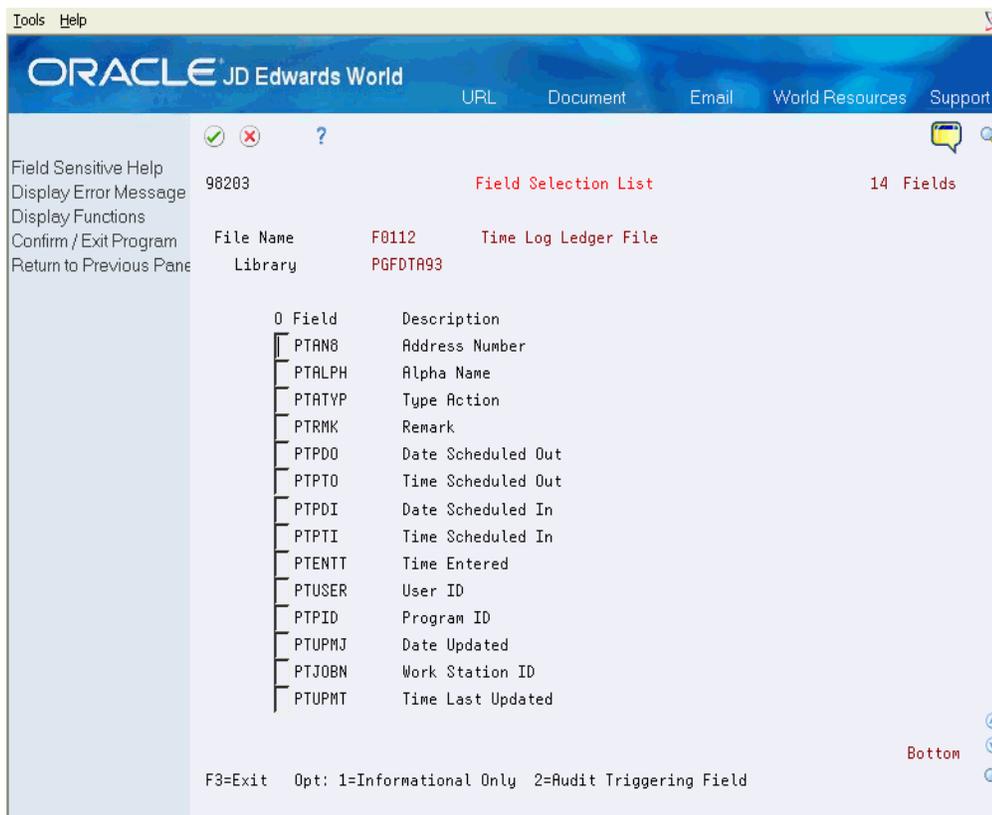
1. To remove triggers from a file, type 5 in the O (Option) field to select a file. Choose Enter to remove the triggers.
2. To make a change to the triggers for a file, type 2 in the in the O (Option) field for the file. Choose Enter to display the Change Audit Definition (P98200W) screen.

Figure 3–10 Change Audit Definition Window



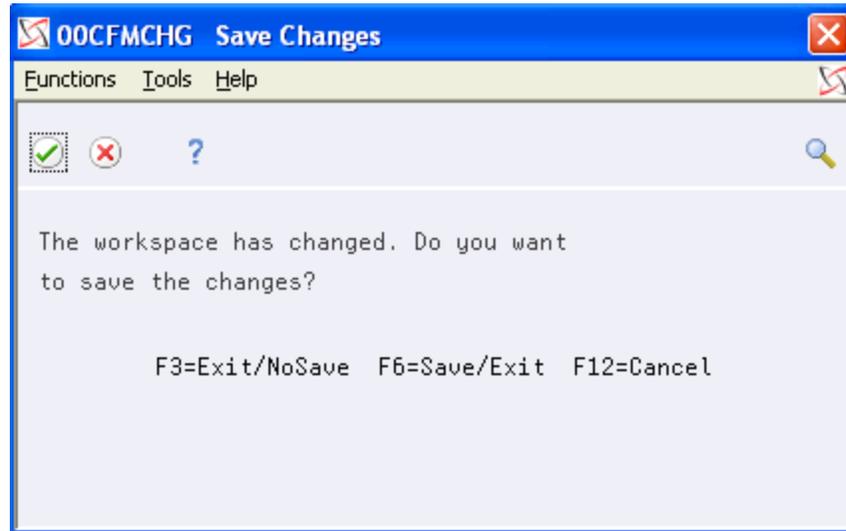
3. Type a 1 in the Sel (Selection) field for Field Selection List. Choose Enter to display the Field Selection List (P98203) screen.

Figure 3–11 Field Selection List screen



4. Do one of the following to select the additional fields required:
 - Type 1 in the O (Option) field to write the field to the audit file for informational reasons only
 - Type 2 in the O (Option) field to write a record to the audit file.
5. Choose Exit (F3) to display the Save Changes screen (P00CFMCHG).

Figure 3–12 Save Changes Window



6. Choose Enter to save the changes and display the Audit Manager Workbench (P98200).
7. On Audit Manager Workbench, enter 1 in the Option field to build the new file definition.
8. From a command line, use the IBM command DSPFFD to verify the new fields were added to audit file. The fields will appear at the end of the list.
9. On Audit Manager Workbench, enter 4 in the Option field to place the triggers back on the selected file.

Note: Adding additional fields to an audit log file that already contains data means that those newly added fields will contain no data for existing records. Data will only be recorded into those fields after they have been added and the trigger rebuilt and reactivated.

3.3 Deleting an Audit Process from a File

Navigation

From **Advanced and Technical Operations (G9)**, choose **Security Officer**

From **Security Officer (G94)**, choose **Database Audit Manager**

From **Database Audit Manager (G946)**, choose **Audit Manager Workbench**

To delete an audit configuration, you must perform the following tasks:

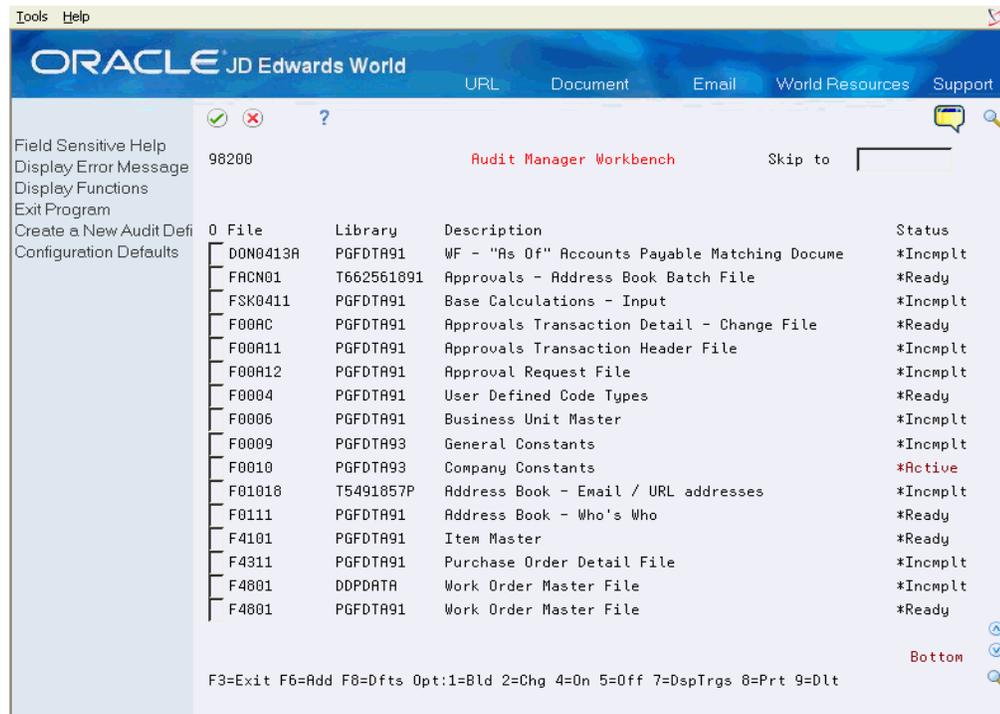
- Remove audit triggers from the file

- Delete the audit configuration

To remove audit triggers from a file

On Audit Manager Workbench (P98200)

