Oracle® Fusion Middleware

Administrator’s Guide for Universal Records Management

11*g* Release 1 (11.1.1)

E10789-01

May 2010

ORACLE®

Oracle Fusion Middleware Administrator's Guide for Universal Records Management, 11*g* Release 1 (11.1.1)

E10789-01

Primary Author: Jean Wilson

Contributor: Brian Carlson, Brian Johnson, Lisa Jones, Tok Hui Mackenthun, Rene Madsen, Jason Ogaard, Victor Owuor, Alex Sanchez

Contents

12 Monitoring, Customizations and Audit Tools

13 Archiving and Transfering Information

14 FOIA and Privacy Act Tracking

15 Using Federated Search and Freeze

A User Interface

Preface

This guide provides instructions to administer and maintain Oracle Universal Records Management software (Oracle URM) on a Oracle Universal Content Management Content Server.

Audience

This guide provides instructions to configure and administer the product. The guide is intended mainly for administrators, records managers, and privileged users responsible for managing retention policies.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

The following documentation is available:

- *Installation Guide* for your product: This document provides information about installing the software on your system.
- *Oracle Fusion Middleware Setup Guide for Universal Records Management*: This document provides information about setting up the software.
- *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*: This document provides information about administering and managing the software.
- *Oracle Fusion Middleware User's Guide for Universal Records Management*: This document provides information about common tasks performed by users when using the software.

In addition to these guides, you can also access information about the product with context-sensitive tooltips, quick help, and help menu.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
IntradocDir`/ucm/urm/config`	The default location for configuration files mentioned in this documentation. *IntradocDir* is used to refer to the root directory for the actual configuration and data files specific to an instance deployed on the Oracle UCM domain on an Oracle WebLogic Server.

1 Introduction

This section covers the following topics:

- "About This Guide" on page 1-1
- "What's New" on page 1-2
- "Using Help" on page 1-4

1.1 About This Guide

This guide provides instructions to administer the product software. In general, it does not contain details about setting up the product. For example, this guide contains instructions for processing dispositions (those rules used to manage content life cycles), but it does not contain instructions for creating those dispositions. Details about setting up the software is contained in the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

A glossary of frequently used terms is also included in the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

Details about processes are contained in either this guide or the *Oracle Fusion Middleware User's Guide for Universal Records Management*. If a task can only be accomplished by users with administrative privileges, that task is discussed in the Administrator's Guide. If the task can be accomplished by users with administrative *or* user privileges, it is discussed in the User's Guide.

The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified.

This guide assumes you are using the Trays layout and that you have some familiarity with Oracle UCM and its use. References to Fusion Middleware documentation are made throughout this documentation to assist in finding the information.

In this document and other documents in this product set, the terms "content" and "record" are synonymous and can be used interchangeably.

1.2 About This Product

Oracle Universal Records Management (Oracle URM) is an enterprise-wide 5015.2 Chapter 2 and Chapter 4 certified electronic and physical records management system. It provides a single application that can be used to create and administer the information life cycle for both physical and electronic information. It allows organizations to apply retention policies as well as legal discovery and holds to relevant content across the enterprise, from e-mail attachments and content stored in file servers to physical records in a warehouse.

It also has a framework for extension to other repositories via adapters. This guide discusses records management features in both Oracle UCM and Oracle URM. Features involving physical content management and external adapter management are only available when Oracle URM is installed.

The following options are available after installing the software:

- **Minimal**: installs a small amount of Oracle URM metadata fields and a limited subset of disposition actions. This is the initial default when the software is enabled.
- **Typical**: enables Physical Content Management as well as all disposition actions and all features except for DoD Configuration (Department of Defense), Classified Topics, FOIA/PA tracking (Freedom of Information Act/Privacy Act), and Email.
- **DoD Baseline**: enables the features from a Typical installation with the addition of DoD Configuration and Email.
- **DoD Classified**: enables all features except for FOIA/PA.
- **Custom**: enables the ability to choose a variety of features. Note that some disposition actions are dependent on other actions. If such an action is selected, dependent actions are also automatically selected.

Throughout this documentation, the term "Oracle URM" refers to those features available in the majority of configuration scenarios. The features available at your site will vary depending on the options chosen during configuration.

1.3 What's New

Previous versions of this software were divided into two editions:

- Records Manager DoD Edition, which was used for DoD compliance tracking
- Corporate Edition, which did not contain many of the features included in Records Manager DoD Edition.

As of this release, much of the product functionality has been merged and functionality can be chosen after installation by selecting different features for configuration.

The classification scheme hierarchy functionality for use with the *Model Requirements for the Management of Electronic Records* (MoReq2) specification is also new for this release. This functionality can be enabled by setting a configuration variable.

Sites which are upgrading from previous versions of the software will see increased flexibility and functionality. Specific differences are available in the Installation Guide for the product.

The following list discusses some specific changes to the product from previous releases. The features will vary depending on the options chosen at installation:

- The **definition of a record** is now configurable. Options on the Create Retention Category page allow a records administrator to choose whether items in that category can be revised, deleted, edited, or will be permanent.
- **Setting up** the software now consists of three main steps:
  - Initial choices: this should be done immediately after installation. Depending on the choices made, specific components will be enabled for use.

- Initial configuration of global settings: this includes setting configuration variables, configuring the time periods used in the software, setting up triggers, and other global settings used for retention management.
- Configuring the retention elements of the software: this includes setting options to use custom security fields, to use classification guides, and to choose how revisions, deletions, and edits to content are handled.

- **Physical Content Management** documentation is incorporated into this documentation at this release. Separate documentation no longer exists for Physical Content Management.
- **Page navigation** menus on the search results page have changed. If more results are returned than are configured in the User Profile page, the page navigation dropdown menu indicates that other pages of information are available for viewing.
- A **print** option is now available on every screen.
- When using Physical Content Management **offsite storage** of content can be configured.
- **Menus** have been extensively changed. Most options are now available by using the **Records** or the **Physical** menu option on the Top menu.
- You can easily **view your assigned rights** by going to the My Profiles page. Retention administration rights are displayed there as are the assigned roles.
- A **dashboard** is now available which can be used to quickly organize product features for easy access and use. This is discussed in detail in the *Oracle Fusion Middleware User's Guide for Universal Records Management*.
- A new interface is provided to manage **reports**. Templates can be created for reports and can be checked in to the repository in the same way other content can be checked in.
- **Out of date content** (not the current version) is now designated as such with a line through the content name in search results. Any item which is obsolete, canceled, rescinded, and so on is designated in this manner.
- A **Favorites** listing can be created, similar to bookmarked browser "Favorites". Users and aliases as well as categories, freezes and other retention objects can be added to the Favorites menu. Favorites items are used to populate option lists, such as when creating freezes. For example, if an item is on your Favorites list, it appears on the pulldown list when you choose a freeze name. This helps to narrow the choices when using this functionality.
- When creating **disposition rules** involving moves (such as Archive, Accession, Transfer, and Move), a location can be specified. If a location is chosen, content is copied to the specified location as part of the disposition step. In previous releases, a zip file of the copied content was created; the content was not copied to a location.
- Disposition rules can now be reviewed in a **workflow** before implementation.
- Content stored in folders can now be transferred to **volumes**. When a volume is created, all content in the folder is moved to a newly created volume folder.
- **Services** used in this product are now documented in the *Oracle Fusion Middleware Services Reference Guide for Universal Content Management*. See that guide for details about the services used and how to implement new services.
- **Screening** can now be accessed through the search menu.

- **Performance monitoring** can now be done through the Oracle URM interface. Performance statistics for batches, items, and processes can be tracked.
- **Folios** can be used to easily manage content. With this release, when a folio is locked (either by freezing or filing in a category that prohibits edits), the folio and its content are automatically cloned, and the bundle is locked, thus preventing the folio from being edited.
- **Categories and disposition rules** can be copied from existing categories to a new category, making retention schedule creation easier and less prone to error.
- **Related content links** for items can be created as needed on the content checkin page.

1.3.1 Conceptual Changes in this Product

In previous releases of this product, the term ’record’ was used to designate those items of content which could not be revisioned. Therefore, a designation was made between ’content’ and ’records’.

In this release, any item of content can be revisioned if revisioning is allowed. One of the initial setup choices is to allow revisions or to prohibit revisions of content. You can now finely tune which categories, folders, and content are revisionable, editable, or which can be deleted. Content, categories, and folders are no longer designated as ’record categories’ or ’record folders’.

1.3.2 Documentation Changes in this Product

The documentation set for this product has been substantially revised to reflect new functionality and changes.

In addition, several task descriptions have been moved from the administrative guides. Any task which can be performed by either a user or a privileged user (administrator or user with other administrative privileges) is now documented in the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

1.4 Using Help

In addition to the guides provided with the product, you can access information about product functionality with context-sensitive tooltips, quick help, and the help menu.

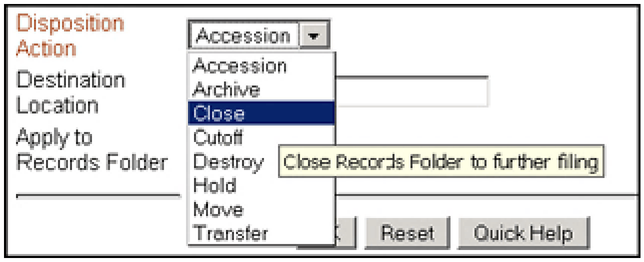
1.4.1 Tooltips

If the mouse cursor is held over a field label in a web browser, context-sensitive information on the field label is displayed. A question mark is displayed then the tooltip appears.

Figure 1–1 Field Label Tooltip

When using Netscape or Firefox as a web browser, tooltips are also available for items in options lists, provided the list items are not custom entries.

Figure 1–2 Option List Item Tooltip (Only Supported by Netscape and Mozilla Browsers)



1.4.2 Quick Help

Click the **Quick Help** button where available on pages and screens to view context-sensitive help for that page or screen.

2

Introduction to Records and Retention Management

This section covers the following topics:

2.1 Management of Retained Items

Oracle URM effectively manages content items on a retention schedule. The focus of *records management* tends to be the preservation of content for historical, legal, or archival purposes while also performing retention management functions.

Oracle URM combines both record and retention management into one software system. Oracle URM can track and to preserve content as needed, or dispose of content when it is no longer required.

The focus of *retention management* tends to be the scheduled elimination of content based on a schedule designed by a record administrator.

This section covers the following topics:

2.1.1 Needs for Retention

There are various reasons why organizations may need to retain content:

2.1.1.1 Regulatory Needs

Many organizations are subject to regulations that require the retention of information for a specified period:

- Sarbanes Oxley:
  - Applies to all publicly traded corporations or companies that may become public
  - Audit-related working papers, communications, and correspondence must be retained for five years after the audit
- Government organizations: DoD 5015.2, General Records Schedule
- Pharmaceutical/health care industry: HIPAA, FDA regulations
- Financial services: SEC Rule 17a
- Telecommunications industry: 47 CFR 42, and so on

2.1.1.2 Litigation Needs

There may be litigation-related needs for effective and efficient retention management:

- Policy-based retention of content:
  - Retain information needed for litigation (for example, a contract and any communication relating to it).
  - Centralized searching and retrieval of that information
- Systematic disposition of eligible content:
  - Less material to search through during discovery
  - Less material to give to opposing counsel
- Suspend/freeze disposition of content relating to pending litigation:
  - Avoid appearance of cover-up and possible liability when content relating to pending litigation is destroyed.

2.1.1.3 Business Needs

There may be business-related needs for effective and efficient retention management:

- "Islands of content" problem. Content items that are:
  - Generated across the organization
  - Created in a variety of forms, for example, e-mail, office application documents, sheets of paper, CDs, DVDs, microfiche, recordings of corporate events and conference calls, and so on
  - Stored in an ad-hoc fashion in a variety of locations, for example, employee desks, employee computers, corporate servers, central file storage, offsite storage.
- There is a need to:
  - Provide a uniform infrastructure for retrieving and sharing the content across the organization.
  - Ensure that content items are retained over the period they are useful to the business.

Oracle URM manages all content, regardless of source, in a single, consistent, manageable infrastructure.

2.1.2 What Do I Retain?

Items for retention are any form of information, both physical and electronic, that is **important** enough for an organization so they must be **retained** for a specific period and may be **disposed** of when no longer needed. However, it can be revisioned, retained and can be managed on a disposition schedule. An organization may choose to manage content to eliminate outdated and misleading information and track documents related to legal proceedings.

This can include the following types of items:

- DoD 5015 record: As defined previously with the stipulation that it is also made or received by an agency of the United States Government. The U.S. Government defines records as follows:

  "Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value in them."

  In this documentation, the term "content" is synonymous with "record" and includes those items which can be tracked for DoD purposes.

- Business content: As defined above with the stipulation that it is used in the transaction of public business.
- Content items: As defined above with no additional governmental or public business criteria. An organization may choose to manage content to eliminate outdated and misleading information, track documents related to legal proceedings, and manage storage resources.

See the following sections for more information:

- "Importance of Content" on page 2-4
- "Retention" on page 2-4
- "Disposal" on page 2-4

2.1.2.1 Content Retention Qualities

Content retention qualities include:

- **Benefits**: A benefit of content retention is reduced risk and cost of discovery for litigation, reduced costs associated with storage, elimination of clutter to promote user efficiency, and dissemination of only current information to improve communication.
- **Ability to Revision**: Content can be checked out, modified, and checked back in to create multiple revisions and tracked through the revisioning process.
- **Disposition**: Disposition schedules can be assigned to content by their location in the Retention Schedule. This defines how content should be retained and disposed of and helps eliminate outdated or superseded information, manage storage resources, or handle legal procedures.

- **Filing**: Content can be filed into record folders or into categories for easier management of groups of content.
- **Other Functionality**:
  - Classification/Supplemental Markings
  - Permanence
  - Record Folders
  - Freeze
  - Link
  - Subject to Review

2.1.2.2 Importance of Content

Retained information can be **important** for a variety of reasons:

- The information may be required for the day-to-day operations of the organization and must be kept for historical, tracking, or audit purposes (for example, receipts, order histories, completed forms, personnel files, corporate announcements).
- The information may be necessary to the success or survival of the organization (for example, software source code, contracts, financial data).
- There may be internal policies or external regulations requiring the information to be retained (for example, transaction documents, financial statements, lease agreements).
- The data may be important in preparation for possible litigation or discovery.

2.1.2.3 Retention

The information may need to be **retained** for different periods of time, depending on the type of content, its use within the organization, and the need to comply with external laws or regulations.

- The retention may be time-based (for example, five years from the filing date).
- The retention period may be event-based (for example, an employee termination).
- The retention period may be both time-based and event-based (for example, two years after employee termination).
- The retention period may be based on usage if usage is being tracked.
- The retention may be based on revision (for example, after four revisions).

2.1.2.4 Disposal

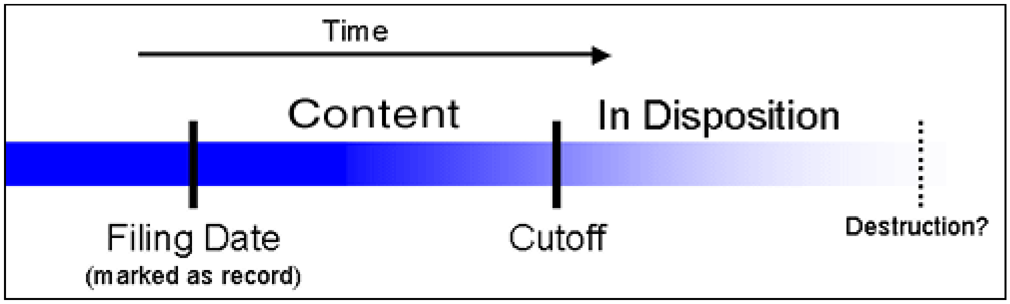
After a retention period, content items are disposed of by authorized people according to the requirements of the organization. Disposition actions can include:

- Destroy (physical or electronic), possibly after a certain period of retention.
- Store within the organization (physical or electronic).
- Transfer to an external storage facility (physical or electronic).
- Some content is deemed so important it will never be destroyed (for example, due to historical significance). "Disposal" in this instance indicates a status changes from active use.

2.1.3 Lifecycle for Retained Content

The lifecycle of retained content goes through several stages.

Figure 2–1 Life Cycle of Retained Content



The **filing date** is the date a content item is marked as an item being tracked. This often coincides with the check-in date. However, it is possible for an active content item already checked in to be tracked.

The **cutoff** of a content item is the moment the status of the item changes and the item goes into disposition. An item may be cut off after a specific period, at a specific event, or after an event.

2.1.4 Types of Retained Content

Retained content can be divided into categories depending on the perspective:

- "Internal and External Retained Content" on page 2-5
- "Classified, Unclassified, Declassified Content" on page 2-5
- "Non-Permanent, Transfer or Accession, and Reviewed Content" on page 2-6

2.1.4.1 Internal and External Retained Content

An ***internal*** retained content item is an electronic item stored within Oracle UCM and managed by Oracle URM.

External content can also be managed. An ***external*** retained content item is a source file not stored in Oracle UCM or Oracle URM. It can be in a variety of formats, both physical or electronic. If the source file is not specifically stored in Oracle URM, then it is considered external. The software can manage the disposition schedule, search metadata associated with the external file, and manage an electronic rendition of an external file. An electronic rendition can either be checked in as a primary file of an external item, or be filed as a separate file, and then linked to the external file metadata.

2.1.4.2 Classified, Unclassified, Declassified Content

Content can be ***classified***, ***unclassified***, or ***declassified***.

Classified content is that which requires protection against unauthorized disclosure (for example, because it contains information sensitive to the national security of the United States or because it is essential for a corporation's operation).

Unclassified content is not and has never been classified.

Declassified content was formerly classified, but that classified status has been lifted.

A *classification* specifies the security level of a classified content item. A *classification guide* provides default classification values for check-in pages.

Options can be chosen during the initial setup to insure that the system complies with the DoD 5015.2 standard (including Chapter 4). The software has been certified by the Joint Interoperability Test Command (JITC) to comply with that standard. A copy of the standard is available on the official web site of the Department of Defense, Washington Headquarters Services, Directives and Records Division at `http://www.dtic.mil/whs/directives/`.

Important: Executive Order 12958: Classified National Security Information describes in detail the system for classifying, safeguarding, and declassifying national security information. This guide assumes you are familiar with proper classification protocols.

2.1.4.3 Non-Permanent, Transfer or Accession, and Reviewed Content

For disposition purposes, content is categorized into **non-permanent**, **transfer or accession to NARA**, and **subject to review**. Most items fall into the non-permanent category.

Non-permanent items are usually destroyed after a retention period. Permanent items are deemed important for continued preservation and are retained indefinitely (for example, because of their historical significance).

Items can be scheduled for periodic reviews by authorized people. This complies with the DoD Vital Record Review criteria.

2.2 Basic Retention Management Concepts

Oracle URM is used to manage content, regardless of source or format, in a single, consistent, manageable infrastructure. Managed items are assigned retention schedules and disposition rules which allow users to schedule lifecycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

Content and its associated metadata are stored in retention schedules, which are hierarchies with categories that define disposition instructions. Access to the items is controlled by rights assigned to users by a Records Administrator. The items can be accessed, reviewed, retained, or destroyed in an easy and efficient manner by authorized people according to the requirements of an organization.

Disposition schedules of content in the repository can also be managed, enabling the scheduling of lifecycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

The following concepts are important to understand in the context of retention management:

- **record administrator**: individuals in the organization who are responsible for setting up and maintaining the retention schedule and other aspects of the management system.
- **record user**: individuals who use the software to check content in and out of the system, to search for records, and to perform other non-administrative tasks.
- **record officer**: individuals who have limited administrative responsibility in addition to the responsibilities of a record user.

- **administrator**: individuals who may maintain the computer system, network, or software at the site where the management system is in place.
- The **retention schedule** is an organized hierarchy of series, categories, and record folders, which allows users to cluster retained content into similar groups, each with its own retention and disposition characteristics.
- A **series** is an organizational construct in the retention schedule which assists in organizing categories into functional groups. Series are normally static and are used at a high level in an organization hierarchy. They can be especially useful if a large amount of categories are used. A series can be nested, which means a series may contain other series.
- A **retention category** is a set of security settings and disposition instructions in the retention schedule hierarchy, below a series. It is not an organization construct but rather a way to group items with the same dispositions. A category helps organize record folders and content into groups with the same retention and disposition characteristics. A retention category may contain one or more record folders or content items, which then typically follow the security settings and disposition rules associated with that retention category. Retention categories *cannot* be nested, which means a retention category cannot contain other retention categories.
- A **record folder** is a collection of similar content items in the retention schedule. Folders enable content to be organized into groups. A folder typically follows the security settings and disposition rules associated with its assigned retention category. Folders can be nested, which means a folder may contain other folders.
- **Disposition** is the collective set of actions taken on items. Disposition actions include wait times and activities such as transfer to external storage facilities, the destruction of temporary content, deletion of previous revisions, and deletion of all revisions.
- A **disposition instruction** is created within a retention category, and typically consists of one or more disposition rules, which define how content is handled and what actions should be taken (for example, when and how content should be disposed of).
- A **period** is the segment of time that must pass before a review or disposition action can be performed. Several built-in periods are provided (for example, "one year"), but custom periods can be created to meet unique business needs.
- A **trigger** is an event that must occur before a disposition instruction is processed. Triggers are associated with disposition rules for retention categories. Examples of triggering events include changes in status, the completed processing of a preceding disposition action, or a retention period cutoff.
- A **link** is a defined relationship between items. This may be useful when items are related and need to be processed together. Links are available for items stored both in and out of the retention schedule.
- A **classification** specifies the security level of a classified item. It is used in the process of identifying and safeguarding content containing sensitive information. Typical classification levels are "Top Secret,", "Secret," and "Confidential," and "Unclassified."
- A **classification guide** is a mechanism used to define default values for several classification-related metadata fields on the content check-in pages for content. A guide enables convenient implementation of multiple classification schemes.
- **Freezing** inhibits disposition processing for an item. Frozen content cannot be altered in any way nor can it be deleted or destroyed. This may be necessary to

comply with legal or audit requirements (for example, because of litigation). Freezing is available for items stored both in and out of the retention schedule.

- **External items** are those which are not searched and processed in the same fashion as retained content. External content usually refers to content managed by Physical Content Management or managed by an adapter (an add-on product to Oracle URM).
- **Federation, Federated Search, Federated Freeze** are functionality used to manage the process of legal discovery. Using Federated Search or Freeze, a legal officer can search content across all repositories to gather information needed for legal proceedings.

2.3 Physical Content Management

While Oracle URM enables organizations to manage the retention and disposition of content, Physical Content Management provides the capability of managing physical content that is not stored in the repository in electronic form.

All items, internal and external regardless of their source or format, are managed in a single, consistent, manageable infrastructure using one central application and a single user interface. The same retention schedules are used for both electronic (internal) and physical (external) content.

PCM tracks the storage locations and retention schedules of the physical content. The functionality provides the following main features:

- **Space management**, including definition of warehouse layout, searching for empty space, reserving space, and tracking occupied and available space.
- **Circulation services**, including handling reservation requests for items, checking out items, and maintaining a due date for checked-out items.
- **Chargeback services**, including invoicing, for the use of storage facilities and/or actions performed on physical items.
- **Barcode file processing**, including uploading barcode information directly into the system, or processing barcode files manually.
- **Label creation and printing**, including labels for users, storage locations, or individual physical items.
- **Retention management**, including periodic reviews, freezes and litigation holds, and e-mail notifications for pending events.

2.4 Interaction with Oracle UCM

The following layouts and search templates are supported. Users can change layouts and templates by setting them in their user profile):

- Supported layouts:
  - Trays
  - Top Menus
- Supported search templates:
  - Headline View
  - Thumbnail View
  - My Headline View

The Classic layout or the Classic View search template are not supported. This guide assumes you are using the Trays layout.

2.5 Basic Retention Processes

The following steps outline the basic workflow of retained content:

1. The retention schedule and any required components, such as triggers, periods, classifications, and custom security or metadata fields are created.
2. Items are filed into the retention schedule by users. The filed items assume the disposition schedules of their assigned category.
3. Disposition rules are processed in accordance with the defined disposition schedules, which usually have a retention period. The processing is activated by either a system-derived trigger or custom trigger. The trigger could affect one or more items simultaneously.
4. Whenever a disposition event is due for action (as activated by a trigger), an e-mail notification is sent to the person responsible for processing the events. The same is true for review. The pending events and reviews are displayed in the pages accessed from the Retention Assignments links within the user interface.
5. The Records Administrator or privileged user performs the review process. This is a manual process.
6. The Records Administrator processes the disposition actions on the pending dispositions approval page. This is a manual process.

Many disposition schedules are **time-based** according to a predictable schedule. For example, content is often filed then destroyed after a certain number of years. The system tracks when the affected content is due for action. Notification email is sent to reviwers with links to the pages where reviewers can review and approve content and folders that are due for dispositions.

In contrast, **time-event** and **event-based** dispositions must be triggered with a non-system-derived trigger (a trigger that was defined for a particular scenario). For example, when a pending legal case starts litigation, the Records Administrator must enable the custom trigger and set its activation date because the start date information is external. Custom triggers can define event and time-event based disposition actions based on the occurrence of a particular event.

3 Interface Overview

This chapter describes the key elements of the product interface. It covers the following topics:

For a glossary of terminology used in this documentation, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

Also see the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about profiles, the task panel, the My Favorites functionality, and other interface elements used by both users and administrators.

3.1 Interface Overview

After installation, new links appear in the Top menu, used to configure and manage the software. If enabled, a link also appears to manage Physical Content Management.

3.1.1 Configuring The System

Administrative users will see all options from the menus. Other users (for example, those assigned privileged roles) may see a much smaller subset of the administrator menu, depending on their assigned rights. The exact menu options any user sees depend on the rights assigned to the user. For details about rights assigned to different roles, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

The following is an overview of the options on the **Records** menu:

- **Rights**: Used to view assigned rights and roles. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for information about viewing rights and roles.
- **Favorites**: Accesses the Favorites interface, displaying items added to your Favorites list. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about using Favorites.
- **Dashboard**: Used to configure a dashboard which is a shortcut to frequently used screens. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for information about configuring dashboards.
- **Approvals**: Displays a menu to access items awaiting review, approval or completion.
- **Scheduled**: Accesses scheduled actions, reports, and freezes.

- **Reports**: Used to access reports created by users as well as system reports.
- **Import/Export**: Accesses menus allowing import and export of archives and XSD data.
- **Audit**: Used to view checked-in audit entries or search the audit trail. Also used to configure performance monitoring tools and to screen disposition rules and failed dispositions.
- **Configure**: Used to configure many aspects of the system, such as freezes, triggers, security, audit trail information and reports.
- **Global Updates**: Used to update categories, folders, or content.
- **Batch Services**: Used to process notifications, run all pending batch actions, or to process actions and reviews.
- **Sources**: Used to display information about other content sources, either physical or external (such as Oracle URM Adapters) where content is retained or tracked.

3.1.2 Configuring Reports

Use the Configure Report Settings Page to determine the output format for reports about freezes, screening, and labels. Default reports provided with the software can be used or new report templates can be created. The data used in the reports is limited depending on the security permissions of the person creating the report. In this way, the reports, while available to most users, can still be kept secure.

To access this page, click **Records** then **Configure** from the Top menu. Click **Reports** then **Settings**. See Chapter 11, "Generating Reports" for details.

See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about creating custom reports using BI Publisher.

3.1.3 Configuring PCM

Use the **Physical** menu in the Top menu to access most aspects of Physical Content Management. The exact menu options any user sees depend on the rights assigned to that user.

Administrative users will see all options. Other users (for example, those assigned privileged roles) may see a much smaller subset, depending on their assigned rights.

The following is an overview of the options on the **Physical** menu:

- **Reservations:** Displays a list of all current reservations. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about reservations.
- **Storage**: Displays the Exploring Storage page where storage locations can be defined and edited.
- **Invoices**: Displays current invoices and allows creation of new invoices.
- **Requests**: Displays pending requests, checked-out requests, and overdue requests for physical items.
- **Process Barcode File**: Accesses a screen to upload barcode data.
- **Configure**: Used to configure many aspects of the physical management system, including general settings, chargeback types, and customers.

If Batch Services and Offsite Storage have been enabled, those options also appear. Batch Services are used to immediately process reservation requests, storage count updates, and other actions. Offsite Storage allows a site to interface with an offsite storage providers.

3.2 Individual Page and Action Menus

When using this product, individual Action menus are available for items on a page and in many cases for individual items. The options on the Action menus vary depending on the page used and the type of item used (content, physical, retention category, and so on).

The following list summarizes the most commonly seen menu options:

- **Information**: displays a submenu used to access information pages for folders, the life cycle of the item, recent reviews, metadata history, and retention schedule reports.
- **Edit**: provides quick links to edit pages for folders or reviews, and options to alter an item’s status by moving, closing, freezing, or unfreezing an item.
- **Set Dates**: provides quick links to actions associated with dates, such as marking items for review, canceling, rescinding, and expiring items.
- **Delete**: provides options to delete the item or perform a recursive delete (delete an entire tree if multiple items are checked).
- **Create**: provides options to create items appropriate to the location in the hierarchy. For example, if this is the Action menu for a retention category, Create suboptions include Series and Retention Category.

Clicking the Info icon (a lower-case ’i’ in a circle) displays the Information Page for the item.

In addition, several pages have a page-level Action menu which appears next to the Page title. The options on that menu apply to actions that can be performed at that level in the retention hierarchy.

3.3 Menus

After installation, the Search and Checkin menus are changed to include default profile pages. These profiles provide a filtered view of checkin and search pages, allowing you to customize what users will see. Additional options may appear depending on profiles created at your site and the choices made during configuration.

These menu options can be used to help quickly narrow searches and choose the type of checkin to perform. The Screening option on the Search menu is dependent on security rights assigned to the user.

When viewing search results, a query menu is added to the search results page.

4

Screening and Updating Content

Screening is an enhanced search capability that specific search criteria to filter search results. Screening can be performed by both administrative users and end users. Details are discussed in the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

When using Oracle Text Search the system does not index external items, including physical items. Therefore those items and other items stored externally (for example, on an adapter system) are not available for searching.

This chapter provides overview information about screening, which can be performed by end users and by administrative users. Detailed information about performing global updates is included here because updates cannot be performed by end users.

For details about Federated Search, used during the legal discovery process, see Chapter 15, "Using Federated Search and Freeze".

Concepts

- "About Screening" on page 4-1
- "Updating Information" on page 4-2

Tasks

- "Enabling or Disabling User-Friendly Captions" on page 4-2

4.1 About Screening

In addition to search-like functionality, screening enables users to isolate retention categories, record folders, and content by their attributes. Screening lets a user see what has happened or what could happen within a retention schedule. Screening can be done at increasingly finer granularity within the retention schedule object levels. Within all levels, screening can be done by disposition information.

Screening reports can be created immediately or they can be scheduled to be generated at a later time. This is especially useful for screening reports affecting large sets of content. Creating the screening report immediately might put a heavy load on the system, which could diminish its responsiveness and/or result in browser time-outs for end-users. To avoid overloading, schedule screening reports to be performed at midnight, an off-peak time in most environments.

Reports can also be scheduled to run at recurring intervals. Many screening functions can be performed from the Search menu. After installing and configuring the software, an additional Screening menu is available on the Search menu. The same screening activities described in this chapter can be performed using that functionality.

While users can perform screening activities, the results returned are dependent on that user's roles and permissions. Only information which the user is privy to will be returned. Other information is filtered and not displayed.

4.1.1 Enabling or Disabling User-Friendly Captions

User friendly captions are captions in 'plain English' that do not use official retention language. User-friendly captioning can be enabled and disabled at any time. This setting also affects the captions in disposition instructions.

Permissions: The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Click **Records** then **Configure** from the Top menu. Click **Retention** then **Settings**.

   The Configure Retention Settings Page is displayed.
2. Select the **User-friendly disposition** box.
3. Click **Submit Update**. A message is displayed saying the configuration was successful.
4. Click **OK**.

To disable user-friendly captions, clear the **User-friendly disposition** box.

4.2 Updating Information

Permissions: The admin.noRmaSecurity right and the Admin role are required to perform updates. The noRmaSecurity right is not assigned by default to any role and must be assigned, with the Admin role, for the **Update** options to appear on the Configure Retention Settings Page.

The Update functionality quickly finds and changes large amounts of information. The information can be changed immediately or at a later time by using a scheduled update option. For example, you can change any items in a category matching a certain disposition to a different review type or to a new reviewer.

Note that a maximum of 2048 records can be searched for and updated using Oracle Text Search and Database Full Text Searching.

To access this functionality, click **Records** then **Global Updates** from the Top menu. Select the type of update to perform.

The Define Query Page is displayed. The options on this page are similar to those on the Screen for Topic page, discussed in the User Guide. The options in the Query section depend on the type of query being performed (category, record folder, or internal content).

Follow these steps to define a query:

1. Choose a field for use from the menu.
2. Select a substring from the displayed list.
3. Select a query value from a displayed list.

4. Select a field to be updated for all items matching the first query.
5. Select a substring for the value from the displayed list.
6. Select a new value for the field.
7. To preview the results of the update, click **Preview Results** in the upper right corner of the screen.

   The Update Preview Page is displayed. This screen shows those items which will be changed by the update. To return to the Define Query Page, click **Continue Defining Search** on the Page menu.
8. Continue adding update criteria if needed. To schedule the update for a later time, click **Schedule**. See "Scheduling Updates" on page 4-3 for more details. Click **Run Now** to run the change immediately. A message is displayed, indicating the selected items were updated. Click **OK** to return to the Define Query Page.

4.2.1 Scheduling Updates

To run the update at a later time, click **Schedule** to open the Query Schedule Section of the Define Query Page.

Select a time and date for the update to run and click **Submit**. Enter a name for the update event and click **OK**. The Scheduled Update Page is displayed.

Use this page to change the scheduled event. To edit an event, select **Edit Scheduled Event**. To delete the event, select **Delete Scheduled Event**. And to run the event immediately, select **Run Now**.

5 Managing Content

This chapter discusses the tasks associated with the general administrative maintenance and processing of content. It covers the following topics:

Concepts

Tasks

For information about creating and finding information, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*. Screen depictions and complete interface details are also in that guide.

5.1 About Content Processing

Maintaining and processing content involves tasks such as moving them, initiating a freeze, or handling events such as canceling, expiring. Items can also be rescinded items or marked as obsolete.

Options for maintaining and processing content are accessible from the Page menu on the content information page of an item. The available actions vary depending on what type of content is being used.

5.2 Managing Content

The following tasks are involved in managing content:

- Viewing Content Item Information
- Freezing, Rescinding, and Other Content Actions
- Managing Classified Content

For details about creating content, searching for content, and using the Content Basket, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

5.2.1 Viewing Content Item Information

Permissions: The Record.Read right is required to perform these actions. All predefined management roles (Records Administrator, Records Officer, and Records User) have this right.

Viewing information can be done in several ways depending on the location in the product hierarchy. First locate the item by browsing, searching, or screening. Then perform one of the following actions:

- On the search or screening results page, select the option (**Life Cycle**, **Recent Reviews**, and so on) from the item's **Actions** menu.
- On the search or screening results page, click the **Info** icon of the item.

  The Content Information Page is displayed. On the Page menu, select **Information** then the option needed (**Life Cycle**, **Metadata History**, and so on).

5.2.1.1 Viewing Content Life Cycles

Use the previously described procedure to access the Information menu or page for a content item. When **Life Cycle** is selected, the Life Cycle Page is displayed.

The page shows the complete life cycle of the item according to its scheduled disposition, including the calculated dates of each disposition action. If a separate notification reviewer has been assigned for the item, the person's user name is displayed. In addition, the retention category identifier from which the record folder inherits the instruction is given for each disposition action because content can be filed into multiple folders.

5.2.1.2 Viewing Content Review History

Use the previously described procedure to access the Information menu or page for a content item.

Click **Information** then **Recent Reviews** from the Page menu. The Review History for Item Page is displayed. The page shows a list of the last three reviews of the item. See "Reviewing Items" on page 5-5) for details. It also shows the date and time of review.

On the Recent Review Page, click **View Complete History** from the Page menu to see the entire review history of an item

5.2.1.3 Viewing Content Item Metadata History

Use the previously described procedure to access the Information menu or page for an item. When **Metadata History** is selected, the Metadata History Page is displayed.

The page shows an overview of all changes made to the editable properties of the item and the affected metadata field name, the modification date and time, and the old and new values.

Important: You can view the metadata history for content items checked into the Retention Schedule. You cannot view metadata history for content not checked into the Retention Schedule.

5.2.1.4 Viewing Classified Metadata History

Use the previously described procedure to access the Information menu or page for an item. When **Classified Metadata History** is selected, the Classified Metadata History Page is displayed.

This page shows a list of all changes made to the security classification of the item.

5.2.1.5 Viewing an Item's Freeze Details

Use the previously described procedure to access the Information menu or page for a content item. If the item is frozen, the **Is Frozen** field value is 'Yes' and a **Details** hyperlink is displayed next to the field value. Click the **Details** hyperlink. The Freeze Details Page is displayed.

This page shows all freezes currently applied to the item. If the item inherited its freeze status from its parent record folder, the folder's name is shown in the **Inherited From** column for the inherited freeze. Click the **Info** icon for a freeze in the list to display the content information page of the item.

To save the information on this page to a file (in the report format specified on the Configure Retention Settings Page), choose the **Save Freeze Details** option from the Page **Create** menu.

5.2.2 Freezing, Rescinding, and Other Content Actions

Managing content information can be done in several ways depending on the location in the product hierarchy. First locate the item by browsing, searching, or screening. Then perform one of the following actions:

- On the search or screening results page, select a Table menu then the option.
- On the search or screening results page, click the **Info** icon of the item.

  The Content Information Page is displayed. On the Page menu, select **Edit**, **Delete,** or **Set Dates** then the needed option.
- Actions can be performed on multiple items by clicking the selection box next to the item and choosing an option from the Table menu.

5.2.2.1 Deleting Metadata History of Content Items

Permissions: The Record.DeleteHistoryFile right is required to perform this action. This right is assigned by default to the Records Administrator role.

Use the previously described procedure to find an item and delete its metadata history. When **Delete Metadata History** is selected from a menu, a message prompts for confirmation. Click **OK** to confirm the action or **Cancel** to cancel it.

5.2.2.2 Freezing or Unfreezing an Item

Freezing inhibits disposition processing for an item. Content in a frozen folder inherits the freeze status from the parent folder, but it can also be frozen independently of the folder (usually with a different freeze).

In addition to content filed within a retention schedule, content not in a retention schedule can be frozen and therefore associated with a retention schedule.

More than one freeze can be applied to an item. View the Freeze Details Page (see "Viewing an Item's Freeze Details" on page 5-3) for the item to see a list of all freezes currently applied to it.

Unfreezing an item releases the item again for disposition processing. When a content item is frozen, *all* revisions of that content item are frozen. The revision is frozen directly and the other revisions inherit the freeze.

Permissions: The Record.Freeze/Unfreeze right to perform these actions. This right is assigned by default to the Records Administrator role.

Use the previously described procedure to find an item to freeze.

1. Click **Freeze** or **Unfreeze** on the appropriate menu. A dialog is displayed.
2. In the Freeze Name list, select the freeze to be applied or canceled if unfreezing. If freezes were added to a My Favorites list, this freeze list contains those freeze names. Otherwise the list contains all defined freezes.
3. Enter a reason for the action (optional).
4. Click **OK** to confirm the action. Click **Cancel** to abort the entire action.

   If the action is confirmed, the Retention Schedule Information area of the content information page displays "Is Frozen: Yes" and a **Details** hyperlink, which links to the detail page for the item. If the item was unfrozen, "Is Frozen: No" is displayed.

Important: After a content item is frozen, you cannot edit its freeze reason. If the freeze is no longer correct, you should unfreeze the item and freeze it with a new reason.

5.2.2.3 Canceling, Rescinding or Expiring Content

When an item is canceled, rescinded, or expired, its status becomes obsolete.

Content can be expired as part of a disposition action or as needed. When an item expires, its status becomes obsolete.

Permissions: The Record.Edit right is required to perform these actions. This right is assigned by default to the Records Officer and Records Administrator roles.

Use the previously described procedure to find an item to use. Select **Cancel**, **Rescind**, or **Expire** from the **Set Dates** menu.

A prompt appears for a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty. Click **Cancel** to abort the entire action.

If confirmed, the Retention Schedule Information area of the content information page displays the date the item was canceled, rescinded, or expired, and also displays a corresponding obsolete date.

This action can be undone by choosing **Clear Dates** in the **Actions** list of the item's content information page. This clears a cancel, rescind, expire, or obsolete action.

5.2.2.4 Marking an Item as Obsolete or Removing Obsolete Designation

Content items can be made obsolete as part of a disposition action or through an ad hoc action.

This procedure makes an item obsolete for any reason other than expiration, cancellation, or rescinding.

> **Permissions:** The Record.Edit right is required to perform these actions. This right is assigned by default to the Records Officer and Records Administrator roles.

Use the previously described procedure to find an item to use. Select **Obsolete** to mark the item as obsolete or **Clear Dates** from the **Set Dates** menu to undo an obsolete action.

A prompt appears for a reason for the action. Enter a reason or leave the text box empty. Click **OK** when done. Click **Cancel** to abort the entire action.

If confirmed, the Retention Schedule Information area of the content information page displays the date the item was made obsolete.

5.2.3 Reviewing Items

Use this procedure to mark an item as reviewed, either after receiving a review notification (as part of a disposition instruction) or as an ad hoc review.

> **Permissions:** The Record.Edit right and the RecordEditReview review are required to perform this action. The Record.Edit right is assigned by default to the Records Officer and Records Administrator role. The Record.EditReview right is assigned by default to all defined roles.

Use the previously described procedure to search for content items. Select **Mark Reviewed** from the **Set Dates** menu. A prompt appears to enter a reason for the action. Enter a reason and click **OK** to confirm. Click **Cancel** to abort the entire action. If confirmed, the Retention Schedule Information area of the content information page displays the date the item was reviewed.

To find items awaiting review click **Records** then **Approvals** from the Top menu. Click **Pending Reviews**.

If you have administrative permissions, you can click **List All** on the Table menu on the page. This shows all items awaiting review and the person assigned to do those reviews. Click **List Mine** to show only those items awaiting the logged-in user's approval.

5.2.4 Managing Classified Content

Managing classified information is done by using the Page menu at the top of the Content Information Page for the specific item. You must have the appropriate clearance to assign a security classification to an item. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for more details.

- On the search or screening results page, select **Content Information** from the item's **Actions** menu.

- On the search or screening results page, click the Info icon of the item.

  The Content Information Page is displayed. On the Page top menu, select **Information** then the option needed.

5.2.4.1 Reviewing Classifications

If category authors must review the classification of an item with a higher security classification level than they have, they cannot perform that action. A records manager or system administrator with the appropriate classification level must to do it for them.

> **Permissions:** The Record.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

Use the previously described procedure to find an item to use. Select **Information** then select **Review Classification** from the Page menu. The Review Classification Page is displayed. Review the information and provide the following information in the marked fields:

- The date and time of the classification review
- The person (or other entity) who performed the classification review

When done, click **Submit Update**.

5.2.4.2 Upgrading or Downgrading Classification

Upgrading the classification of an item is rare. It is typically an ad-hoc action and not part of a retention instruction.

Note the following considerations:

- You cannot downgrade content that had the Restricted Data or Formerly Restricted Data supplemental markings assigned. The Downgrade On field is disabled for content with a restricted supplemental marking history.
- If category authors must upgrade or downgrade the classification of an item with a higher security classification level than they have, they cannot perform that action. A records manager or system administrator with the appropriate classification level must do it for them.
- If a date was specified for the "Downgrade on date" metadata field for a classified item (upon check-in or later), a notification is sent on the due date with a reminder to downgrade the item.

> **Permissions:** The Record.Upgrade/Downgrade right is required to perform this action. **None of the predefined roles have this right by default.** You must assign that right to a user first.

Use the previously described procedure to find an item to use. Select **Edit** then select **Upgrade Classification** or **Downgrade** from the Page menu.

The Upgrade or Downgrade Classification Page is displayed. This page is similar to the Review Classification Page with the addition of fields where the classification can be changed.

Provide the following required information in the marked fields:

- The date and time of the classification change
- The person (or other entity) who changed the classification
- The new classification level
- The reason for the classification change

When done, click **Submit Update.**

5.2.4.3 Declassifying Content

Important: You cannot declassify content that had the Restricted Data or Formerly Restricted Data supplemental markings assigned. The Downgrade On field is disabled for content with a restricted supplemental marking history.

Use this procedure to completely declassify an item, either after receiving a review notification (as part of a disposition instruction) or ad hoc. If an item is exempt from declassification, an exemption reason must be entered.

After content has been declassified, access to the content is unrestricted and in the absence of any other security restrictions, any user can view it.

If category authors must declassify content with a higher security classification level than they have, they cannot perform that action. A records manager or system administrator with the appropriate classification level must do it for them.

Permissions: The Record.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

Use the previously described procedure to find an item to use. Select **Edit** then **Declassify** from the Page menu.

The Declassify Page is displayed. It is similar to the Review Classification Page with the addition of fields to specify the declassification.

Provide the following required information in the marked fields:

- The date and time of the declassification
- The person (or other entity) who declassified the item
- The reason for the declassification

When done, click **Submit Update**.

5.2.4.4 Undoing a Cutoff

After undoing a cutoff, the item is no longer cut off. Display the Content Information Page for the item. Select **Set Dates** then **Undo Cutoff** from the Page menu.

Permissions: The Record.UndoCutoff right is required to perform this action. This right is assigned by default to the predefined Records Administrator role.

5.2.5 Deleting, Moving, and Changing Content Items

Actions involving individual content items are usually done on the Content Information Page using the **Content Actions** Page menu. Select **Update** from that menu to access the menu choices discussed here. A frozen content item cannot be moved, deleted, or changed.

5.2.5.1 Moving an Item to Another Category or Record Folder

> **Permissions:** The Record.Edit right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

1. Select **Content Actions** then **Update** on the item's Content Information Page.

   The Info Update form is displayed.
2. Click the **Browse** button following the **Category or Folders** field label.

   The Select Category or Folders screen is displayed.
3. Click **Clear** to remove the current location.
4. Click the plus sign (+) or the icon to expand the retention schedule. Navigate to the retention category or record folder where the item will be moved. Click the category or folder to select it. The locator links display the hierarchical path of the category or folder in the retention schedule.
5. Click **OK**. The Select Category or Folders screen closes.
6. On the content information page, click **Submit Update**.

   The content information page displays the folder or category ID of the new location.

5.2.5.2 Deleting an Item

Use this procedure to delete content immediately outside of its disposition schedule. Metadata is not preserved. A frozen item cannot be deleted.

> **Permissions:** The Record.Delete right is required to perform this action. This right is assigned by default to the Records Administrator role. Delete permission (D) for the item's security group is also required (unless Folders is installed).

1. Display the item's Content Information Page.
2. In the Revision History area, click **Delete**. A prompt appears to confirm the permanent delete action.
3. A message is displayed stating the item was deleted successfully.

5.2.5.3 Assigning Disposition Schedules to Content Items

Use this procedure to assign a disposition schedule to an existing content item.

1. Select **Content Actions** then **Update** on the item's Content Information Page.

   The Info Update form is displayed.

2. Select the desired object. In the **Life Cycle** list, select the retention category whose disposition instructions should be assigned to the item.
3. Click **Submit Update**.

The content item is now processed in accordance with the disposition instructions associated with the selected retention category.

6

Managing Physical Content

This section discusses the creation and management of physical items with Physical Content Management. It covers the following topics:

Concepts

Tasks

6.1 About Physical (External) Content

As opposed to internal, electronic content managed by content management products, no copy of external, physical content is stored in the repository. Only its metadata (including storage information and retention schedule, if any) is stored when the information is checked in to the system.

When a user "checks in" an external, physical content item, the user must provide its basic metadata information and specify where the item is stored by selecting a location in the defined storage space hierarchy. If the user has the appropriate privileges, a retention schedule can also be assigned to the item, which determines its life cycle.

Physical items can be created within other physical items. This may be useful in situations where a "container" physical item is needed (for example, of object type "Box") and add "content" physical items within it (for example, of object type "Folder").

6.2 Managing Physical Items

This section discusses the tasks involved in managing physical items. Some tasks are allowed for administrators and for end users while others are restricted only to people with administrative privileges.

The following user tasks are discussed in the *Oracle Fusion Middleware User's Guide for Universal Records Management*:

- Creating a physical item

- Creating a physical item within another item
- Editing a physical item
- Moving a physical item
- Adding physical items to a content basket
- Marking physical items as reviewed
- Viewing reservations for physical items

The following tasks can be performed by administrators and are discussed in the following subsections:

- "Deleting a Physical Item" on page 6-2
- "Freezing and Unfreezing a Physical Item" on page 6-2
- "Printing a Label for a Physical Item" on page 6-4

6.2.1 Deleting a Physical Item

Permissions: The PCM.Physical.Delete right is required to perform this task. This right is assigned by default to the PCM Administrator role.

Use this procedure to delete an existing physical item. When deleting a physical item, its metadata, storage, and retention information are removed from the repository. Therefore, the item can no longer be tracked and managed.

A physical item cannot be deleted if it has other physical items contained within it.

1. Search for the physical item to delete.
2. On the search results page, choose the **Delete External Item** option in the item's Action menu.

   You can also choose the **Delete External Item** option on the Physical Item Information Page.

The physical item is deleted immediately, without any further prompts. If no errors occur, a message is displayed stating the physical item was deleted successfully.

6.2.2 Freezing and Unfreezing a Physical Item

Permissions: The Record.Freeze/Unfreeze right is required to perform this task. This right is assigned by default to the Records Administrator role. This right is not assigned by default to any PCM roles.

Use this procedure to freeze or unfreeze an existing physical item.

Freezing a physical item inhibits disposition processing for that item. For example, it will not be flagged for destruction, even if the action is due, until the item is unfrozen (when its frozen status revoked). This may be necessary to comply with legal or audit requirements (for example, because of litigation).

More than one freeze can be applied to an item. View the freeze details for the item to see a list of all freezes currently applied to the item.

If a physical item containing other physical items is frozen, all of those items are also frozen.

After a physical item is frozen, its metadata cannot be edited.

To freeze a physical item, complete the following steps:

1. Search for the physical item to freeze.
2. On the search results page, click **Edit** then click **Freeze** in the item's Action menu.

   You can also choose **Edit**, then select **Freeze** option on the Physical Item Information Page.

   To freeze all items on the search results page, choose the **Freeze Results** option in the Page menu.
3. In the Freeze Name list, select the freeze to be applied to the item. The list contains all defined freezes. A reason can be given for the freeze or leave the text box empty.
4. Click **OK** to confirm the freeze. Click **Cancel** to abort the entire action.

   If confirmed, the information page of the affected item displays "Is Frozen: Yes" and a **Details** link, which links to a detailed page for the item.

After an item is frozen, the freeze reason cannot be edited. If the freeze is no longer correct, unfreeze the item and freeze it with a new reason.

To unfreeze a physical item (cancel its frozen status), complete the following steps:

1. Search for the physical item to unfreeze.
2. On the search results page, click **Edit** then click **Unfreeze** in the item's Action menu.

   You can also choose **Edit**, then select **Unfreeze** on the Physical Item Information Page.

   The Unfreeze dialog is displayed.
3. In the Freeze Name list, select the freeze to be canceled for the item. The list contains all freezes currently applied to the item (at the item level). If needed, provide a reason for the unfreeze action or leave the text box empty.
4. Click **OK** to confirm. Click **Cancel** to abort the entire action.

   If confirmed, the Retention Schedule Information area of the content information page displays "Is Frozen: No" and no **Details** link is displayed.

Important: Multiple freeze may be applied to an item. Therefore, after an item is unfrozen, the Actions menu for the item may continue to include an **Unfreeze** option if other freezes are still applied to the item.

6.2.3 Printing a Label for a Physical Item

Permissions: The PCM.Admin.PrintLabel right is required to perform this task. This right is assigned by default to the PCM Administrator role.

Use this procedure to print a label for a physical item. By default, the label contains a barcode for the item, and its name, title, security group, and account (if applicable).

1. Search for the physical item for which to print a label.
2. On the search results page, click **Create Report** then the type of label.

You can also choose the Print Label option on the Physical Item Information Page.

6.3 Importing Physical Content Manually

If an import file already exists for physical content, that data can be imported into the system for tracking by PCM. This section describes the format for the file needed for correct importing.

6.3.1 Required File Format

The import file to be used must be an .hda file with three result sets:

- "LocalDataProperties" on page 6-4
- "ImportExportManifest" on page 6-4
- "ExternalItemsExtItems" on page 6-5

In the following examples, blank lines must be included where shown.

6.3.1.1 LocalDataProperties

This result set is used for the local data used by the Import service when importing the data. Set `aIncludeERM_Physical=1` for physical data to be imported.

```
@Properties LocalData
aIncludeERM_Physical=1
blFieldTypes= dCreateDate date,dLastModifiedDate date
blDateFormat='{ts' ''yyyy-MM-dd HH:mm:ss{.SSS}[Z]'''}'!tAmerica/Chicago
@end
```

If importing dates, the data must be in the format `{ts 'yyyy-mm-dd hh:mm:ss.mmm'}` if using the blDateFormat property set as shown in the Local Data result set. That format can be modifed but imported dates must then be in the same format.

6.3.1.2 ImportExportManifest

This result set provides the import function with the necessary data to import physical items. This result set can be copied into an .hda file as is.

```
@ResultSet ImportExportManifest
28
Name
Order
Caption
ResultSetName
```

```
ExportScript
ExportConditions
ExportClass
ExportAction
ExportParameters
ExportActionCopy
ImportScript
ImportConditions
ImportClass
ImportAction
ImportParameters
ImportPassName
UpdateClass
UpdateAction
UpdateParameters
UpdatePassName
UpdateForced
DeleteClass
DeleteAction
DeleteParameters
DeletePassName
Group
dSource
idcComponentName
aIncludeERM_Physical
300
csaIncludeExternal
ExternalItemsExtItems
<$hasCustomRights("ecm.pcm.physical.read")$>

Service
EXPORT_EXTERNAL_ITEMS
dSource,Physical

 <$hasCustomRights("ecm.pcm.physical.create")$>

Service
CREATE_EXTERNAL_ITEM


Service
EDIT_EXTERNAL_ITEM








content
Physical

@end
```

6.3.1.3 ExternalItemsExtItems

This result set contains the physical data being imported.

```
@Result Set ExternalItemsExtItems
11
dID 3 19
```

```
dDocName 6 100
dDocTitle 6 200
dDocAuthor 6 30
dDocType 6 30
dSecurityGroup 6 30
dPermLocation_Barcode 3 19
dActualLocation_Barcode 3 19
dExtObjectType 6 30
dMediaType 6 32
dSource 6 8
@end
```

Important: Set only one location value for each current and permanent location. The following list shows multiple options for setting these values.

The following fields are required:

- dID: the document identifier. This field can be left blank, but the field has to be in the definition. The system assigns a value if this is left blank.
- dDocName: the document name
- dDocTitle: the document title
- dDocAuthor: the assigned author/creator
- dDocType: the assigned document type
- dSecurityGroup: the assigned security group
- dExtObjectType: the object type for the item being imported (for example, a box or a document). The object type must exist in the system prior to importing.
- dSource: the source identifier. This must be set to `Physical`.
- dPermLocation_Barcode: the permanent location value. Set this value if the location value is the barcode value of the storage or container item where the object is being assigned.
- dActualLocation_Barcode: the current location value. Set this value if the location value is the barcode value of the storage or container item where the object is being assigned.
- dPermLocation: the permanent location value. Set this value if the location value is the dObjectID value of the storage item where the object is being assigned.
- dActualLocation: the current location value. this value if the location value is the dObjectID value of the storage item where the object is being assigned.
- dPermContainer: the permanent container location value. Set this value if the location value is the dID of the contain item where the object is being assigned.
- dActualContainer: Set this value if the location value is the dID of the contain item where the object is being assigned.

The following fields are optional:

- dMediaType: used to assign a media type to an item.
- dBarcode: used to provide a specific barcode for an item. Leave this blank and the system assigns the dDocName as the barcode.

Include any custom fields or other fields required for import.

6.3.2 Sample File

The following sample file demonstrates all result sets in an .hda file.

```
<?hda version="10.1.3.5.1 (090717)" jcharset=UTF8 encoding=utf-8?>
@Properties LocalData
aIncludeERM_Physical=1
blFieldTypes=xRecordFilingDate date,xArchiveDate date,xRecordCutoffDate
date,xRecordExpirationDate date,xRecordObsoleteDate date,xNewRevisionDate
date,xPublicationDate date,xRecordActivationDate date,xRecordSupersededDate
date,xRecordCancelledDate date,xRecordDestroyDate date,xDateClosed
date,xRecordRescindedDate date,xNoLatestRevisionDate date,xDeleteApproveDate
date,xRecordReviewDate date,xSuperSupersededDate date,dCreateDate
date,dLastModifiedDate date
aIncludeChargeTransactions=0
dLastModifiedDate={ts '2009-06-01 17:00:00.000'}
aExportDate=6/01/09 5:00 PM
blDateFormat='{ts' ''yyyy-MM-dd HH:mm:ss{.SSS}[Z]'''}'!tAmerica/Chicago
@end
@ResultSet ImportExportManifest
28
Name
Order
Caption
ResultSetName
ExportScript
ExportConditions
ExportClass
ExportAction
ExportParameters
ExportActionCopy
ImportScript
ImportConditions
ImportClass
ImportAction
ImportParameters
ImportPassName
UpdateClass
UpdateAction
UpdateParameters
UpdatePassName
UpdateForced
DeleteClass
DeleteAction
DeleteParameters
DeletePassName
Group
dSource
idcComponentName 6 30
aIncludeERM_Physical
300
csaIncludeExternal
ExternalItemsExtItems
 <$hasCustomRights("ecm.pcm.physical.read")$>

Service
EXPORT_EXTERNAL_ITEMS
dSource,Physical
```

```
 <$hasCustomRights("ecm.pcm.physical.create")$>

Service
CREATE_EXTERNAL_ITEM


Service
EDIT_EXTERNAL_ITEM







content
Physical

@end
@ResultSet ExternalItemsExtItems
11
dID 3 19
dDocName 6 100
dDocTitle 6 200
dDocAuthor 6 30
dDocType 6 30
dSecurityGroup 6 30
dPermLocation_Barcode 3 19
dActualLocation_Barcode 3 19
dExtObjectType 6 30
dMediaType 6 32
dCreateDate 5 20
dSource 6 8

B0000003050
ImportTestBox
sysadmin
ADACCT
Public
TSTIMPORT
TSTIMPORT
Box

{ts '2009-06-04 11:50:50.497'}
Physical

F0000003050
ImportTestFolder
sysadmin
ADACCT
Public
B0000003050
B0000003050
Folder

{ts '2009-06-04 11:50:50.497'}
Physical
@end
```

6.4 Processing Physical Content

This section explains how to process physical items used by PCM. It discusses the following topics:

- "Retention Schedules for Physical Items" on page 6-9
- "Disposition Events for Physical Items" on page 6-9
- "Pending Options for Physical Items" on page 6-10
- "Audit Log Files for Processed Events" on page 6-10

6.4.1 Retention Schedules for Physical Items

Physical items can be assigned retention schedules which define their life cycle. This links the physical item to a set of retention and disposition rules, which specify how long an item should be stored and when and how it should be disposed.

The same retention schedules and disposition rules may be used for physical items as for electronic items, but disposition rules can be defined specifically for physical items.

6.4.2 Disposition Events for Physical Items

A disposition event is any action needing to be performed on an item as part of its retention schedule (for example, after the retention period of the item has ended). Disposition events for physical items consist of three steps:

1. Approving the event
2. Performing the action(s) associated with the event such as physical destruction of the affected item(s).
3. Marking the event as completed.

> **Note:** The Destroy disposition event requires two steps for physical items, but not for electronic items. This is because the software can destroy electronic items for you, but it cannot destroy physical items. Destruction of physical items requires human intervention.

Physical items can be assigned the same disposition actions as electronic items. For an in-depth discussion of the available disposition actions, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

Due to the nature of physical items, some of the available disposition actions are less relevant than for electronic items:

- Disposition actions related to revisions because physical items cannot be revisioned:
  - Deleting old revisions
  - Checking in new revisions
  - Deleting previous revisions
  - Deleting revisions
  - Deleting all revision
- Disposition actions involving digital data:

- Scrubbing data. This includes overwriting it multiple times to prevent recovery as part of the destruction process.

If any of these disposition actions are assigned to physical items and they are due for completion, nothing specific needs to be done and they can be marked completed immediately.

6.4.3 Pending Options for Physical Items

Any pending events for physical items are included on the **My Approval List** page. To access this page, click **Records** then **Approvals** from the Top menu. Choose the type of approval to perform:

- Reviews
- Dispositions

To complete an action such as approval, review or a disposition, click the appropriate completion action from an item's **Action** menu. Some dispositions require approval before disposition processing.

Note: If the event action does not move to the completion list, then all affected items are frozen and cannot be processed. If the event action does move but also remains in the approval list, some affected items are frozen. The frozen items will not be processed until they are unfrozen.

6.4.4 Audit Log Files for Processed Events

When a disposition event for physical items is completed, an audit log file is created automatically and, if possible, is checked into the repository using the default metadata for audit logs. These checked-in log files can be used for audit trail purposes or as a verification tool.

Use the Search Audit Trail Page to search for disposition event that were processed for physical items by setting the Source field to 'Physical'.

The Admin.Audit right is required to search the audit trail.

Note: All completed disposition actions are included in the audit trail.

7

Managing Reservations and Barcodes

Physical Content Management offers circulation services for physical content items, in much the same way as a library circulates content. Users can receive items, keep them for a specific period then return them so they can be stored at their designated location again for someone else to check out. Users can also put a hold on unavailable items. If more than one person makes a reservation request for an item a waiting list, which specifies the order in which people made a reservation for the item. Barcode functionality is used in conjunction with reservations to easily track items which are either checked out or requested.

This chapter covers the following topics:

Concepts

- "About Reservations" on page 7-2
- "The Reservation Process" on page 7-3
- "About Barcodes" on page 7-6
- "Managing Barcodes" on page 7-9

The following tasks are typically performed when using reservations. These tasks can be performed by users depending on how the system has been set up. Therefore, these tasks are all discussed in the *Oracle Fusion Middleware User's Guide for Universal Records Management*:

- Creating a reservation request
- Editing a reservation request
- Deleting a reservation request
- Searching for reservations
- Saving reservation search results
- Viewing reservations for physical items
- Viewing your own reservation requests
- Editing a request item
- Canceling a request item
- Deleting a request item
- Changing the status of a request item

7.1 About Reservations

Reservations in Physical Content Management are handled using a special criteria workflow called "ReservationProcess," which is used for approval and notification purposes. This workflow must be configured and enabled. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about setting up that work.

The reservation workflow is not used if the "Check in internal content item for reservation workflow" setting on the Configure Physical Content Management Page is disabled. Users can still make reservations but e-mail notifications are not received (not even by the system administrator). If this is done, a different procedure to process reservations should be in place.

Users with the predefined PCM Requestor role can make reservations for physical items. Users with the predefined 'pcmadmin' role can also edit and process reservation request.

By default, if a user submits a reservation request for one or more items, a new content item is checked into the repository in the Reservation security group. If the workflow is enabled, this content item automatically enters the ReservationProcess workflow and the administrator receives a workflow review notification about the request.

Default metadata values can be set to be assigned to the reservation workflow item checked into the repository. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details.

The person in the administrator role receives e-mail notifications about pending reservations and the requesting user is not notified. Change this behavior by changing the ReservationGroup alias in the User Admin utility. For example, you could set up the workflow to also send e-mail notifications to the user who made the reservation request.

Clicking the **Review workflow item** link in the notification e-mail opens the Workflow Review for Request page, where the administrator can acknowledge the reservation request. As soon as the administrator clicks the **Approve** button on this page, the reservation request exits the workflow.

The administrator can then proceed and fulfill the reservation request in accordance with the applicable procedures within the organization.

The reservation process can be modified to suit an organization's need by changing the ReservationProcess workflow. For more information about workflows, see the *Oracle Fusion Middleware Application Administrator's Guide for Content Server*.

By default, each user can place only one reservation request for the same item. If users make reservation requests on behalf of multiple people (for example, manager assistants), it may be useful to override this behavior. To do so, add the following variable to the physicalcontentmanager_environment.cfg configuration file:

```
AllowMultipleRequests=true
```

7.1.1 Reservations History

All completed reservation requests are automatically logged in the reservations history. A reservation request is considered completed if none of its request items are still pending (in process), on a waiting list, or checked out.

By default, completed reservation requests are stored in the history log until it is deleted. A log is kept in the audit history table until it is archived.

Limit the maximum number of days a completed request is included in the history by modifying settings on the Configure Physical Content Management Page.

An administrator can view the current reservations history by searching for reservations with the Completed field set to 'Yes'.

7.2 The Reservation Process

The following is a typical fulfillment process of a reservation request:

1. A user creates a reservation request for one or more physical items.
2. As soon as the user submits the reservation request, the status of each requested item is automatically set to "In Process." If it was already "In Process" or "Checked Out," it is set to "Waiting List." See "Request Status" on page 7-4, "Transfer Method" on page 7-5 and "Priority" on page 7-5 for information about data used in reservation requests.
3. A reservation workflow is initiated and the administrator receives an e-mail notification to review the reservation request.
4. The administrator acknowledges the reservation request. If any items in the reservation request are not available or should be denied, the administrator can change their status accordingly.
5. All available requested items (not already checked out) are gathered from their storage location, in accordance with the organization's procedures. During this process, an appropriate transaction barcode is scanned to indicate it is checked out, the requestor’s barcode is scanned, and the barcode for the desired item is scanned.
6. The status of each available requested item is changed to "Checked Out" automatically after the barcode file is uploaded to PCM and the data is synchronized.
7. When the item’s status changes to "Checked Out," its current location (as shown on the Physical Item Information Page) is automatically set to the deliver-to location specified when the reservation request was created. If no deliver-to location was specified, the current location is set to "OTHER." The current location comment on the Physical Item Information Page is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
8. The requesting user can be notified and the reservation fulfilled in accordance with the applicable procedures within the organization. This is not handled by PCM but by the organization.
9. The user keeps the items for a specific number of days. If a bar code system is in place, after the item is returned, the item’s barcode is once again scanned, the barcode for the location of the item’s placement is scanned, and a transaction barcode is scanned to indicate the item is checked in and its location.
10. The status is changed to "Returned" and its current location set to its assigned storage location automatically after the barcode file is uploaded to PCM.
11. If a waiting list exists for the item, the status for the next requestor on the list should be changed from "Waiting List" to "In Process," so the item can be processed for the user. This can be done manually on any of the reservation pages, but if a barcode scanner is used to scan the item for check-in, it can be done automatically, depending on how the system is configured.

12. The status of the item continues to be "Returned" until the reservation is deleted. This can be done manually or automatically (after a certain number of days).

Depending on the procedures in place at the site, a charge may be levied for reservations and processing. Chargebacks and billing are discussed in the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

7.2.1 Reservation Request Properties

Each reservation request has several properties, including the following:

- "Request Status" on page 7-4
- "Transfer Method" on page 7-5
- "Priority" on page 7-5

7.2.1.1 Request Status

The request status specifies the current status for a reserved physical item, which can be any of the following:

- **Waiting List**: The request item is currently already checked out to someone else. It will become available to the next requestor upon its return (unless the system administrator chooses to override the waiting list order).
- **In Process** (initial default): The reserved item is available and is being prepared for delivery. Only one request item for a reservation can have the "In Process" status.
- **Not Found**: The request item could not be located in its designated location.
- **Unavailable**: The request item cannot currently be processed for delivery.
- **Denied**: The reservation request has been rejected by the administrator and cannot be fulfilled.
- **Canceled**: The reservation request was called off before it could be fulfilled.
- **Checked Out**: The reserved item is currently in the possession of someone as part of a reservation request. If a physical item is checked out, its current location (as shown on the Physical Item Information page) is automatically set to the value of the Deliver To Location field for the associated reservation request. If no value was entered in this field, the current location is set to "OTHER." Also, the current location comment on the Physical Item Information page) is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
- **Overdue**: The reserved item is currently checked out to someone who has failed to return the item within the configured checkout time. As a result, the reservation request cannot currently be fulfilled.

  By default, an e-mail notification is sent out to the user who has an overdue item. This e-mail notification can be disabled.
- **Returned**: The checked-out item was returned to the storage repository, so it is available for other users to reserve and check out.

A reservation request is considered completed if none of its request items are still pending (in process), on a waiting list, or checked out (including overdue).

The PCM.Reservation.Process right is required to change the status of a reservation request item. By default, this right is assigned to the predefined 'pcmadmin' role.

7.2.1.2 Transfer Method

The transfer method specifies how the person who made the request (the requestor) will receive the reserved item. Users specify the transfer method when a reservation request is created. The following transfer methods are supported:

- **Copy**: The physical content item will be duplicated and the copy will be provided to the intended recipient. The copy can be physical (for example, a copied DVD) or electronic (for example, an ISO image of a CD).
- **Fax**: The physical content item will be faxed to its intended recipient.
- **Mail**: The original physical content item will be mailed to its intended recipient.
- **Pickup**: The intended recipient will pick up the physical content item in person.
- **E-mail**: The content item will be e-mailed to its intended recipient.

The default transfer method is set on the Configure Physical Content Management Page.

7.2.1.3 Priority

The priority of a reservation request specifies the urgency with which it needs to be fulfilled. User specify the priority when they create a reservation request. The following priorities are supported:

- **No Priority**: Delivery of the requested item does not have any particular priority (there is no rush). The item can be delivered in accordance with the applicable fulfillment procedures.
- **ASAP Rush**: The requested item should be delivered to its intended recipient as soon as possible after the reservation was made.
- **This Morning**: The requested item should be delivered to its intended recipient the same morning the reservation was made.
- **Today**: The requested item should be delivered to its intended recipient the same day the reservation was made.
- **This Week**: The requested item should be delivered to its intended recipient the same week the reservation was made.

The default priority is set on the Configure Physical Content Management Page.

7.2.1.4 Request Item Actions

If you are an administrator, you can perform actions on a request item to change its status as part of the reservation fulfillment process. These actions are accessible through the Action menu for a request item on the Reservation Search Results Page or the Items for Request page. You can also perform the actions on multiple items simultaneously using the **Actions** menu on the Items for Request page.

Not all actions may be available for a particular request item, depending on the item's current status. For example, if the item is currently checked out, it can only be deleted or returned.

The following actions are supported:

- **Delete**: Deletes an item from a reservation request. If deleted, the request for that item is not included in the reservation log. The item is no longer in the item list for the reservation request. This option is available only if the system has been set up to allow users to delete items from a reservation request. In addition, requested items can be deleted only by a user with the PCM.Reservation.Delete right (assigned to the predefined PCM Administrator role by default).

- **Deny**: Rejects the reservation request for an item. The item will remain to be part of the reservation request, but it will not provided to the requestor.
- **Not Found**: Changes the status of an item because it could not be located in its designated location. The item will remain to be part of the reservation request, but it cannot currently be provided to the requestor.
- **Unavailable**: Changes the status of an item because it cannot currently be processed for delivery. The item will remain to be part of the reservation request, but it cannot currently be provided to the requestor.
- **Cancel**: Cancels the reservation request for an item before it is fulfilled. If a request item is canceled, the request for that item is still included in the reservation log (the item is still on the item list for the reservation, with its status set to "canceled"). Request items can be canceled only users with the PCM.Reservation.Edit right (assigned to the predefined 'pcmadmin' role by default). Only request item with the "In Process" status can be canceled.
- **Check Out**: Changes the status of an item because it was handed off to its intended recipient, who can now keep the item for the configured checkout period. After checking out a request item, its current location (as shown on the Physical Item Information Page) is automatically set to the value of the Deliver To Location field for the associated reservation request. If no value was entered in this field, the current location is set to "OTHER." Also, the current location comment on the Physical Item Information Page) is set to the location comment specified for the associated reservation request. If no comment was provided, it is set to the login name of the user who made the reservation.
- **Returned**: Changes the status of a checked-out item because it was returned handed off to its intended recipient, who can now keep the item for an agreed period.

7.3 About Barcodes

Barcode files are generated by barcode devices which scan storage information contained in barcodes located on physical content items or storage containers. A barcode is a machine-readable symbol used to store bits of data. In the context of physical content management, they can be used for purposes of identification, inventory, tracking, and reservation fulfillment.

Figure 7–1 Example of Barcode

Barcodes can be printed on labels attached to physical content items or storage containers holding such items (for example, a box). This helps track their location and status. User labels can also be created which help process reservation requests by users.

> **Important:** View barcode reports using HTML but print reports using PDF in order to ensure proper formatting.

The following technical information applies to barcodes in PCM:

- Physical Content Management uses the Code 3 of 9 barcoding standard (also called Code 39). This is a widely used standard for alphanumeric barcodes that can store upper-case characters, decimal numbers, and some punctuation characters (dash, period, dollar sign, slash, percent sign, and plus symbol).
- All lower-case letters are automatically converted to upper case. For example, if a user login is 'jsmith' then its barcode value is 'JSMITH'.
- Any accented letters and double-byte characters (such as Japanese and Korean) are encoded in their hexadecimal values. For example, if a user login is 'kmüller', then its barcode value is 'KMC39CLLER' (Ü = hex C39C). Therefore the barcode length increases as multiple hexadecimal characters are used to represent each accented letter or double-byte character.
- Barcode values for users default to their login names. This behavior can be changed for a user by setting a specific, unique barcode value for the user in the User Admin utility.

After scanning barcode information using a barcode reader, load the information into Physical Content Management. This can save time and money, and is especially useful to process large numbers of items (for example, during the initial Physical Content Management implementation).

There are two ways to load barcode information into Physical Content Management:

- Directly using the PCM Barcode Utility software.
- Manually by processing generated barcode files (see "Processing a Barcode File" on page 7-12.)

7.3.1 Barcode Files

Barcode files are generated by barcode scanners which read storage information from barcode labels and write this information to a file. Use the optional PCM Barcode Utility to directly load barcode information into the system or the barcode file can be processed manually.

Barcode files are plain-text files that are viewable using any text editor. Figure 7–2 shows an example of a barcode file.

> **Important:** Barcode files are created by barcode scanners and processed by Physical Content Management, and there is normally no reason to view or modify barcode files.

Figure 7–2 Example of Barcode File

```
H 20050721130204 00 0000000000
20050721130145 00 2000
20050721130151 00 +W1R1R1B1S1P3
20050721130152 00 B3
20050721130153 00 2000
20050721130154 00 +W1R1R1B1S1P4
20050721130156 00 B4
T 000
```

7.3.1.1 Barcode File Actions

When a barcode file is processed (automatically or manually), one of three actions are performed (specified for each item in the barcode file):

- "Check In" on page 7-8
- "Check Out" on page 7-8
- "Set Home & Actual" on page 7-8

7.3.1.1.1 Check In The Check In barcode action assigns an item to the location specified in the barcode file for the item. It is only the current location that is set, not the permanent location. Both the location and the item must already exist in Physical Content Management. If either does not exist, an error is reported.

[The location must already exist in the defined storage space hierarchy in Physical Content Management. If an item to be checked in does not yet exist in Physical Content Management, it is created and assigned to the specified location. If the item already exists, its current location is updated to match the value in the barcode file.]

7.3.1.1.2 Check Out The Check Out barcode action checks an item out to the user specified in the barcode file for the item (typically obtained by scanning a user label). The status for the item is set to "Checked Out" and its checkout user to the specified user (both values are shown on the Physical Item Information page). The item's current location is automatically set to the value of the Deliver To Location field for the associated reservation request (if there is one). If no value was entered in that field or if no reservation request exists, the current location is set to "OTHER," and the Location Comment field will show the name of the checkout user.

7.3.1.1.3 Set Home & Actual The Set Location barcode action assigns an item to the current and permanent locations specified in the barcode file for that item, allowing it to be moved to a different location. Both the locations and the item must already exist in Physical Content Management. If any of them do not exist, an error is reported.

The locations and items must already exist in the defined storage space hierarchy in Physical Content Management. The item’s current and permanent locations are updated to match the values in the barcode file.

7.3.2 The Barcode Utility Software

The Barcode Utility software is a Windows application providing an interface to the Videx LaserLite barcode scanner used with Physical Content Management. With this functionality, information can be read into the barcode scanner and uploaded into PCM. The barcode information can also be read and written to a file for manual processing at a later time. In addition, the Barcode Utility enables the reprogramming of the barcode scanner, should that be necessary.

The Barcode Utility software for Videx is provided but not automatically installed with the PCM software. To use, install the software after enabling PCM. The installer for the Barcode Utility is included on the PCM software distribution media.

Microsoft .NET Framework Version 1.1 Redistributable Package is needed to run the Barcode Utility. If not already on the computer, it can be downloaded from the Microsoft website at www.microsoft.com

The Barcode Utility can be installed on any computer that has a web connection to the server.

Important: If you upgrade the Barcode Utility from an earlier version, you ***must*** uninstall the existing instance before installing the new release. If you do not, an error message is reported during the installation and you will not be able to proceed.

To install the Barcode Utility, complete the following steps:

1. Locate the executable installer file, named *BarcodeUtility.exe* on the Physical Content Management distribution media. This is typically stored in the ucm\Distribution\urm*language* directory (different files are included for the different languages that are supported).
2. Double-click the setup.exe file to continue the installation.
3. Follow the instructions on screen to install the software.

From **Start**, select **Programs**, then select **Oracle**, then select **Barcode Utility**, then select **Barcode Utility**. You can also double-click the utility icon on the Windows desktop.

An interface is also provided to a Wedge Reader type of scanner which plugs in directly to the computer. If that type of scanner is enabled, data is automatically uploaded to a location on the screen where the cursor rests after three scans have taken place.

7.4 Managing Barcodes

This section discusses the following common barcode tasks:

- "Programming the Barcode Scanner" on page 7-9
- "Uploading Barcode Data Directly to PCM" on page 7-10
- "Saving Barcode Data to a File" on page 7-11
- "Uploading Previously Saved Barcode Data to PCM" on page 7-11
- "Processing a Barcode File" on page 7-12

For details about enabling a mobile bar code scanner, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

7.4.1 Programming the Barcode Scanner

The Videx Wand scanner may be pre-programmed for use at installation. Use the following procedure, if needed, to program the barcode scanner:

1. Start the Barcode Utility application.

   The Main Barcode Utility Screen is displayed.
2. Click **Options** then **Program Videx Wand**.

The Program Videx Barcode Wand Screen is displayed.

3. Choose the type of scanner to be programmed from the **Communication Device** list.
4. Choose the communication port where the device is connected.
5. Click **Program**.

   A message appears, indicating that the application is communicating with the scanner. The dialog closes when the programming finishes.
6. Click **Done** on the Main Barcode Utility Screen.
7. Push the **Scan** button on the scanner.

7.4.2 Uploading Barcode Data Directly to PCM

After gathering data with the scanner, the data can be directly uploaded to the server running the PCM software. The data can also be saved to a file and uploaded later.

Complete the following steps to upload the scanned barcode data directly to PCM:

1. Connect the scanner to the computer where the Barcode Utility is installed, either by placing the scanner in its base station or by using the connection cable.
2. Start the Barcode Utility application.

   The Main Barcode Utility Screen is displayed.
3. Select the scanner type.
4. Select the communication port where the barcode scanner is installed. Normally this is COM1, a commonly used serial port.
5. Make sure that the **Download To File Only** and **Allow File Selection** boxes are both cleared.
6. Click the **Process** button.

   A prompt appears to begin the upload process.
7. Select **Yes** to continue.
8. Select the host name of the instance where data files will be uploaded. The software must be installed on this computer.

   To configure the list of available hosts, complete the following steps:

   a. Click the **Advanced** button.
   b. The Configure Host List Screen is displayed.
   c. Enter the name of the instance where the repository is stored and the CGI URL for the instance.
   d. Click **Update** to add multiple names.
   e. Click **Done** when finished.
9. Enter the user name and password for a person who is allowed to upload data. To upload data, the user must have the predefined PCM Administrator role. Click **OK** after selecting the user name.

   The data is now transferred from the scanner to the PCM system. After all data has been transferred, a message is displayed, indicating the operation is complete.
10. Click **OK** to continue.

Important: If you select **No** when asked to confirm the upload, the data is erased from the barcode scanner and nothing is uploaded. The data is still available in a file called DATA.TXT (located in the installation directory of the Barcode Utility), but this file is overwritten the next time data is uploaded or saved to a file.

7.4.3 Saving Barcode Data to a File

Complete the following steps to save the scanned barcode data to a file:

1. Connect the scanner to the computer where the Barcode Utility is installed, either by placing the scanner in its base station or by using the connection cable.
2. Start the Barcode Utility application.

   The Main Barcode Utility Screen is displayed.
3. Select the scanner type.
4. Select the communication port where the barcode scanner is installed. Normally this is COM1, a commonly used serial port.
5. Make sure the **Download To File Only** box is selected.
6. Click the **Process** button.