Figure 3–13 Audit Manager Workbench screen



1. Type a 5 in the O (Option) field to select a file.
2. Choose Enter to turn off or remove the triggers from the file.

To delete a trigger program

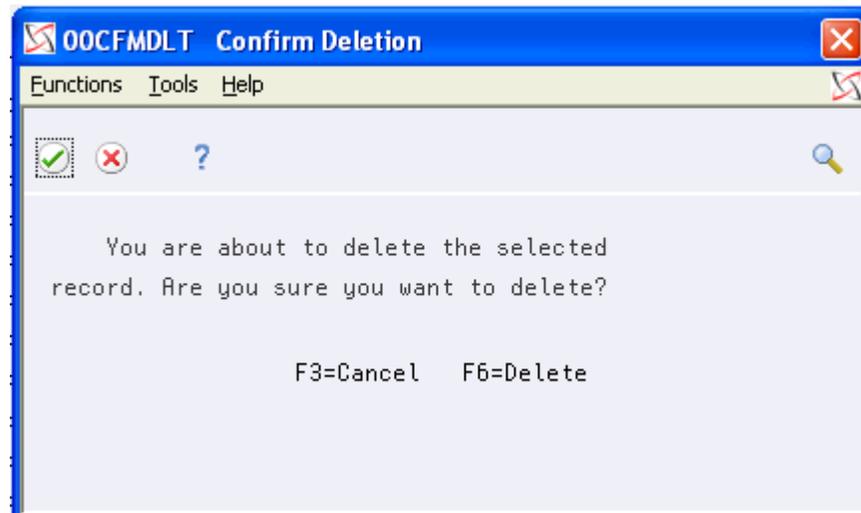
On Audit Manager Workbench (P98200)

Figure 3–14 Audit Manager Workbench screen



1. In the Option field, type 9 and choose Enter to display the Confirm Delete screen.

Figure 3–15 Confirm Deletion Window



2. From the Confirm Deletion (P00CFMDLT) screen, choose Enter to delete the configuration objects and setup records.

Note: This process deletes the trigger programs and removes the records from the setup and program SVR files only. It does not delete the audit file or the audit file SVR record. Federal regulations require the records in the audit files are kept.

3.4 Displaying Triggers for a File

Navigation

From Advanced and Technical Operations (G9), choose Security Officer

From Security Officer (G94), choose Database Audit Manager

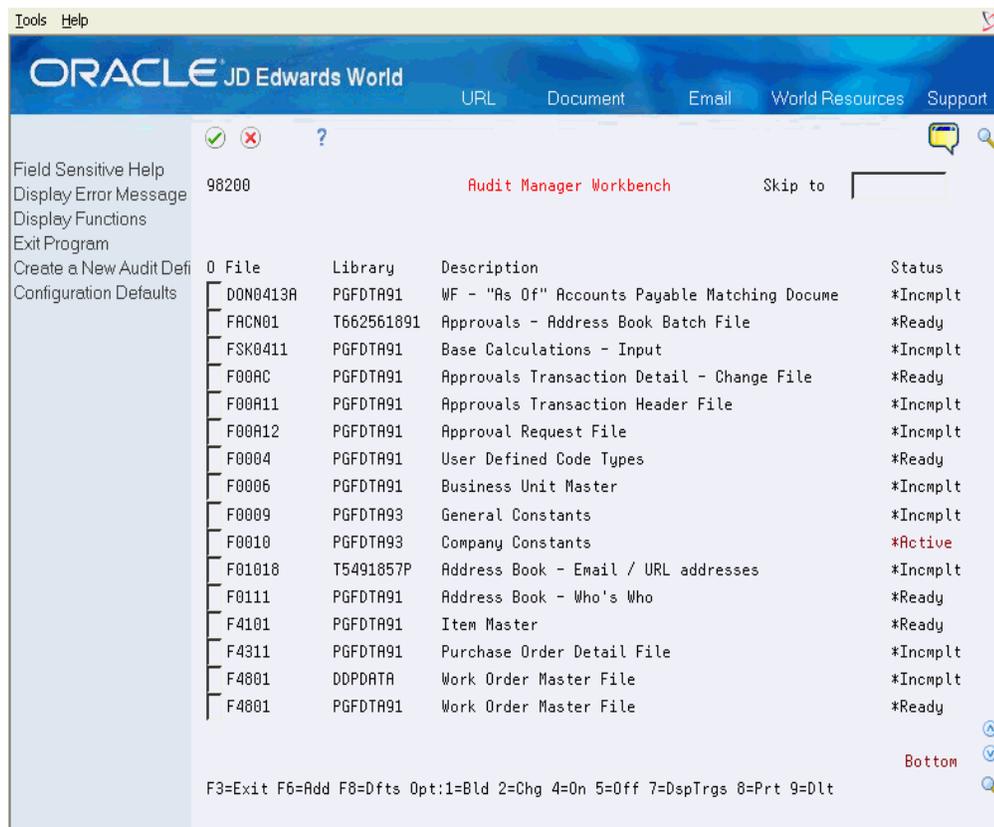
From Database Audit Manager (G946), choose Audit Manager Workbench

Before you define new triggers for a file, check the file for pre-existing triggers. If the IBM release is prior to V5R1 and the file has pre-existing triggers, these triggers may be overwritten with the new audit triggers.