   The data is stored in a file called DATA.TXT, which is located in the installation directory of the Barcode Utility. See "Uploading Previously Saved Barcode Data to PCM" on page 7-11 for details about uploading this data file at a later time.

Note: Data is always stored in a file named DATA.TXT. If not renamed, the file is overwritten the next time data is downloaded and stored as a file.

7.4.4 Uploading Previously Saved Barcode Data to PCM

If barcode data was saved to a file for later processing (see "Saving Barcode Data to a File" on page 7-11), use the Barcode Utility application to move the data to the PCM software for use.

Complete the following steps to upload a previously saved barcode data file:

1. Start the Barcode Utility application.

   The Main Barcode Utility Screen is displayed.
2. Make sure the **Allow File Selection** box is selected and click the **Process** button.

   A file selection dialog is displayed, showing the contents of the Barcode Utility installation directory (which is the default location of saved barcode data files).
3. Select the file to be uploaded, or navigate to the directory where the data files were stored and select a file from that location. Click **Open**.

   The Barcode Upload Screen is displayed.
4. Select the host name of the instance where the data file will be uploaded. The software must be installed on this computer.

   If you need to configure the list of available hosts, complete the following steps:

a. Click the **Advanced** button.
b. The Configure Host List Screen is displayed.
c. Enter the name of the instance where the repository is stored and the CGI URL for the instance.
d. Click **Update** to add multiple names.
e. Click **Done** when finished.

5. Enter the user name and password for a person who is allowed to upload data. To upload data, the user must have the predefined PCM Administrator role.
6. Click **Submit**.

   The barcode data file is processed and uploaded to the selected instance.
7. After the file upload has completed, a message is displayed. Click **OK**.

   The Barcode Upload Results Screen is displayed, allowing a review of the results of the upload.
8. Click **Done** when finished.

7.4.5 Processing a Barcode File

Permissions: The PCM.Barcode.Process right is required to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to process a barcode file containing information obtained using a barcode scanner.

1. Click **Physical** then **Process Barcode File** from the Top menu.

   The Barcode Processing Page is displayed.
2. Click the **Browse** button to select a barcode file to be processed.

   A file selection dialog is opened.
3. Navigate to the barcode file to be processed, select it, and close the file selection dialog.
4. Click **Process File**.
5. The barcode file is processed, and the Barcode File Processed Page is displayed. If any errors occurred, these are reported in the Message column. Click the **Info** icon to see more specific information about the error message.
6. When finished viewing the results of the barcode processing, click **OK** to return to the Barcode Processing Page.

8

Setting Up PCM Offsite Storage

This section explains how to set up and manage offsite storage in Physical Content Management. Offsite storage is an optional feature that enables users to set up requests for storage and to track storage processing.

This chapter covers the following topics:

Concepts

Tasks

8.1 Using Offsite Storage

With this release of Oracle URM functionality has been added to to allow customers to integrate storage with Iron Mountain SafeKeeper PLUS and other offsite storage facilities.

> **Important:** Iron Mountain configurations will vary from customer to customer. Be sure to test the integration in a development instance before using for production data.

The Offsite Storage link is an automated interface process for daily inventory and activity management between Oracle URM and offsite storage. This interface provides the following features:

- the automated creation of requests, both reference and permanent, for boxes and files from offsite storage.
- the automated creation of pickup requests for new and refiled boxes and files for storage and return to the offsite location.
- transfer of transmittal and individual list data for new boxes and files, and transmittal and list maintenance for existing boxes and files.

- the creation of a nightly log file listing inventory transaction history for a given day. This serves as a confirmation and data synchronization between the two systems.

To use this functionality, first map default values for different types of storage file formats to districts where the content is stored. Types of file formats include legal storage, insurance, loans, medical, and other storage types. Default districts are provided and default values for the fields used for storage.

After setting up the mapping, specify the storage parameters on the check-in page for physical content. After the content is checked in, a criteria workflow can be started to handle the approval of items pending transfer. This workflow must be created and enabled before the Offsite functionality can work. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about setting up this workflow. While not required, it is recommended that this workflow be used.

Iron Mountain is currently the primary offsite provider. After the appropriate configurations are in place, the files are first stored on the computer before being sent to and from Iron Mountain using File Transfer Protocol (FTP). After the files are compiled, they are uploaded to the /toplus directory in the software directory structure.

A confirmation file is sent from Iron Mountain and stored in the /fromplus directory in the Iron Mountain directory structure. A nightly history download log is also stored in the /fromplus directory after each night's district job is processed. Verify beforehand that the chosen FTP location has these directories already created.

Pickup lists are automatically created for items that must be transferred. Manual pickup lists can also be created as needed.

8.1.1 Setting Up Default Customer Information

First set up default customer information about the account to be used by the offsite provider. These defaults identify your company to the provider and are used to monitor and process offsite requests.

Follow these steps to configure defaults for offsite storage.

1. Click **Physical** then **Settings** from the Top menu.

   The Configure Physical Content Management Page is displayed.

2. Click **Enable Offsite Storage Functionality** then click **Submit Update**. The Configure Physical Content Management Page is displayed.

3. Refresh the browser window. Click **Physical** then **Offsite Storage** then **General Setup**.

   The Offsite Storage General Setup Page is displayed.

4. Fill in the necessary fields:

   - Customer ID: the customer ID used with this offsite storage facility.
   - Default District: the district to use. Select from a predefined list. If the district has not previously been defined, the definition must be mapped beforehand. See "Mapping New Districts" on page 8-3 for details.
   - FTP Address: enter the address associated with the FTP site.
   - FTP User: enter the user associated with the FTP site.
   - FTP Password: enter the password associated with the FTP site.

- Transfer checkboxes: choose options associated with the transfer:
  - Automatically transfer new items: enable automatic transfer of new items.
  - Automatically return checked-in items: enable automatic returns of items that have been checked in.
  - Enable workflow: start a workflow for this transfer action. The workflow must be created before this step. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about creating the workflow.
  - Use general requestor for Offsite Requests: choose a user from the list to use as the requestor. There is a limit of five characters for this value.
- Box Identifier: choose what identifier will be associated with the box. Options include **Name** or **Title**.

5. When done click **Submit Update**.

   A message is displayed indicating the offsite storage data has been configured.

8.1.2 Mapping New Districts

Several default districts are provided with Physical Content Management to use for offsite storage. Reconfigure any of these districts as necessary for your particular offsite solution.

The district mapping uses a wizard which steps through each stage of the process. When one stage is finished, the wizard displays the next screen in the process. For details about each screen and the fields displayed, see "District Mapping Screens" on page A-15.

The values used to populate the option lists for each field are based on data provided by Iron Mountain. For details about the field values, consult Iron Mountain documentation.

Follow this procedure to map district data:

1. Click **Physical** then **Offsite Storage** then **Map District Metadata** from the Top menu.

   The Choose District Mapping Page is displayed.

2. Select a district to configure from the list by scrolling through the list and highlighting a selection. Click **Configure** to select the district.

3. The next screen in the wizard appears. The process for mapping information is the same on each screen. Scroll through the values provided for the different fields and highlight a selection.

   Click **Save** to proceed to the next screen in the process. Click **Exit the Wizard** to exit the process without saving selections. Click **Reset** to clear the selections on the current screen. To move forward or back in the process and skip screens, select a different page from the page menu at the top of the screen.

   Eight screens are available for configuration:

   1. map box metadata
   2. map standard file metadata
   3. map account file metadata
   4. map insurance (1) metadata

   5. map insurance (2) metadata
   6. map law metadata
   7. map loan file metadata
   8. map medical file metadata
4. When finished configuring districts, click **Save**. A message is displayed indicating a successful exit from the wizard.

8.1.3 Creating Manual Pickup Requests

This function can be used to create requests to the offsite storage provider for pick up of materials.

Use this procedure to set up pickup requests:

1. Click **Physical** then **Offsite Storage** then **Create Manual Pickup Request** from the Top menu.

   The Create Manual Pickup Page is displayed.
2. Select a district ID from the list of IDs.
3. Enter a pickup location or select a location by using the **Browse** button to look at stored locations.
4. Enter the remainder of the information on the page.
5. To discard entries, click **Reset**. When done, click **Submit Update**.

8.1.4 Browsing Uploaded Files

You can browse all of the uploaded files and view the status of the files. If a file has failed to upload, the upload request can be resent from this page.

Use this procedure to view files:

1. Click **Physical** then **Offsite Storage** then **Uploaded Files List** from the Top menu.

   The Browse Uploaded Files Page is displayed.
2. To work with a file, check the box next to the file name. To delete a file, select **Delete** from the Table menu or the item's Action menu. To resend a file for processing, select **Resend**.

8.1.5 Browsing Processed Files

You can browse all of the processed files and view the status of the files. If a file has errors, you can then use this page to correct the errors.

Use this procedure to view files:

1. Click **Physical** then **Offsite Storage** then **Processed History Files List** Listfrom the Top menu.

   The Browse Processed History Page is displayed.
2. To delete a file, check the box next to the file name then select **Delete** from the Table menu or the item's **Action** menu.

8.1.6 Transferring Files to Offsite Storage

Transferring files for offsite storage occurs in two stages: files must first be generated then transfered.

To generate files for files for transferring, click **Physical** then **Offsite Storage** then click **Generate Offsite Transfer Files** from the Top menu.

To upload, download, or process the files, click **Physical** then **Offsite Storage** then click **Upload, Download, Process Offsite Files** from the Top menu. The files will be automatically transferred with other scheduled batch processes during the nightly services that are processed.

9 Scheduled Tasks

It is possible to set up a schedule to perform retention-related tasks at times that are more convenient for your environment. This chapter discusses scheduling tasks which can be performed at a later time. It covers the following topics:

Concepts

Tasks

Important: If jobs were scheduled in previous versions of this product, those jobs must be rescheduled. Schedule times and frequency are not automatically assigned when the product is updated.

9.1 Using Scheduled Tasks

Some of the tasks performed may involve large sets of content. Tasks such as processing retention assignments, performing archives, or customizing metadata may interfere with normal daily operations or put a heavy load on the system, which is undesirable during regular business hours.

With the scheduling feature tasks can be set to be performed at a later time, during off-peak times on the system. Freezes can also be scheduled to be performed at specific times. For details about creating and using freezes, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

See "Updating Information" on page 4-2 for details about viewing scheduled updates and searches.

9.1.1 Changes in Scheduling From Previous Product Versions

The following changes have been made to scheduling from previous versions of this product:

- **Dispositions can no longer be scheduled** and will be removed from any schedule after upgrading. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about dispositions.
- **Scheduled freezes** are migrated but they are not functional if the search engine type was changed (for example, from database to Oracle Text Search).
- **Scheduled screening reports** are migrated but they must be modified to use the correct query and the correct report template. If a template is not chosen a default template is used.
- **Scheduled freeze notifications** are not rescheduled after upgrading. The notifications should be resubmitted.

9.2 Managing Scheduling

This section discusses the following scheduling tasks:

- "Scheduling Screening Reports" on page 9-2
- "Editing Recurring Screening Reports" on page 9-2
- "Viewing Recurring Screening Report History" on page 9-3
- "Scheduling Freezes" on page 9-3

9.2.1 Scheduling Screening Reports

The scheduling functionality is discussed in detail in the *Oracle Fusion Middleware User's Guide for Universal Records Management*. This section provides an abbreviated overview of the process.

To schedule a screening report, first screen for information using the screening function. Click the **Schedule** button in the Screen for Topic Page. Choose the scheduling criteria such as name for the report, start date, indication if it will recur, and the recurrence frequency for the report. You can also subscribe to the report and be notified when the report is generated. Click **OK** when done.

The screening report is then put in the queue of actions to be performed. All scheduled screening reports are generated daily at midnight by default.

9.2.2 Editing Recurring Screening Reports

To edit a recurring scheduled screening report, complete the following steps:

1. Click **Records** then **Scheduled** then **Screening Reports** from the Top menu.

   The Scheduled Screening Reports Page is displayed.

2. Choose **Edit** in the **Actions** menu of the screening report to modify and select the Edit option to use:Modify the schedule or the criteria or the subscription to the report.

   - **Edit schedule**: used to change the scheduling criteria for the job. After clicking, the Edit Recurring Report Schedule Page is displayed. Change any schedule details and click **Submit Update** when done.
   - **Edit criteria**: used to change the criteria used for screening. After clicking, the Screen for Topic Page is displayed. Choose the new criteria for screening and click **Submit Update**.

- **Edit subscription**: if the user is subscribed to the report, that subscription can be changed to include other users or a group of users. Choose the new users and click OK when done.

9.2.3 Viewing Recurring Screening Report History

To view the history of recurring scheduled screening reports, complete the following steps:

1. Click **Records** then **Scheduled** then **Scheduled Screening Reports** from the Top menu.

   The Scheduled Screening Reports Page is displayed.

2. Choose **Report History** in the **Actions** menu of the recurring screening report whose history will be viewed.

   The View History Page is displayed.

3. To view a report, click its link in the Name column.

9.2.4 Scheduling Freezes

Use this procedure to schedule a recurring freeze of selected items.

1. Search for the items to include in the scheduled recurring freeze.
2. On the Search Results page, click **Edit** then **Freeze All Search Results** from the Table menu.
3. A dialog is displayed. Select the freeze reason from the list.
4. Enter a freeze reason (optional).
5. Check the box next to **Schedule Recurring Freeze Inclusion** then click **OK**.
6. The Scheduled Freezes Page is displayed.

9.2.5 Viewing Scheduled Job Information

Follow this procedure to view a list of all scheduled jobs (reports, freezes, and any other Oracle UCM scheduled jobs).

1. Click **Administration** then **Scheduled Jobs Administration** from the Main menu. Click **Active Scheduled Jobs**.
2. The Scheduled Jobs Listing Page is displayed, showing all scheduled jobs.
3. To view details about a particular job, click the **Info** icon for that job. To edit details about the scheduled job, select **Edit** from the Actions menu for a particular item.
4. The Job Information Page/Edit Job Information Page is displayed. This page can be used to edit job details such as priority, the type of job, and so forth. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for more details.

10 Processing Retention Assignments

Retention assignments are the items and events (disposition actions) for which users are responsible for reviewing or processing. A user can quickly access retention assignments by clicking **Records** then **Approvals** from the Top menu. They can also be accessed by clicking **My Content Server** then **My Records Assignments** from the Main menu.

This section discusses processing retention assignments, which include reviewing items subject to review and processing disposition actions. It covers the following topics:

Concepts

- "Items Subject to Review" on page 10-2
- "Approval and Completion" on page 10-2
- "Frozen Items and Event Processing" on page 10-3
- "Using Batch Processing" on page 10-3
- "Specifying an Alternate Reviewer" on page 10-3

Tasks

- "Viewing Pending Reviews and Dispositions" on page 10-6
- "Marking Content Items as Reviewed" on page 10-6
- "Editing Review Information" on page 10-7
- "About Disposition Processing" on page 10-8

10.1 About Retention Assignments

The **Approvals** menu options provide a link to items needing to be reviewed and all pending events needing to be processed.

A disposition is an action taken on content after a triggering event has occurred. For complete details about setting up dispositions, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

This chapter describes how dispositions are processed and what approvals may be needed in order for some specific types of disposition actions to proceed.

This section discusses the following topics:

- "Items Subject to Review" on page 10-2
- "Approval and Completion" on page 10-2

- "Frozen Items and Event Processing" on page 10-3
- "Searching Retention Steps and Actions" on page 10-3
- "Using Batch Processing" on page 10-3
- "Specifying an Alternate Reviewer" on page 10-3

10.1.1 Items Subject to Review

Content can be subjected to periodic review whether it is managed in a disposition or not. From a DoD perspective, content subject to review are 'vital'. According to NARA, the National Archives and Records Administration in the United States, 'vital records' are essential government agency content needed to meet operational responsibilities under emergency or disaster conditions, or are required to protect legal and financial rights of the Government. and update for any purpose so designated.

Organizations that are not government agencies may have content that is vital to their type of business and therefore subject to review.

Content that is subject to review typically comprise about five percent of content deemed critical to a business. Some examples of content of this type include:

- software source code
- patents and copyrights
- legal documents such as trusts, estates, and wills
- regulatory compliance data

Cycling vital content that is subject to review refers to the periodic replacement of obsolete copies of content with copies of current content. Initial reviews are based on the content release date content and the filing date for record folders. The next review date is based on the reviewer's last review date.

To find items awaiting review click **Records** then **Approvals** from the Top menu. Click **Pending Reviews**.

If you are a member of the RmaReviewers alias, click **List All** on the Table menu on the page. This shows all items awaiting review and the person assigned to do those reviews. Click **List Mine** to show only those items awaiting the logged-in user's approval.

10.1.2 Approval and Completion

Some pending triggering events require only approval by the person specified as the Notification Reviewer when the disposition was first set for the category. After the action has been approved, it is marked as such and is processed when dispostions are run, usually overnight. The disposition actions are logged in the audit log and are subsequently removed from the approval list.

Some events require two steps, depending on the event type and the item to be processed. First, they must be approved and after an action has been carried out manually, they must be marked as completed after the required event action has been executed (for example, physical transfer to a different location). See "Multi-Step Disposition Processing" on page 10-9 for details.

To view items awaiting disposition click **Records** then **Approvals** from the Top menu. Click **Pending Dispositions**. To also access pending dispositions click **My Content Server** then **My Records Assignments** from the Main menu.

10.1.3 Frozen Items and Event Processing

After an event has been processed (approved and marked as completed if required) it should automatically be removed from the pending event pages (approval list and/or completion list). If an event remains on these pages there is probably a frozen item or folder preventing its removal.

For example, if a total of ten items are affected by a Destroy event and one of them is frozen, then the event for that one item will remain in the approval list, and the event will move to the completion list for the other nine items. These nine items can then be destroyed and the event marked as completed, but the frozen item cannot be processed until it is unfrozen.

See "Viewing Failed Dispositions" on page 10-5 for information about how to find those dispositions that did not succeed.

10.1.4 Searching Retention Steps and Actions

Use the Retention Step Search Page to screen for disposition steps. For example, a user can screen to discover what actions have been approved, who approved them, and what actions are done. From the screening results, a report can be created that can then be used as a destruction certificate, if needed. To access this page, click **Records** then **Audit** then **Retention Steps** from the Top menu. See "Searching Retention Steps and Actions" on page 10-3 for details.

Information can also be displayed about any disposition actions which did not process correctly. The Failed Dispositions Page shows those dispositions actions which did occur as specified. To access this page, click **Records** then **Audit** then **Fail Dispositions** from the Top menu. See "Viewing Failed Dispositions" on page 10-5 for more details.

10.1.5 Using Batch Processing

Pending events and review cycles are processed by the system every night on a 24-hour cycle. Notifications are sent daily at midnight.

Use the **Batch Services** options on the **Records** menu to process certain actions immediately rather than wait for the scheduled processing time. Options on the Batch menu include:

- **Run All**: processes all events pertaining to reviews or dispositions
- **Process Dispositions**: processes all disposition-related pending events
- **Process Reviews**: processes pending reviews regardless of whether items are in a disposition or not.
- **Send Notifications**: sends any pending notifications relating to dispositions
- **Run Other**: processes other batch services unrelated to disposition processing such as notification of monitoring alerts, scheduled key rotation, and so on.

10.1.6 Specifying an Alternate Reviewer

It may be useful to select another user than yourself to perform review actions and process disposition events, for example when you are out of the office for some time. Alternate reviewers can be specified in your user profile. They will then receive e-mail notifications of any pending actions assigned to you and can act on them.

Permissions: The Admin.PerformActions or Admin.PerformPendingReviews right is required to perform this action. The Admin.PerformActions right is assigned by default to the Records Administrator role. The Admin.PerformPendingReviews right is assigned by default to all roles. A user can also ask your Records Administrator to specify an alternate reviewer.

Log in and open your user profile. Select an alternate reviewer from the list. The list includes all users who have been specified as default notification recipients as discussed in the *Oracle Fusion Middleware Setup Guide for Universal Records Management*. The selected person will now receive e-mail notifications of pending actions and events assigned to you.

By default, only the alternate reviewer will receive notifications and not the users. The system can be configured so both the users and the alternate reviewer are notified. To accomplish this, make sure the config.fg configuration file contains the following line:

```
RmaNotifyReviewerAndAlternateReviewer=true
```

Restart the content server for this setting to take effect.

10.2 Managing Disposition Tasks

The following tasks are performed when processing disposition actions:

- "Screening for Retention Steps" on page 10-4
- "Viewing Failed Dispositions" on page 10-5
- "Viewing Pending Reviews and Dispositions" on page 10-6
- "Marking Content Items as Reviewed" on page 10-6
- "Editing Review Information" on page 10-7
- "About Disposition Processing" on page 10-8

10.2.1 Screening for Retention Steps

Permissions: The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To screen for disposition actions and events, complete the following steps:

1. Click **Records** then **Audit** then **Retention Steps** from the Top menu.

   The Retention Step Search Page is displayed.

2. Select the criteria for the search from the provided pulldown lists. The options on the lists will vary depending on customizations in place at the site. This list provides some examples of the type of criteria available:

   - Sources: Select the repository source for the search. Click the Select button to display a list of sources which can be used.
   - Disposition Criteria: Includes criteria specific to dispositions such as a derived triggering event or location type.

- Category Criteria: Includes criteria specific to retention categories such as restrictions (edits, revisions, deletions) and review information (review periods and reviewers).
- Records Folder Criteria: Includes criteria specific to folders such as cutoff date, profile trigger, and freeze name for freezes applied to the folder.
- Content Criteria: Includes criteria used for content such as author and content type.
- Retention Steps Criteria: Includes options for retention actions such as freezing dispositions and action state.

3. Select sorting preferences in the **Results Options** area.
   a. Use the defaults or select another option from the **Sort By** list.
   b. Sort by default descending order or select ascending order.
4. To view the results of the screening immediately, click **Search**. Any results matching the screening criteria display in the Retention Step Audit Result Page.
5. To schedule the retention report to run later, select the criteria for the screening and click the **Schedule** button.

   The Schedule Retention Step Audit Report Page is displayed.
6. Provide a **name** for the screening report.
7. Provide the **start date** of the screening report. This is the date the scheduled screening report will be generated. If the screening report is recurring, the first screening report will be generated for the first time on this date, and all subsequent reports at the end of each recurring period after this date.
8. To create a screening report periodically rather than just once, select the **Is Recurring** box. Specify the interval at which the recurring screening report will be created (for example, every 2 weeks).
9. Click **OK** when done.

10.2.2 Viewing Failed Dispositions

Permissions: The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

Follow this procedure to find disposition actions which have not succeeded and 'replay' those actions as needed.

1. Click **Records** then **Audit** then **Failed Dispositions** from the Top menu.

   The Failed Dispositions Page is displayed.
2. Use this page to view information about failed disposition actions. The following actions can also be performed:
   - To restart the disposition, select the checkbox for the item and click **Retry** from the Table menu.
   - To create a report of failed dispositions, select the items to include in the report then click **Create Reports** from the Table menu.

- To mark the disposition as complete regardless of whether the action succeeded or not, click the checkbox for the item and click **Skip** from the Table menu. Use this option with caution because it may have unforeseen consequences when a disposition is skipped.

10.2.3 Viewing Pending Reviews and Dispositions

Permissions: The Folder.Read right and Record.Read right are required to perform this action. All predefined management roles have this right. The Admin.PerformActions right is required to view your own or pending events of others. This right is assigned by default to the Records Administrator role.

Follow this procedure to view pending actions to be taken:

1. Click **Records** then **Approval** from the Top menu. Choose the type of pending approval to view: Reviews or Dispositions.

   The Pending Dispositions Page or Pending Reviews Page is displayed.

2. These pages listactions awaiting approval. It lists actions assigned to the logged-in user as well as actions assigned to other users if the logged-in user has permission to see those actions.

10.2.4 Marking Content Items as Reviewed

Follow this procedure to perform reviews. Use this procedure to review items that have been marked as Subject to Review, or items in a category that has a disposition that is Subject to Review.

Permissions: The Admin.PerformPendingReviews right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator role. When performing reviews of items assigned to others, you must also be designated as the main notification recipient.

1. Follow the link in the e-mail sent by the system to notify the reviewer or click **Records** then click **Approvals** then **Pending Reviews**.

   The Pending Reviews Page is displayed.

2. Click the checkbox of the item to be reviewed then click **Set Dates** and **Mark Reviewed** from the Table menu. If this is a folder to review, the option **Mark Reviewed Recursive** can be used to mark all items in the folder as reviewed.

   In addition, you can click **Set Dates** then select **Mark reviewed** from the **Actions** menu for individual items.

   To perform a different action involving dates (mark the item as expired, canceled, or obsolete, for example), click the item’s **Action** menu then click **Set Dates** and choose the appropriate menu option.

3. Enter a comment for the action (review, expiration, and so on) or leave that field blank if a comment is not needed.

The current date is inserted to indicate the date on which the action happened. This date can be changed by typing a new date or selecting one from the calendar icon.

After inserting the information, click **OK**. The item is then removed from the list of pending reviews.

10.2.5 Editing Review Information

Permissions: The Category.EditReview right or Folder.EditReview right is required to perform these actions. This right is assigned by default to the Records Administrator role.

Follow this procedure to edit retention category or record folder review information:

1. Find the Retention category or folder to use.
2. Click **Edit** then **Edit Review** from the page **Action** menu (if editing a category review) or the item's **Action** menu (if editing a folder review).

   The Edit Review Information for Retention Category/Folder Page is displayed.
3. To change a review category to non-review category, clear the **Subject to Review** box. The remaining fields become gray and unavailable. To change a non-review category to a review category, select the **Subject to Review** box.

   Tech Tip: Remember the review setting is inherited. If items or record folders should stay as subject to review, make sure to set the review information for the child record folders that no longer inherit review status from their retention category. Any content filed directly into retention categories are directly affected by review status changes.

   ---
4. To select, remove, or change a reviewer, select the reviewer from the **Reviewer** list. Select the topmost blank to remove the reviewer and allow the system default to designate the reviewer.
5. To edit or enter the review period, enter an integer and select a review period in the **Review Period** box and list.
6. Click **Submit Update**. An update message is displayed, and the Retention Category Information Page displays the review information that was entered.

When editing folder review information, keep the following points in mind:

- The Folder.EditReview right is required to perform the action. This right is assigned by default to the Records Administrator role.
- Follow the same procedure to change folder review information as that used to change an item's review information. Remember the review setting is inherited, and if any child folders should stay as subject to review, make sure to set the review information for record folders that no longer inherit it from a parent folder or category.
- The selected reviewer must have the Records Administrator or Records Officer role because users assigned the Records User role cannot mark a record folder as reviewed.

10.2.6 About Disposition Processing

This section contains procedures for processing pending events.

- "Accessing the Pending Approval Interface" on page 10-8
- "Event Processing" on page 10-8
- "Pending Approvals" on page 10-8
- "Pending Review" on page 10-9

10.2.6.1 Accessing the Pending Approval Interface

In the following event descriptions, all events are accessed by clicking **Records** then **Approvals** and selecting **Pending Review** or **Pending Disposition** or by clicking the link in the email notifiying a user of dispositions or reviews to be performed.

Events for yourself are listed. To view assignments to other users, you must be added to the RmaReviers alias. Then click **List All** on the Table menu on the Pending Dispositions Page or Pending Reviews Page.

10.2.6.2 Event Processing

The following list describes common functionality regardless of the type of action being processed:

- The Admin.PerformActions right is required to perform these actions. This right is assigned by default to the Records Administrator role.
- For most events, when the disposition event is processed, an audit log file is created automatically. A screening can be done for that audit log and it can be checked in as a content item if needed. An audit log is not created for a *Move* event or a *No Action* event.
- Most actions are run automatically with the batch services that are run nightly or when a Batch Services option is selected by clicking **Records** then **Batch Services**.

10.2.6.3 Pending Approvals

The following persons may receive notifications of events triggered by disposition rules, depending on the system configuration:

- the author or "filer" of a retention category
- members of the RmaReviewers alias group
- the additional notification reviewer, if specified when the disposition rule was set up for the category

The pending events appear in both the other notification recipient's approval list and the filer's own approval list. If the main recipient processes the event, the event is removed from the author's approval list and vice versa. Some events only require approval. After approval of these events, their associated disposition actions are executed when the dispositions are run, usually nightly, unless otherwise processed by selecting an option from the Batch Services menu. The processed events are subsequently removed from the approval list.

Some events require multiple steps, depending on the event type and the item to be processed. First, they must be approved and after approval they must be marked as completed. Items marked as completed often must be physically moved to complete the action (for example, transferring an item to different location).

When an event must be marked as complete, it still appears on the Pending Dispositions Page and the name of the event is changed to indicate it must be marked complete (for example, **Mark Transfer Complete**). To mark the item as complete, check the box for the item then click **Approve** from the Table menu.

10.2.6.4 Pending Review

To mark multiple items as reviewed, click the checkbox for the item and choose **Mark Reviewed** from the **Set Dates** menu on the Pending Reviews Page. A prompt appears to enter any review comments.

The current date is inserted as the review date. This date can be changed by typing a new date or selecting one from the calendar icon.

After inserting the review information, click **OK**. The item is then removed from the list of pending reviews.

10.3 Processing Dispositions

Disposition actions can be divided into two types: those requiring one step for completion and those requiring multiple steps. This section describes each type of disposition processing.

Dispositions are grouped and held in batches. They are automatically scheduled and executed at the same time as other batch processes, normally at midnight or later.

To execute dispositions immediately, click **Records** then **Batch Services** from the Top menu. Select the type of action to process (dispositions, review, notifications, and so on). See "Using Batch Processing" on page 10-3 for information about the options on the Batch Services menu.

If a processed event does not become available to mark as complete, then affected items (for example, content in a folder) are frozen and cannot be processed. Use the **List Disposition Folders and Content** option from the item's **Action** menu to view the contents of the folder. The frozen items will not be processed until they are unfrozen. It is also possible the disposition failed. See "Viewing Failed Dispositions" on page 10-5 for information about checking on a disposition status.

10.3.1 Multi-Step Disposition Processing

The follow disposition events require multiple steps for processing. For complete details about disposition events, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*:

- **Accession**: An accession is one of the last actions in a disposition sequence. Files for accession are stored in a directory (typically in the *weblayout_dir*/groups/secure/rm/RmaAccessionApp directory) and a user can then choose how to hand off the files to the final archive institution.

  The option also is available to destroy the items while retaining their metadata or to destroy items without retaining metadata. This option is selected when the category's disposition is created. An accession event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed.

- **Archive**: The Archive action creates a zip file of the content and folder. Within each zip archive, there is a copy of each item and its metadata. The *meta* files contain the item metadata in the format specified by the Archive Meta Data Format setting on the Configure Retention Settings Page (hda, xml, or csv). An archive event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed. The .zip file is stored in a location on the computer. To see the location, click **Archive Location** from the Action menu of an Archive action on the Pending Dispositions Page.

- **Move**: A move action does not leave a copy of internal (electronic) items on the system. This action should not be confused with moving retention items within the retention management system, which is accomplished with the **Move** command within the retention schedule (Browse Content menu). A move event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed.
- **Transfer**: A transfer action leaves a copy of internal (electronic) items on the retention management system. A transfer event can be considered complete when an organization sends the items to another organization. A transfer event consists of two steps: it must be approved first and then, after the action has been carried out, it must be marked as completed. A *terminal transfer* action is when the transfer disposition action is the last action for a disposition schedule. If the Transfer action is the last step (rule) in a disposition action, the items must be destroyed before the step can be marked as completed.

One aspect of these events is the ability to destroy items in conjunction with the processing. For example, you can choose to transfer items and destroy the metadata after the transfer, or you can retain the metadata. Another example is to move content and either destroy or keep the metadata. These actions are chosen when the disposition for the category is set up initially. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details.

The number of disk scrubbing passes that accomplish the destruction can be configured by setting the following parameter in the config.cfg environment file:

```
RecordsManagementNumberOverwriteOnDelete
```

Restart the content server after setting this variable. By default, the number of scrubbing passes on the hard disk is set to 2.

The destroy process can consist of one or two steps. For electronic (internal) items, multiple actions are carried out automatically by the system. If metadata was to be destroyed with the items, that is done as well.

For physical (external) items, which are managed using Physical Content Management, two steps are required: the event must be approved first and then, after the external items have been destroyed manually, it must be marked as completed.

10.3.1.1 Approval Step

The name listed in the ID column is the name of the category involved in the disposition followed by a step number. Note that numbering begins with step 0.

1. Click **Records** then **Approvals** from the Top menu. Click **Pending Dispositions** or click the link in the notification email.

   The Pending Dispositions Page is displayed.

2. To view information about the disposition action, click the action name. The Disposition Information Page is displayed. To view what items are included in this action, click **List Disposition Folders and Content** from the **Actions** menu of a disposition action. An individual disposition can also be approved from this menu.

3. Click the checkboxes of the actions to approve and click **Approve** on the Table menu.

   The Disposition Parameter Dialog is displayed.

4. Enter a reason for the action and click **OK**. To abort the entire action, click **Cancel**.

5. The action is approved. After processing (either during the scheduled processing time or after a batch service is run) the event appears on the Pending Dispositions Page and is available to mark as completed if needed.

10.3.1.2 Completion

After an item has been marked as approved and is processed, it remains on the Pending Dispositions Page but the name of the action is changed to **Mark** *action* **Complete** (for example, Mark Accession Complete).

Internal items are completed as needed automatically. This action is transparent to users but the system approval steps are listed in the disposition.

Follow these instructions to mark an action as completed:

1. Click **Records** then **Approvals** from the Top menu. Click **Pending Dispositions** or click the link in the notification email.

   The Pending Dispositions Page is displayed. Note that all disposition actions awaiting approval are displayed, not just those actions awaiting completion.

2. To view information about the disposition action, click the action name. The Disposition Information Page is displayed. To view what items are included in this action, click **List Disposition Folders and Content** from the **Actions** menu of a disposition action. An individual disposition can also be approved from this menu.

3. Click the checkboxes of the actions to approve (mark complete) and click **Approve** on the Table menu.

4. The Disposition Parameter Dialog is displayed. Enter a reason for the disposition action and click **OK**. Click **Cancel** to abort the entire action.

   If the action requires a decision involving destruction (that is, to detroy or keep metadata associated with the action), choose a destruction method from the pulldown menu in the Disposition Parameter Dialog. Disposition actions that involve such a choice are Accession, Archive, Move, and Transfer.

5. The action is removed from the Pending Dispositions Page. If further approvals are needed (that is, if another action must be taken to complete the disposition) that action will appear on the Pending Dispositions Page after processing (either during the scheduled processing time or after a batch service is run.

10.3.2 Single Step Disposition Processing

The following dispositions require single step processing:

- **Classified Records Actions**
  - **Review Classification**: This action indicates it is time to review the security classification status of an item.
  - **Upgrade Classification**: This action indicates it is time to increase the security classification of an item. Classifications can be increased as high as the classification of the user applying the classification.
  - **Declassify**: This action indicates it is time to declassify content.

   - **Downgrade Classification**: This action indicates it is time to lower the security classification of an item.

- **Dispose Actions**
   - **Delete Previous Revision**: This action indicates it is time to delete the revision before the content item revision that triggered the disposition action. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
      - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 4 is marked for deletion.
      - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 2 is marked for deletion.
   - **Delete Revision**: This action indicates it is time to delete the content item revision that triggered the disposition action. This revision may be the latest revision of a content item, but does not need to be.
      - If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then only revision 5 is marked for deletion.
      - If a content item has 5 revisions and this disposition action is activated for revision 3, then only revision 3 is marked for deletion.
   - **Approve Deletion**: This action indicates it is time to approve record folders or content for deletion.
   - **Delete All Revisions**: This action indicates it is time to delete the content item revision that triggered the disposition action and all earlier revisions. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
      * If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then revisions 1 through 5 are marked for deletion (effectively removing the content item altogether).
      * If a content item has 5 revisions and this disposition action is activated for revision 3, then revisions 1 through 3 are marked for deletion.
      - If the DoD Config module is enabled, all revisions can be deleted and the metadata destroyed or kept, or only old revisions destroyed. Metadata cannot be retained unless the DoD Config module is enabled.
   - **Delete Old Revisions**: This action indicates it is time to delete all revisions before the content item revision that triggered the disposition action. The revision that activated the trigger may be the latest revision of a content item, but does not need to be.
      * If a content item has 5 revisions and this disposition action is activated for revision 3, then revisions 1 and 2 are marked for deletion.
      * If a content item has 5 revisions and this disposition action is activated for revision 5 (the latest revision), then revisions 1 through 4 are marked for deletion.
   - **Delete Working Copy**: This action deletes the working copy of a cloned content item. It first deletes the direct working copy of the clone. Then all previous revisions of the working copy are deleted until a revision of the fixed clone itself is found. The deletions stop at that point.
   - **Delete Previous Clones**: This action deletes the previous clone of a content item.

- **Other**
  - **Check in New Revision**: This action indicates it is time to take the latest revision of the affected content items and check a copy of this revision as a new revision. This may be useful to process a content item revision based on changed historical information, "refresh" an expired document, or enter a content item into a criteria workflow for disposition processing.
  - **Activate**: This action indicates it is time to activate record folders or content.
  - **Close**: This action indicates it is time to close record folders.
  - **Cutoff**: This action indicates it is time to cut off content or record folders from further processing. Cutoff refers to changing the status of items to prohibit further processing.
  - **Cutoff and Create Volume**: This creates a volume folder, content is placed inside, and the volume is cut off.
  - **Expire**: This action indicates it is time to expire record folders or content.
  - **Obsolete**: This action indicates it is time to mark content as obsolete.
  - **Mark Related Content**: This action marks any content linked to the current content.
  - **No Action**: This action indicates there is no action to take currently. This action usually found mid-disposition. A No Action action acknowledges a disposition milestone has passed, and the next step in the disposition begins processing.
  - **Notify Authors**: This action indicates it is time to notify the author of the affected category that disposition actions are due for the category.
  - **Supersede**: This action indicatesthat new content will be checked into the category or folder, superseding the original content item. The superseded item is indicated by a strikethrough on its name.

10.3.2.1 Approving Events

1. Click **Records** then **Approvals** from the Top menu. Click **Pending Dispositions** or click the link in the notification email.

   The Pending Dispositions Page is displayed.

2. To view information about the disposition action, click the action name. The Disposition Information Page is displayed. To view what items are included in this action, click **List Disposition Folders and Content** from the **Actions** menu of a disposition action. Individual items affected by the current action can also be approved using this menu.

3. Click the checkboxes of the actions to approve and click **Approve** on the Table menu.

   The Disposition Parameter Dialog is displayed.

4. Enter a reason for the action and click **OK**. To abort the entire action, click **Cancel**.

5. The action is approved and is removed from the Pending Dispositions Page.

11

Generating Reports

Several types of reports are provided with the software. These reports can be used to track user and group usage of the system and provide summary information for content and items involved with physical content such as invoices, chargebacks, and storage.

In addition, reports can be created as needed about the data that appears on the screen as a search result, content information, and so on. If these kinds of reports are available, an option appears on the Page menu on the screen, indicating the default reports available for that data.

Customized reports can also be created that are based on existing reports. Creating a customized report requires in-depth knowledge of service calls and queries. That type of report creation is discussed in the *Oracle Fusion Middleware Setup Guide for Universal Records Management*. This chapter discusses how to set default report options and how to produce the default reports provided with the software.

The following topics are discussed in this chapter:

11.1 Configuring Report Options

Reports are initially configured through menu options on the Configure Report Settings Page. During configuration a profile can be specified to be used when creating or updating a report template, and a profile to be used when creating or updating a report. A report format can also be chosen and if the report or template should be included when performing searches.

> **Note:** If barcode labels will be printed, specify PDF for the report format. Labels will display in HTML output but they can only be printed correctly using the PDF option.

Follow this procedure to configure default options to be used with all reports:

1. Click **Records** then **Configure** from the Top menu. Click **Reports** then **Settings**.

   The Configure Report Settings Page is displayed

2. Choose the report template profile from the option list or use the default profile provided.

3. Choose the profile to use when creating or updating a report.
4. Choose the report format to use. Options include HTML, PDF, RTF, or XLS. Note that if barcode labels are to be printed, this must be set to PDF.
5. Check the box to exclude all report templates during search operations.
6. Check the box to exclude all checked-in reports during search operations.
7. When finished, click **Submit Update**.

11.2 User and Group Reports

After creating users and alias groups, and assigning management roles and rights to users, reports can be generated to view at a glance which users and alias groups have access to the system. The following reports are available:

- "User Report" on page 11-2 (which includes bar code reports)
- "User Roles Report" on page 11-5
- "Group Report" on page 11-5
- "Group-User Report" on page 11-6

For details about the audit report, see Chapter 12, "Monitoring, Customizations and Audit Tools".

Reports are generated in the format specified by the setting on the user's profile page. To see the user format that is specified, click the user name in the top right corner of the screen and the User Profile page is displayed. If the system format is used, that is specified on the Configure Report Settings Page.

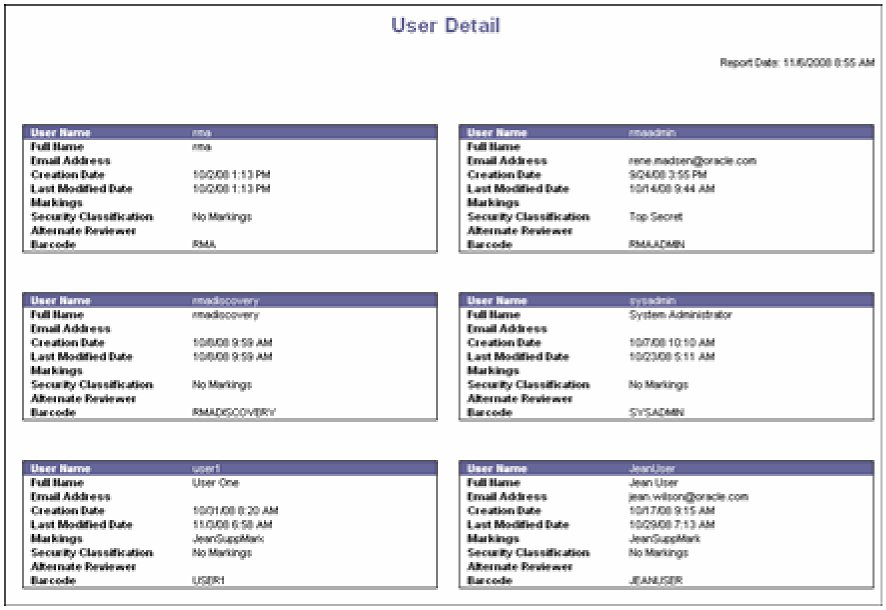
If the generated report file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

To generate reports, click **Records** then **Reports** then the report type from the Top menu.

Permissions: The Admin.Reports right is required to produce any reports. This right is assigned by default to the Records Administrator role. The Admin role is also required.

11.2.1 User Report

A list can be generated of all users who have access to the system as well as a barcode list for the users. A report can also be created that can be used to produce barcode labels. The users and the bar codes assigned to them are defined in User Admin utility.



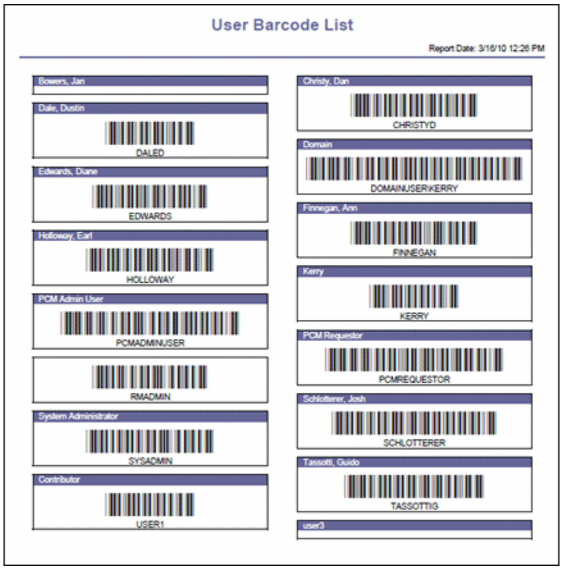
This report lists overview information for each user.

Column	Description
User Name	Displays the name of the user as entered in the User Admin utility.
Full Name	Displays the full name of the user as entered in the User Admin utility.
E-mail Address	Displays the e-mail address of the user.
Creation Date	Displays the date and time the user was created in the User Admin utility.
Change Date	Displays the date and time the user information was last modified.
Supplemental	Displays any supplemental markings assigned to a user.
Security Classification	Displays the classification assigned to the user.
Alternate Reviewer	Indicates the alternate reviewer for this user.
Barcode	Displays the barcode designation for the user.

11.2.2 User Barcode Reports

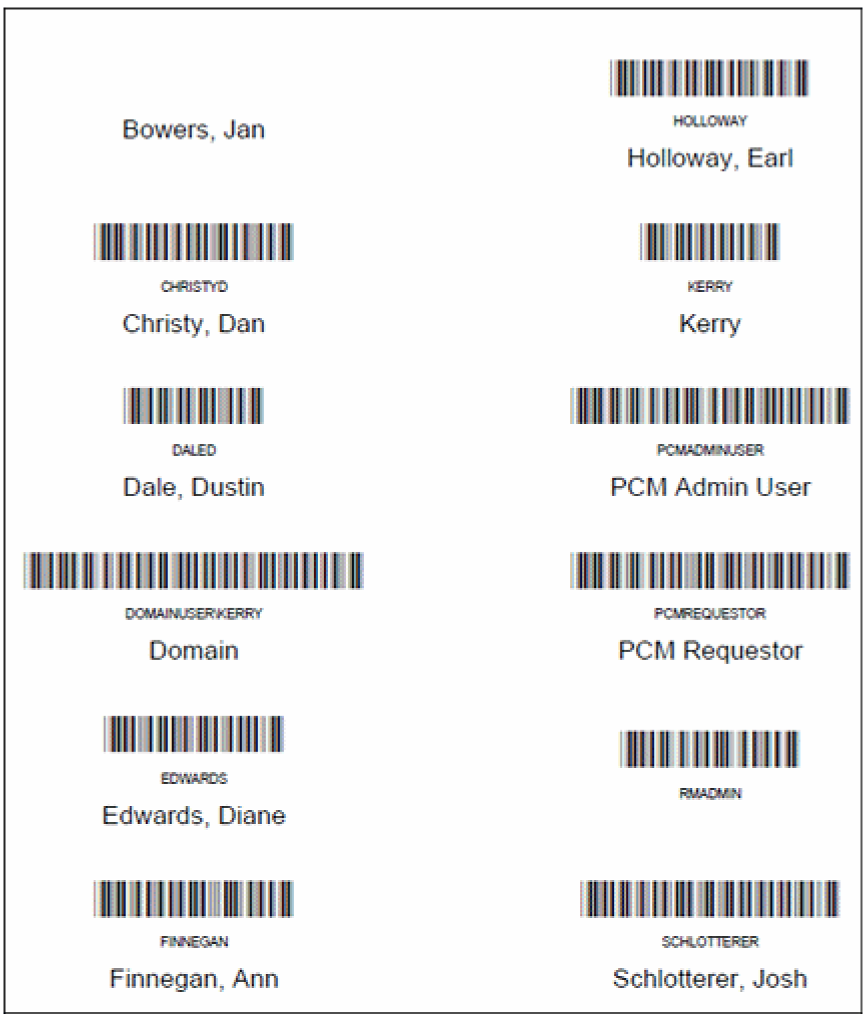
A report can be generated that lists barcode information and another type which can be used to produce barcode labels. The users are defined in the User Admin utility then assigned rights and roles.

View barcode reports using HTML but print reports using PDF in order to ensure proper formatting.



This report lists the barcode information for each user.

The following report produces a barcode list that is suitable for label printing.



11.2.3 User Roles Report

Use this report to view a list of all users and their assigned roles.

User Roles

Report Date: 3/16/10 12:35 PM

User Name	Role
bowersj	admin pcmadmin rmaadmin sysmanager
christyd	admin guest rmaadmin
daled	pcmadmin rmaadmin
edwards	rma
finnegan	rma
holloway	rma
pcmAdminUser	pcmadmin
pcmRequestor	guest pcmrequestor
rmadmin	chargebacksadmin contributor ermadmin guest pcmadmin rmaadmin
schlotterer	rmaprivileged
sysadmin	admin ermadmin ermrequestor pcmadmin pcmrequestor retadmin retuser rma rmaadmin rmaprivileged sysmanager
tassottig	rma
user1	contributor pcmrequestor
user3	contributor pcmrequestor
DomainUser\Kerry	ermadmin guest pcmadmin rmaadmin rmaprivileged
Kerry	chargebacksadmin ermadmin ermrequestor guest pcmadmin pcmrequestor rmaadmin

Column	Description
User	Displays the user name of the user as entered in the User Admin utility.
Roles	Displays the roles assigned to the user.

11.2.4 Group Report

Use the All Groups report to view a list of all aliases defined for the system.

Aliases

Report Date: 3/16/10 12:39 PM

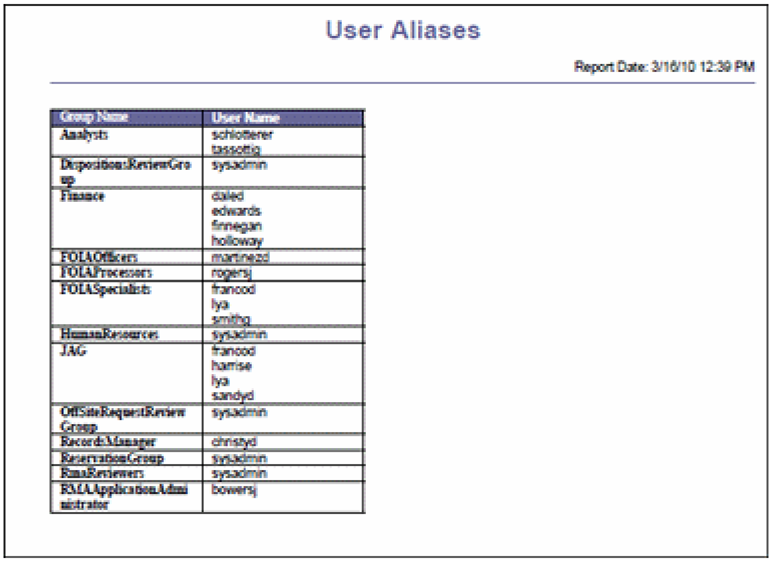
Group Name	Description
Analysts	Analysts
Finance	Finance
FOIAProcessors	FOIA Processors
HumanResources	HumanResources
OffSiteRequestReviewGroup	OffSite Request Review Group
ReservationGroup	ReservationGroup
RmaReviewers	RmaReviewers

Group Name	Description
DispositionsReviewGroup	DispositionsReviewGroup
FOIAOfficers	FOIA Officers
FOIASpecialists	FOIA Specialists
JAG	Judge Advocate Generals
RecordsManager	Records Manager
RMAApplicationAdministrator	RMA Application Administrator

Column	Description
Group Name	Lists all alias groups defined in the User Admin utility.
Description	Displays a short description of each alias group.

11.2.5 Group-User Report

Use this report to view a list of all users and groups (aliases) currently defined for access. The users and groups (aliases) are assigned in the User Admin utility.


User Aliases

Report Date: 3/16/10 12:39 PM

Group Name	User Name
Analysts	schlotterer tassottig
DispositionsReviewGroup	sysadmin
Finance	daled edwards finnegan holloway
FOIAOfficers	martinezd
FOIAProcessors	rogersj
FOIASpecialists	francod lya smithg
HumanResources	sysadmin
JAG	francod harrise lya sandyd
OffSiteRequestReviewGroup	sysadmin
RecordsManager	christyd
ReservationGroup	sysadmin
RmaReviewers	sysadmin
RMAApplicationAdministrator	bowersj

Column	Description
Group	Lists all alias groups defined in the User Admin utility.
User	Lists every user assigned to an alias group.

11.3 Content and Physical Item Reports

Several default reports and templates are provided with Oracle URM. These reports are available in a variety of locations within the software such as search result page, content information pages, and so on. The type of reports depend on the configuration of the system and which components have been enabled.

This section describes how to generate content reports using the default templates provided. For details about generating user and group reports, see "User and Group Reports" on page 11-2. For information about creating custom reports, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

11.3.1 Creating a Report

The creation of new reports is composed of two steps: finding the information for the report then choosing the appropriate report option.

1. Use searching or screening to find the information.
2. Use one of the following methods to create a report for an individual item:
   - Click the **Info** icon for the item. On the item's Content Information Page, click **Create Reports** then the type of report.

- On the Search Results Page, click the checkbox for an item. Click **Create Reports** then **Selected Items** then the type of report.

3. To create a report for multiple items, click the checkboxes of the items then click **Create Reports** then **Selected Items** then the type of report.
4. To create a report for all items on the page (such as all search results), click **Create Reports** then **Full Results** then the type of report.

This section provides several examples of reports.

11.3.2 Internal Item Detail Report

The following is an example of an Internal Item Detail Report. This report shows details about one item or about a group of items if several items are selected for use for the report.

Internal Item Detail

Report Date: 9/22/2009 11:09 AM

Content ID	STAGE5_URM_001227
Title	R3

Security Information

Author	christyd	**Security Group**	RecordsGroup
Type	Document		
Account			
Supplemental Markings			
Security Classification			

General Information

Record Format	Text	**Media Type**	Electronic
Originating Organization	Default	**Life Cycle**	

Records Information

Is Record	No	**Is Cutoff**	No
Category ID		**Folder ID**	F2
Subject To Audit	No	**Audit**	
Is Frozen	No	**Freeze Name**	0
		Freeze Reasons	
Vital	No	**Vital Reviewer**	
		Vital Period	0
Superseding Content		**Superseded Date**	

Date Information

Release Date	9/22/09 11:47 AM	**Received Date**	
Record Activation Date		**Record Obsolete Date**	
Record Filing Date	9/22/09 11:47 AM	**Record Rescinded Date**	
Record Expiration Date		**Record Cutoff Date**	
Record Review Date	9/22/09 11:47 AM	**Superseded Date**	
Record Cancelled Date		**Superseded Twice**	
Delete Approve Date		**Record Destroy Date**	
Publication Date	9/22/09 11:47 AM	**Received Date**	
New Revision Date	9/22/09 11:47 AM		

An external detail report is similar to this report, but it includes the bar code for the item as well as other information which pertains only to external items.

11.3.3 Search Results Report

The following is an example of a Search Results report. This report shows basic information about items.

Search Results

Report Date: 9/22/2009 11:16 AM

Content ID	Title	Release Date	Author
STAGE5_URM_001227	R3	9/22/09 11:47 AM	christyd
STAGE5_URM_001225	R1	9/22/09 11:43 AM	christyd
STAGE5_URM_001223	freezconten2	9/22/09 11:12 AM	christyd
FREEZE1NAME	freeze1Name	9/22/09 10:49 AM	christyd
7440643DA24B6FAFD99E15A9BBFB03	Move	9/22/09 10:06 AM	Rene
STAGE5_URM_001219	don't do it	9/22/09 9:33 AM	christyd
1E9C066786675AF30DA325DE4547BB	Delete All Revisions (Destroy Metadata)	9/22/09 8:59 AM	Rene
ACB9F4DB8E29C2D92888B7F7810BC7	Accession	9/22/09 8:58 AM	Rene
AUDITLOGARCHIVE	Log	9/21/09 9:24 PM	weblogic

11.3.4 Records Destruction Certificate Report

The following is an example of a Records Destruction Certificate report. This report shows those items which are scheduled for destruction.

The following item(s) are due for destruction. Please sign below to authorize destruction of the following items.

Department/Division	Records Manager	
Email	Telephone	

Records to be Destroyed

Object Type	Name	Title	Author	Category ID	Record Destroy Date
Box	STAGE5_URM_000803	phys2	Rene	taskpaneltest2	
Box	STAGE5_URM_000802	phys1	Rene	taskpaneltest2	
Micro	STAGE5_URM_000204	some pcm content item	rmadmin	file plan test cat	

Destruction Approvals:

Legal Approval (print) Signature Date

Records Manager (print) Signature Date

Records Destroyed By ______________________________ on ____________________

12

Monitoring, Customizations and Audit Tools

Several optional tools are available to help administrators customize and track system performance and usage:

- Performance monitoring can be used to check the length of time needed to process service requests, to monitor batch requests and to check for items that have failed to process.
- Custom scripts can be written and applied to content for access control and to add notifications. This complies with DoD Chapter 4 certification requirements.
- Audit trails capture and record all user activity configured to be included. An audit trail is critical for tracking user actions within a record management system.

This chapter discusses using monitoring, custom scripts, and audit trails. It covers the following topics:

Concepts

Tasks

12.1 Using Performance Monitoring

Performance monitoring can be enabled to check the status of batch processing, service calls, and other system information.

Several default numbers have been set as a starting point for monitoring. Actual performance variations will depend on the hardware used at the site and other variables such as total amount of content and software in use.

Performance monitoring statistics are written to a database table and can be accessed later.

12.1.1 Enabling Performance Monitoring

Follow this procedure to use performance monitoring:

1. Click **Records** then **Audit** from the Top menu. Click **Configure** then **Performance Monitoring**.

   The Configure Performance Monitoring Page is displayed.
2. Select the items to monitor and the time intervals for reports and alerts.
3. Click **Submit Update** when done.

12.1.2 Checking Performance Results

After enabling performance monitoring, current performance information can be checked using this procedure:

1. Click **Records** then **Audit** then **Performance Monitoring** from the Top menu.

   The Performance Processing Results Page is displayed.
2. Choose the type of information to view by clicking the tab at the top of the body section of the page:

   - **Performance Processing**: this page contains a summary of requests processed, total items processed, total number of queries run, total time to run queries, total time to validate data, total service request parse time and total service request time per each external source. Averages for these are also included.
   - **Report by Batch**: this page contains a summary of batches/items pending, processed, and failed with a total for each source. If an item has failed, a batch file is created that can be re-run. Click on any value in a column to display a page showing details about that item and to access the option to re-run the batch.
   - **Report by Item**: this page contains the details per batch for a particular source, status or batch type as well as totals. The detail page for the item contains the batch type, start time, completed time, elapsed time, and number of items processed for each batch.

12.1.3 Viewing Performance Alerts and Details

If any performance activites exceed the limits set on the Configure Performance Monitoring Page, a Performance Monitoring Alert Message is displayed automatically when you log in to the system.

Click any link on the Performance Monitoring Alert Message to see details about the specific alert. For example, the Monitoring Details Page is displayed when the first alert message is clicked. Click any link to display details about the specific items that caused the alert.

12.2 Using Custom Scripts

Custom scripts can be created using Idoc Script, a proprietary scripting language. This functionality is enabled by default when the DoD Configuration component is enabled. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about different options.

Custom scripting can be disabled by deselecting the **Enable Custom Script** box in the DoD Config section of the Configure Retention Settings Page. To access that page click **Records** then **Configure** then **Settings** from the Top menu.

When enabled, new content fields are available which allow you to define which scripts will apply to a folder or category.

Caution: You must have a thorough understanding of Idoc Script to use this feature. The Oracle URM software does not validate the script. You are responsible for creating usable scripts. See the *Oracle Fusion Middleware Idoc Script Reference Guide* for details about Idoc Script and its use.

Two types of scripts can be created using the Custom Script functionality:

- **Security scripts**, which allows users with the Records Administrator role to define and manage access control to content.
- **Custom Notification scripts**, which notify users of events. One custom script is provided, which notifies a list of reviewers when items are due for destruction after being superseded. Notification is send in one consolidated email when batches are run. Additional scripts can be created.

Scripts can be applied at a category or folder level and will apply to the children in those objects. A script inherits the security on the folder or category to which it is applied.

Note: Custom scripts comply with the DoD 5015.2 specification, chapter 4.19 and chapter 4.20.

12.2.1 Creating or Editing Scripts

Note: Any custom Idoc script which is entered is NOT verified for accuracy. You should have knowledge about Idoc script and its uses before creating scripts.

Follow this procedure to set up a custom script. Use the same procedure for both types of scripts.

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Custom Scripts**.

   The Configure Custom Script Page is displayed. Select the type of script to use (Notification or Security) by clicking the tab for the script type. To edit an existing script, select **Edit** from the existing script's Action menu. To add a script, click **Add** or select **Edit** on the Custom Script Information Page.

2. The Create or Edit Custom Script Page is displayed.

3. Add or edit the name for the script.
4. Add or edit the description for the script (optional).
5. Add or edit the Idoc code for the script. Note that the code is not verified for accuracy.
6. When finished adding a new script, click **Create**. When editing a script, click **Submit Update**. To reset the page without saving, click **Reset**.

12.2.2 Deleting a Custom Script

Follow this procedure to delete a custom script. Use the same procedure for both types of scripts.

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Custom Scripts**.

   The Configure Custom Script Page is displayed. Select the type of script for deletion by clicking the tab for either a Notification or a Security script.

2. To delete the script, click the box next to the script name and click **Delete** or select **Delete Script** from the script's Action menu. You can also click **Delete** on the Custom Script Information Page.

12.2.3 Viewing Script Information

Follow this procedure to view a script's information:

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Custom Scripts**.

   The Configure Custom Script Page is displayed. Select the script for viewing by clicking the tab for either a Notification or a Security script.

2. To view the script information, click the script name or select **Script Information** from the script's Action menu.

   The Custom Script Information Page is displayed.

12.3 Using the Audit Trail

The audit trail is generated in the format specified by the Report Format setting on the Configure Report Settings Page.

Permissions: The Admin.Audit right is required to work with audit trails. This right is assigned by default to the Records Administrator role. Administrative privileges are required to check in the audit trail.

At certain points, the current audit trail can be cut off and archived and checked into the repository. This action can also be scheduled to occur on a regular basis. The audit trail must be cycled for growth reasons the same as other items. Be sure to check in the audit trail log on a regular basis to keep the file size smaller and the report generation time faster. Each current audit trail is generated from the time the system was installed or archived until the request to generate an audit trail.

An audit trail can be generated at any time. The columns within the audit trail correspond directly with the fields by which you can search within the Search Audit Trail Page.

If the generated file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

Several tasks are involved in managing Audit Trails:

- "Configuring the Audit Trail" on page 12-5
- "Specifying Metadata Fields to Audit" on page 12-5
- "Searching within the Audit Trail" on page 12-6
- "Setting Default Metadata for Checking In Audit Trails" on page 12-6
- "Checking In and Archiving the Audit Trail" on page 12-7
- "Searching an Archived Audit Trail" on page 12-7
- "Viewing an Archived Audit Trail" on page 12-7

12.3.1 Configuring the Audit Trail

The configuration on the Configure Audit Page determines the administrator and user actions recorded for an audit trail.

> **Permissions:** The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To configure an audit trail, complete the following steps:

1. Click **Records** then **Audit** from the Top menu. Click **Configure** then **Audit Trail**.

   The Configure Audit Page is displayed.
2. Select the boxes for the actions to audit for each entity.
3. Click **Submit Update**. A message indicates configuring the audit was successful. The next time the audit trail is generated, the trail reflects the chosen selections.
4. Click **OK**. The Configure Audit Page is displayed again with the updated settings.

> **Caution:** If actions are deselected for objects, the actions are *not* captured by the audit trail. It is recommended you leave all settings selected and use the Search Audit Trail Page to narrow down searches of the audit trail. If transactions are heavy and the audit log grows too large too fast, you might want to consider turning off capturing browsing actions to manage the audit trail size.

12.3.2 Specifying Metadata Fields to Audit

Use this procedure to specify which metadata fields should be included in the audit trail.

> **Permissions:** The Admin.SelectMeta right is required to perform this action. This right is assigned to the Records Administrator role by default.

1. Click **Records** then **Audit** from the Top menu. Click **Configure** then **Audit Fields**.

The Audit Fields Page is displayed.

2. Select the boxes for the metadata field to include in the audit trail.
3. Click **Submit Update** when done.

Any changes take effect immediately without restarting the system.

12.3.3 Searching within the Audit Trail

Use this procedure to further refine a search within the current audit trail. For example, you can search for all delete actions, or all delete actions by a particular user, or all actions by a particular user, and so on. To search within archived audit trails, see "Searching an Archived Audit Trail" on page 12-7.

Permissions: The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

---

1. Click **Records** then **Audit** from the Top menu. Click **Search Audit Trail**.

   The Search Audit Trail Page is displayed.
2. Make the selections to narrow the search. As much or as little detail can be included. To adjust the scope (narrow or widen) of the search, use the Boolean operators before each field.
3. Click **Search**. The search results are displayed in the format specified by the Report Format setting on the Configure Report Settings Page.

12.3.4 Setting Default Metadata for Checking In Audit Trails

Setting the default metadata is useful for setting similar check-in attributes. You *must* set the default metadata before checking in an audit trail for the first time. This is a required step during the setup of the software.

Permissions: The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

To set the default metadata for checking in and archiving a portion of the audit trail, complete the following steps:

1. Click **Records** then **Audit** from the Top menu. Click **Checked-in Audit Entries**.

   The Checked-in Audit Entries Page is displayed.
2. Click the **Default Metadata for Checked-In Audit Entries** link.

   The Default Metadata for Checked-In Audit Entries Page is displayed.
3. Make selections reflecting the metadata most commonly used when checking in an archived audit trail. When finished, click **Submit Update**. A message is displayed saying the default metadata has been updated successfully.
4. Click **OK**.

12.3.5 Checking In and Archiving the Audit Trail

A user must have performed at least one action while logged into the system to generate an audit trail entry. If an empty audit trail is submitted for checkin, a message is displayed indicating there are no entries in the audit trail. Before checking in an audit trail for the first time, set the default metadata for the check-in (see "Setting Default Metadata for Checking In Audit Trails" on page 12-6).

> **Permissions:** The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Click **Records** then **Audit** from the Top menu. Click **Checked-in Audit Entries**.

   The Checked-in Audit Entries Page is displayed.
2. In the Check In Audit Entries area, specify the date and time to cut off the audit trail in the **Date** box, and click **Archive**.
3. The check-in confirmation page is displayed. The content ID of the checked-in audit trail is `AUDITLOGARCHIVE`. Every time it is checked in, a new revision is generated.
4. Click **Content Info** to view the information about the archived audit log. The Content Information Page is displayed. To view the audit log just checked in, click the **Web Location** or the **Native File** in the **Links** area of the content information page.

12.3.6 Searching an Archived Audit Trail

Use this procedure to search for all checked in and archived audit trails.

Prerequisites

- "Checking In and Archiving the Audit Trail" on page 12-7

> **Permissions:** The Admin.Audit right is required to perform this action. This right is assigned by default to the Records Administrator role.

1. Click **Records** then **Audit** from the Top menu. Click **Checked-in Audit Entries**.

   The Checked-in Audit Entries Page is displayed.
2. Click **Search Audit Entries**. The results of the search are displayed in the search results page. From the search results page, click options in the **Query Actions** list to:
   - search within the results
   - save the search

12.3.7 Viewing an Archived Audit Trail

Use this procedure to view an archived audit trail for which you have searched.

Prerequisites

- "Searching an Archived Audit Trail" on page 12-7

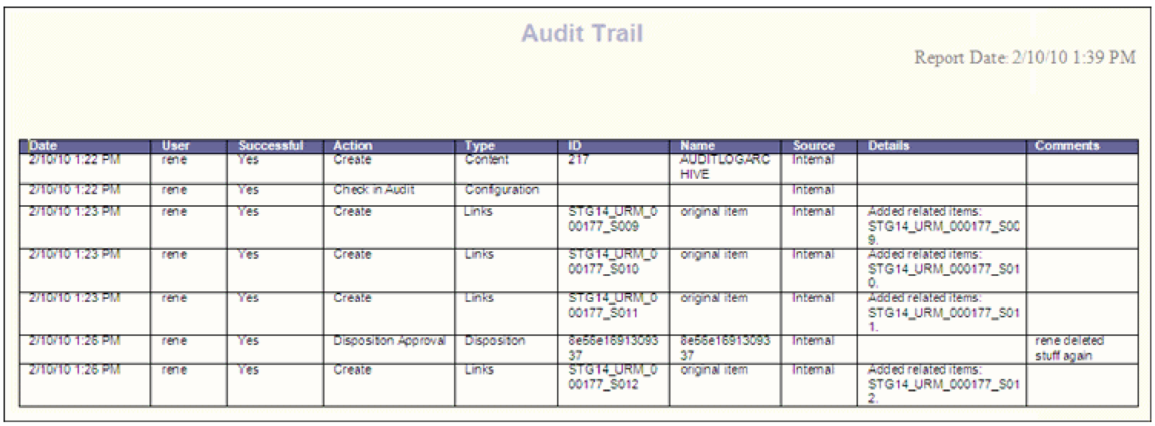
To view an archived audit log from the search results page, do one of the following:

- click the ID (quickest method)
- click the information icon then click the PDF links on the content information page.

12.3.8 Creating an Audit Trail Report

An audit trail report is automatically generated in the format specified by the Report Format setting on the Configure Report Settings Page. If the generated file is in PDF format, Adobe Acrobat version 6.0 or later is required to view it.

The following is a sample audit trail report.


Audit Trail

Report Date: 2/10/10 1:39 PM

Date	User	Successful	Action	Type	ID	Name	Source	Details	Comments
2/10/10 1:22 PM	rene	Yes	Create	Content	217	AUDITLOGARC HIVE	Internal		
2/10/10 1:22 PM	rene	Yes	Check in Audit	Configuration			Internal		
2/10/10 1:23 PM	rene	Yes	Create	Links	STG14_URM_0 00177_S009	original item	Internal	Added related items: STG14_URM_000177_S00 9.	
2/10/10 1:23 PM	rene	Yes	Create	Links	STG14_URM_0 00177_S010	original item	Internal	Added related items: STG14_URM_000177_S01 0.	
2/10/10 1:23 PM	rene	Yes	Create	Links	STG14_URM_0 00177_S011	original item	Internal	Added related items: STG14_URM_000177_S01 1.	
2/10/10 1:26 PM	rene	Yes	Disposition Approval	Disposition	8e56e16913093 37	8e56e16913093 37	Internal		rene deleted stuff again
2/10/10 1:26 PM	rene	Yes	Create	Links	STG14_URM_0 00177_S012	original item	Internal	Added related items: STG14_URM_000177_S01 2.	

13 Archiving and Transfering Information

If an environment is set up on one computer (including a retention schedule, security scheme, and so on), you may want to copy this configuration information to another computer, for example, from a development machine to a production machine or a mirrored site. This can be done using built-in archive import and export features.

You can also import and export records, folders, and metadata in XML format by creating a XML Standard Definition (XSD). XSD is a an XML schema language used to define the structure of an XML document. The XSD file is created to make the file usable in the Oracle URM system. This allows the content from the system to be imported into a third-party system using a different archive file format or to export data from another system and import it into Oracle URM.

This functionality is compliant with the DoD 5015.2 specification which requires the ability to create different XSD schemas.

This chapter discusses exporting archives and importing them into other instances to duplicate the retention schedule and a variety of other configuration settings. It also discusses importing and exporting XSD schema to transfer content.

This chapter covers the following topics:

Concepts

Tasks

13.1 About Archives

The archive process is use to back up or restore a retention schedule and other configuration settings. It is not used to archive copies of content. For details about archiving content, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

The export feature copies a variety of configuration settings to a separate *.hda* file that can be imported into another instance or stored in a safe location for backup purposes. The *.hda* file is a plain text, serialized data file that can be opened in any text editor.

Retention Schedule objects should be imported before importing other content. Content server content should be imported before importing the content-related objects.

Permissions: See "Archive Import/Export Rights and Permissions" on page 13-4 for details.

The archive export and import features enable exporting and importing of the following items:

- Supplemental markings
- Security classifications, also known as Classified Markings
- Custom categories metadata and custom folder metadata
- Custom security fields, also known as Custom Supplemental Markings
- Periods
- Triggers
- Retention schedules
- Dispositions history: a log of all actions that have been performed
- Custom disposition actions
- Freezes
- Recurring scheduled tasks
- Classification guides and classification topics. These are only available if the ClassifiedEnhancements component is enabled.
- PCM location types
- PCM storage space definitions
- custom PCM metadata
- reservations

Note the following considerations when using imports and exports:

- When using PCM, the export feature copies the space management definitions (the setup and hierarchy of warehouses, rooms, and so on) but none of the metadata of the items stored at those locations is archived.
- When importing an archive, existing items can be overwritten or can be left unchanged.
- Set the default archive metadata format by clicking **Records** then **Configure** then **Settings**. The Configure Retention Settings Page is displayed. Expand the General section and select the metadata format from the dropdown list.

- When custom category metadata fields or custom folder metadata fields are imported, the order of the fields is not updated. Restart the Content Server after importing custom fields.
- The disposition history is not updated. Only new dispositions are imported.
- The export feature copies the retention schedule definition (that is, the defined hierarchy) and disposition instructions, not the items within the retention schedule.
- If an add-on is enabled, there may be additional items available for export.

Important: If your organization uses additional security (ACLs) on your retention schedule, the import and export only includes items that can be accessed by the user performing the import or export. For example, if the person does not have ACL access to a particular category, that category is not imported or exported. A message is displayed during the import or export process if any objects are not processed due to ACL access. Make sure you have ACL access to all items to export and import.

13.1.1 Exporting Auxiliary Metadata Sets

Permissions: You must have administrative privileges to add tables to the list of schema tables used.

When exporting an auxiliary metadata set, add the AuxiliaryMetadataSets and AuxiliaryMetadataSetDefs table to the list of schema tables used. Follow this procedure to add those tables:

1. Click **Administration** then **Admin Applets** from the Main menu.
2. Click **Configuration Manager**. The Configuration Manager applet is displayed.
3. Click the **Tables** tab. A Table List is displayed. Click **Add Table**.
4. Highlight AuxiliaryMetadataSets and click **OK**. The Table list is redisplayed.
5. Highlight AuxiliaryMetadataSetDefs and click **OK**. The Table list is redisplayed.
6. Close the Configuration Manager.

After adding the MetadataSet tables to the list of tables, they become available in the list of tables that can be added from the Archiver.

13.1.2 The Export/Import Process

The process of importing and exporting content consists of three distinct parts.

1. First import or export a retention schedule and any of the objects in that schedule. This corresponds to the **Include Retention Schedules Plan** portion of the Export and Import screens.
2. Then import or export the content using the Oracle UCM Archiver. See the *Oracle Fusion Middleware Application Administrator's Guide for Content Server* for details about using the Archiver.

3. After content has been imported or exported using the Archiver, import or export the Disposition History of related objects. This corresponds to the **Include Dispositions History** portion of the Export and Import screens.

13.1.3 Archive Import/Export Rights and Permissions

The following export rights are needed for specific objects. These rights are included by default with the Records Administrator role:

- Admin.RetentionSchedulesArchive right to export a Retention Schedule.
- Admin.Triggers right to export triggers.
- Admin.PerformActions right to export Disposition Histories.
- Admin.RecordManager right to export objects other than those mentioned previously.

The following import rights are needed for specific objects:

- Category.Edit, Folder.Edit, and Record.Edit rights to import a Retention Schedule (because these objects are part of a Retention Schedule).
- Admin.Triggers right to import triggers.
- Admin.PerformActions right to import Disposition Histories.
- Admin.CustomDispositionActions to import Disposition Actions.
- Admin.RecordManager right to import objects other than those mentioned previously.
- If ACL security is enabled, make sure you have access to all retention schedule components and objects to import.

13.2 Managing Imports and Exports

The following tasks are performed when importing or exporting archives:

- "Exporting an Archive" on page 13-4
- "Importing an Archive" on page 13-5

13.2.1 Exporting an Archive

Use this procedure to export an archive that can be imported into another instance (located on the same or a separate system) or for backup purposes. Choose which of the available items should be exported.

Permissions: See "Archive Import/Export Rights and Permissions" on page 13-4 for details.

---

1. Click **Records** then **Import/Export** then **Archives** from the Top menu.

   The Import/Export Archive Page is displayed.

2. Select all items to be included in the export.
3. Click **Export**. A download dialog is displayed.

   To save the archive, click **Save**. Navigate to the location to save the file, and enter a filename.

4. Click **Save**.

   The file is saved to the specified location, and the Import/Export Archive Page is redisplayed.

13.2.2 Importing an Archive

Use this procedure to import an archive that was exported on another instance (located on the same or a separate system). Choose which of the available items in the archive should be imported. The items to import must have been included in the export of the archive.

> **Permissions:** See "Archive Import/Export Rights and Permissions" on page 13-4 for details.

1. Click **Records** then **Import/Export** then **Archives** from the Top menu**.**

   The Import/Export Archive Page is displayed.

2. Select all items to be included in the import. Click **Attempt Update** to specify whether to update existing items or leave them untouched. If you do not have update checked and the imported item(s) already exist, an error may occur. Read the error message to determine the best course of action to pursue.
3. Click **Browse** next to the **Archive File** box to select the archive file (*.hda*) to import.
4. After selecting the file, click **Import**. The import adds all new items and updates any existing ones, if applicable. The results of the imported archive are tracked in the audit trail for the enabled actions.

If an error occurs, the error message indicates the number of checkbox items which failed, not necessarily the number of individual errors for all retention schedule components. If classified markings are imported, they should be reordered after importation.

13.2.3 Importing a Batch-Created Storage Hierarchy

> **Permissions:** See "Archive Import/Export Rights and Permissions" on page 13-4 for details.

Use this procedure to import a storage hierarchy definition file (*StorageImport.hda*) that was created using the batch storage creation feature.

1. Click **Records** then **Import/Export** then **Archives** from the Top menu**.**

   The Import/Export Archive Page is displayed.

2. Make sure the "Include Storage" checkbox is selected. You do not have to unselect all the other items; they will simply be ignored as none of them are included in the *StorageImport.hda* file.
3. Click **Browse** next to the **Archive File** box to select the *StorageImport.hda* archive file that was created when you batch-created the storage hierarchy.
4. After selecting the file, click **Import**. The import adds the storage hierarchy contained in the *StorageImport.hda* file to the existing storage space at the location specified in the *hda* file.

13.3 XSD Data Transfer

XSD schemas can be used to manage records, folders, and content to comply with the DoD 5015.2 specification. Exporting and importing data using a format defined as XSD format (XML Schema Definition) conforms with standard transfer schema defaults.

The information must be mapped before proceeding with exporting or importing. After the correct mapping is in the place, data can be imported and used in Oracle URM. It can then later be transferred as needed to NARA or another system using the XSD schema for that site.

13.3.1 Important Considerations Before Exporting

Two considerations should be evaluated before beginning the import and export process:

- "Special Handling of <choice> Elements" on page 13-6
- "Required Fields on Import" on page 13-6
- "Target Namespace and Qualified Locals" on page 13-6

13.3.1.1 Special Handling of <choice> Elements

The `<choice>` element type allows only one of the elements contained in the selected group to be present within a containing element. This differs from an option list in which one field can have multiple possible values.

A document whose data is being exported can only contain a value in one of the fields contained in the `<xs:choice>` group. This restriction determines which field to use when the XML file is generated for output. If more than one of the fields in the choice group contain a value, an error occurs and the export cannot finish because of ambiguity as to which field should be used.

The following example shows this type of `<choice>` list. In this example, an employee can be only one of the three types of employees (full-time, part-time, or contractor). So only one of the three corresponding fields can be contained in the `<choice>` element.

```
<xs:complexType name="employee">
  <xs:choice>
     <xs:element ref="full-time" />
     <xs:element ref="part-time" />
     <xs:element ref="contractor" />
  </xs:choice>
</xs:complexType>
```

13.3.1.2 Required Fields on Import

If your server has required fields, all of those fields must have a value set in order to perform an import. Mapping the required fields to an XML node provides the value. However, if any of the required fields are not mapped, a profile must be created that sets these values on import. If this is not done, the import fails.

13.3.1.3 Target Namespace and Qualified Locals

Explicitly declare a target namespace in the .xsd file and also specify that locally defined elements and locally defined attributes are qualified. The target namespace is specified by the `targetNamespace` attribute.

Local elements and attributes can be qualified globally by using the `elementFormDefault` and `attributeFormDefault` attributes on the schema element. They can be specified separately for each local declaration using the `form` attribute. Attribute values can be set to *unqualified* or *qualified*, to indicate if locally declared elements and attributes must be unqualified.

13.3.2 Configuring XSD for Importing and Exporting

Use this procedure to configure the schema definition for the export.

1. Click **Records** then **Import/Export** from the Top menu. Click **Configure** then **Import/Export Schema**.
2. The Configure Import/Export Schema Page is displayed. Click **Add** to create a schema definition to use for the export. The Create Import/Export Schema Page is displayed.
3. Enter the necessary information and click **Browse** to find an archive file for use. When done, click **Create**. The Upload Confirmation Page is displayed. Click **Configure Top Level Nodes** from the Page menu.
4. The Configure Top Level Schema Nodes Page is displayed. *Top level nodes* are those that represent an entire object, such as a record or a folder. Highlight the nodes to include in the list, using the left or right arrows to move or remove the node. Choose mapping options in the mapping section, choosing the appropriate type from the menu lists. Click **Save** when done.
5. Click **Map Fields** from the Page menu to map folder and content fields. The Configure Mappings Page is displayed. Use this page to map XSD fields to Oracle URM metadata fields for both records and folders. These mappings will be used for both exporting and importing. The custom mapping at the bottom of the screen is used to resolve ambiguity when two different objects that are defined inthe same XSD reference a common sub-object that must be mapped to different fields. To add fields, click **Add** at the bottom of the page and enter the new custom field. To delete custom fields, click the delete icon (a red X). Click **Save** when done.