To display triggers defined for a file

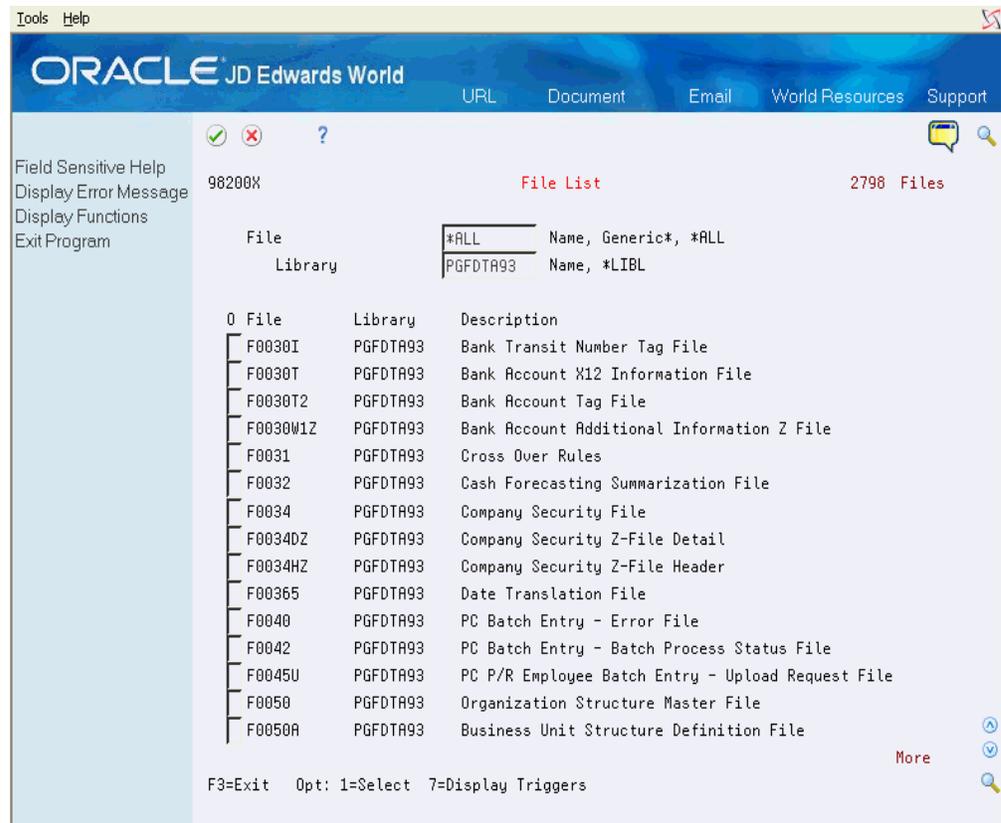
On Audit Manager Workbench (P98200)

Figure 3–16 Audit Manager Workbench screen



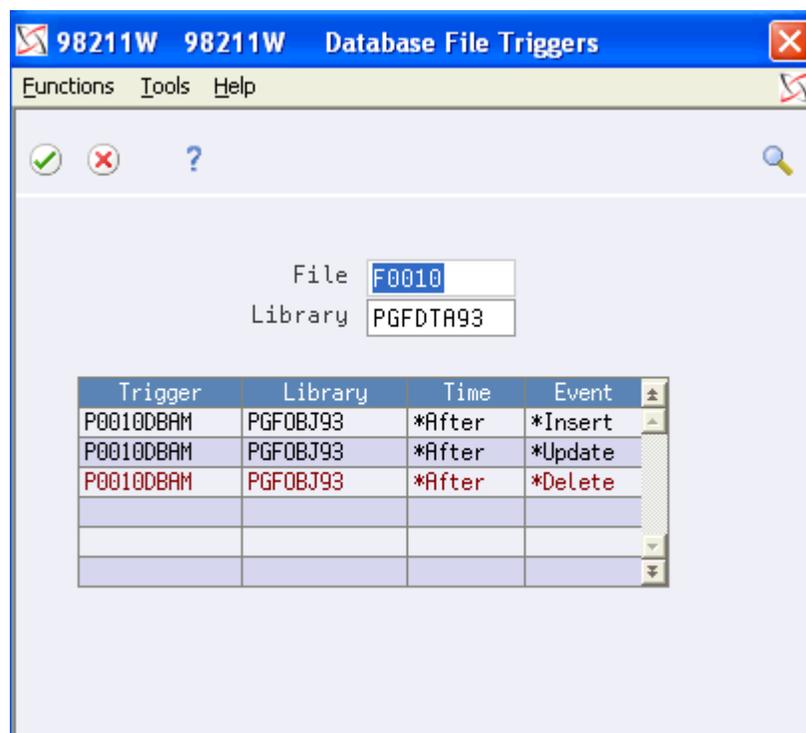
1. Choose Add (F6) to display the Files List (P98200X) screen.

Figure 3–17 File List



2. Enter 7 in the O (Options) field to view attached triggers of the selected file.

Figure 3–18 Database File Triggers Window



- On Database File Triggers (P98211W), view the trigger programs defined on the file selected.

3.5 Maintaining Reason Codes

Navigation

From Advanced and Technical Operations (G9), choose Security Officer

From Security Officer (G94), choose Database Audit Manager

From Database Audit Manager (G946), choose Reason Code Maintenance

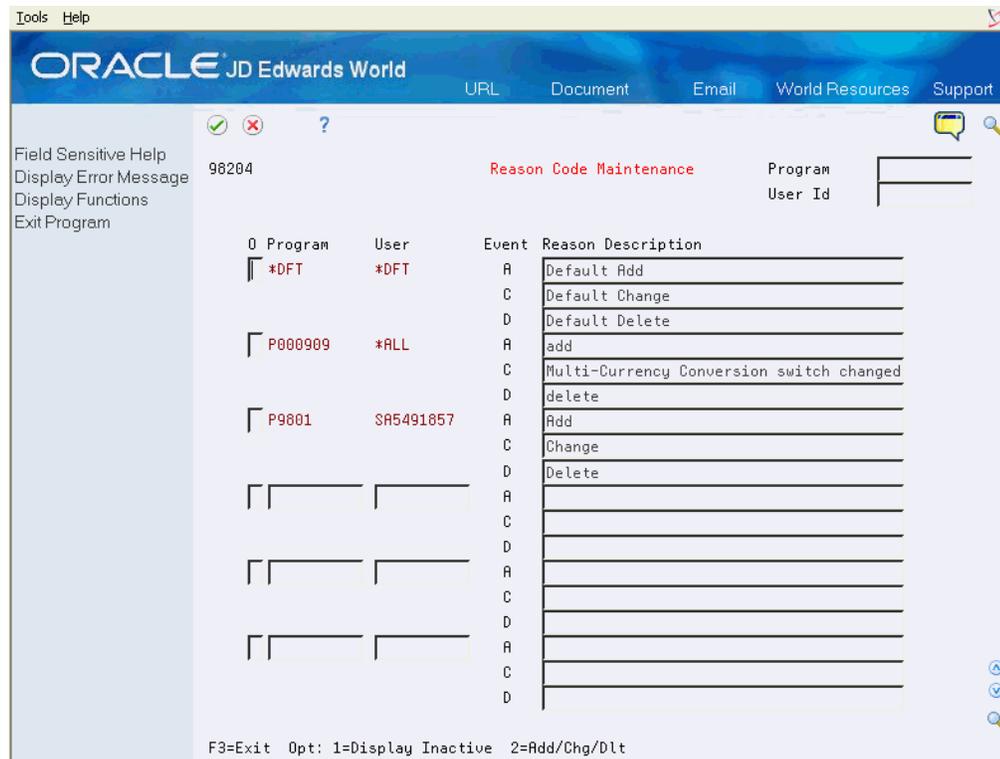
Reason codes are codes that are associated with text. The text describes the type of change made to a data field in a file. When you make a change that triggers an audit process, the reason code in the target file identifies what type of change was made to the data fields in the audited file. Using the Reason Code Maintenance (P98204) screen, you can do the following:

- Add reason codes to a new program
- Edit reason codes
- Search for a reason code
- View inactive reason codes

To add reason codes to a new program

On Reason Code Maintenance (P98204)

Figure 3–19 Reason Code Maintenance screen



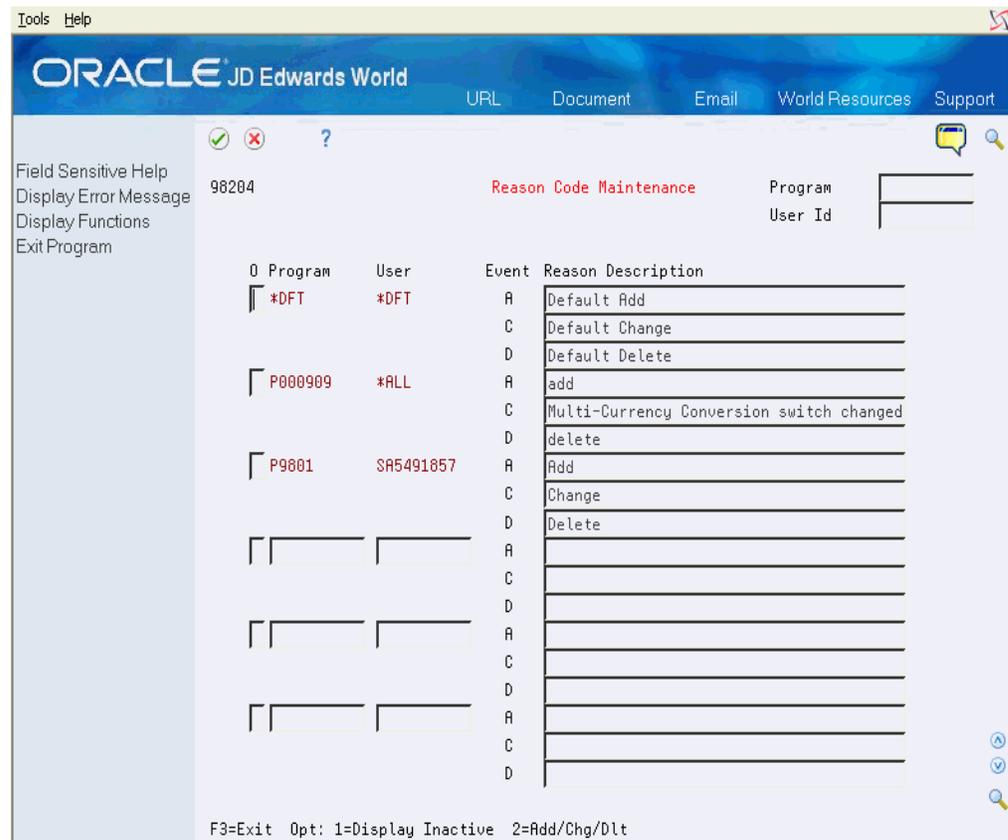
- Page down to the first blank line.

2. In the O (Option) field, type 2.
3. Complete the following fields:
 - Program
 - User
 - Reason Description
4. Choose Enter to complete adding the reason code.

To edit reason codes for a program

On Reason Code Maintenance (P98204)

Figure 3–20 Reason Code Maintenance screen

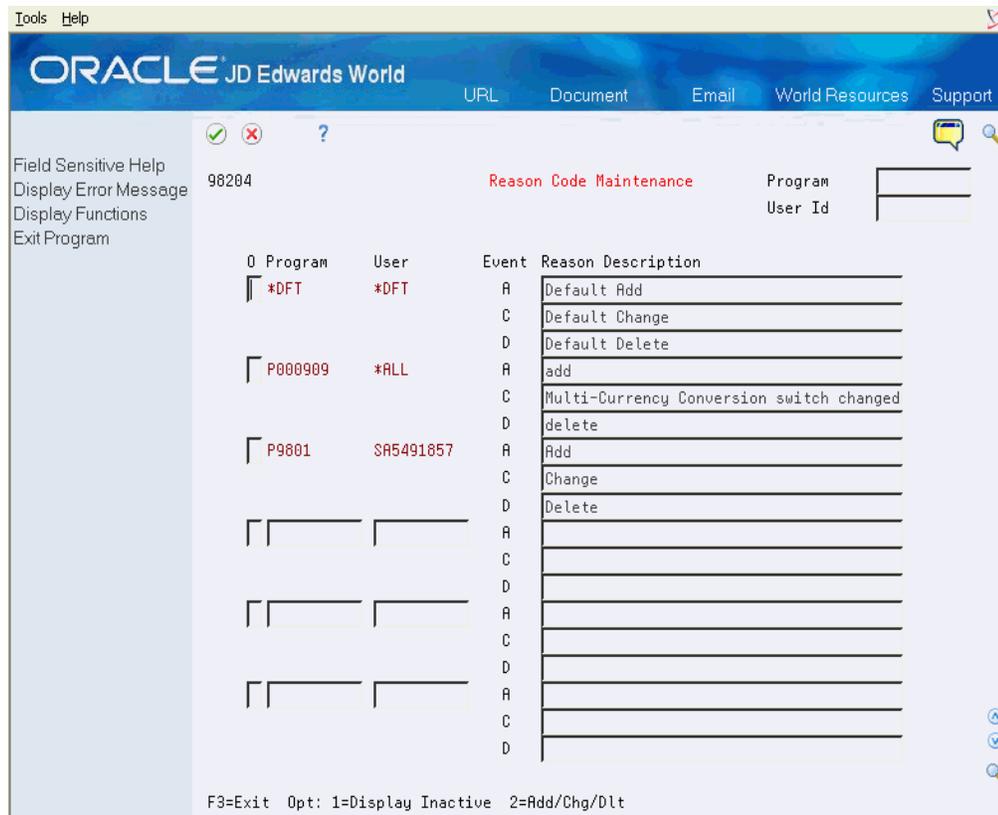


1. Type 2 in the O (Option) field of the reason codes you want to edit.
2. Complete the following field:
 - Reason Description
3. Choose Enter to complete the edit.

To search for reason codes

On Reason Code Maintenance (P98204)