13.3.3 Exporting and Importing XSD Data

After configuring the data to be exported, you can proceed with the import or export process.

1. Click **Records** then **Import/Export** from the Top menu. Click **Export with Schema**.
2. The Export with Schema Page is displayed.
3. Choose a schema name from the list and assign an archive batch name by expanding the existing archive batch names and selecting one.
4. Click **Export**.

Follow a similar procedure to import an archive using XSD mapping by choosing **Import with Schema** from the menu.

1. Click **Records** then **Import/Export** from the Top menu. Click **Import with Schema**.
2. The Import with Schema Page is displayed.
3. Choose a schema name from the list. Select an archive file by clicking the Browse button and navigating to the location where archives are located.
4. Click **Import**.

14

FOIA and Privacy Act Tracking

Important: The FOIA/PA component in Oracle URM is an example of usage and should not be used as is. It shows the types of decision points, workflow branches, and forms used in a typical FOIA/PA process. The process in use at your site may vary signficantly from that shown here.

Oracle URM contains the functionality needed to comply with the Freedom of Information Act (FOIA) and the Privacy Act (PA) to track requests for information. The process is similar for both types of information requests. The main difference lies in the type of forms used in the information processing.

This functionality is available only if the FOIA/PA component is enabled during configuration. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for details about choosing options.

When enabled, new links appear on the Setup Checklist page. Make sure to click **Install Data Resource Files (Schema, etc.)** to enable the necessary services to use this component. In addition, import the necessary archive by clicking **Import FOIA Privacy Act Archive**. This imports the workflow and other items needed for the component. Note that the workflow must be modified before enabling it for use.

When the FOIA/PA component is enabled, default users are added to populate different default alias groups.Because of the complexity of the FOIA/Privacy Act specification, the users are left in place to make it easier to match the FOIA configuration with the specification.

A FOIA profile is also installed making the necessary metadata fields available. If the FOIA component is later disabled, the FOIA profile and metadata fields remain. They should be removed if the component is disabled. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for information about profiles. See the *Oracle Fusion Middleware Application Administrator's Guide for Content Server* for information about managing metadata fields.

This chapter provides an overview of the process of tracking, fulfilling, or denying information requests using Oracle URM. This type of information processing is accomplished by using workflows. This chapter provides an overview of workflow usage but does not discuss the details of setting up or maintaining workflow. For complete details about using workflows including how to customize a workflow, see the *Oracle Fusion Middleware Application Administrator's Guide for Content Server*.

The forms used with the functionality can be edited as needed. The forms are checked in as content items. To alter the forms, search for the form name then check out the form and edit the .hcsw or .hcsf files using an ASCII editor.

Concepts

Tasks

14.1 FOIA and DB2 Databases

The FOIA/PA functionality contains an archive that is imported. This archive contains a table, FOIAPAMETA, that is used to store auxiliary metadata. This table contains 99 fields, 21 of which are memo fields. Memo fields are normally 2000 characters in length.

However, DB2 has a smaller row size limit than Oracle or SQL Server. With 21 memo fields, the FOIAPAMETA table would fail to import on a DB2 database because of this limit. Normally, when a memo field is created on a DB2 system, Configuration Manager uses a special DB2 data type called "long varchar". But that doesn't apply when Archiver is importing a table.

To accomodate this, the memo fields in the FOIAPAMETA table have been manually changed so the size is set to 1000. This may not match the memo field size on the server where this component is installed if DB2 is used. There are two solutions for this problem:

- Change the memo field size setting for the instance to 1000 to match what was imported with this table.
- Change the length of the 21 fields in the FOIAPAMETA table to match what is expected on the server where the instance resides.

The second method is the recommended method for implementation.

14.2 About Workflows

Workflows are used to route content for review, approval, and eventual release. In this case, the content that is routed are the forms required for the FOIA/PA process.

Effective workflow design is an iterative process, continually refined as the process is implemented. Three types of workflows can be created:

- *Criteria workflows* are used for content that enters the workflow process automatically based on content metadata that matches predefined criteria. Criteria workflows are used for FOIA and PA approvals.
- *Basic workflows* are used for specific content items (for example, a particular document to be reviewed) and must be initiated manually.

- *Sub-workflows* can also be used to split complex workflows into manageable parts and can be used with either a criteria or a basic workflow.

Workflows are composed of *steps* in which content is reviewed, approved or denied. Multiple reviewers can be assigned to approve or reject the content at each step. A set of users and the step type must be defined for each step in the workflow. Users assigned to a step can only perform the tasks allowed for that step type.

Workflows can be customized in several ways. Tokens can be used to designate unknown users. Aliases can be used to include a group of people in a workflow step. Jumps enable the creation of conditional statements to branch content through different paths in the same workflow or to route content to a different workflow. Exit conditions can prevent content from moving to the next step unless essential conditions are met. Custom metadata fields can be created and used to trigger different workflows.

For details about these customization tips and for examples of workflows, see the *Oracle Fusion Middleware Application Administrator's Guide for Content Server*.

14.3 The FOIA/Privacy Act Workflow

The FOIA/PA workflow provided with Oracle URM should be considered a starting point for the process to be used. It must be customized with users added as reviewers, specific rules added to reflect the process in place at different organizations, and additional steps added as needed. In addition, this version of the workflow reflects draft requirements specified by the Joint Interoperability Task Force (JITC). It should be expected that these requirements will change in the future and the procedures outlined here may then be outdated.

Only those request forms requiring approval go through a workflow process. Other necessary supporting forms must be filled out and filed in the requestor's folder. Those forms are linked to the main request using the Related Content functionality.

There is no set time frame for filing of those forms, but they must be completed before the workflow is completed when the request is either denied or serviced. Those forms are not discussed in this chapter.

This section discusses the current default workflows provided with the software. It is divided into task groupings, most of which are based on the decision points in the workflow. The finished, customized workflow at your site may have different decision points and tasks than those discussed here.

14.3.1 Processing Details

When a workflow is started to process an information request, the stages of the workflow are automatic and may branch depending on the choices made during the process (for example, a denial of the information request, or the servicing of a request). It is important to know the stage where a request is currently in process because that will determine which workflow must be used for action.

The Active Workflows Screen shows all types of workflows available with the system. When a user accesses a request being processed, the appropriate stage of the workflow must be chosen. The stage of the workflow is shown on the Workflow Content Page in the Step column.

Time limits are set according to the specification guidelines for each stage of processing. These limits are set within the workflow and be changed if needed. See the *Oracle Fusion Middleware Application Administrator's Guide for Content Server* for details about editing workflows.

To view current workflow assignments, click **My Content Server** then **My Workflow Assignments** from the Main menu or click the **My Workflow Assignments** link on the Active Workflows Screen.

14.3.2 Initial Required Setup

As mentioned earlier, the default workflow must be customized to add the appropriate users, steps, and decision points for your working environment. This must be done before using this functionality.

Forms are submitted from within a record folder, so make sure to set up the category structure beforehand. Categories should be created where FOIA and PA requests will be stored (for example, "Open FOIA Requests" and "Open PA Requests"). As information requests are received, a new folder must be created for each request within the appropriate category. This folder will house all of the paperwork associated with the request.Therefore, any people involved in the workflow process should be those users who have the necessary rights and roles to allow them to create and move folders. Depending on how the system is set up, users will receive notification email with links to actions that can be performed depending on the user's rights and roles.

Categories must be created to store the finished requests. The naming and disposition rules for those categories is an organizational decision. Categories could be created based on final outcome (Granted in Full, Refused, and so on) or by date (for example, "December 2009 requests") or some other filing method.

In addition to creating folders, plan to track expenses associated with the request process. Information such as the fees collected, the staff allocated to the request, the time and money spent servicing the request, and the final result of the request should all be tracked independently in order for final reports to be produced. As noted previously, the workflow and reports documented here are based on the draft specification which may change in the future.

14.3.3 Begin Request Processing

The initial stage of the request process involves creating a folder for the request and filling out the appropriate form for the request.

14.3.3.1 Create a Request Folder

When a request for information is received, a new folder for the request must be created. All information associated with the request will be stored in that folder. For complete details about creating folders, see the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

1. Click **Browse Content** then **Retention Schedule** from the main menu. Click the category name for use.
2. The Exploring Category Page is displayed. Click **Create** then **Create Records Folder** from the Page menu. The Create Record Folder Page is displayed.
3. Enter the appropriate metadata information and click **Submit** when finished.

14.3.3.2 Create a Request

After the folder is created, initiate a form for the request from within the folder.

1. Click **Create** then the type of request from the Action menu of the folder or select these options from the Page menu of the Folder Information Page. The same menus are available for FOIA Requests or Privacy Act Requests but different

default data is filled in on the forms depending on the type of request. Request types include:

- Access Request Form: used to request access to records under the Freedom of Information Act or the Privacy Act (depending on which menu option is chosen).
- Amendment Record Form: used to request a change or amendment to a record.
- Disclosure Record Form: used to initiate the process to make records available for disclosure.
- **Other**: forms used to track information for the request. The form used will vary depending on the type of request and how it progresses through the workflow.
  - Access Record Form
  - Accounting Record Form
  - Appeal Request Form
  - Denial Record Form
  - Disclosure Record Form
  - Dispute Record Form
  - Exemption Record Form
  - Matching Program Records Form
  - Privacy Act File
  - System of Records Form

2. If adding supplementary information to a previously file request, choose one of the forms from the **Other** category. The appropriate form is displayed. Fill out the form and click **Submit** when done. The form is filed in the folder with other documentation for the request.

   If beginning the request process, click one of the request types. The chosen form is displayed: the Access Request Form, the Amendment Record Form, or Disclosure Request Form.

3. Fill in the appropriate information for the request and click **Submit** when done.
4. A submission confirmation is displayed.

14.3.4 First Decision Point: Expedited or Non-Expedited

When a request is submitted for information, the first decision point revolves around if the request will be expedited or not. The request form contains a field which specifies if the requester wants expedited processing, but that is not what determines this decision. This decision should be made by the FOIA/PA processors.

An *expedited request* is immediately serviced without further information needed. A *non-expedited request* requires review and may be denied after review.

14.3.4.1 Review Request Form and Route

The first decision point in the workflow will be to route the request to the proper workflow by choosing the type of request.

1. Click **Content Management** from the main menu. Click **Active Workflows**. A list of current workflows is displayed.
2. Click **FOIA Requests**. A Workflow Content Page is displayed listing items in workflows and the steps where the workflow is currently processing. Click the Workflow Review icon for the item to review (the document icon next to the Actions menu icon).
3. The submitted request is displayed within a Workflow Review Page.
4. Click **Expedited** or **Non-Expedited** in the Review Workflow pane (on the left side of the screen) to route the request. The Workflow Review Page is displayed, showing that appropriate sub-workflow is started in the Step column.
5. Click the Workflow Review icon to continue workflow processing.

14.3.4.2 Send Acknowledgements

An acknowledgement of the request must be sent regardless of the request type (expedited or non-expedited).

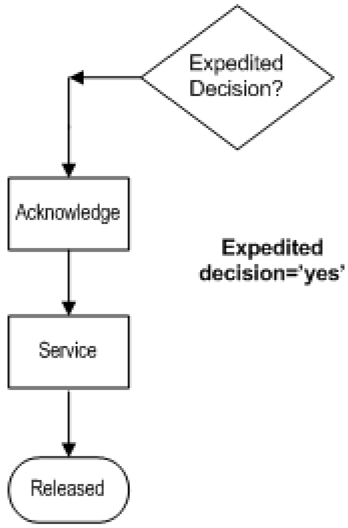
1. If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Requests** to display all requests currently in the initial stage of processing (this is applicable for FOIA requests and Privacy Act Requests). The Workflow Review Page is displayed.

   If still in the workflow process, click the Workflow Review icon for the request to process. The Workflow Review Page is displayed. Note that the action options in the Workflow Review Pane have changed to match the current workflow step.
2. Click **Acknowledged**. A search screen is displayed. Use this screen to search for items that were used to acknowledge the request.
3. Enter metadata for the search fields. Click **Search** when done.
4. A list of content items matching the criteria is displayed. Click the checkbox of the item to use and click **OK**. The Workflow Review Page is displayed again with the new workflow step indicated in the Step column.

14.3.5 Second Decision Point: Service or Denial

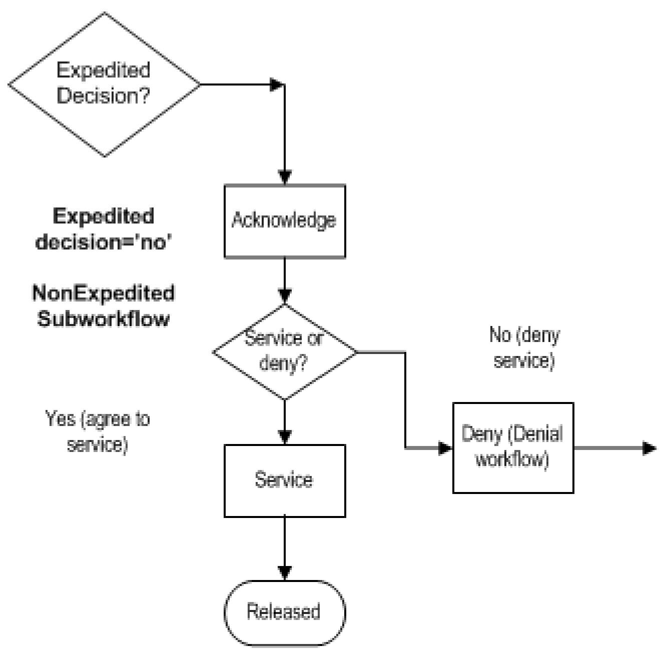
If this is an expedited request, the next step will be to service the request by providing the requested information. If a request is denied, fill out the appropriate forms to indicate why the request is denied and what steps the requestor can take to appeal the denial.

Figure 14–1 Expedited Sub workflow



If this is a non-expedited request, the request will be evaluated and perhaps serviced or denied.

Figure 14–2 Non-expedited sub workflow



14.3.5.1 Servicing a Request

The Oracle URM system is not used to fulfill the request but is used to track the *process* of fulfilling the request. Therefore, after the information has been released to the requestor, it must be indicated in the workflow that the request has been serviced.

1. If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **Expedited Subs** if this was an expedited request that will be immediately serviced. The Workflow Content Page

is displayed, showing all requests in that sub-workflow. Click the Workflow Review icon for the request to be serviced.

If still in the workflow process, click the Workflow Review icon for the request to be serviced on the Workflow Content Page.

2. The Workflow Review Page is displayed. Note that the action options in the Review Workflow pane have changed to match the current workflow step. Click **Serviced** on the Workflow Review Pane.
3. A search screen is displayed. Enter metadata to search for items that will fulfill the request. Click **Search** when done.
4. A search results page is displayed. Click the checkbox for those items used to fulfill the request. Click **OK** when done.
5. The Final Result Dialog is displayed. Enter the information to be included on the final reports, including the final result, fees collected, number of people involved in servicing the request and total cost of servicing. Click **OK** when done.

14.3.5.2 Denying a Request

A request may be denied for a variety of reasons. If the request is denied, a Denial Request Form must be filled out before proceeding.

Note that at this stage of the workflow process, it is possible you are not creating a new denial but are reviewing a denial created outside of the workflow (a direct denial) to make a decision about its outcome. Choose the appropriate Denial Form depending on the type of denial in process.

1. If still in the workflow process, click the Workflow Review icon for the request.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Non-Expedited Sub** (a request cannot be denied that was initially chosen as expedited). See "Review Request Form and Route" on page 14-5 for details. Click the Workflow Review icon of the request to process.
2. The Workflow Review Page is displayed. Note that the action options in the Review Workflow Pane have changed to match the current workflow step.
3. Click **Recommend Denial - New** or **Recommend Denial - Existing** from the Review Workflow pane. The Denial Record Form is displayed.
4. If this is a new denial, enter the necessary data for the denial and click **OK**. If this is a previous denial, a search dialog is displayed. Select the submitted denial form. This links the two forms together. Click **OK** when done.
5. A submission confirmation screen is displayed. Click **OK**.
6. The Workflow Content Page is displayed. The request is listed and the Step column is changed to **DenialDecision**.

The denial form is filed into the request folder and the workflow process moves to the next step. The denial is forwarded to the appropriate reviewers for a decision.

14.3.6 Third Decision Point: Denial Processing

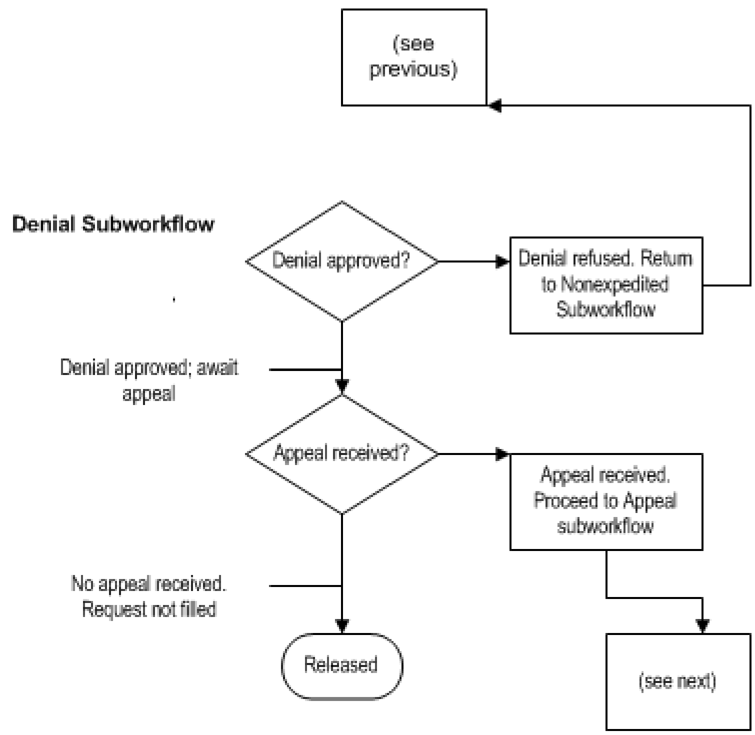
A denial of request can have one of two different outcomes:

- **The denial can be disapproved**. This means the denial will be returned to the reviewer who denied it and it must be serviced (see "Refusing a Denial" on page 14-9 and "Servicing a Request" on page 14-7.

- **The denial can be approved**. If a denial of service is approved, the requestor is notified of the denial and can appeal that decision within a sixty-day time frame. See "Fourth Decision Point: Appeal and Decision" on page 14-10 for more details about the appeal process.

  If a request is denied and an appeal is not received within the sixty day time frame, the FOIA/PA workflow is concluded. See "Final Actions" on page 14-12 for details about the final processing of the workflow.

Figure 14–3 Denial processing sub workflow



14.3.6.1 Refusing a Denial

1. If still in the workflow process, click the Workflow Review icon for the request.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Denial Sub**.

   The Workflow Content Page is displayed listing all items in this stage of processing. The Step column for a denied request is "DenialDecision." Click the Workflow Review icon of the request to process.

2. The Workflow Review Page is displayed. In the Review Workflow pane, click **Disapprove Denial** to refuse the denial and have the request serviced.

3. The Workflow Content Page is re-displayed with the item listed. The Step column indicates the request has moved back to the "Serviced" stage. Click the Workflow Review icon.

4. The Workflow Review Page is displayed. In the Review Workflow pane, click **Serviced** to route the request for servicing.

14.3.6.2 Approve Denial

1. If still in the workflow process, click the Workflow Review icon for the request.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Denial Sub**.

   The Workflow Content Page is displayed listing all items in this stage of processing. The Step column for a denied request is "DenialDecision." Click the Workflow Review icon of the request to process.

2. The Workflow Review Page is displayed. In the Review Workflow pane, click **Approve Denial** to approve the denial and refuse to fill the request.

3. The Workflow Content Page is re-displayed with the item listed. The Step column indicates the request has moved to the "AwaitAppeal" stage.

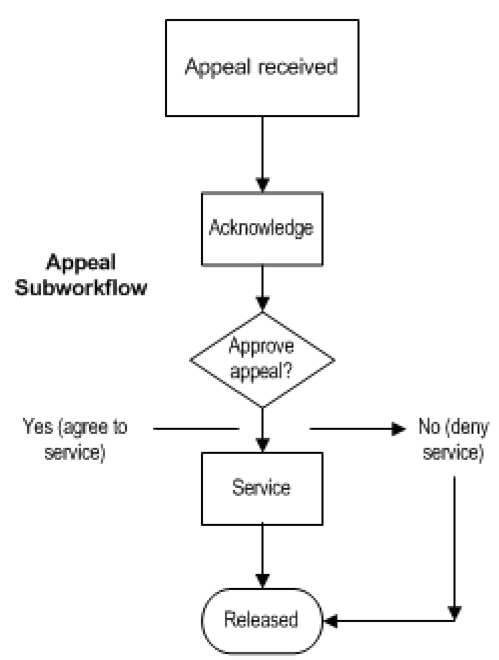
14.3.7 Fourth Decision Point: Appeal and Decision

If a request has been denied, the requestor has sixty days to file an appeal of that denial. If an appeal is not filed, the workflow for that request concludes.

When notification is received that an appeal has been filed, access the folder housing the original request and file an Appeal Request form. An acknowledgement that the appeal was received and is being reviewed must also be sent. All paperwork for the appeal is filed using the same identification as the original denial and the original Access Request Form, thus linking the records together.

It may be possible that you are not creating a new appeal form but are reviewing an appeal created outside the workflow process to make a decision about its outcome. Choose the appropriate Appeal Form depending on the type of appeal being processed (a similar action can occur when processing denials).

Figure 14–4 Appeal process sub workflow



14.3.7.1 Initiating an Appeal

1. If still in the workflow process, click the Workflow Review icon for the request on the Workflow Content Page.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Denial Sub**. A list of all requests in this stage is displayed. Click the Workflow Review icon for the request being processed.

2. The Workflow Review Page is displayed. Note that the action options in the Review Workflow Pane have changed to match the current workflow step. Click **Appeal Received - New Form** or **Appeal Received - Existing Record**.

3. If this is a new appeal, a search screen is displayed. Use this screen to search for the original request item. That item will be linked to this denial form and the denial stored in the appropriate folder.

   If this is an existing appeal, a search screen is displayed. Use this screen to search for the appeal already submitted.

4. The Workflow Content Page is displayed. The request is listed and the Step column is changed to Acknowledge.

14.3.7.2 Acknowledging an Appeal

1. If still in the workflow process, click the **Review Workflow** icon for the request on the Workflow Content Page.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Appeal Sub**. A list of all requests in this stage is displayed. Click the Workflow Review icon for the request being processed.

2. The Workflow Review Page is displayed. Note that the action options in the Workflow Review Pane have changed to match the current workflow step.

3. Click **Acknowledged**. A search screen is displayed. Use this screen to search for items used to acknowledge the request.

4. Enter metadata for the search fields. Click **Search** when done.

5. A list of content items matching the criteria is displayed. Click the checkbox of the item to use and click **OK**. The Workflow Content Page is displayed again with the new workflow step ("AppealDecision") indicated in the Step column.

14.3.7.3 Reviewing the Appeal

1. If still in the workflow process, click the **Review Workflow** icon for the request on the Workflow Content Page.

   If the workflow process was exited, click **Content Management** then **Active Workflows** to display all available workflows. Click **FOIA Appeal Sub**. A list of all requests in this stage is displayed. Click the Workflow Review icon for the request being processed.

2. The Workflow Review Page is displayed with the original access request. Note that the action options in the Workflow Review Pane have changed to match the current workflow step.

   Click **Approve Appeal** to approve the appeal and route the request for servicing. See "Servicing a Request" on page 14-7 for details.

Click **Disappprove Appeal** to end the workflow process. The Final Result Dialog is displayed. Enter the information to be included on the final reports, including the final result, fees collected, number of people involved in servicing the request and total cost of servicing. Click **OK** when done.

14.3.8 Final Actions

When processing is finished for a request, move the folder to the appropriate category that was previously created (see "Initial Required Setup" on page 14-4).

Follow these instructions to move a folder to a new location:

1. Navigate to the folder to be moved. Click **Edit** then **Move** from the Page menu.
2. The Select Category or Folder Page is displayed. If necessary, click the plus sign icon to expand the view of the items.
3. Click the category name where the folder should be moved then click **OK**.
4. The Exploring Retention Category Page is displayed listing all folders in that category.

15

Using Federated Search and Freeze

"Federation" is a term used to describe the process of providing a single point of contact/entry for searching multiple disparate data sources. This is often used during the legal discovery process. For example, by using the Federated functionality with Oracle URM, a legal officer can search all repositories and catalogs for items pertaining to a legal matter. The search results then 'connect' all the items together in one place to perform searches.

Federated search is most effective when used with the Oracle URM Adapters that manage content on remote repositories.

This chapter describes how to use Federated Search to gather information needed for a discovery action and how to use Federated Freeze to freeze those items. It discusses the following topics:

- "Federated Searches" on page 15-1
- "Performing a Search" on page 15-3
- "Federated Freeze" on page 15-5

Important: Federated Search functionality is not visible until the RmaNoSecurity right is added to a role. This right is not added by default to any role and must be enabled for the functionality to be accessible. This right should not be treated lightly or granted indiscriminately.

In addition, a system administrator role is needed to use this functionality.

15.1 Federated Searches

Federated Search is available when an external repository (an adapter) is installed.

As part of a discovery process, organizations might search for or freeze content across multiple repositories which are managed by adapters. Oracle URM uses external adapters to search metadata and full text of remote repository items. With this functionality, a user can:

- Create searches by sending the search criteria to the adapter. External adapters check periodically to see if there are searches pending, perform the searches, and return the search results. The adapters may perform the search in a delayed timeline, requiring users to wait for the search results to complete.

- Freeze the content returned from a completed scheduled search. While scheduled freezes are initiated immediately, Oracle URM performs the freeze in the background.
- View detailed information about a scheduled search or freeze.
- View search or freeze results.
- Delete a scheduled search or freeze.

15.1.1 Federated Search Query Builder

To access the Federated Search Query Builder click **Search** then **Global Search** in the Top menu. The following options are available:

- **Central Catalog Search** is used for external content already registered with Oracle URM. This is a search of local metadata and is usually a faster search than Remote Repository items.

  Note that it is up to the adapter configuration to make adapter content visible to the Oracle URM server. If the adapter has not made its content available, Oracle URM will not find that content in a search.

- **Remote Repositories Search** is used to find items stored on external content systems whether they have been cataloged on the Oracle URM server or not. This is a search of all possible content using adapters to schedule the search. The adapters use the criteria entered for a Remote Repository Search as the criteria used for the search on that remote repository. Searching for content in Remote Repository is not in real time and is dependent on adapters to complete the search. This option provides the most accurate and up-to-date results but it may take a long time to complete.

  > **Note:** Federated Search adds functionality to the Search Query Builder Form. See the *Oracle Fusion Middleware User's Guide for Content Server* for additional help using the Search Query Builder.

- **SES Search** is similar to a Remote Repository Search but the search is not scheduled and run by an adapter. Instead, a connection is made to an SES server, which has done a scheduled crawl of content on the adapter(s). Oracle URM connects directly to the SES server, which has been configured ahead of time. If this option is selected and no servers have been configured, an error message is displayed.

The Federated Query Builder Page enables users to build and schedule queries across all repositories. Select the repositories to include in the search from the **External Sources** list. Multiple sources can be included in the search.

This query builder form is similar to other query builder forms used in Oracle URM and Oracle UCM. Select a field to use as sorting criteria and click **Search** when done. When performing a remote repository search, a search name must be entered. Users can only search using fields that are mapped to *all* of the selected external sources. Errors occur if a search is done against a source using a field that is not mapped.

After pressing **Save** enter a title for the action. The search is scheduled and the Federated Searches Page appears. The list of scheduled searches includes the number of external sources requested in the search, and number of external sources that have completed the search request.

The search is scheduled and waits for the external search adapters to return results.

To return to the Federated Searches Page, click **Records** then **Scheduled** then **Federated Searches** from the Top menu.

15.2 Performing a Search

Follow this procedure to perform a search of a remote repository:

1. Click **Search** then **Global Search** from the Top menu. Choose the type of repository search to perform.

   The Federated Query Builder Page is displayed.

2. Select the external sources to use in the query from the pull-down list.

3. Click the **Include Content** box to retrieve copies of the content that match the search criteria. This option is only available when performing a remote repository search.

   Do not click this box unless search results are certain. Returning a copy of the data takes long and uses space. Fine tune the query first and verify what items will be returned before actually retrieving the content. See "About Returned Content" on page 15-3 for more information about content retrieved during a search.

4. Choose the fields to use for searching. The **Search Builder** pull-down menu is used to select fields for use in the query. Only search using fields that are mapped to *all* of the selected external sources. Errors occur if a search is done against a source using a field that is not mapped.

   After a field is selected for use, additional menus are available to further refine the criteria. Boolean operators can be used to combine fields. Click the insert symbol (a plus sign) to access a menu of Boolean operators. Click the remove symbol (a lowercase 'x') to clear previous selections. Additional wildcard search operators, such as **Matches** and **Substring**, enable further flexibility in query building.

5. Enter a search term for full-text searching. If a search is done across all sources, be aware that some adapters may not be able to perform a full text search. When choosing a search type, make sure to choose types that are valid for the adapters in use. For example, if a user chooses full-text search to use with an adapter that does not allow that option, an error is returned.

6. Enter a search name. A Federated search is performed on the adapter's schedule, so it may not occur immediately. A search name allows users to check the status of the scheduled Federated search. No uniqueness validation is performed on this field because the unique identifier is an assigned Federated Search ID.

7. Select the result output criteria by indicating a number of results per page and the sorting criteria used for the results.

8. Click **Search** when done. The query is routed to the chosen adapters and is completed according to the adapter configuration.

15.2.1 About Returned Content

Saved content is stored in a zip file and is checked into Oracle URM as internal content. These returned content items can be accessed and treated as standard local items in Oracle URM. Users can set dispositions on the files, establish specific rules for their handling, and so on.

Some adapters may return the content in multiple files because the adapter may be configured to chunk data into manageable units. This behavior is controlled on the adapter side and cannot be modified

15.2.2 Checking Search Progress

Federated searches are performed according to adapter schedules, which may vary according to the different configurations. To check the progress of the search, click **Records** then **Scheduled** then **Federated Searches** from the Top menu. Or click the Federated Searches Link on the Federated Query Builder Page.

The Federated Searches List Page is displayed. This page shows the scheduled searches and their progress. The following options are available on the **Action** menu for each search:

- **Show Search Results:** displays the Federated Search Results Page for the selected search. If multiple external sources were selected in the search, the Search Results Page organizes the results by external source. The search results for individual external sources can also be displayed.
- **Show Search Details:** displays the details for the selected search. Within the Federated Search Details Page, users can view the search results for individual external sources, freeze the search results, download the files returned for the search, and create a similar search.

> **Note:** Users can freeze items in the returned search results per external source. If multiple external sources have been defined in the search, but have not all returned results, users can schedule a freeze on the sources that returned results for the scheduled search.

- **Subscribe to Search**: subscribes the user to the search and displays the Content Information Page for the query. See "Subscribing to a Search" on page 15-4 for more details.
- **Create Similar Search:** displays the Federated Query Builder Page, pre-populated with search criteria used in the selected search. Users can modify or add criteria to schedule a new search.
- **Delete Search:** delete the selected scheduled search. See Deleting a Search for details.

15.2.3 Subscribing to a Search

When a Federated search is created, a content item is checked into the local repository with details of the search. If a user clicks **Subscribe to Search** on the Actions menu for an item on the Federated Searches List Page, the user is subscribed to the content item for that query.

As results are returned for the saved search, the content item is updated. For example, if a query is set to use three repositories and results are returned from one, the content item is updated and a notification is triggered to those people who are subscribed to the content item.

15.2.4 Deleting a Search

A Federated search can be deleted at any time. Search results do not have to be returned to delete the search.

To delete a search, click the checkbox for the search on the Federated Searches List Page then click **Delete** on the Table men. A message is displayed, indicating the search and all returned results will be deleted. Any pending search results will be ignored.

15.3 Federated Freeze

Federated Freeze is used in conjunction with Federated search, to freeze search results from a Federated query.

> **Note:** Federated Freeze adds functionality to content freezing used in Oracle URM. See the *Oracle Fusion Middleware Setup Guide for Universal Records Management* for additional information about freezes.

When freezing content on an external repository, first schedule a Federated Search, then run a Federated Freeze on the returned results. If the search result that is selected for freezing has not been registered with Oracle URM yet, an external record is created for it automatically using the metadata returned in the search results. This new external record is then frozen by Oracle URM.

The Frozen Federated Search Content Page is displayed for review or further action. The list of frozen scheduled searches includes the external source of the frozen content, and the status (scheduled, completed or errors) of the freeze.

The following options are available from the **Actions** menu for a frozen item:

- **Show Freeze Errors**: displays the items with errors during the selected freeze. Freeze errors may occur if the checked-in items from the Federated Search do not have all required fields defined or if the items do not pass validation.
- **Refreeze Errors**: reschedules the freeze for the error items in the selected search task.
- **Delete Freeze**: deletes the selected freeze.

15.3.1 Freezing Search Results

Follow this procedure to freeze search results:

1. Click **Records** then **Scheduled** from the Top menu. Click **Federated Searches**.

   The Federated Searches List Page is displayed.
2. Click **Show Search Results** from the Action menu of a search.

   The Federated Search Results Page is displayed.
3. Click the checkbox of the items to freeze then click **Freeze** from the Table menu.

   A dialog box is displayed.
4. If freezes have been added to a My Favorites list, they appear on the dropdown list. Choose a freeze name from the dropdown list or click **Show All Freezes** to display all defined freezes.
5. Enter a reason for the freeze.
6. Click **OK**.
7. The search results are frozen.

15.3.2 Viewing Scheduled Freezes

Use this procedure to view which results are frozen:

1. Click **Records** then **Scheduled** from the Top menu. Click **Federated Search Freezes**.

2. The Frozen Federated Search Content Page is displayed, showing all items items found during a federated search that are frozen.

A

User Interface

This section contains information about the interface used with the product.

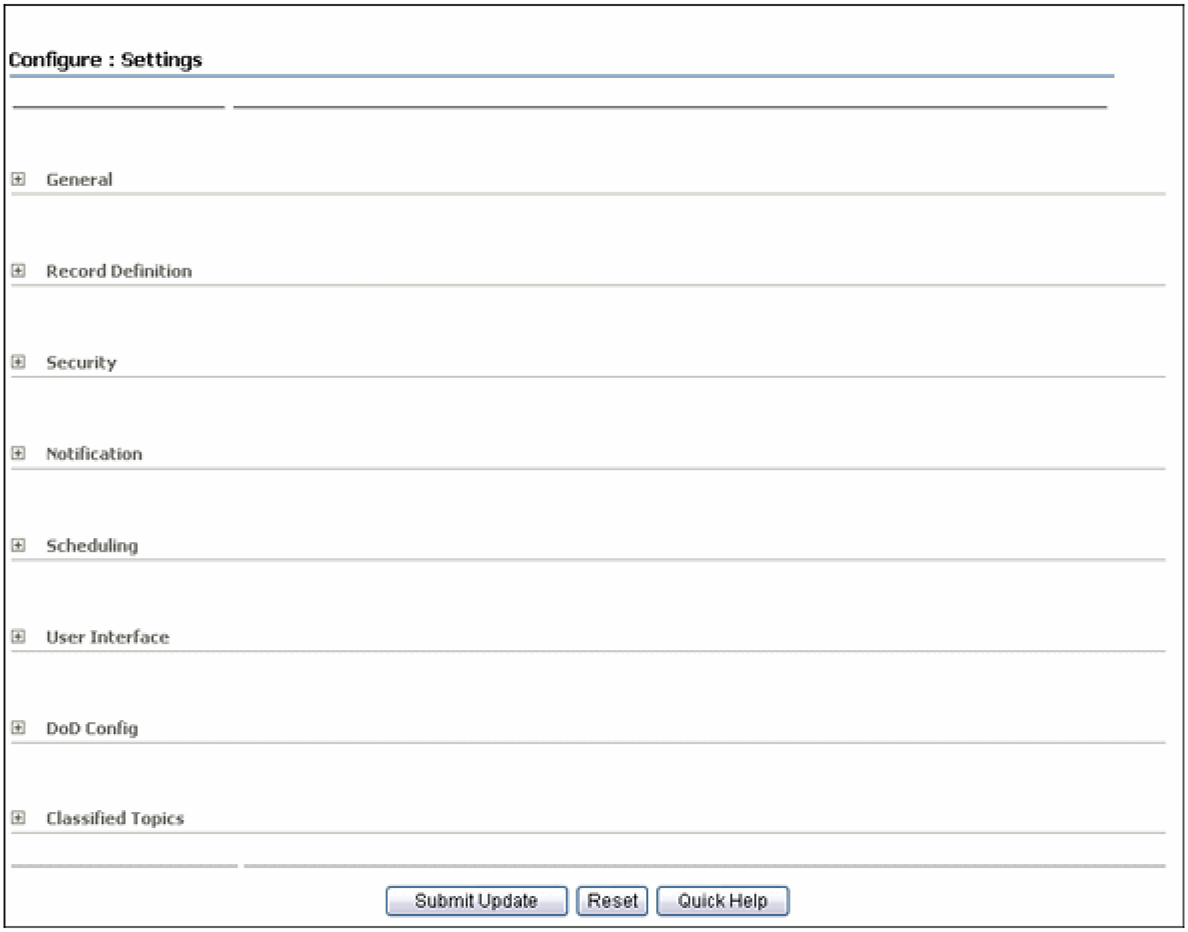
The following screens are shown in this chapter:

Several buttons are common to many pages and are not discussed unless additional information is available:

- **Submit**: submits the changes made to the page
- **Reset**: clears any entries and resets the page to its default
- **Quick Help**: displays the help entry for the screen
- **Delete**: removes the item on the screen
- **Create**: submits the information provided and creates the item
- **Info**: displays the information page for the item
- **Thumbnail View**: Displays the page in thumbnail view.
- **Headline View**: Display the page in headline view.

A.1 Configure Retention Settings Page

Use this page to set most of the configuration options for the system. When initially opened, the options on this page are unexpanded. Click a link next to an option to expand it.



Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role.

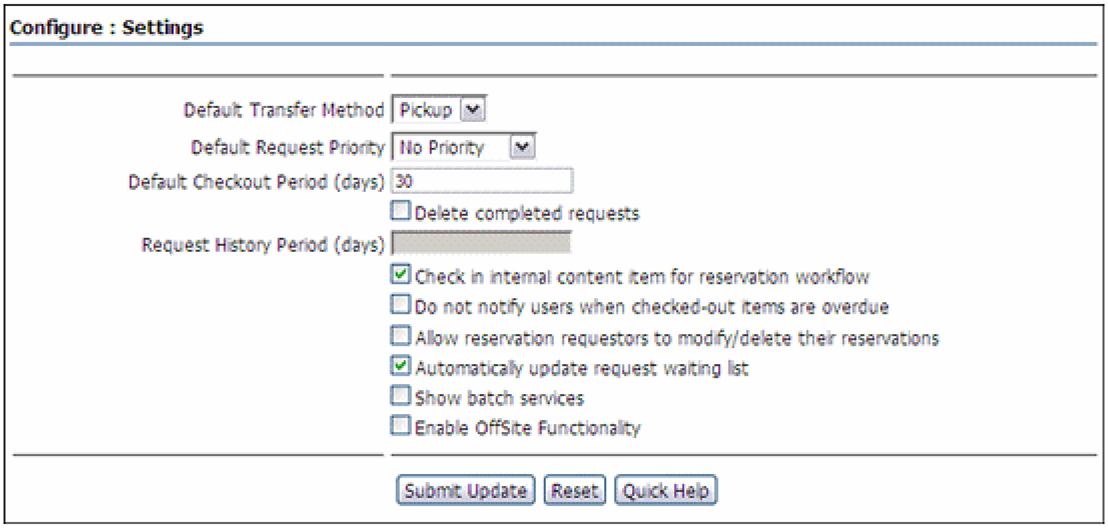
To access this page, click **Records** then **Configure** then **Settings** from the Top menu.

Most configuration tasks are discussed in the *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

A.2 Configure Physical Content Management Page

Use this page to configure many aspects of PCM.

The Physical Item Information Page, also discussed in this section, contains information about individual physical items which are managed by PCM.



Permissions: The PCM.Admin.Manager right is required to access the Configure Physical Content Management page. By default, this right is assigned to the predefined PCM Administrator role.