Figure 3-21 Reason Code Maintenance screen

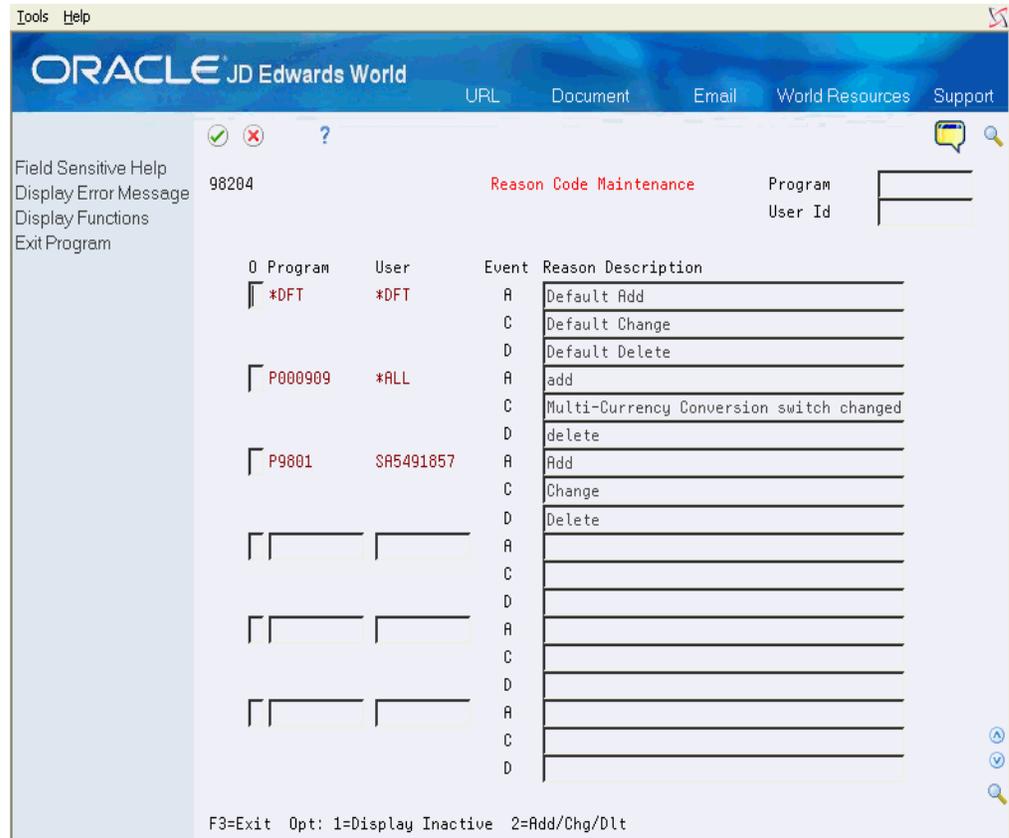


1. Complete one or both of the following fields at the top of the screen:
 - Program
 - User
2. Choose Enter. The screen displays the reason codes that match the search criteria entered.

To view inactive reason codes

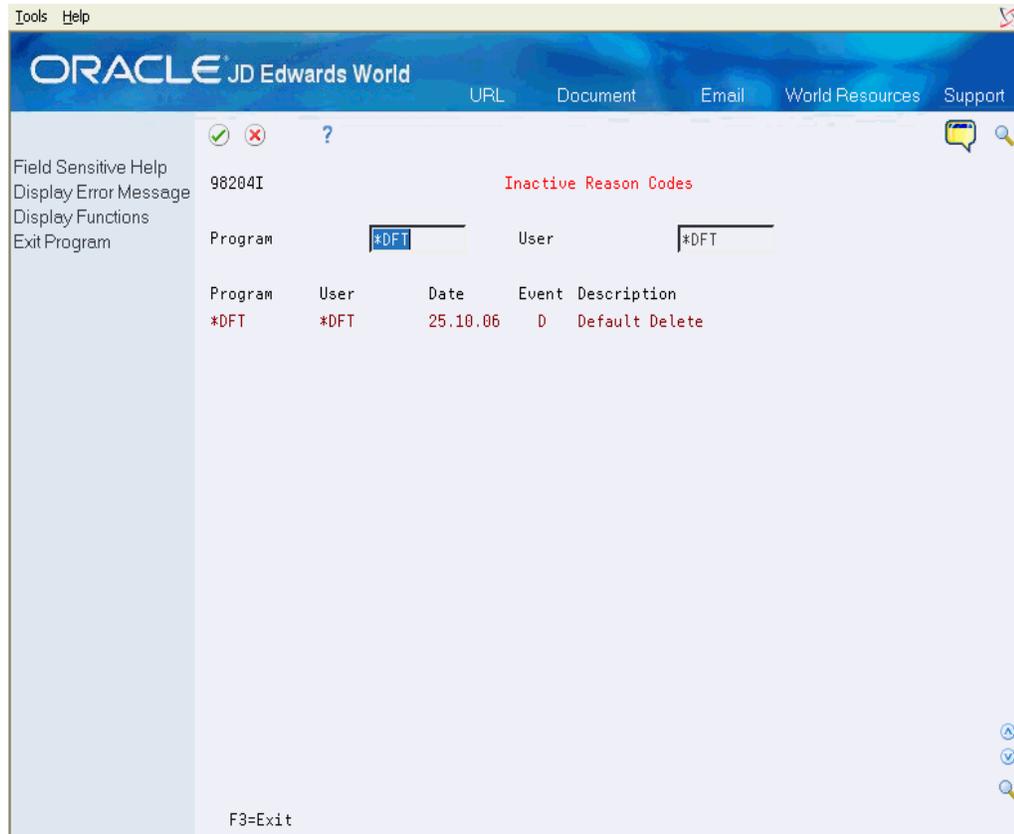
On Reason Code Maintenance (P98204)

Figure 3-22 Reason Code Maintenance screen



1. Type 1 in the O (Option) field for a program.

Figure 3–23 Inactive Reason Code screen



2. View the inactive reason codes associated with the program on the Inactive Reason Codes (P98204I) screen.

3.6 Changing Configuration Defaults

Navigation

From **Advanced and Technical Operations (G9)**, choose **Security Officer**

From **Security Officer (G94)**, choose **Database Audit Manager**

From **Database Audit Manager (G946)**, choose **Audit Configuration Defaults**

Configuration defaults are used by the system to create a new audit process.

To change configuration defaults

On **Audit Configuration Defaults (P98201)**

Figure 3–24 Audit Configuration Defaults screen

Tools Help

ORACLE JD Edwards World URL Document Email World Resources Support

Field Sensitive Help 98201 Audit Configuration Defaults
 Display Error Message
 Display Functions
 Exit Program

Library Locations

| | |
|------------------|----------|
| Database Files | PGFDTR93 |
| Audit Log Files | JDFAUDIT |
| Trigger Programs | JDFAUDIT |

Output Trigger Source

| | |
|-------------|----------|
| Library | JDFAUDIT |
| Source File | JDESRC |

Trigger Source Template

| | |
|-------------|----------|
| Library | JDFSRC93 |
| Source File | JDESRC |
| Member | #BASETRG |

F3=Exit

1. In Library Locations, complete the following fields:
 - Data Files
 - Audit Files
 - Trigger Programs
2. In Output Trigger Source, complete the following fields:
 - Library
 - Source File
3. In Trigger Source Template, complete the following fields:
 - Library
 - Source File
 - Member
4. Choose Enter.

Tips and Techniques

This chapter contains these topics:

- [Section 4.1, "Sleeper,"](#)
- [Section 4.2, "Issues and Assumptions,"](#)
- [Section 4.3, "Impact on Other Applications,"](#)
- [Section 4.4, "Coexistence,"](#)
- [Section 4.5, "Performance Impact,"](#)
- [Section 4.6, "Reporting."](#)

4.1 Sleeper

Sleeper may need to be used when files are open and existing locks prevent triggers from being applied or if the processing is to be done after hours. By running audit programs in batch mode, use Sleeper with hidden selection 82 to hold the JOBQ and release in sleeper at a later time. When using sleeper it is necessary to review the sleeper log for successful completion. For more information about hidden selection 82 or sleeper, refer to the *JD Edwards World Technical Foundation Guide*.

4.2 Issues and Assumptions

OS V5R1 allows you to place multiple triggers on a database file (300). Prior to V5R1, the maximum triggers on a file were six: one for each event (action) Add/Change/Delete, and one for each time *BEFORE/*AFTER the file was updated.

An audit file created using the Database Audit Manager tool cannot be audited by DBAM.