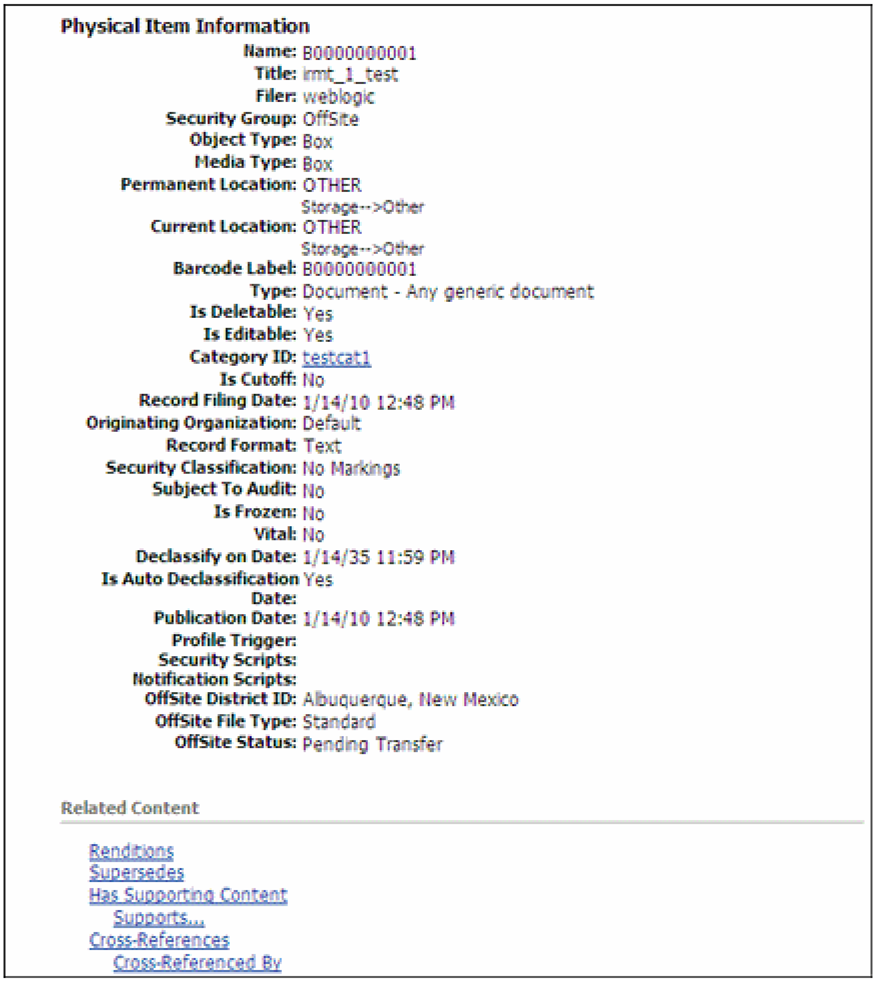
To access this page, click **Physical** then **Configure** then **Settings** from the Top menu.

The Batch Services option is only displayed if the corresponding option on the Configure Physical Content Management Page is enabled.

The menu items available to users depend on the rights they have been assigned. A content administrator with all access rights (typically assigned the predefined PCM Administrator role) will see all administrator menus. Other users (for example, those assigned the default 'pcmrequestor' role) may see a much smaller subset of the administrator menus, depending on their assigned rights.

A.2.1 Physical Item Information Page

Use this page to view information about an existing physical item.



Permissions: The PCM.Physical.View right is required to use this screen. This right is assigned by default to the PCM Requestor and PCM Administrator roles.

To access this page, search for the item. On the search results page click **Information** then **External Item Information** in the item's **Action** menu.

This page shows the current properties of the physical item, including its basic metadata (name, title, filer, and security group), its freeze status, its object and media types, its storage location, and barcode label.

Note the following:

- If the repository is set up to auto-generate content IDs (in the System Properties utility), the name of a physical item was generated automatically. It is typically a number, possibly preceded by a prefix (for example, ID_002319).
- If the physical item was assigned a life cycle (retention schedule and disposition rules), the information page also includes a Retention Schedule Information section providing disposition processing and security information for the item.
- If the physical item is currently checked out, its current location is set to the value of the deliver-to location as specified when the associated reservation request was created. If no location was provided, the current location is set to "OTHER." If a

location comment was specified for the associated reservation request, the Current Location Comments field shows this comment. Otherwise it contains the login name of the user who created the reservation request.

- If the physical item is contained within another physical item, the current location and/or permanent location field includes a **Container Details** link, which opens the information page of the parent physical item (the "container").

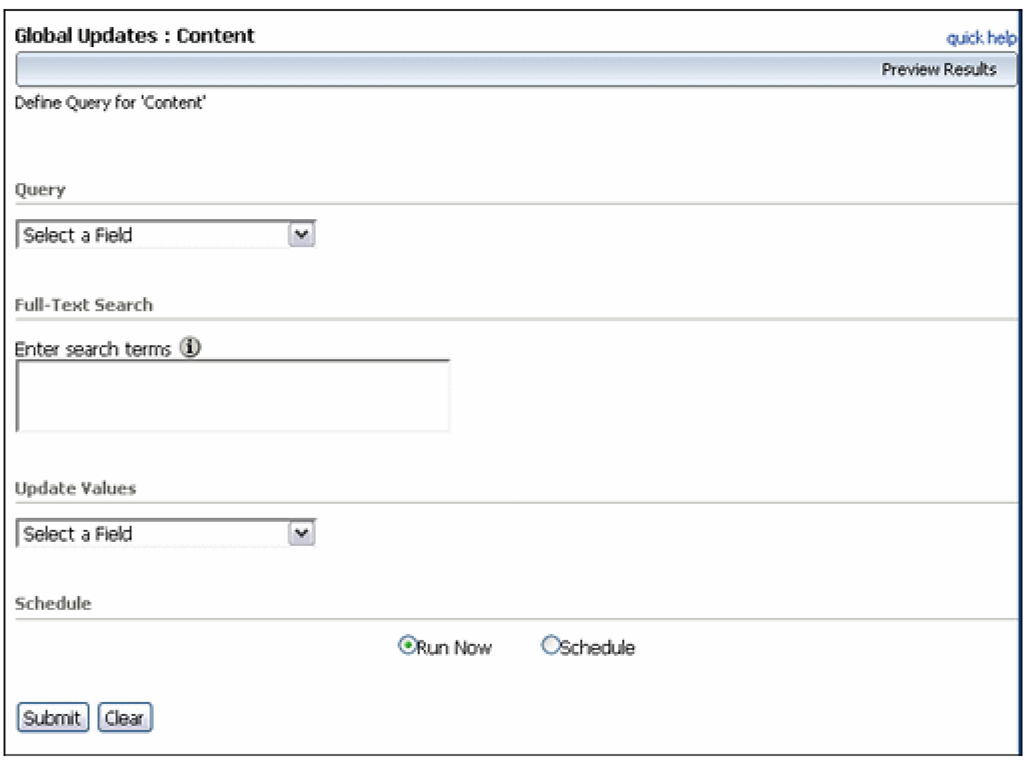
A.3 Update Interface

The following screens are accessed when using the update functionality:

- "Define Query Page" on page A-5
- "Query Schedule Section" on page A-6
- "Scheduled Update Page" on page A-6
- "Update Preview Page" on page A-6

A.3.1 Define Query Page

Use this page to define what fields will be updated and what values will be used for updating.



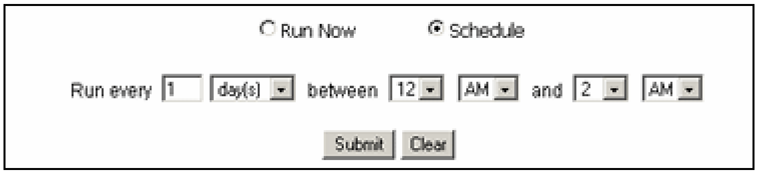
To access this screen, click **Records** then **Global Updates** then the type of update from the Top menu.

Frozen content cannot be updated.

The options on this screen are specific to the type of query being created. After an option is selected, additional menus open to help further refine the query. See the *Oracle Fusion Middleware User's Guide for Content Server* for complete details about using queries.

A.3.2 Query Schedule Section

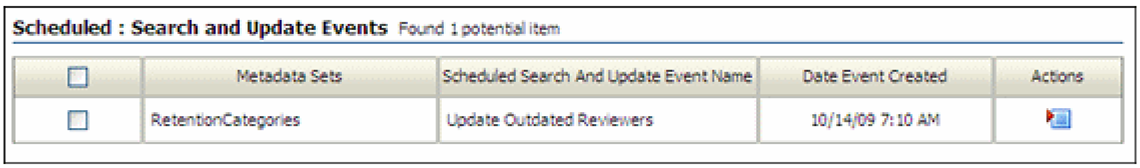
The Schedule portion of the Define Query Page is used to choose the times when updates will occur.



To access this portion, click the **Schedule** button on the Define Query Page. Select values from the lists for the update schedule and select **Submit** when finished.

A.3.3 Scheduled Update Page

This screen shows the results of scheduling an update action. It is displayed after scheduling an update or search or by selecting **Records** then **Scheduled** then **Search and Update Events** from the Top menu.

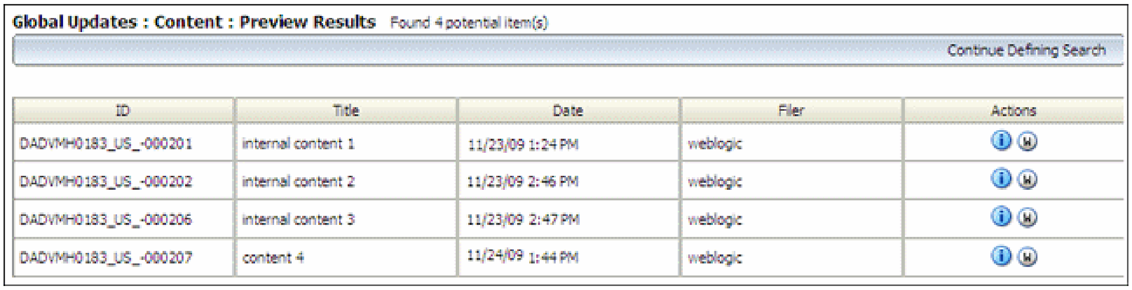


Use the **Actions** menu for the individual event to change the options for the event. .

Element	Description
Metadata Sets	The type of update which was selected.
Scheduled Search and Update Event Name	The event name entered when the update was created.
Date Event Created	The date when the scheduled event was created.
Actions	A menu with options to be used on the individual events: ■ **Run Now**: Runs the event without waiting for the scheduled time. ■ **Edit Scheduled Event**: Opens the Define Query Page where the event can be edited. ■ **Delete Scheduled Event**: Deletes the event. A prompt appears to confirm the deletion.

A.3.4 Update Preview Page

This screen shows those items which will be changed when an update is done. To access this screen, select **Preview Results** on the Define Query Page.


Global Updates : Content : Preview Results Found 4 potential item(s)

Continue Defining Search

ID	Title	Date	Filer	Actions
DADVMH0183_US_-000201	internal content 1	11/23/09 1:24 PM	weblogic	
DADVMH0183_US_-000202	internal content 2	11/23/09 2:46 PM	weblogic	
DADVMH0183_US_-000206	internal content 3	11/23/09 2:47 PM	weblogic	
DADVMH0183_US_-000207	content 4	11/24/09 1:44 PM	weblogic	

The **Update** icon (a capital W in a circle) indicates that the item is not locked and can be changed. Click the **Info** icon to view the Information Page for the item.

To return to the Define Query Page, click **Continue Defining Search** on the Page menu.

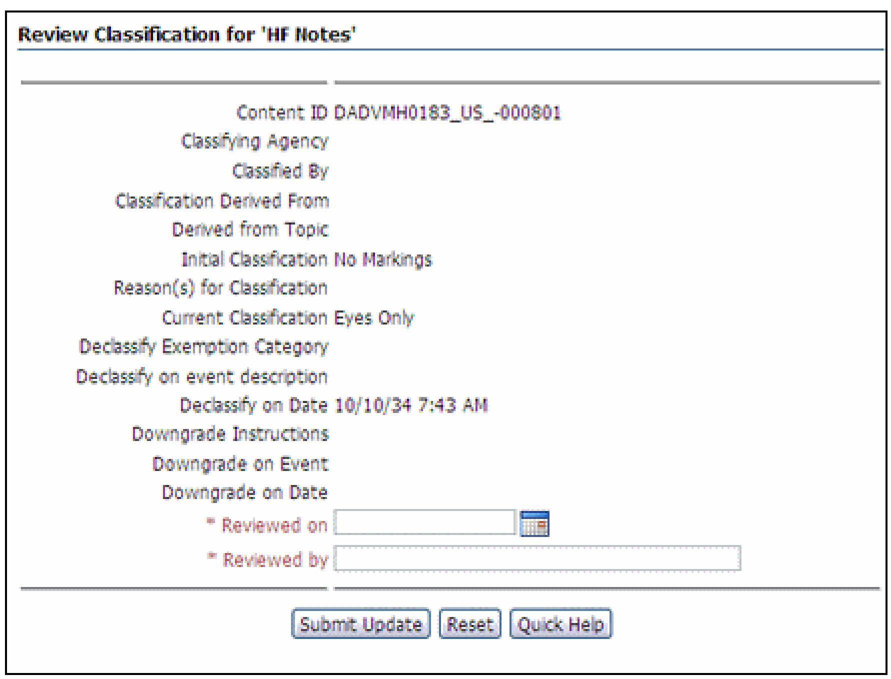
A.4 Classified Content Interface Screens

The following screens are used when reviewing or altering the classification of items:

- "Review Classification Page" on page A-7
- "Upgrade or Downgrade Classification Page" on page A-8
- "Declassify Page" on page A-8

A.4.1 Review Classification Page

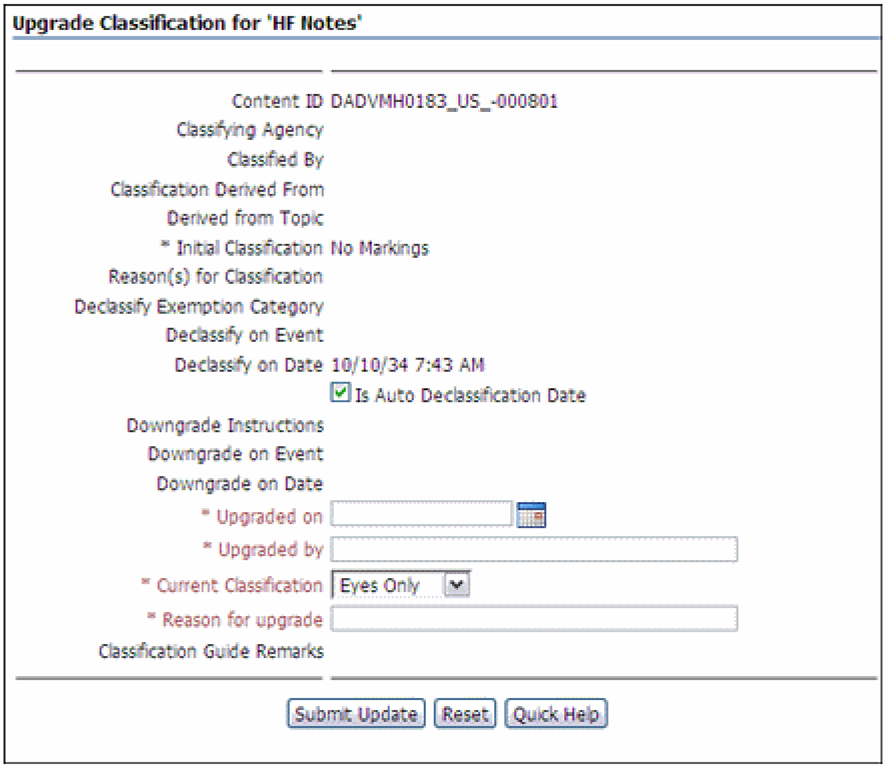
The following screen is used to review the classification of content.



To access this screen, click **Information** then **Review Classification** from the Page menu on a Content Information Page.

A.4.2 Upgrade or Downgrade Classification Page

The following screen is used to change the classification of an item.



To access this page, click **Edit** then **Upgrade Classification** or **Downgrade Classification** from the Page menu on a Content Information Page.

A.4.3 Declassify Page

The following screen is used when declassifying content.

To access this page, click **Edit** then **Declassify** from the Page menu on a Content Information Page.

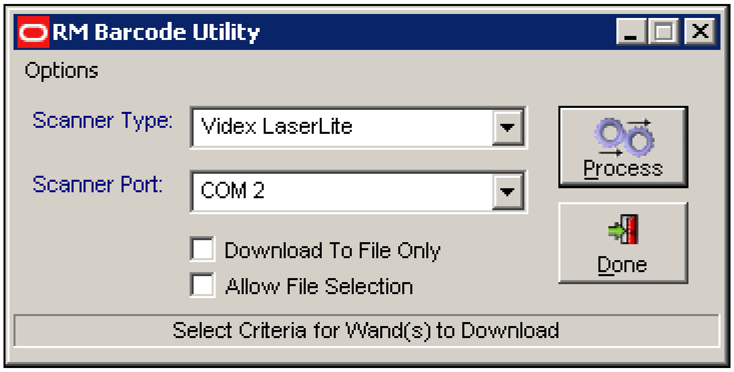
A.5 Barcode Interface

Barcode processing has the following user interface screens:

- "Main Barcode Utility Screen" on page A-9
- "Barcode Upload Screen" on page A-10
- "Configure Host List Screen" on page A-11
- "Barcode Upload Results Screen" on page A-11
- "Program Videx Barcode Wand Screen" on page A-12
- "Barcode Processing Page" on page A-12
- "Barcode File Processed Page" on page A-13

A.5.1 Main Barcode Utility Screen

This screen is used to upload information to the PCM software or write it to a file.

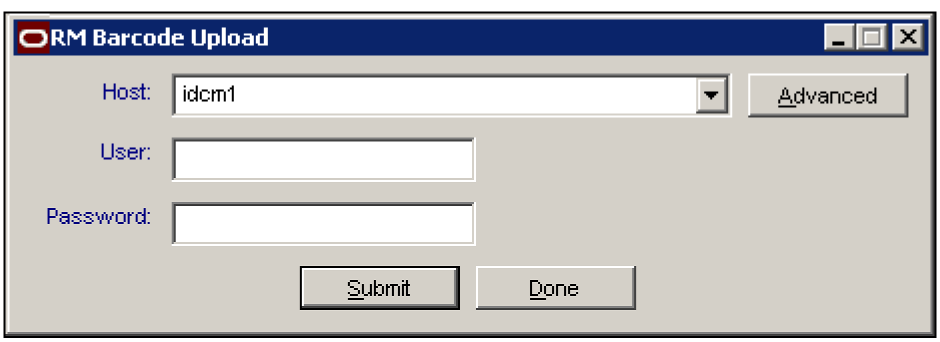


Access this screen by starting the Barcode Utility application.

Element	Description
Options menu	Displays the Program Videx Barcode Wand Screen.
Scanner Type	The barcode scanner type. One type is currently supported.
Scanner Port	The communication port where the barcode scanner or its base station is connected. Normally this is COM1, a commonly used serial port.
Download to File Only	Writes barcode scanner data to a file for later processing.
Allow File Selection	Selects a previously stored file for processing.
Process button	Starts the upload process. The barcode scanner data will either be directly uploaded to Physical Content Management or, if **Allow File Selection** was selected, a file selection dialog is displayed, where the file to be uploaded can be selected.
Done button	Closes the Barcode Utility application.

A.5.2 Barcode Upload Screen

This screen is used to specify the instance where data will be uploaded.



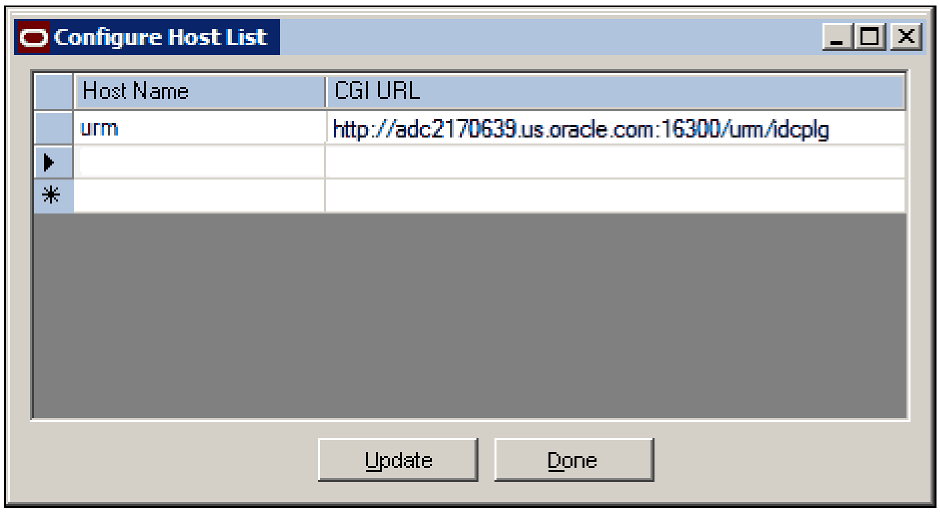
To access this screen, click **Allow File Selection** on the Main Barcode Utility Screen. Click the **Process** button.

Element	Description
Host	The name of the instance where the barcode information should be uploaded. This instance should be running the Physical Content Management software.

Element	Description
User	The login name of the user who will connect to the instance to upload the barcode data.
Password	The login password of the user who will connect to the instance to upload the barcode data.
Advanced button	Displays the Configure Host List Screen, where all instances where barcode data can be uploaded are specified.

A.5.3 Configure Host List Screen

This screen is used to specify the instances where barcode data can be uploaded. The defined hosts are included in the Host list on the Barcode Upload Screen.

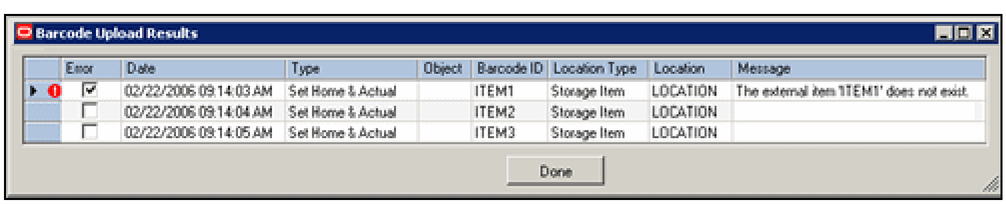


To access this screen, click the **Advanced** button in the Barcode Upload Screen.

Element	Description
Host Name	The name of a instance where barcode information can be uploaded. This instance should be running Physical Content Management.
CGI URL	The URL of the 'idcplg' directory of the instance. This information is required to establish a connection to the instance.

A.5.4 Barcode Upload Results Screen

This screen provides information about what barcodes were processed and also shows the upload results of each item processed (including any error messages).

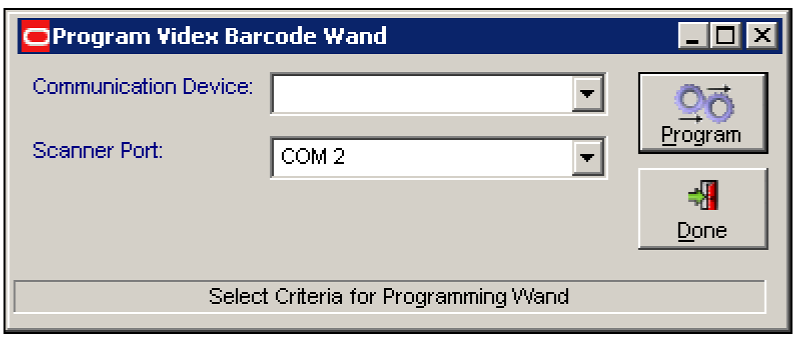


This screen appears after uploading a stored barcode file.

Element	Description
Error	Indicates if an error occurred during processing of an item. The error message is displayed in the Message column.
Date	The date and time the information for the item was scanned by the barcode scanner.
Type	The type of action performed for the item. Three actions are possible: Check In, Check Out, and Set Home & Actual.
Object Type	The object type of the data item (for example, "Box" or "Folder").
Barcode ID	The barcode value of the item as read by the barcode scanner. For storage items, this is the item's name (as specified when it was created in Physical Content Management).
Location Type	The location type of the item (for example, "Box" for items in a box, or "User" for checked in or checked out items).
Location	The barcode of the location where the item is assigned (stored in).
Message	A message if an error occurred during the transfer.

A.5.5 Program Videx Barcode Wand Screen

This screen is used to program the barcode scanner for use with Physical Content Management.

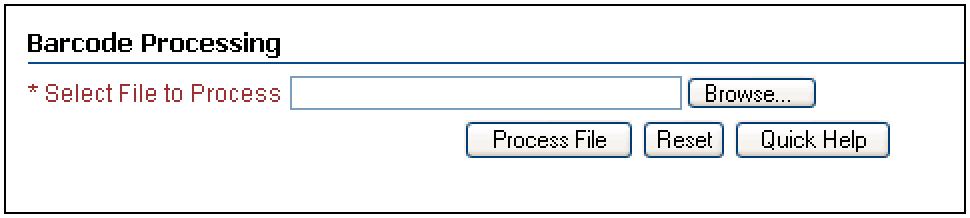


To access this screen, click **Options** then **Program Videx Wand** from the Main Barcode Utility Screen.

Element	Description
Communication Device	Selects the device used to connect the barcode scanner to the computer. There are two options: **Jet Eye**: An infrared receiver device connected to a COM port on the computer. Point the barcode scanner at the receiver to communicate with the computer. **Base Station**: A holder for the barcode scanner linked directly to the computer using a cable.
Scanner Port	Selects the communication port where the barcode scanner or its base station is connected. Normally this is COM1, which is a commonly used serial port.
Program button	Starts the programming cycle of the barcode scanner.

A.5.6 Barcode Processing Page

Use this page to select a barcode file to be processed.



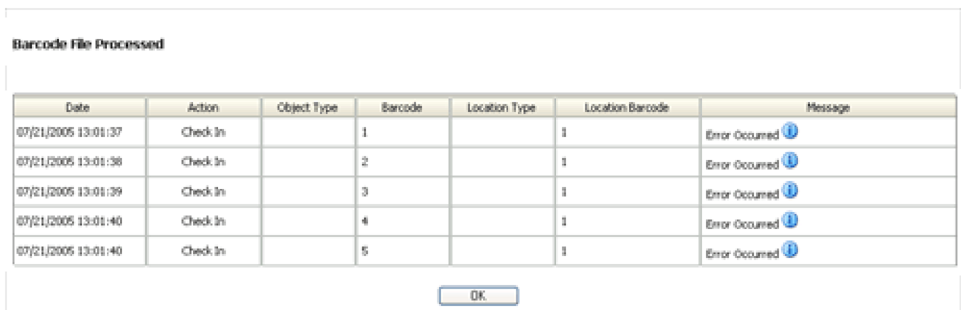
Permissions: The PCM.Barcode.Process right is required to use this screen. This right is assigned by default to the predefined PCM Administrator role.

To access this page, click **Physical** then **Process Barcode File** from the Top menu.

Element	Description
Select File to Process	A barcode file to be processed. Enter a name or use the Browse button to select a file.
Process File	Starts the analysis and processing of the selected barcode file.

A.5.7 Barcode File Processed Page

This page shows information about all the items in the barcode file, the actions performed on them and any status and error messages.



This page is displayed after a barcode file has been selected on the Barcode Processing Page and processed.

Element	Description
Date	The date and time the item was read by the barcode scanner.
Action	The action performed on the item in the barcode file (as specified in the barcode file).
Object Type	The object type of the item (for example, "Box").
Barcode	The barcode of the item as read by the barcode scanner.
Location Type	The location type of the item (for example, "Position").
Location Barcode	The barcode of the location where the item should be assigned.
Message	Displays 'Error Occurred' if the action was not completed successfully for an item. Click the info icon to display more specific information about the error message.

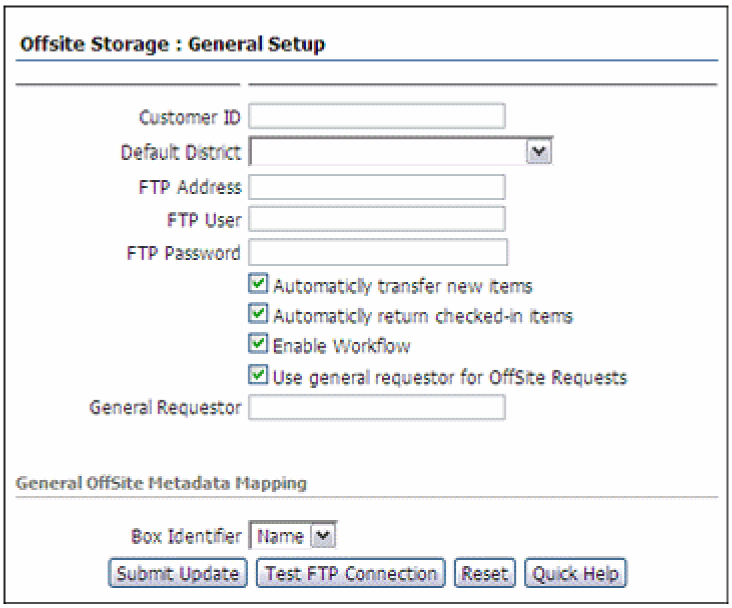
A.6 Offsite Storage Interface Screens

The following screens are used to set up and use the offsite storage functionality:

- "Offsite Storage General Setup Page" on page A-14
- "District Mapping Screens" on page A-15
- "Create Manual Pickup Page" on page A-17
- "Browse Uploaded Files Page" on page A-17
- "Browse Processed History Page" on page A-18

A.6.1 Offsite Storage General Setup Page

Use this screen to begin setting up offsite storage.



To access this page, click **Physical** then **Offsite Storage** then **General Setup** from the Top menu.

Element	Description
Customer ID	A customer ID for this storage session.
Default District	The default district to be used with this customer ID. Several districts are provided. New districts can be also be created.
FTP Address	The FTP address associated with this storage location.
FTP User	The user associated with the FTP account.
FTP Password	The password associated with the FTP account.

Element	Description
Transfer boxes	Options associated with the transfer: ■ Automatically transfer new items: enables automatic transfer of any new items. ■ Automatically return checkd in items: enables automatic returns of checked in items. ■ Enable workflow: starts a criteria workflow to handle the approval of items pending transfer. An internal file is checked in with a list of objects for approval. Objects can be removed from the list or approved for transfer. ■ Use general requestor for Offsite Requests: indicates a requestor should be used.
General Requestor	Enter a requestor. This field must be 5 characters or less.
Box Identifier	A method of identifying boxes used in transfer. Select an item from the list.

A.6.2 District Mapping Screens

Several similar screens are used to map metadata to districts used when configuring offsite storage. A sample screen is depicted and described here.

- "Choose District Mapping Page" on page A-15
- "Map Metadata Pages" on page A-16

A.6.2.1 Choose District Mapping Page

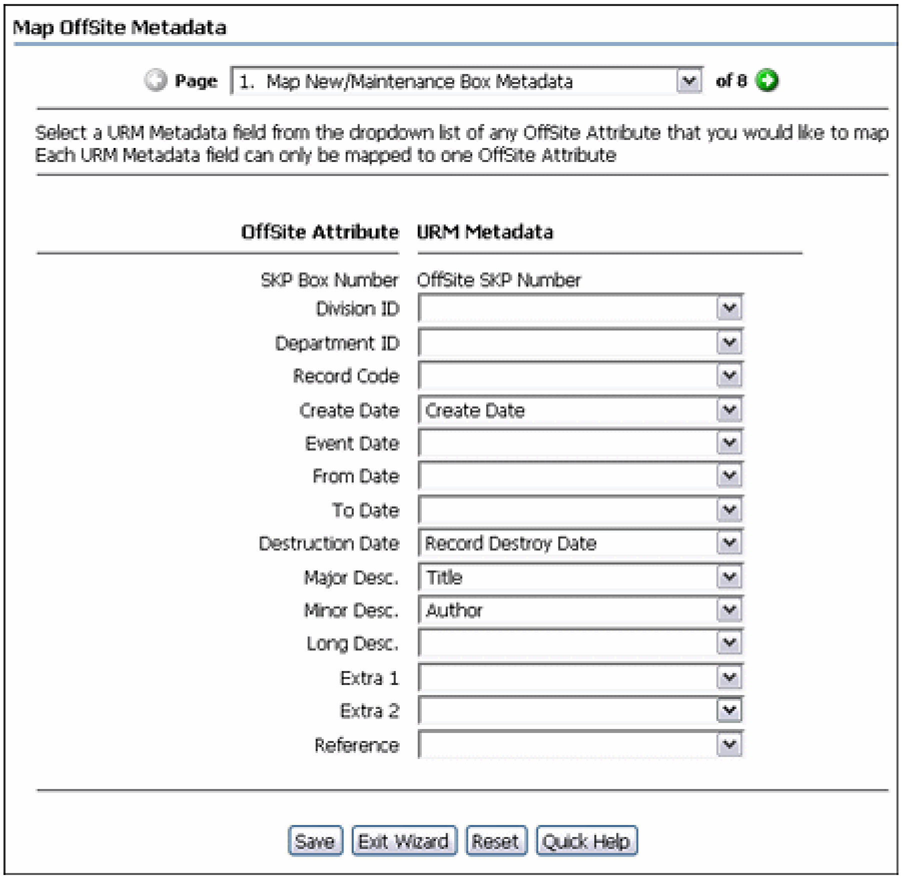
Use this screen to select the district for which to map data.

To access this page, click **Physical** then **Offsite Storage** from the Top menu. Click **Map District Metadata**.

Scroll up or down in the list and select a district by highlighting the name. Districts which are already mapped are in bold face type at the top of the list. After highlighting a district, click **Configure**.

A.6.2.2 Map Metadata Pages

After selecting a district to configure on the Choose District Mapping Page, the next screen in the District Mapping process is displayed.



Choose a district to map on the Choose District Mapping Page and click **Configure**. This screen is displayed.

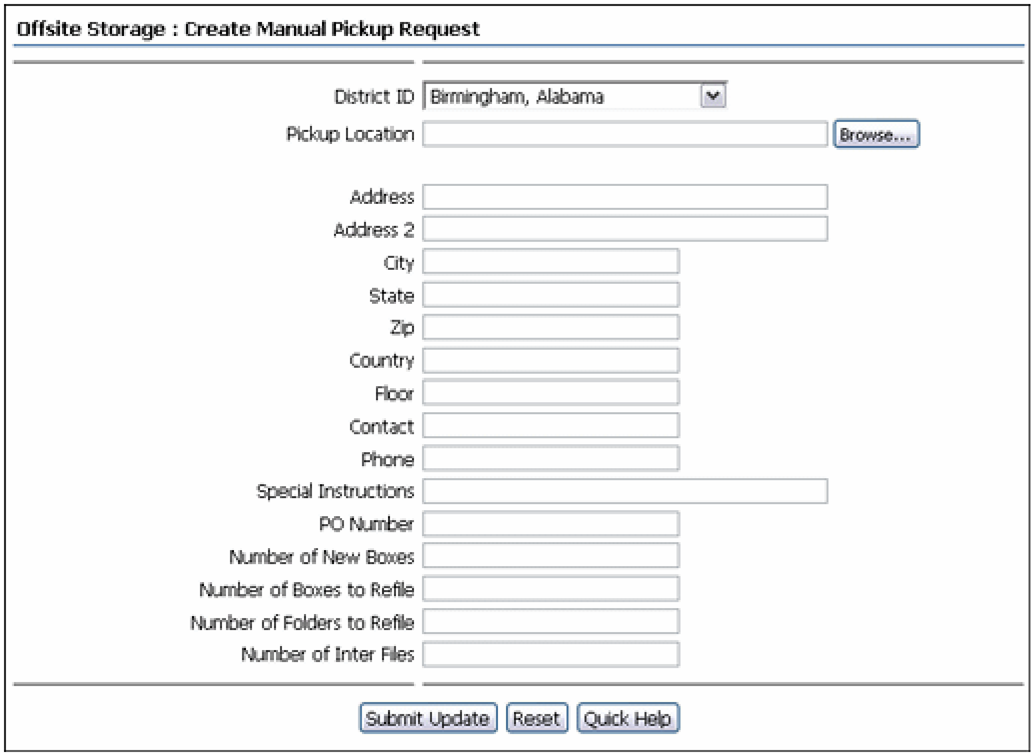
All screens in this process are similar. The fields and field values in the option lists on these screens are provided by Iron Mountain. For a description of the fields and their values, see the Iron Mountain documentation.

The following screens can be configured. Either configure all screens in sequence or skip to a specific screen by selecting the screen name from the menu list at the top of the screen:

- Box metadata
- File metadata
- Accounting metadata
- Insurance1 and Insurance 2 metadata
- Law metadata
- Loan metadata
- Medical metadata

A.6.3 Create Manual Pickup Page

Use this screen to create a request for pickup of boxes and files for offsite storage.

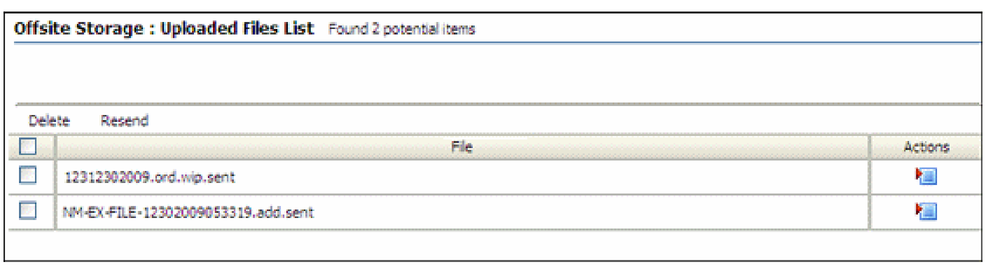


To access this page, click **Physical** then **Offsite Storage** then **Create Manual Pickup Request** from the Top menu.

The fields on this page are determined by Iron Mountain. Consult the Iron Mountain documentation for details.

A.6.4 Browse Uploaded Files Page

Use this screen to view a list of all uploaded files and their status.

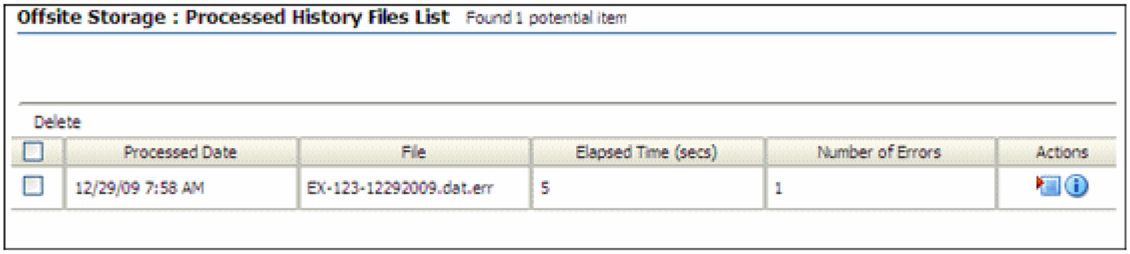


To access this page, click **Physical** then **Offsite Storage** then **Uploaded Files List** from the Top menu.

Element	Description
Delete	Used to delete a checked item.
Resend	Used to resend the checked item.

A.6.5 Browse Processed History Page

Use this screen to view a list of all processed history files and their status.



To access this page, click **Physical** then **Offsite Storage** then **Processed History Files List** from the Top menu.

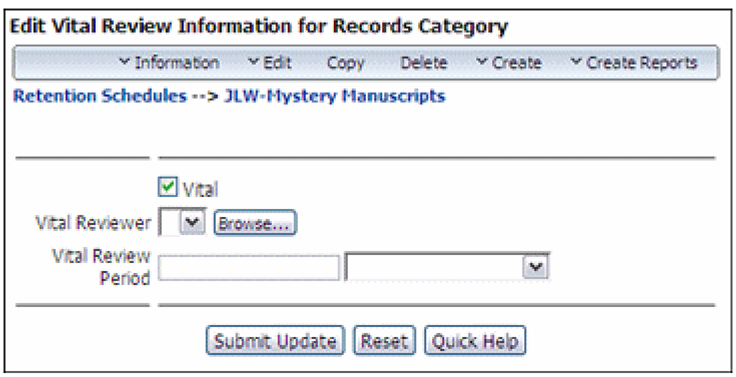
A.7 Subject to Review (Vital) Interface Screens

The following screen is used to manage review information:

- "Edit Review Information for Retention Category/Folder Page" on page A-18

A.7.1 Edit Review Information for Retention Category/Folder Page

This screen is used to edit information about reviewers for retention categories.



To access this page, find a retention category to edit. Click **Edit** then **Edit Review** from the item's **Actions** menu. User-friendly captions are noted in parentheses in the following table.