4.3 Impact on Other Applications

Triggers running within interactive jobs have negligible performance impacts. It is the same as taking a menu option, a selection or function exit from another program. Batch jobs are where the impact can be significant as the trigger fires for every record add/change/delete. DBAM trigger code has been highly optimized to minimize performance issues in batch programs as much as possible. For extremely high volume transaction processing, analysis and consideration of trigger removal, then reapplying may be feasible or necessary.

4.4 Coexistence

Customers who are coexistent with both JD Edwards World and JD Edwards EnterpriseOne must determine if the file to be audited is used and maintained by JD Edwards World and JD Edwards EnterpriseOne applications in the designated audit environments. Some customers choose to coexist with certain applications and not others and so it may be difficult to establish if a file is truly coexisting--you can use cross-reference tools to help determine this. If it is found that the file to be audited is maintained by both JD Edwards World and JD Edwards EnterpriseOne, it must be setup under the JD Edwards EnterpriseOne audit tool rather than the JD Edwards World audit tool. If the file is only used and maintained through the JD Edwards World applications, then the file should be setup under the JD Edwards World audit tool.

4.5 Performance Impact

Trigger programs can affect system performance. The generated trigger programs will be designed to minimize adverse system performance.

4.6 Reporting

Reporting on audit files may be created using the JD Edwards World Writer programs. For assistance, contact the JD Edwards World Support Services - JD Edwards World technical.

Each audit file will contain 12 fields in addition to the fields selected on the Field Selection List (P98203) screen. Note the file prefix on these fields will be the same as the file that is setup for auditing; this is used to avoid any possible duplication of fields from the audited file.

| Name | Description |
|-------------|----------------------------------|
| TRGEVT | Trigger event (A/C/D) |
| RCDIMP | Record image type (Before/After) |
| SRLNBR | Reason code serial number |
| ESGVFY | Signature verified |
| ESGUSR | Signature UserID |
| ESGRSN | Signature description reason |
| TXUnid | Associated text key |
| JOBNAM | Updated by Job Name |
| PGMNAM | Updated by Program |
| USERID | Updated by UserID |
| UPDDAT | Updated on Date |
| UPDTIM | Updated at time |

Electronic Signatures

This appendix contains these topics:

- [Section A.1, "Overview,"](#)
- [Section A.2, "Definitions,"](#)
- [Section A.3, "Implementation,"](#)
- [Section A.4, "Two Levels of Signatures,"](#)
- [Section A.5, "Signature Servers,"](#)
- [Section A.6, "Application Program Code Samples."](#)

A.1 Overview

Electronic signature is a regulatory requirement of the Food and Drug Agency (CFR21 Part 11). This regulation states that transaction history logs must be maintained, and database transactions must be authorized and documented at the time of the database transaction. An electronic signature is required for every database transaction that is encompassed by the regulation.

The Database Audit Manager (DBAM) incorporates user configurable database transaction logging, credential verification, and the mechanisms necessary to support documentation of transactions thereby assisting JD Edwards World customers with compliance.

In Release A9.1, electronic signature functionality has been implemented into high priority programs selected based on customer input. This document can be used to implement this functionality in other World programs or custom programs.

JD Edwards World does not provide customer support for programs you customize, including those in which you implement this functionality.

A.2 Definitions

Electronic signature is the process of verifying the credentials, or authenticity, of the user performing or authorizing the record add, change, or delete, at the time of the database transaction, and including that authorization with the transaction in the transaction history log.

Signatures applied to single record updates are referred to as record level signatures. User verification is performed for each and every database transaction. However, to eliminate the continual prompting during transaction processes, subfile programs for example, it is permitted that one signature be applied to the transaction block.

Signatures applied to multiple record updates are referred to as transaction level signatures.

A.3 Implementation

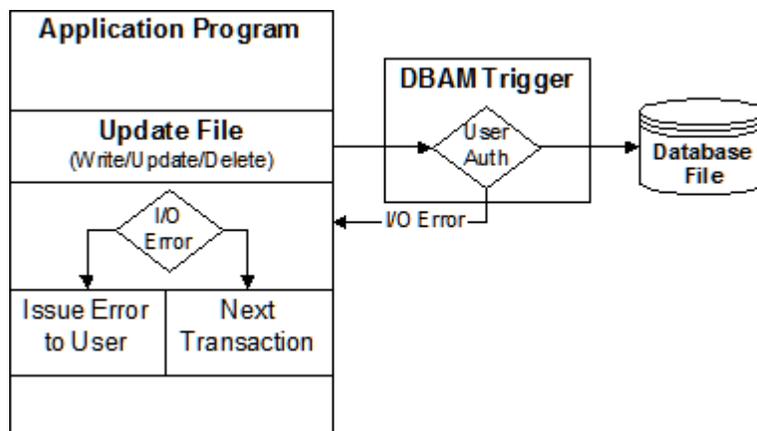
DBAM utilizes database trigger technology for recording transactions and implementing user credential authentication at the time of the database transaction.

A.4 Two Levels of Signatures

A.4.1 Record Level Authorizations

Record level authorizations are implemented by database triggers configured *Before transactions are applied to the database. If user identity is not validated (authorization received), the trigger program will cancel the database action. An I/O error is returned to the application program. The application program must respond to that error and convey it to the user. If authorization is received, the transaction is processed normally.

Figure A-1 Record Level Authorizations



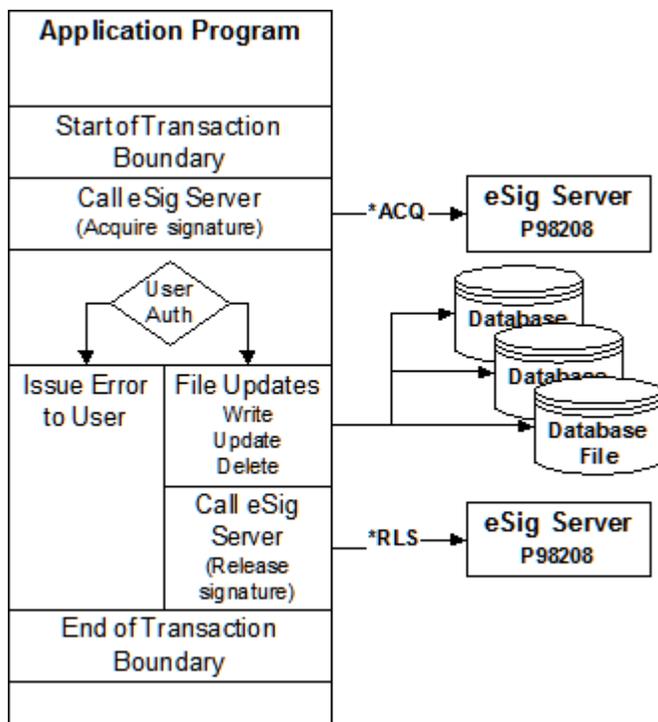
A.4.2 Transaction Level Authorizations

Transaction level authorizations are implemented by database triggers configured *After the transactions have been applied to the database. Application programs determine the boundaries of the transaction, establish the authorization point, obtain the electronic signature, perform the database transactions, and then release the signature.

The application invokes and responds to the server accordingly. If user identity is not validated (authorization received), the program does not process the transactions and conveys the error to the user.