Element	Description
Vital (Subject to Review) box	Enables the retention category as a subject to review category. After enabling, enter a reviewer user name in the text box and select the associated period from the list. **Default: Not selected.** Not a retention category that is subject to review. If a retention category has a review period of shorter duration than the review period set for its child record folder, the child record folder assumes the shorter review period and ignores its own setting. The shorter review period takes precedence.
Vital Reviewer (Reviewer)	A reviewer for the item. Use the system default reviewer as specified on the Configure Retention Settings Page or select one from the list. The selected reviewer receives e-mail notification when it is time to review and cycle content items.

Element	Description
Vital Review Period (Review Period) text box and list	The number of review periods. Select the review period from the list. Required if the Subject to Review box is selected.

A.8 Scheduling Interface Screens

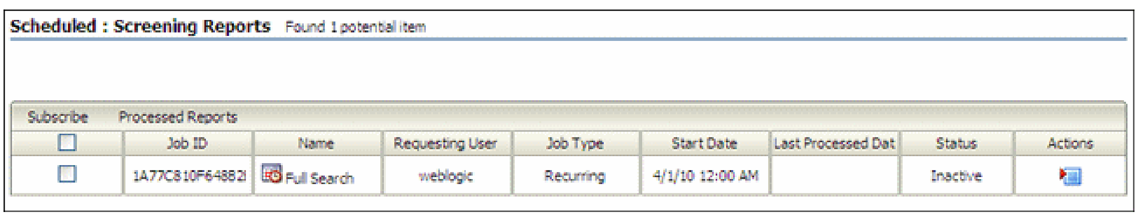
The following screens are used for scheduling:

- "Scheduled Screening Reports Page" on page A-19
- "View History Page" on page A-20
- "Job Information Page/Edit Job Information Page" on page A-21
- "Scheduled Freezes Page" on page A-23
- "Edit Recurring Report Schedule Page" on page A-24
- "Scheduled Jobs Listing Page" on page A-25

For details about scheduled Federated events, see "Federated Search and Freeze Screens" on page A-65. For details about scheduled update events, see "Update Interface" on page A-5.

A.8.1 Scheduled Screening Reports Page

This page lists all screening reports scheduled from screening pages.



To access this page, click **Records** then **Scheduled** then **Screening Reports** from the Top menu.

To see a list of reports that have been produced, click the **Processed Reports** link on the Table menu. A listing is displayed showing those reports that have processed.

After processing, information about the report is available. Click the **Info** icon to view a report’s Information page. If the report did not process properly, the **Info** icon displays the error message received during processing.

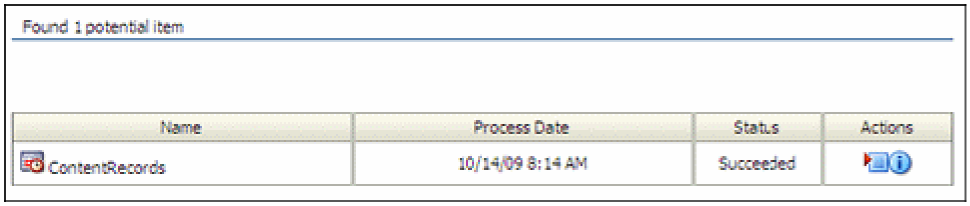
Note that reports that have been scheduled and are not recurring (’one-time’ reports) are not displayed after they are executed but do appear on the Processed Reports page.

Element	Description
Job ID	The assigned identifier for the scheduled job.
Name	The name of the freeze used for the schedule.
Requesting User	The user who initiated the scheduled freeze.
Job Type	An indicator of job type. *One Time* indicates the job is run once. *Recurring* indicates an action done on a repeating schedule. Note that when a job is processed, it is removed from the display.

Element	Description
Start Date	The date the job will be initiated. If the job is a *long* type, the system checks within one day of the start date to see if the job needs to be run. If it is a *short* type, the system checks if the needs to be run within the hour of the start date and time. If the job type is recurring, the job continues executing within a defined interval after the start date.
Last Processed Date	The date and time the recurring action was last generated.
Status	The current status of the scheduled screening report: ■ **Processed**: The scheduled report generated successfully and is not scheduled to be repeated. ■ **Exception**: The scheduled report did not execute successfully. The log file contains more details on the error(s) that occurred. ■ **Active**: The scheduled report is being executed. ■ **Inactive**: The scheduled report is in the queue of tasks to be performed and will be generated when scheduled, usually at midnight. ■ **Canceled**: The scheduled report was aborted before it could be completed successfully.
Action menu	Displays a menu containing options relevant to the scheduled screening report. The available options depend on the type and status of the scheduled screening report, and may include: ■ **View Log**: Displays the content information page of the generated report. ■ **Unschedule**: Cancels the scheduling of the report. ■ **Edit Subscription**: Allows a user to subscribe or unsubscribe to the report. A subscription email will be sent whenever the report changes. ■ **Run Report**: Creates the report immediately. After the report is created, click the link in the Name column to view it. The report is in the format specified by the Report Format setting on the Configure Retention Administration Page. ■ **View History**: Displays the View History Page. ■ **Edit Schedule**: Displays the Edit Recurring Report Schedule Page where the scheduling properties of the recurring screening report can be modified. ■ **Edit Criteria**: Displays the associated screening definition page (for categories, folders, or content items), where the criteria for the screening report can be modified. ■ **Remove**: Removes the disposition action from the list of scheduled actions.
Info icon	Displays the content information page of the automatically generated report file. Use the Web Location or Native File link to view the file.

A.8.2 View History Page

This page shows a list of generated actions. The screen depicted here is for a scheduled screening report. A similar screen is used for scheduled recurring freezes.

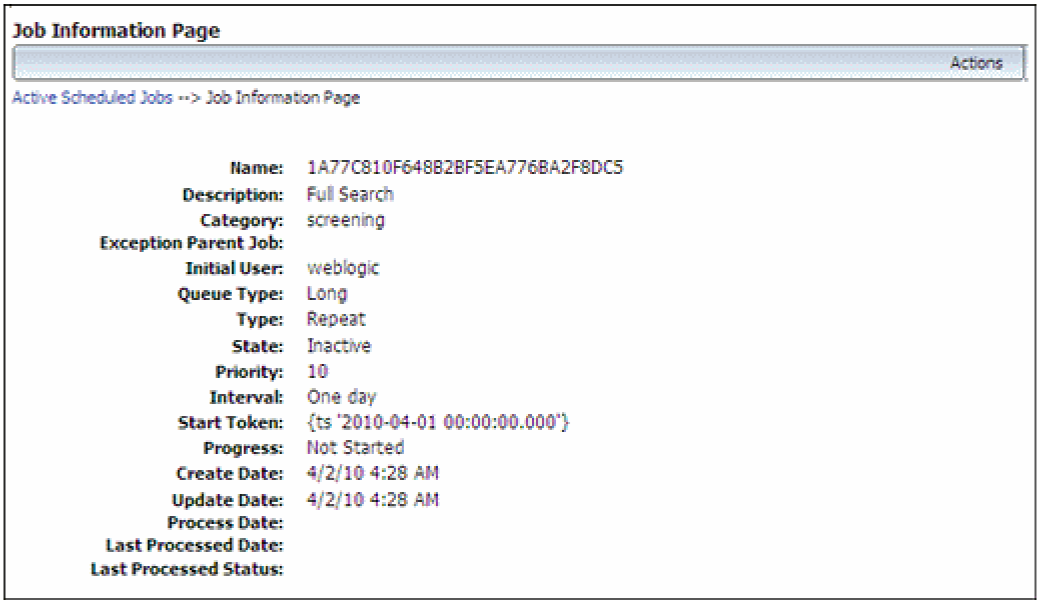


To access this page, click **View History** in the **Actions** menu for a recurring scheduled screening report.

Element	Description
Name	The name of the screening report as specified in the Scheduled Screening Reports Page. Click the link to display the screening report. The report is in the format specified by the Report Format setting on the Configure Retention Administration Page.
Process Date	The date and time the recurring screening report was generated.
Status	The status of the scheduled screening report: ■ **Succeeded**: The scheduled report generated successfully. ■ **Failed**: The scheduled report did not execute successfully. The log file contains more details on the error(s). ■ **Canceled**: The report aborted before it could be completed successfully.
Action menu	Displays a menu containing options relevant to the scheduled screening report: ■ **View Log**: Displays the content information page of the generated screening report. ■ **Remove**: Removes the disposition action from the list of scheduled actions.
Info icon	Displays the content information page of the automatically generated report file. Use the Web Location or Native File link to view the file.

A.8.3 Job Information Page/Edit Job Information Page

This page shows details about a scheduled recurring action. It can also be used to edit certain information about a scheduled job.



To access this page, click **View Report Info** from the **Actions** menu of a scheduled recurring action (for example, Scheduled Recurring Report or Scheduled Recurring Freeze) on the Scheduled Screening Reports Page. You can also access this page by clicking Info from the Action menu of a job on the Scheduled Jobs Listing Page.

The information displayed depends on the type of action in question. The screen depicted here is for a scheduled screening report.

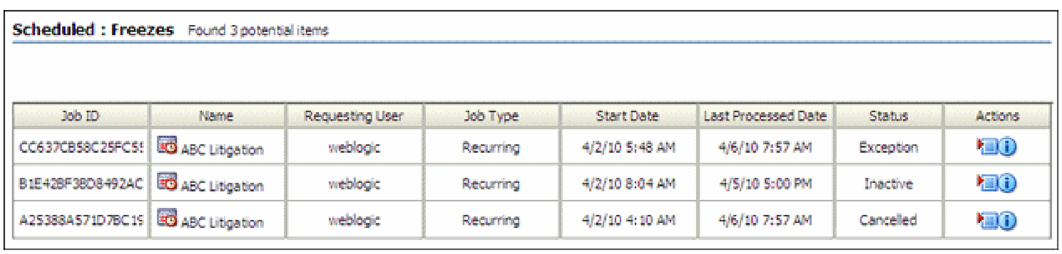
To access the editable version of this page, click **Edit** from the Action page menu while viewing the job information. You can also access an editable version by clicking **Edit** in the Action menu of a job on the Scheduled Jobs Listing Page. This screen is also used to schedule jobs for Oracle UCM and can be used to edit schedule job information for Oracle UCM. The following information can be edited when using this screen for Oracle URM.

Element	Description
Description	The description assigned to the job.
Category	The type of job (for example, screening or freeze).
Initial User	The user who initiated the scheduled freeze.
Queue Type	An indicator of job type. *Long* indicates the job is run in a daily timeframe. *Short* indicates an action is done in an hourly timeframe.
Type	*Once* indicates the job is run once. *Repeat* indicates an action done on a repeating schedule. *Immediate* indicates the job should be processed at once.
Start Token	The exact date and time the job will be initiated.

Element	Description
Status	The current status of the scheduled screening report: ■ **Processed**: The scheduled report generated successfully and is not scheduled to be repeated. ■ **Exception**: The scheduled report did not execute successfully. The log file contains more details on the error(s) that occurred. ■ **Active**: The scheduled report is being executed. ■ **Inactive**: The scheduled report is in the queue of tasks to be performed and will be generated when scheduled, usually at midnight. ■ **Canceled**: The scheduled report was aborted before it could be completed successfully.
Action menu (Job Edit screen only)	Displays a menu containing options relevant to the scheduled recurring freeze. The available options depend on the status of the scheduled freeze and may include: ■ **Edit**: Displays an editable version of the Job Information Page/Edit Job Information Page where criteria can be edited. ■ **Cancel**: Cancels the scheduling of the report. ■ **Delete**: Deletes the scheduled job.

A.8.4 Scheduled Freezes Page

This page shows all scheduled recurring freezes.



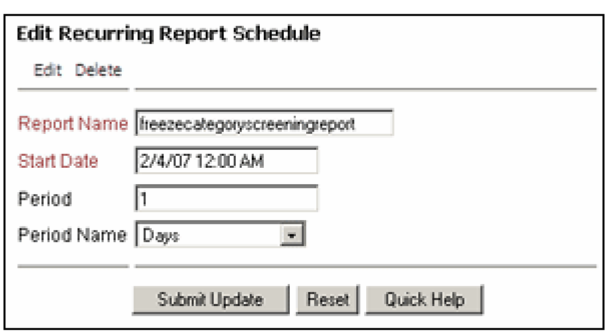
This page is displayed when a freeze is scheduled. It can also be accessed by clicking **Reports** then **Scheduled** then **Freezes** from the Top menu.

Element	Description
Job ID	The assigned identifier for the scheduled job.
Name	The name of the freeze used for the schedule.
Requesting User	The user who initiated the scheduled freeze.
Job Type	An indicator of job type. *One Time* indicates the job is run once. *Recurring* indicates an action is done on a repeating schedule. Note that when a job is processed, it is removed from the display.
Start Date	The date the job will be initiated. If the job is a *long* type, the system checks within one day of the start date to see if the job needs to be run. If it is a *short* type, the system checks if the needs to be run within the hour of the start date and time. If the job type is recurring, the job continues executing within a defined interval after the start date.

Element	Description
Last Processed Date	The date and time the recurring action was last generated.
Status	The current status of the scheduled screening report: ■ **Processed**: The scheduled report generated successfully and is not scheduled to be repeated. ■ **Exception**: The scheduled report did not execute successfully. The log file contains more details on the error(s) that occurred. ■ **Active**: The scheduled report is being executed. ■ **Inactive**: The scheduled report is in the queue of tasks to be performed and will be generated when scheduled, usually at midnight. ■ **Canceled**: The scheduled report was aborted before it could be completed successfully.
Action menu	Displays a menu containing options relevant to the scheduled recurring freeze. The available options depend on the status of the scheduled freeze and may include: ■ **View Log**: Displays the content information page of the generated report. ■ **Edit**: Displays an editable version of the Job Information Page/Edit Job Information Page where criteria can be edited. ■ **Unschedule**: Cancels the scheduling of the report. ■ **Run Freeze**: Creates the freeze. ■ **Reschedule**: Displays a screen where the scheduling properties can be modified. If a job has been canceled using the Unschedule option, using Reschedule changes the status of the job from Canceled to Inactive so it is scheduled again. ■ **Edit Criteria**: Displays the associated screening definition page (for categories, folders, or content items), where the criteria for the screening report can be modified. ■ **View History**: Displays the View History Page. ■ **Remove**: Removes the item from the list of scheduled actions.

A.8.5 Edit Recurring Report Schedule Page

This page is used to modify the scheduling properties of a recurring screening report.



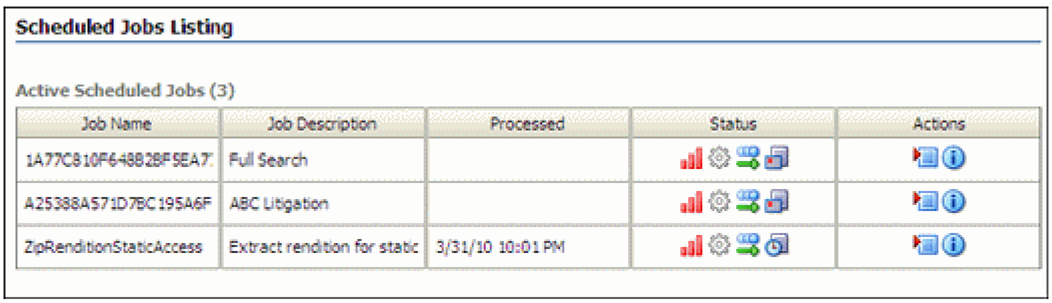
To access this page, click **Edit Schedule** from the **Action** menu of a scheduled recurring screening report in the Scheduled Screening Reports Page.

To modify a recurring screening report to become non-recurring (to run once), run the report manually then cancel it.

Element	Description
Report Name field	A new name for the scheduled screening report (if required).
Start Date field	The new date the first scheduled screening report should be generated according to the new schedule (if required). All subsequent reports will be generated at the end of each recurring period after this date.
Period and Period Name fields	The interval at which the recurring screening report should be created (for example, every 2 weeks).

A.8.6 Scheduled Jobs Listing Page

This page lists all scheduled recurring jobs.



To access this page, click **Active Scheduled Jobs** on a Job Information Page/Edit Job Information Page. This page can also be accessed by clicking **Administration** then **Scheduled Job Administration** from the Main menu. Click **Active Scheduled Jobs**.

The icons in the Status column are a summary of information about the item. To see the meaning of an icon, hover the mouse cursor over the icon.

Depending on the type of action and the status, the following information may appear:

- **Priority**: an indication of the priority. For example, High Priority.
- **Status**: the status of the item. For example, Inactive.
- **Occurrence**: whether the item repeats (recurring) or occurs once.
- **Queue**: an indicator of a short or long queue type for this action. A long queue indicates processing in a daily timeframe. A short queue indicates processing in an hourly timeframe.

A.9 Retention Assignment Interface Screens

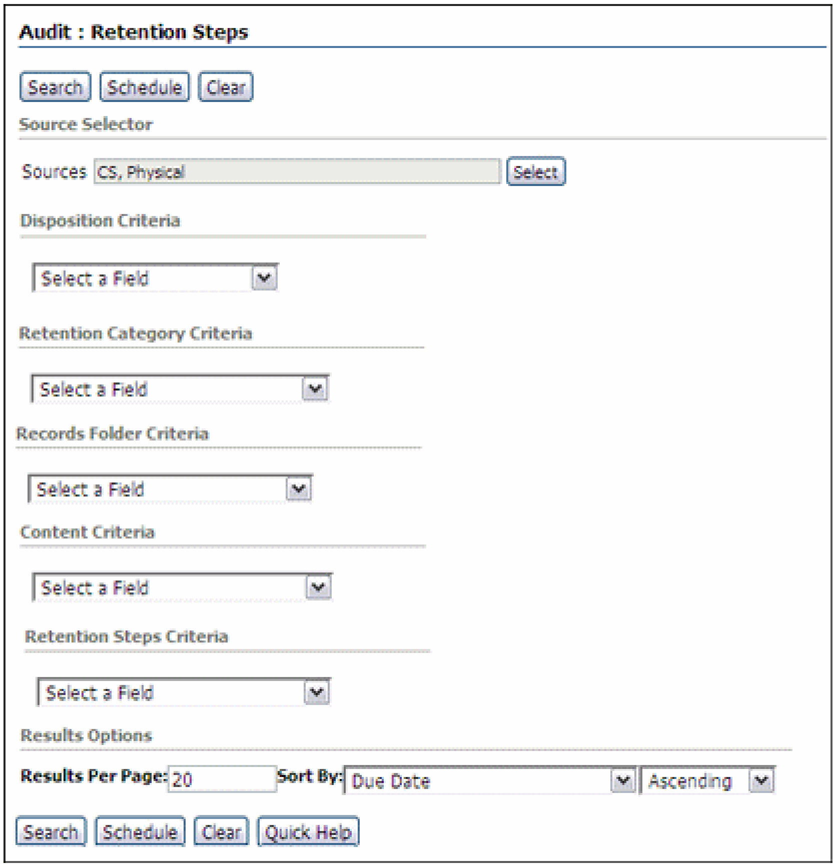
The following screens are used when processing retention assignments:

- "Retention Step Search Page" on page A-26
- "Retention Step Audit Result Page" on page A-26
- "Schedule Retention Step Audit Report Page" on page A-27
- "Failed Dispositions Page" on page A-28
- "Pending Dispositions Page" on page A-28

- "Pending Reviews Page" on page A-29
- "Disposition Information Page" on page A-29

A.9.1 Retention Step Search Page

This page is used to screen disposition rules for specific types of steps.

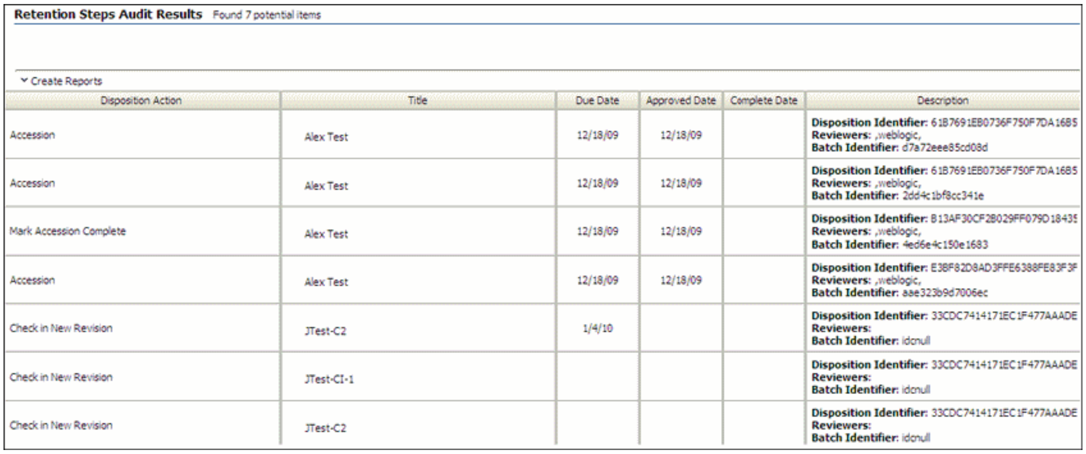


To access this page, click **Records** then **Audit** then **Retention Steps** from the Top menu.

The functionality on this screen is similar to the functionality on a standard search page. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about performing searches and scheduling searches.

A.9.2 Retention Step Audit Result Page

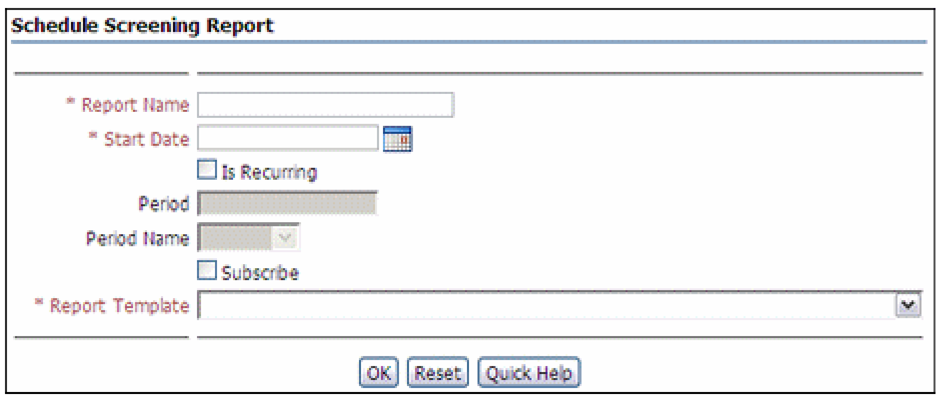
This page displays results from a screening for retention steps.



This page is displayed after clicking **Search** on the Retention Step Search Page.

A.9.3 Schedule Retention Step Audit Report Page

This page is used to schedule a Retention Step Audit Report.

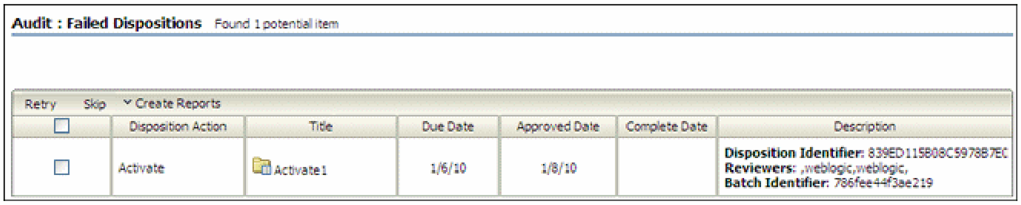


To access this page, click Schedule on the Retention Step Search Page.

Element	Description
Report Name field	Name for the scheduled screening report. Required.
Start Date field	The date the scheduled screening report will be generated. Required. If the screening report is recurring, the first screening report is generated for the first time on this date and subsequent reports at the end of each recurring period after this date. If the start date is in the past, the processing is done with the next scheduled run.
Is Recurring box	Indicator of recurrence. If checked, the scheduled screening report is generated periodically.
Period and Period Name fields	The interval at which the recurring screening report is created (for example, every 2 weeks).
Subscribe	After the report is created, it is checked in. Click Subscribe to subscribe to it and be notified when the report changes.
Report Template	Choose a template to use for this report.

A.9.4 Failed Dispositions Page

This page shows disposition actions which have not processed correctly.



This page is displayed after clicking **Records** then **Audit** then **Failed Dispositions** from the Top menu.

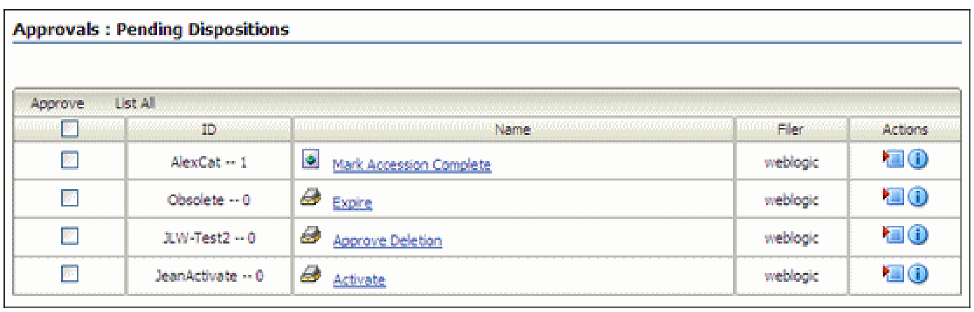
To restart the disposition, select the checkbox for the item and click **Retry** from the Table menu.

To mark the disposition as complete regardless of whether the action succeeded or not, click the checkbox for the item and click **Skip** from the Table menu. Use this option with caution because it may have unforeseen consequences when a disposition is skipped.

To create a report of failed dispositions, select the items to include in the report then click **Create Reports** from the Table menu.

A.9.5 Pending Dispositions Page

This page shows those actions needing approval. This example shows pending dispositions. A similar page is available for Pending Reviews.



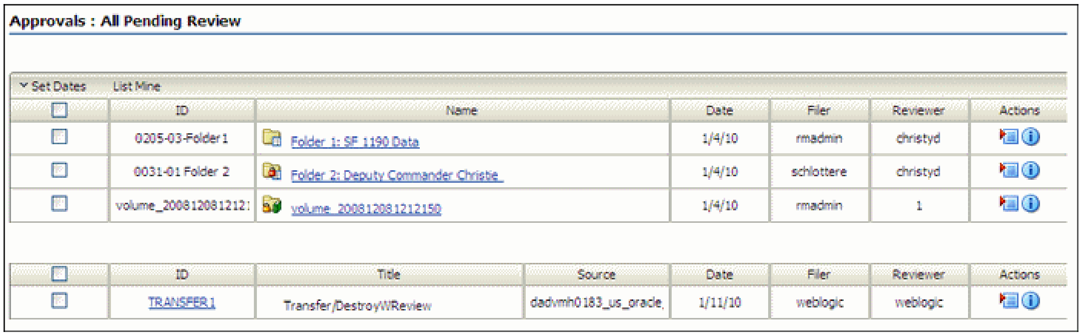
Permissions: The Admin.PerformActions right is required to use this page. This right is assigned by default to the Records Administrator role. In addition, the user must be designated as the notification recipient when performing actions for others.

To access this page, click **Records** then **Approvals** then the type of approval from the Top menu.

Element	Description
ID	The category affected by the disposition and the step involved. Note that processing begins with step 0.
Name	The disposition action.
Filer	The user who initiated the disposition.

A.9.6 Pending Reviews Page

This page shows all reviews that need to be performed.

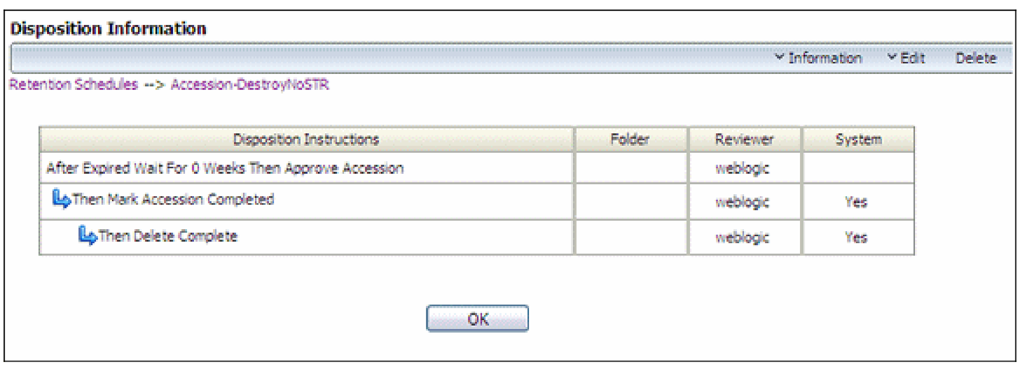


To access this page, click **Records** then **Approvals** from the Top menu. Click **Pending Reviews**.

Permissions: The Admin.PerformActions right is required to use this page. This right is assigned by default to the Records Administrator role. In addition, the user must be designated as the notification recipient when performing actions for others.

A.9.7 Disposition Information Page

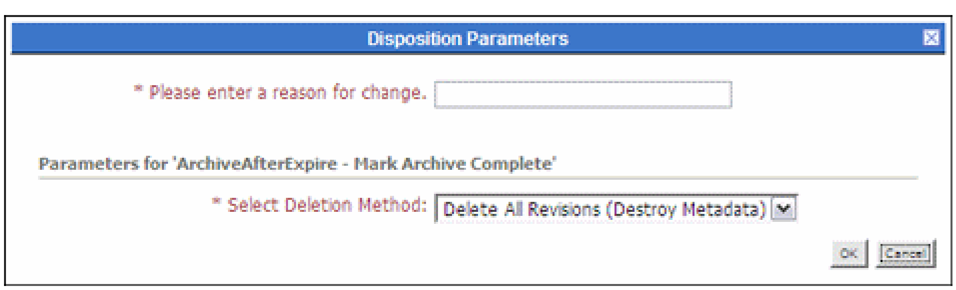
This page shows the actions included in a disposition.



To access this screen click a disposition name on the Pending Dispositions Page or click **Disposition Information** from the **Action** menu of a disposition on the Pending Dispositions Page.

A.9.8 Disposition Parameter Dialog

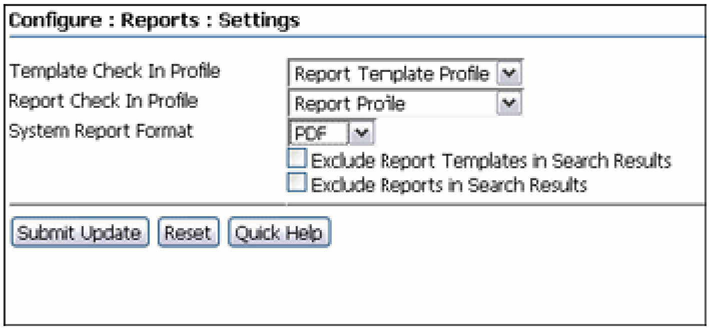
This dialog is displayed when a disposition action is marked as approved.



This dialog is displayed when an action is marked for completion on the Pending Dispositions Page. The bottom portion of this dialog is displayed if an action also involves a deletion method.

A.10 Configure Report Settings Page

Use this page to set up reports for retention items, chargebacks, and other functionality.



Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role.

To access this page, click **Records** then **Configure** from the Top menu. Click **Reports** then **Settings**.

The following options appear on this screen.

Element	Description
Template Check In Profile	Choose a profile to use for the template when it is checked in.
Report Check In Profile	Choose a profile to use when the report is checked in.
System Report Format	Choose the default format for reports.
Exclude Report Templates in Search Results	Check this box to exclude templates from search activities. This box is available for selection only if the **Enable Report Exclude Search Options** box is checked on the Configure Retention Settings Page.
Exclude Reports in Search Results	Check this box to exclude reports from search activities. This box is available for selection only if the Enable Report Exclude Search Options box is checked on the Configure Retention Settings Page.

A.11 Customization, Monitoring and Audit Pages

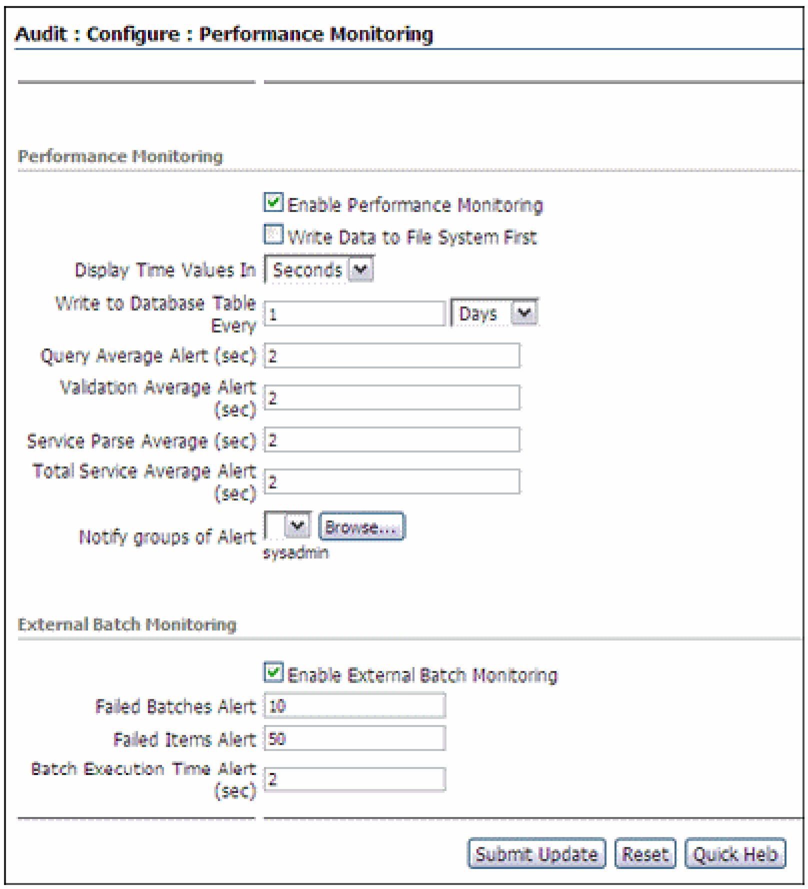
These pages are used to add custom scripts, perform performance monitoring, or run audit reports.

- "Configure Performance Monitoring Page" on page A-31
- "Performance Processing Results Page" on page A-32
- "Configure Custom Script Page" on page A-34

- "Create or Edit Custom Script Page" on page A-34
- Custom Script Information Page
- "Configure Audit Page" on page A-35
- "Audit Fields Page" on page A-36
- "Checked-in Audit Entries Page" on page A-37
- "Default Metadata for Checked-In Audit Entries Page" on page A-38
- "Search Audit Trail Page" on page A-39

A.11.1 Configure Performance Monitoring Page

Use this page to set up and use performance monitoring.



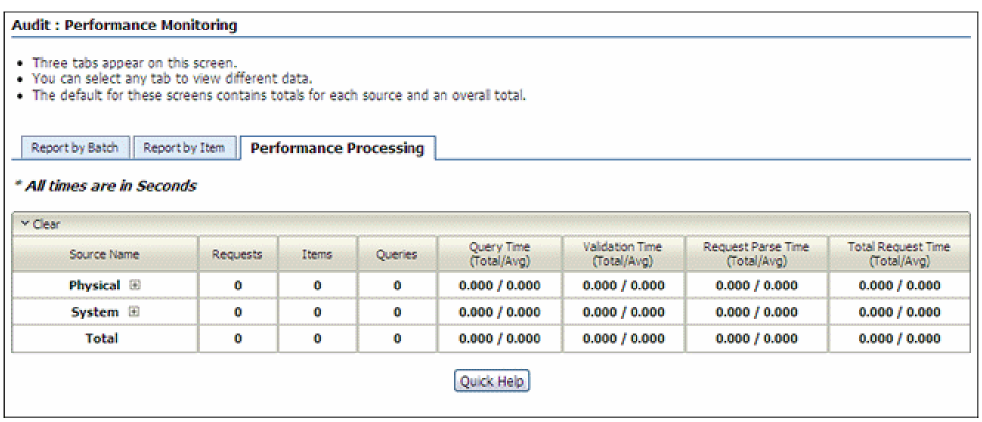
To access this page, click **Records** then **Audit** from the Top menu. Click **Configure** then **Performance Monitoring** from the Top menu.

Element	Description
Enable Performance Monitoring box	Click this box to enable performance monitoring.
Write data to File System First	Enables storage of data before creation of reports. This can speed the process for larger batches of data. If unchecked, the data is not saved temporarily before it is compiled into a log file.

Element	Description
Display Time Values In	Determines the format of time value reporting. Options include seconds, minutes, or hours.
Write to Database Table Every	Determines the length of time between writing the perfomance information to the database.
Query Average Alert (sec)	Determines if queries will be tracked and the average time deemed reasonable for a query. Alerts will be issued if the amount exceeds this number.
Validation Average Alert (sec)	Determines if validations will be tracked and the average time deemed reasonable for a validation. Alerts will be issued if the amount exceeds this number.
Service Parse Average (sec)	Determines if services will be tracked and the average time deemed reasonable for a service parse action. Alerts will be issued if the amount exceeds this number.
Total Service Average Alert (sec)	Determines if services will be tracked and the average time deemed reasonable for a service action. Alerts will be issued if the amount exceeds this number.
Notify Groups of Alert	Used to choose a recipient to receive alerts. This list is populated if users and aliases have been added to a My Favorites list. If none are added, click **Browse** to open a dialog where a user or alias name can be added.
Enable External Batch Monitoring	Begins monitoring of external batch processes.
Failed Batches Alert	Indicates a minimum number of batches which can fail before an alert is sounded.
Failed Items Alert	Indicates a minimum number of items which can fail in processing before an alert is sounded.
Elapsed Time Alert (sec)	Indicates the amount of time that can elapse before an alert is sounded.

A.11.2 Performance Processing Results Page

Use this page to view the results of performance monitoring.



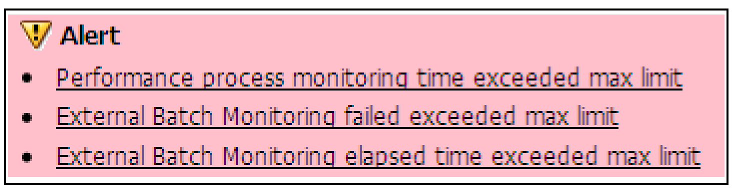
To access this page, click **Records** then **Audit** then **External Performance Monitoring** from the Top menu. This option only appears if performance monitoring has been enabled.

Select any tab to view different data. The default for these screens contains totals for each source and an overall total. If a column is hidden, rest the cursor on the column and the column heading appears in a tooltip.

- **Performance Processing**: this page contains a summary of requests processed, total items processed, total number of queries run, total time to run queries, total time to validate data, total service request parse time and total service request time per each external source. Averages for these are also included.
- **Report by Batch**: this page contains a summary of batches/items pending, processed, and failed with a total for each source. If an item has failed, a batch file is created that can be re-run. Click on any value in a column to display a page showing details about that item.
- **Report by Item**: this page contains the details per batch for a particular source, status or batch type as well as totals. The detail page for the item contains the batch type, start time, completed time, elapsed time, and number of items processed for each batch.

A.11.3 Performance Monitoring Alert Message

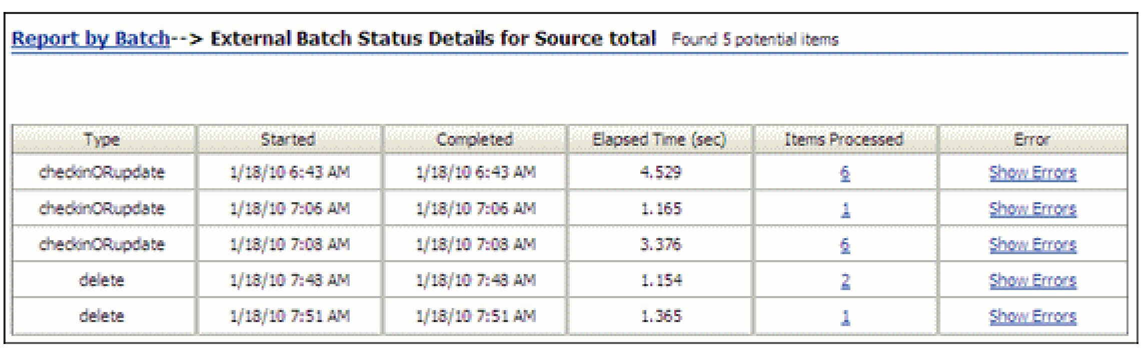
This message appears is performance results exceed the limits set when performance monitoring was configured.



This alert appears automatically and cannot be accessed unless performance limits are reached or exceeded.

A.11.4 Monitoring Details Page

This screen displays detailed information about performance results.