If authorization is received, the transactions are processed. The trigger programs apply the signature to the transactions as they are performed. Following completion of the transactions, the authentication server is called again to release the signature.

Figure A-2 Transaction Level Authorizations



A.5 Signature Servers

DBAM handles user authentication when configured at the record level. The DBAM trigger programs invoke the record level user authentication server. For transaction processing applications, there are two transaction level authentication servers you can use. These two transaction level servers are discussed below.

A.5.1 P98208 Transaction Level Authentication Server

If your application falls under the umbrella of CFR21 regulations, use the P98208 DBAM transaction level authentication server. This server verifies that electronic signature is enabled on the primary transaction file before prompting for user authentication.

Note: If a DBAM audit is not configured on the primary database file, no prompting for signature will occur.

Required Parameter Group

| # | Parameter | Description |
|----|-----------|--|
| 1. | ##PGM | The application program calling the server. If you are using the program status data structure you can load ##PROG to this parameter. Otherwise, use the literal name of your program as in the example below. |
| 2. | ##DBFN | The primary database you are updating for this transaction set. |

| # | Parameter | Description |
|----|-----------|---|
| 3. | ##DBFL | The library name of the primary file. You can use *LIBL for this parameter or if using a file information data structure, the actual file/library opened can be obtain from there: <ul style="list-style-type: none"> ■ FileName at offset 83 ■ Library name at offset 93 |
| 4. | ##DBFA | The transaction type: *ADD/*CHG/*DLT. If you are processing all transaction types within a subfile, use *CHG for the transaction type. |

A.5.2 P00CKPWD Transaction Level Authentication Server (External)

The P00CKPWD server is external from DBAM. It is not dependent upon a DBAM configuration being set up before prompting occurs. It also has these features:

- Backwards compatible to legacy implementations
- DreamWriter ProcOpts control default behavior
- Optional parameters control behavior at runtime
- Can establish a DBAM-compatible transaction level signature

Required Parameter Group

| # | Parameter | Description |
|----|------------|---|
| 1. | ReturnCode | Char(1) - User validation state (Required Parm) |
| | '1' | Users credentials verified. |
| | '0' | Users credentials not verified. |

Optional Parameter Group

| # | Parameter | Description |
|----|-----------|---|
| 1. | Function | Char(4) |
| | *GET | Validate and establish an eSignature |
| | *CLR | Clear the current eSignature |
| 3. | UserId | Char(10) |
| | *CURRENT | Locks userid prompt to current user (job) |
| | *ANYUSER | Opens userid prompt for any userid |
| | *PROCOPT | Uses ProcOpt value from P00CkPwd/ZJDE0001 |
| 4. | eSig | Char(8) |
| | *YES | Establishes an eSignature upon validation |
| | *NO | Does not establish an eSignature |
| | *PROCOPT | Uses ProcOpt value from P00CkPwd/Zjde0001 |
| 5. | PgmName | Char(10) |
| | <Name> | Name of updating program to sign eSignature |
| 6. | eExp | Char(40) |

| # | Parameter | Description |
|---|-----------|--|
| | <Text> | 40 char description to add to eSignature |

Note: When enabling P00CKPWD for electronic signatures, the program invoking it must be changed to call the server again to release the signature when the transaction is completed.

A.6 Application Program Code Samples

Two application program examples are included here. A single record update program impacted by record level signatures, and a subfile transaction processor program that implements transaction level signatures. The single record update program P4108 uses the same file server as the transaction processor P41080. Code segments will vary program to program even if you are handling the file I/O in your program. Programs vary in usage of subroutine S005 or S010 for updating database files.

A.6.1 P4108 - Single record update

This program uses a file server for database I/O. It checks the return code from the server to determine if the database action was successful. If not, it sets on an error indicator. In this program, two more lines were added to set on additional error indicators and set up the error message. Later in the code, it checks if an error occurred and the screen and error are redisplayed to the user, otherwise, the display fields are cleared for the next transaction.

```
CSR CALL 'XF4108 ' C* ---- ----- CSR PARM PS@@1 CSR PARM I4108 C* CSR
SELEC CSR @@IOR WHEQ 'ERR' CSR MOVE *ON *IN99 CSR SETON 93 40 CSR
MOVE '1' @MK,1 CSR ENDSL
```

A.6.2 P41080 - Transaction processor

This is a subfile transaction processor. Since it falls under CFR21 regulations, it now includes the copy members for invoking the DBAM transaction authentication server. At the appropriate place in the program, before processing the subfile, the program calls the DBAM authentication server. (See server description above for parameter descriptions.)

```
* ----- * Check for and acquire electronic
transaction eSignature... * CSR MOVE'P41080' ##PGM P CSR MOVE'F4108' ##DBFN
P CSR MOVE'*LIBL' ##DBFL P CSR MOVE'*CHG' ##DBFA P CSR EXSR C98208 *
-----
```

Upon returning from the transaction signature server check the primary error indicator (*In93). If an error occurred, the program issues an error, exits the subroutine, and displays the error to the user. No transactions are processed.

```
CSR *IN93 IFEQ '1' CSR SETON 9340 CSR MOVE '1' @MK,1 CSR GOTO END005 * ----
----- CSR ENDIF * -----
```

Note: If a DBAM audit is not configured on the primary database file, no prompting for signature will occur. Control returns to your application and the transactions are processed.

After all the transactions have been processed, and before exiting the subroutine, the authentication server is called again to release the signature.

```
* ----- * Release the electronic transaction
signature... * C EXSR C98209 * ---- *
-----
```

The transaction process is now complete. Here is the copy module code to include the required subroutines for invoking the transaction level authentication server. These two modules must be included for transaction level signatures.

```
***** * Copy module to acquire a
transaction eSignature. * C/COPY JDECPY,C98208
*****
```

```
* Copy module to release a transaction eSignature. * C/COPY JDECPY,C98209
*****
```

A.6.3 Example of Single Record Update

When the program updates the database file, it includes an error indicator on the I/O operation. After the file I/O, it checks for an error. In an error was received, it signals the condition to the user. Otherwise, it continues as usual and resets for the next transaction.

```
C***** C* SUBROUTINE S005 -
Scrub Input C* ----- C* CSR S005 BEGSR C* ---- C* Data
validation code here C* Update file. Monitor for I/O error. C* CSR SELEC CSR *IN21
WHEQ '1' CSR WRITEIFILE 93 C* CSR *IN22 WHEQ '1' CSR UPDATIFILE 93 C* CSR
*IN23 WHEQ '1' CSR DELETIFILE 93 CSR ENDSL C* C* Database I/O error. Maintain
screen and issue error to user. C* CSR *IN93 IFEQ '1' CSR MOVE '1' *INxx CSR MOVE
'1' @MK,x CSR ELSE C* C* Clear data fields for next transaction. C* CSR MOVE
#FCLR @@AID CSR EXSR S001 C* ---- CSR ENDIF
C*----- CSR END005 ENDSR
C*****
```

In the above example, the RPG error indicator and error message array position are dependent upon your application requirements.

A.6.4 Transaction Level Interfaces - Copy Modules

Included here are copies of the Copy Modules that must be included in transaction processor applications that are using the DBAM transaction level authentication server.

RPG IV

C98209L - Copy module to invoke the transaction eSignature.

```
***** * SubRoutine C98208 - Check
for and acquire an eSignature... * ----- C
C98208 Begsr * ---- C *Like Define PsPgm ##Pgm C *Like Define PsDbfn ##Dbfn
C *Like Define PsDbfl ##Dbfl C *Like Define PsDbfa ##Dbfa C Call 'P98208' * ----
C Parm *ACQ' PsFunc 4 C Parm PsRtn 1 C Parm ##Pgm PsPgm 10 C Parm ##Dbfl
PSDbfl 10 C Parm ##Dbfn PSDbfn 10 C Parm ##Dbfa PSDbfa 4 * Check return status
from eSignature server... C Select * Return code of *Zero means we have an
authorization... C PsRtn Wheneq '0' C Move '1' ##eSig 1 * Return codes less than 4
indicate that eSignature is not * configured or not turned on... C PsRtn Whenlt '4' C
Move '0' ##eSig 1 * Return codes greater than 3 are errors... C PsRtn Whengt '3' C Move
'1' *In93 C Endsl C E98208 Endsr
```

```

C***** C98209L - Copy module to
release the transaction eSignature.
***** * SubRoutine C98209 -
Release transaction eSignature... * ----- C
C98209 Begsr * ----- C ##eSig Ifeq '1' C Call 'P98208' * ----- C Parm '*END'
PsFunc 4 C Parm PsRtn 1 C Move '0' ##eSig C Endif C E98209 Endsr
*****

```

RPG III

```

C98208 - Copy module to invoke the transaction eSignature.
***** * SubRoutine C98208 - Check
for and acquire an eSignature... * ----- * CSR
C98208 BEGSR * ----- * CSR *LIKE DEFN PSPGM ##PGM CSR *LIKE DEFN
PSDBFN ##DBFN CSR *LIKE DEFN PSDBFL ##DBFL CSR *LIKE DEFN PSDBFA
##DBFA * CSR CALL 'P98208' * ----- CSR PARM '*ACQ' PSFUNC 4 CSR PARM
PSRTN 1 CSR PARM ##PGM PSPGM 10 CSR PARM ##DBFL PSDBFL 10 CSR PARM
##DBFN PSDBFN 10 CSR PARM ##DBFA PSDBFA 4 * * Check return status from
eSignature server... * CSR SELEC * * Return code of *Zero means we have an
authorization... * CSR PSRTN WHEQ '0' CSR MOVE '1' ##ESIG 1 * * Return codes less
than 4 indicate that eSignature is not * configured or not turned on... * CSR PSRTN
WHLT '4' CSR MOVE '0' ##ESIG * * Return codes greater than 3 are errors... * CSR
PSRTN WHGT '3' CSR MOVE '1' *IN93 CSR MOVE '0' ##ESIG CSR ENDSL * CSR
ENDSR ***** C98209 - Copy
module to release the transaction eSignature.
***** * SubRoutine C98209 -
Release transaction eSignature... * ----- *
CSR C98209 BEGSR * ----- * CSR ##ESIG IFEQ '1' CSR CALL 'P98208' * -----
CSR PARM '*END' PSFUNC 4 CSR PARM PSRTN 1 * CSR MOVE '0' ##ESIG CSR
ENDIF * CSR ENDSR *****

```


A

associated text, 2-21
 properties, 2-20
 search, 2-19
Audit Configuration Details, 2-3
Audit Definition Parameters, 2-8
Audit Manager Workbench, 2-5
audit process, 1-1
 deleting, 3-11
 start, 3-6
authorizations
 record level, A-2
 transaction level, A-2

B

batch jobs, 4-1

C

Change Audit Definition, 2-6
Coexistence, 4-2
configuration defaults
 changing, 3-20
Confirm Deletion, 2-13
Copy Modules, A-6
 RPG III, A-7
 RPG IV, A-6

D

Database Audit Manager, 1-1
Database File Triggers, 2-14
defaults
 changing configuration defaults, 3-20
Deleting an Audit Process from a File, 3-11
Displaying Triggers for a File, 3-14

E

Editing an Audit File, 3-6
Electronic Signature, 2-18

F

Field Selection List, 2-11

fields

 file prefix, 4-2
 removing, 3-7

file

 audit file editing, 3-6
 list, 2-7

Food and Drug Administration (FDA), 1-1

G

G946, 1-1, 2-1, 3-1

I

Impact on Other Applications, 4-1
Inactive Reason Codes, 2-17
Issues and Assumptions, 4-1

J

JD Edwards EnterpriseOne
 coexistence, 4-2

O

option number, 2-8, 2-16

P

P00CKPWD Transaction Level Authentication Server
 (external), A-4
P98208 Transaction Level Authentication Server
 (electronic signature), A-3
Programs and IDs
 P00CFMCHG (save changes), 2-13
 P00CFMDLT (confirm deletion), 2-13
 P41080 (transaction processor), A-5
 P98200 (audit manager workbench), 2-5, 3-1
 P98200W (change audit definition), 2-6
 P98200X (file list), 2-7
 P98201 (audit configuration details), 2-3
 P98202 (audit definition parameters), 2-8
 P98203 (field selection list), 2-11
 P98204 (reason code maintenance), 2-15
 P98204I (inactive reason codes), 2-17
 P98208 (electronic signature), 2-18

- P98209 (associated text search), 2-19
- P98209D (associated text), 2-21
- P98209H (associated text properties), 2-20
- P98209X (selection list), 2-22
- P98211W (database file triggers), 2-14

R

reason code

- add to a new program, 3-16
- edit, 3-17
- maintaining, 3-16
- maintenance, 2-15
- search for, 3-17
- view inactive, 3-18

Reports, 4-2

- response time, 2-7

S

- Save Changes, 2-13

Screen

- Associated Text, 2-21
- Associated Text Properties, 2-20
- Associated Text Search, 2-19
- Audit Configuration Details, 2-3
- Audit Definition Parameters, 2-8
- Audit Manager Workbench, 2-5
- Change Audit Definition, 2-6
- Confirm Deletion, 2-13
- Database File Triggers, 2-14
- Electronic Signature, 2-18
- Field Selection List, 2-11
- File List, 2-7
- Inactive Reason Codes, 2-17
- Reason Code Maintenance, 2-15
- Save Changes, 2-13
- Selection List, 2-22
- Transaction Processor, A-5

- Selection List, 2-22

- serial number, 2-15

servers

- signature, A-3
- transaction level authentication, A-3
- transaction level authentication (external), A-4

- set up audit process, 1-1, 3-1

signature

- record level, A-2
- transaction level, A-2

- Single Record Update, A-6

- Sleeper, 4-1

subroutine

- S005, A-5
- S010, A-5

- System Requirements, 1-1

Transaction Level Interfaces

- Copy Modules, A-6

trigger

- activation mode B, 3-3
- adding, 3-6
- amount of, 2-14
- audit process, 1-1, 2-11, 2-14
- changing, 3-9
- delete a trigger program, 3-12
- display for a file, 3-14
- in batch jobs, 4-1
- maximum, 4-1
- minimum, 4-1
- placing on the file, 3-6
- remove audit triggers from a file, 3-12
- removing, 3-9
- running within interactive jobs, 4-1
- system performance, 4-2
- view attached triggers, 3-15

T

- Transaction Level Authentication Server, A-3

- Transaction Level Authentication Server
(external), A-4