Report by Batch--> External Batch Status Details for Source total Found 5 potential items

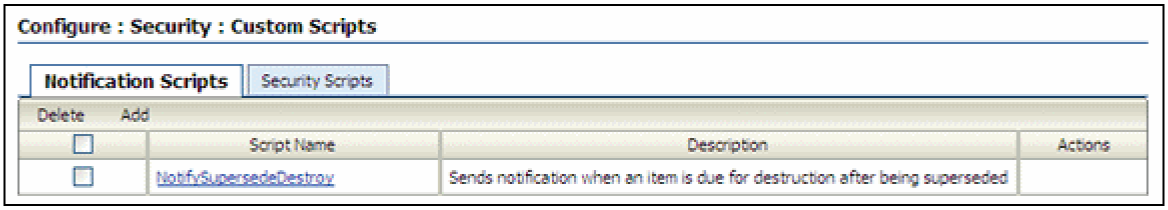
Type	Started	Completed	Elapsed Time (sec)	Items Processed	Error
checkinORupdate	1/18/10 6:43 AM	1/18/10 6:43 AM	4.529	6	Show Errors
checkinORupdate	1/18/10 7:06 AM	1/18/10 7:06 AM	1.165	1	Show Errors
checkinORupdate	1/18/10 7:08 AM	1/18/10 7:08 AM	3.376	6	Show Errors
delete	1/18/10 7:48 AM	1/18/10 7:48 AM	1.154	2	Show Errors
delete	1/18/10 7:51 AM	1/18/10 7:51 AM	1.365	1	Show Errors

A screen of this type is displayed when a link is clicked on the Performance Monitoring Alert Message or (for example) when a batch detail is clicked on the Report by Batch tab on the Performance Processing Results Page.

The specific screen that is displayed depends on the link that is clicked. The screen shown here is one sample of such a screen.

A.11.5 Configure Custom Script Page

Use this page to configure a security script or a notification script.

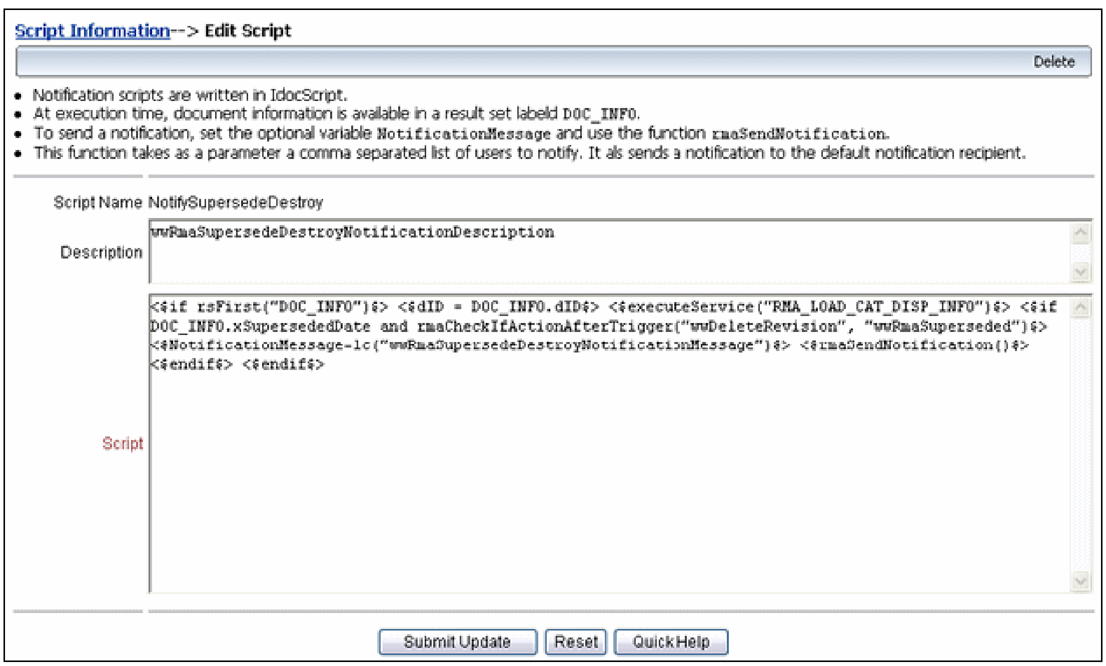


To access this page, click **Records** then **Configure** from the Top menu. Click **Security** then **Custom Scripts**. Use this page to configure notification or security scripts. The two types of security creation pages are similar. Only the notification script screen is depicted in this documentation.

To add a new script, select the script type by clicking on the appropriate tab. Then click **Add**. To edit an existing script, click the script name or select Edit from the script's Action menu.

A.11.6 Create or Edit Custom Script Page

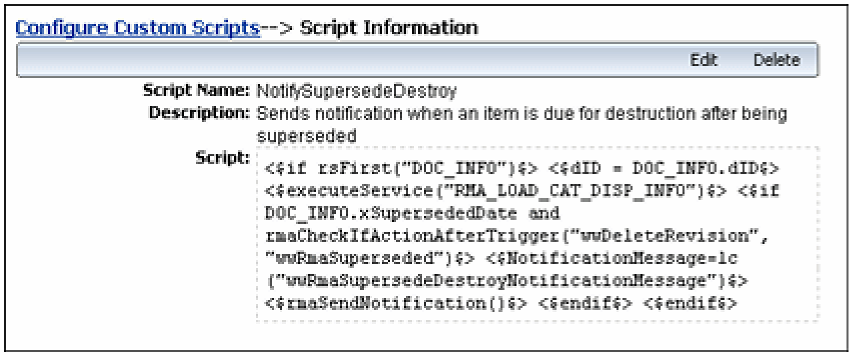
Use this page to enter the Idoc Script needed for a notification or security script or to edit the text of an existing script.



Access this page by clicking **Add** on the Configure Custom Script Page. To access the Edit version of this page, click **Edit** on the Action menu of a specific script on that page or use the **Delete** option on the Edit Page to remove the script.

A.11.7 Custom Script Information Page

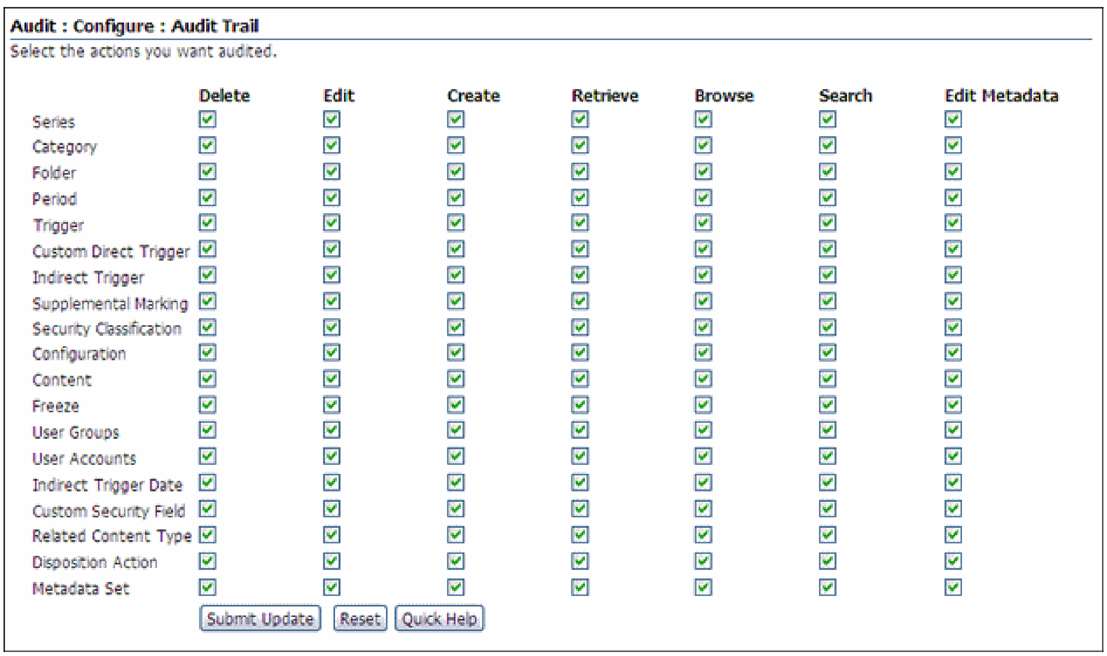
The custom script information page displays the content of a custom script.



To access this page, click the script name on the Configure Custom Script Page.

A.11.8 Configure Audit Page

This page is used to determine what will appear on the Audit Page. By default, all options are selected when the Configure Audit page is first accessed.



Permissions: The Admin.Audit right is required to use this screen. This right is assigned by default to the Records Administrator role.

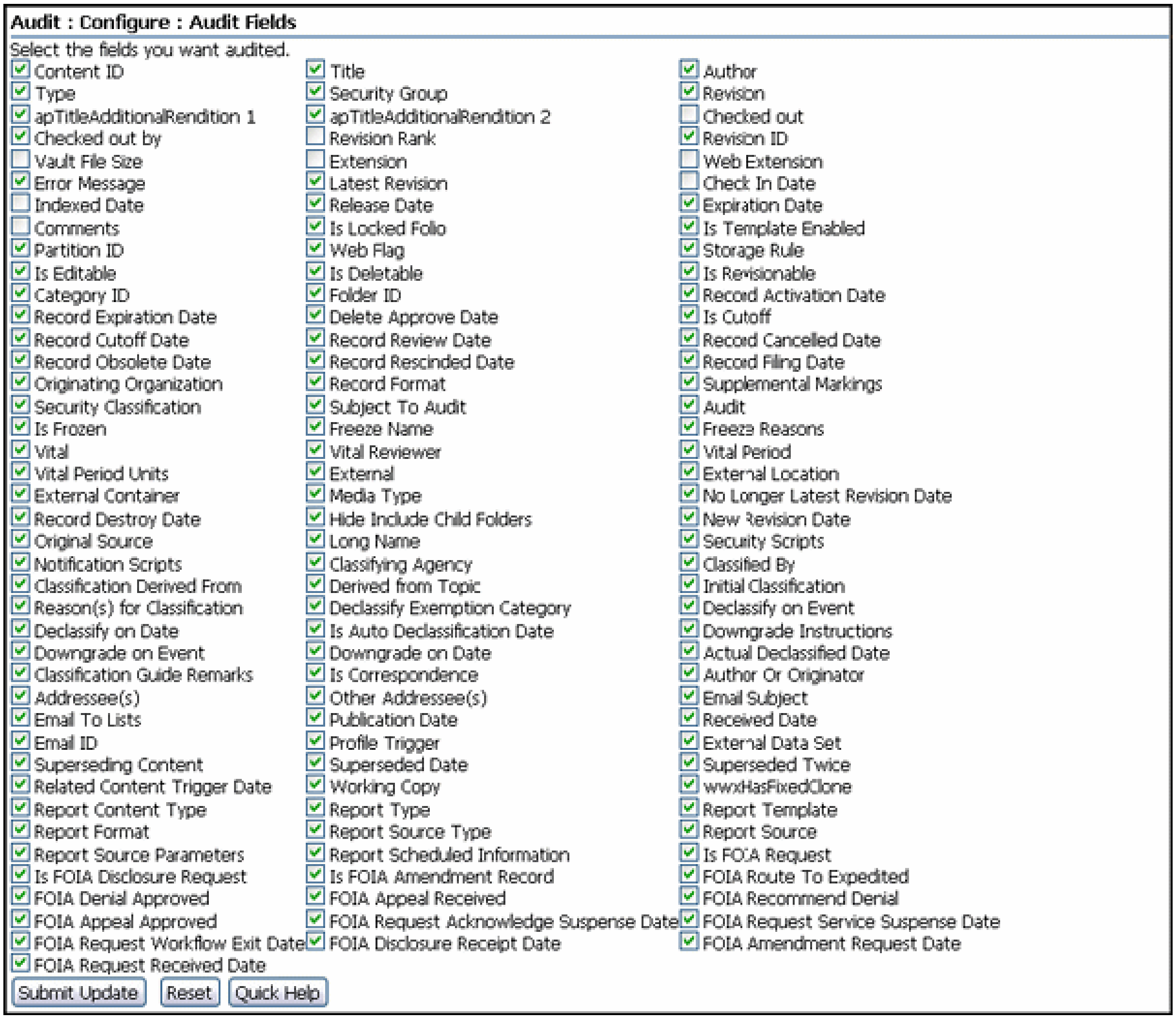
To access this page, click **Records** then **Audit** from the Top menu. Click **Configure** then **Audit Trails**.

Note: The Edit Metadata column is only visible if the Log Metadata Changes option is enabled on the Configure Retention Administration Page.

Audited Objects and Elements	Actions Recorded
Series Category Folder Period Trigger Custom Direct Trigger Indirect Trigger Supplemental Marking Security Classification Configuration Content Freeze User Groups User Accounts Indirect Trigger Data Custom Security Field Related Content Type Disposition Action Metadata Set	The actions to be recorded in the current audit trail: ■ **Delete**: Records all deletion actions. ■ **Edit**: Records all item editing actions. ■ **Create**: Records all actions during item creation. ■ **Retrieve**: Records all items retrieved. ■ **Browse**: Records all browsing actions within the retention schedule ■ **Search**: Records all searching actions for items. Screening is also captured by the Search action. ■ **Edit Metadata**: Records all metadata changes for items, categories, folders, and series. The changed status is recorded and also what the change entails (old and new field values). This column is only visible if the Log Metadata Changes option is enabled on the Configure Retention Administration Page. The User Accounts column represents users and is not to be confused with the accounts-based security model within Oracle UCM. The Configure Audit User Accounts option tracks users and not document accounts. The User Groups options tracks users assigned to an alias group.

A.11.9 Audit Fields Page

Use this page to specify which metadata fields should be included in the audit trail.

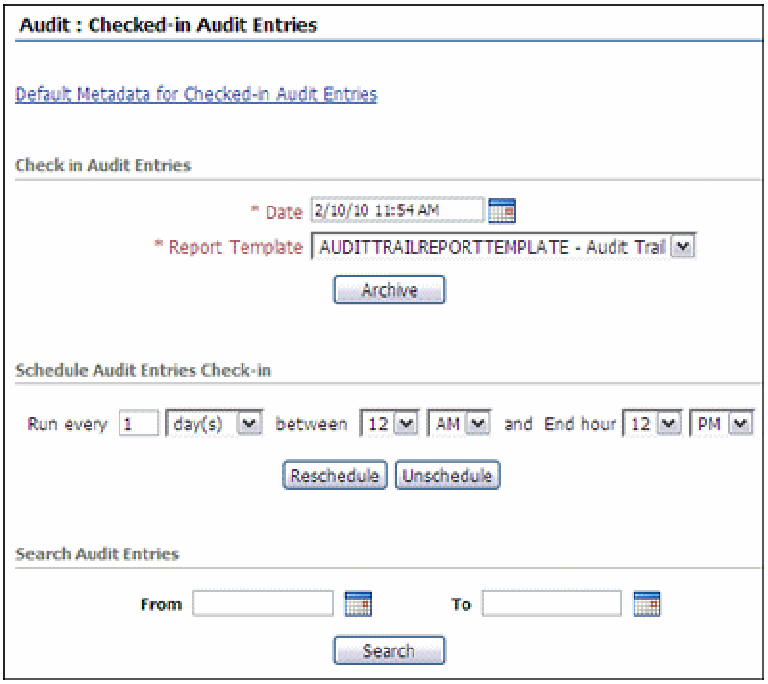


Permissions: The Admin.SelectMeta and Admin.Audit rights are required to use this page. Audit.SelectMeta is assigned to the Records Administrator role by default.

To access this page, click **Records** then **Audit** from the Top menu. Click **Configure** then **Audit Fields**. To enable an option, select its checkbox then click **Submit Update**.

A.11.10 Checked-in Audit Entries Page

Use this page to cut off and check in the audit trail. First set the default metadata for the audit trail when archiving and checking it into the repository. In addition, archived audit trails can be searched from this page.



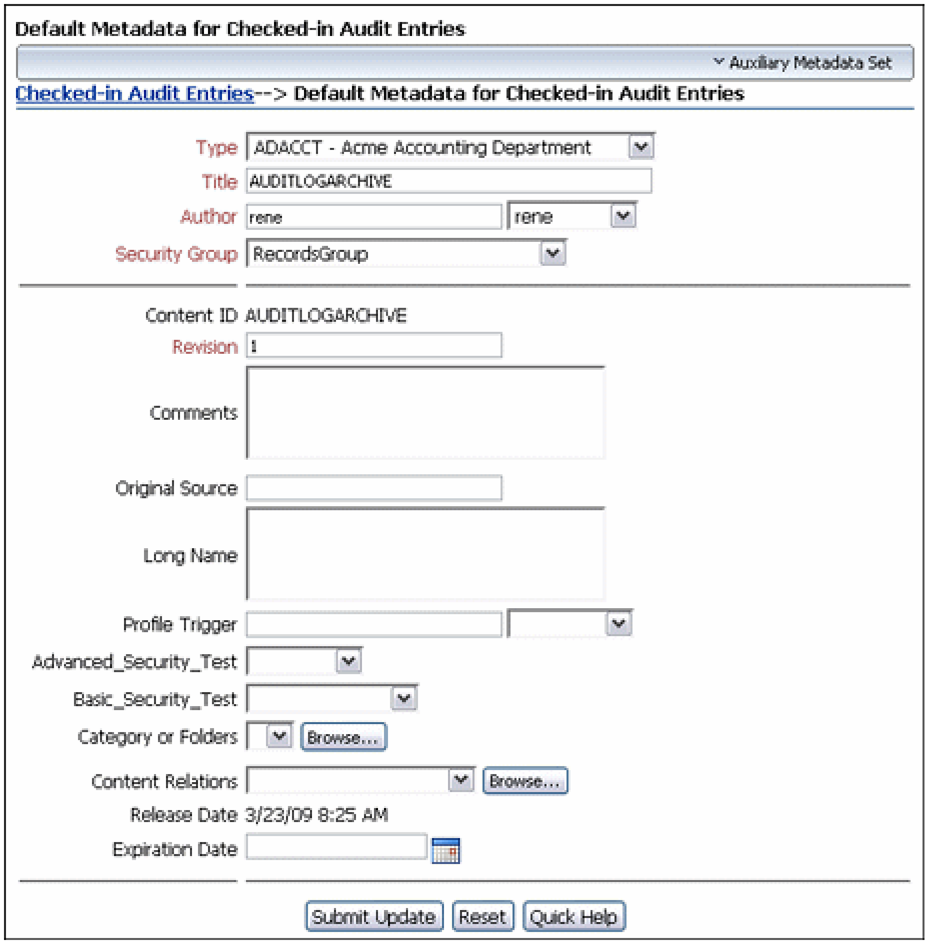
Permissions: The Admin.Audit and the Admin.RecordsManager right is required to use this page.

To access this page, click **Records** then **Audit** then **Checked-In Audit Entries** from the Top menu.

Search Audit Trail Section	Description
Date fields	The date on which to check in the audit log.
Template	The template to use for the checked-in audit log.
Schedule information	The frequency to schedule a report to be run, if needed. Select the frequency by selecting a range of days from the pulldown list. Select the itime parameters for the report to be run. To change a currently scheduled report, click the **Reschedule** button. To remove a report from the schedule, click **Unschedule**.
Search information	Choose a beginning date and an ending date for a search of the audit trail.

A.11.11 Default Metadata for Checked-In Audit Entries Page

Use this page to set the default metadata for checking in archived audit trails.



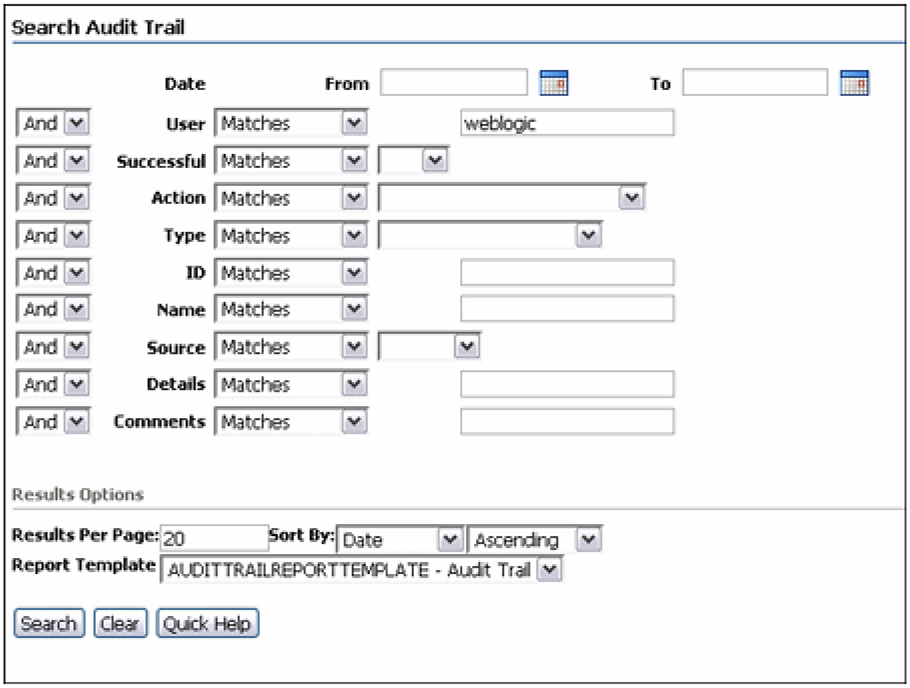
Permissions: The Admin.Audit right is required to use this page. This right is assigned by default to the Records Administrator role.

To access this page, click the **Default Metadata for Checked In Audit Entries** link on the Checked-in Audit Entries Page.The fields on this page vary according to what is installed at individual sites.

Set the default metadata for audits before archiving audit trails. After the default metadata are set, check in with the same metadata or edit the metadata before check-in. Setting the default metadata saves time when checking in an archive with the same metadata. Defining default metadata enables a user to create a "template" for checking in audit logs with similar metadata. The metadata for the audit logs can be edited at any time.

A.11.12 Search Audit Trail Page

Use this page to narrow down a search within an audit trail.



Permissions: The Admin.Audit right is required to use this page. This right is assigned by default to the Records Administrator role.

To access this page, click **Records** then **Audit** then **Search Audit Trail** from the Top menu.

Search Audit Trail Section	Description
Date fields	The date or date range during which to search the audit trail. ■ **From**: Finds actions recorded on or after the From date. ■ **To**: Finds actions recorded before but not on the To date. Click the icon to the right of each field to choose a date from a calendar.
User field	The user name to search for in the audit trail. Any actions by the user name that was entered are retrieved in the search audit report. **Default: current user**.
Successful field	A successful or unsuccessful action by which to search within the current audit trail. Available options are **Yes** (the attempted action was successful) or **No** (the attempted action was unsuccessful).
Action list	The enabled action by which to search within the current audit trail. These actions are enabled on the Configure Audit Page.
Type list	The type by which to search the audit trail. The types displayed are those enabled in the Configure Audit Page.
ID field	An identifier for a series, retention category, record folder, or content item to track. You can also enter the identifier of a custom period, custom trigger, supplemental marking, or custom security field.
Name field	The name of a series, retention category, record folder, or content item to search for in the audit trail. You can also enter the name of a custom period, custom trigger, supplemental marking, or custom security field.

Search Audit Trail Section	Description
Details field	Keywords that contain details to search for in the audit trail. Details tracked include changes to the software configuration, the document ID, the number of results found when searching a folder, and so on.
Comments field	A text string used for searching.

The following table discusses sorting options for the audit trail.

Results Options Section	Description
Sort By field list	The sorting method (such as *by Date* or *by ID*).
Sort By order list	The sort order of the search audit results. ▪ **Descending** (**default**): Sorts alphabetical results from Z-A, numeric results from 9-0 and date results from newest to oldest. ▪ **Ascending**: Sorts alphabetical results from A-Z, numeric results from 0-9 and date results from oldest to newest order.
Search button	The audit trail items matching the search criteria. The search audit report is generated in the format specified by the Report Format setting on the Configure Retention Administration Page. If no search criteria is entered, the entire search audit trail is displayed. To return to the Search Audit Trail page, click the browser's Back button, or click a link to which to navigate in the menu area.

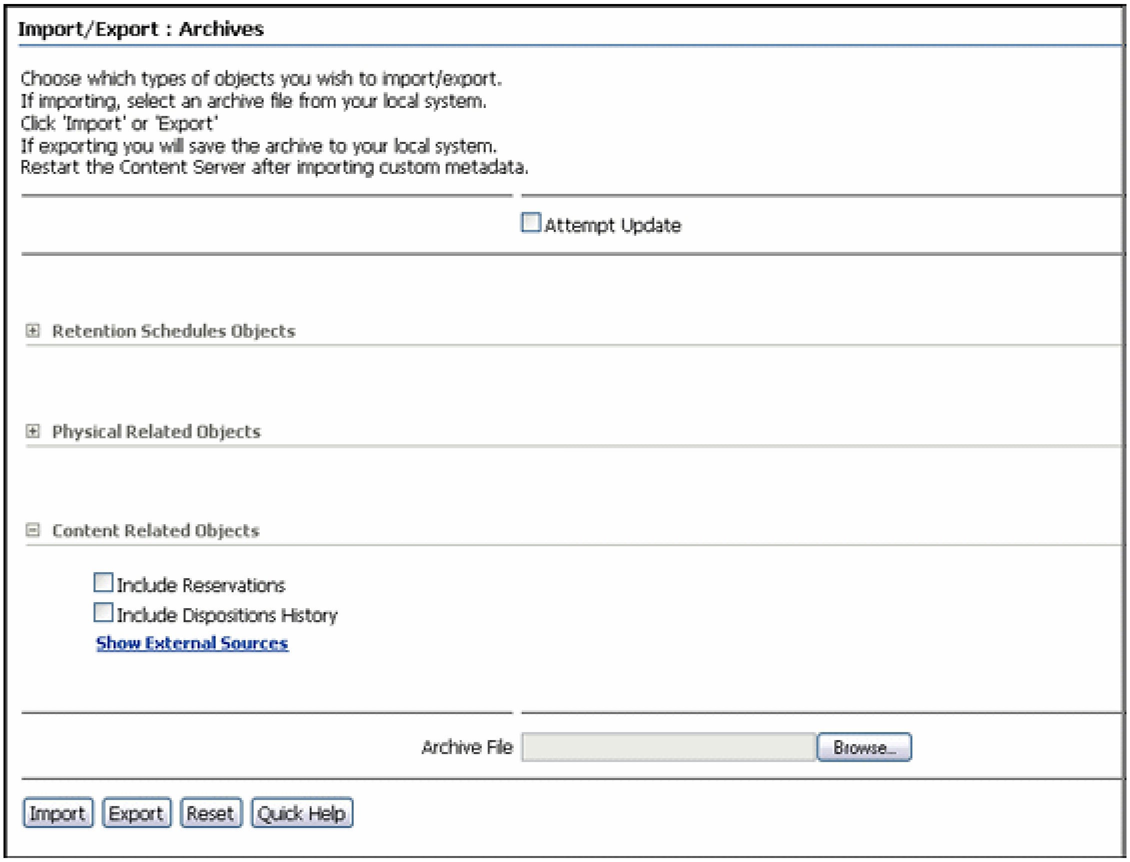
A.12 Import/Export Interface Screens

The following screen is used when managing the import/export process:

- "Import/Export Archive Page" on page A-41
- "Import with Schema Page" on page A-46
- "Export with Schema Page" on page A-47

A.12.1 Import/Export Archive Page

Use this page to import or export an archive.



Options on this page are hidden until the plus sign (+) next to the section heading is clicked.

To access this page, click **Records** then **Import/Export** then **Archives** from the Top menu.

> **Note:** When exporting auxiliary metadata, first include additional tables in the Table list in the Configuration Manager applet. See the detailed task documentation in the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about this procedure.

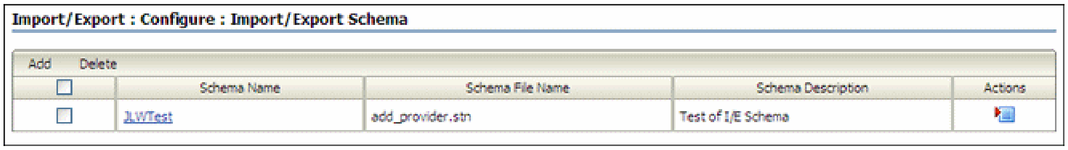
Element	Description
Export Date field	Exports only items that changed since a specific date. Enter the start date or select one using the calendar next to the field. This field is only displayed if the Show Export Date box on the Configure Retention Settings Page has been selected.

Element	Description
Retention Schedule Objects boxes	Objects to include or exclude in the archive. ■ Include Supplemental Markings ■ Include Classified Markings ■ Include Custom Categories Metadata ■ Include Custom Folders Metadata ■ Include Simple Custom Security ■ Include Advanced Custom Security ■ Include Custom Supplemental Markings ■ Include Periods ■ Include Triggers ■ Include Retention Schedule ■ Include Disposition Actions ■ Include Freezes ■ Include Recurring Scheduled Tasks ■ Include Classification Guides ■ Include Classification Topics
Physical Related Objects boxes	Objects to include or exclude in the archive. ■ Include Location Types ■ Include Storage ■ Include Custom PCM Metadata ■ Include Charge Types ■ Include Payment Methods ■ Include Customers ■ Include Charge Invoices ■ Include Charge Transactions
Content Related Objects boxes	Objects to include or exclude in the archive. ■ Include Reservations ■ Include Dispositions History If **Show External Sources** is clicked, any external source systems are displayed. Click the appropriate checkboxes to include metadata from the selected source or to include the disposition history from the selected source.
Attempt Update	Check to update information during the import.
Archive File	A name for the archive file. Click the **Browse** button to search for previously created files.
Import or Export button	Imports or exports the archive file to a specified location and name.

If an add-on is installed, there may be more items available for export than the ones shown in the above screenshot (for example, items related to external sources).

A.12.2 Configure Import/Export Schema Page

This page is used to choose a schema definition for use or to imitate the addition of a new schema.

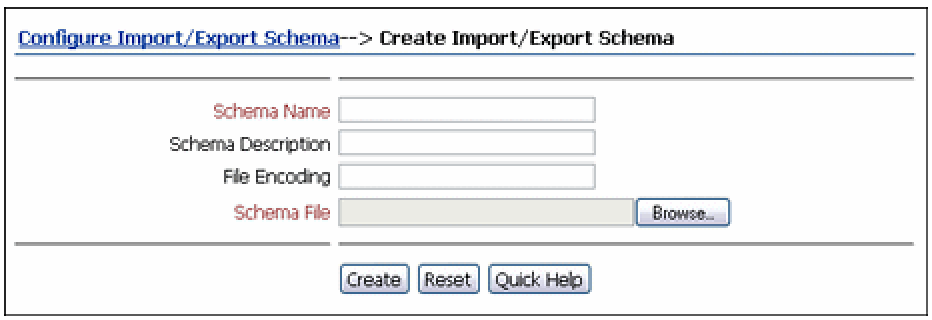


To access this page, click **Records** then **Import/Export** from the Top menu. Click **Configure** then **Import/Export Schema**.

Element	Description
Schema Name	The name of the schema to use.
Schema File Name	The archive file name.
Schema Description	The description given for the schema.

A.12.3 Create Import/Export Schema Page

Use this page to add a new schema for importing or exporting.

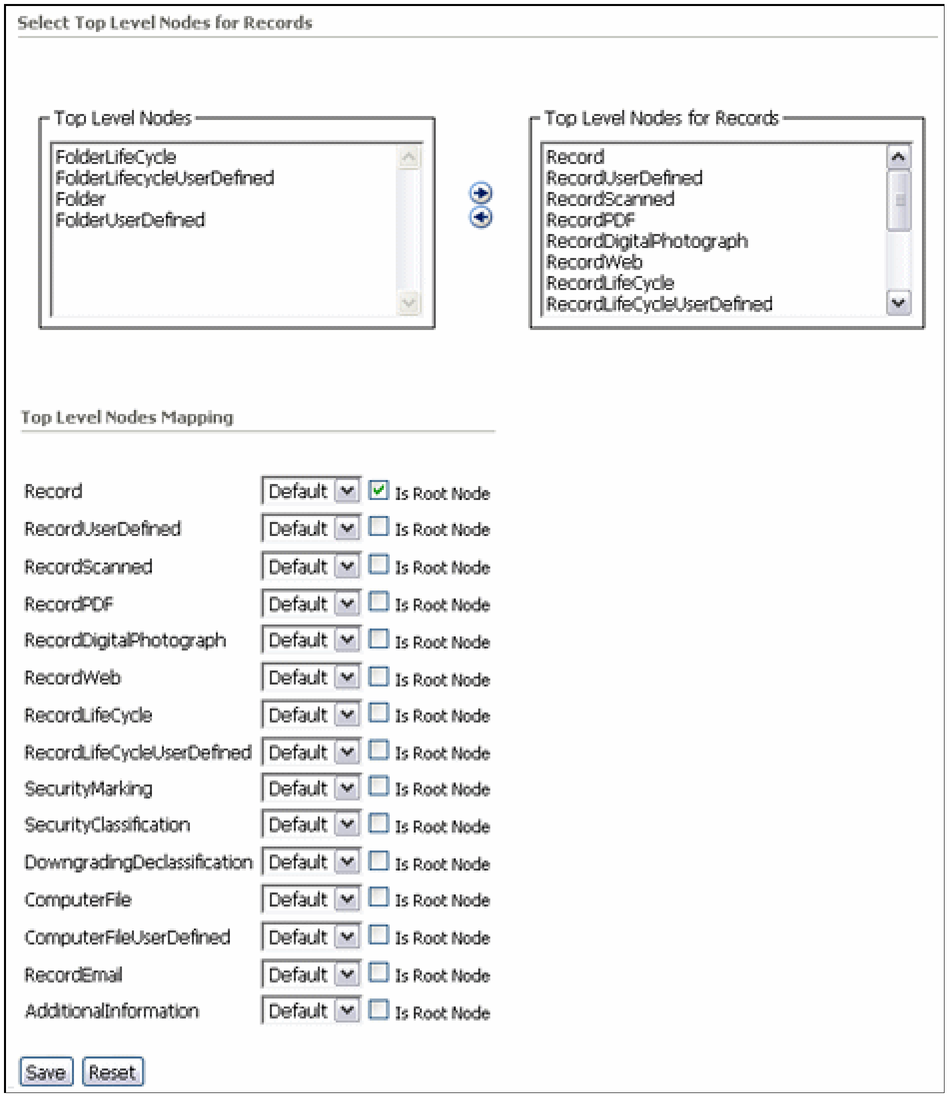


To access this page, click **Add** on the Configure Import/Export Schema Page.

Element	Description
Schema Name	The name of the schema to use.
Schema Description	The description given for the schema.
File Encoding	The encoding type used for the schema.
Schema File	The file to be used for uploading.

A.12.4 Configure Top Level Schema Nodes Page

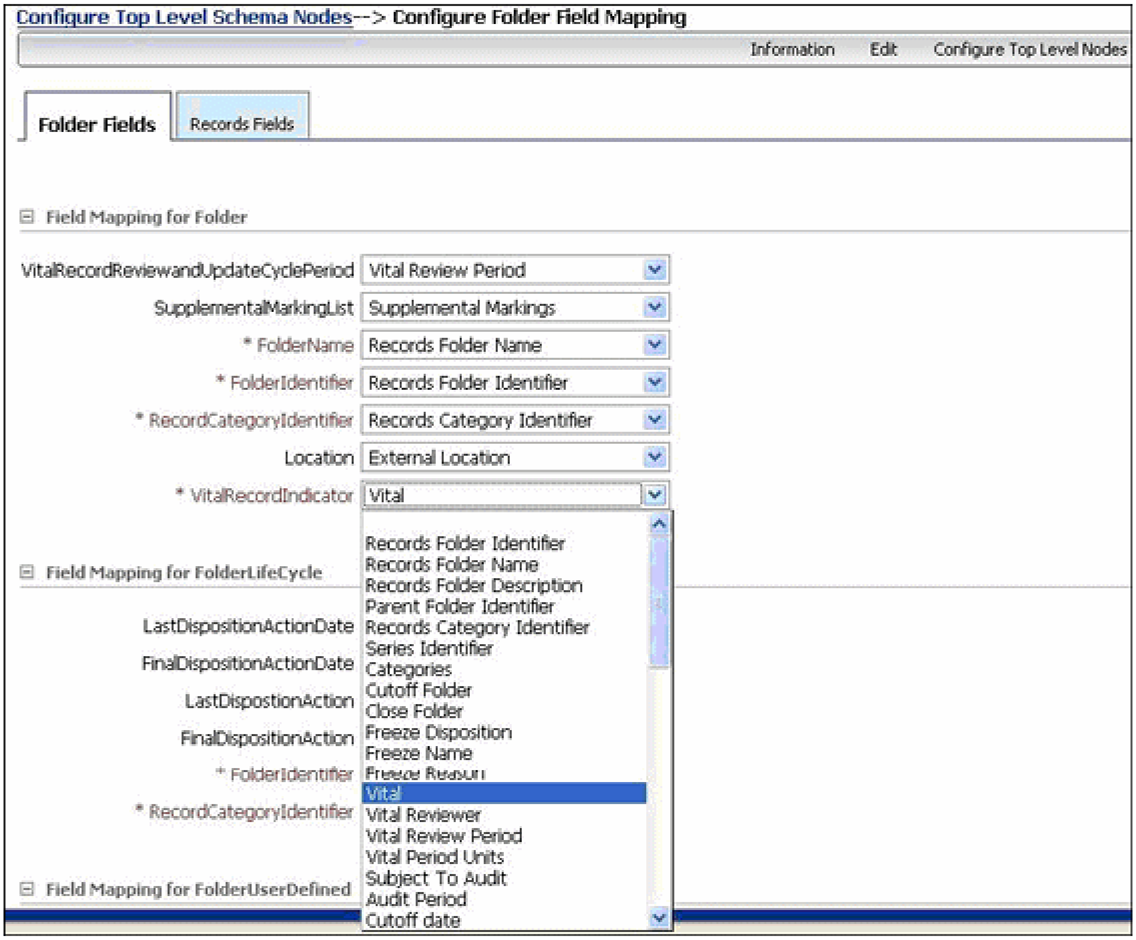
This page is used to specify nodes for inclusion in the export.



To access this page, click **Configure Top Level Nodes** in the Action list of an item on the Configure Import/Export Schema Page.

A.12.5 Configure Mappings Page

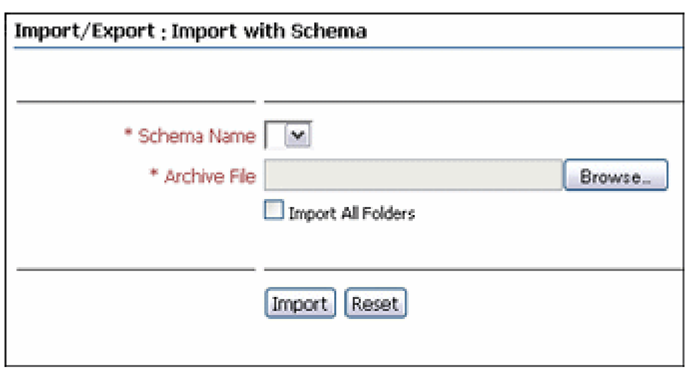
This page is used to map fields for import and export.



To access this page, click **Map Fields** on the Page menu on the Configure Top Level Schema Nodes Page.

A.12.6 Import with Schema Page

This page is used to specify a schema archive for importing.



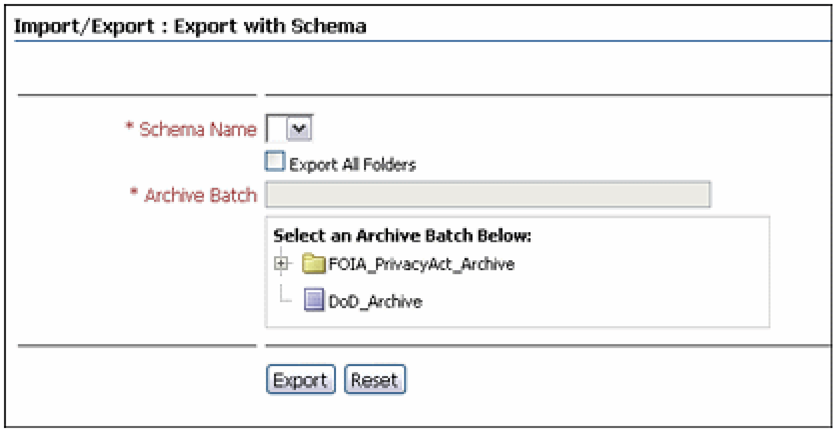
To access this page, click **Records** then **Import/Export** then **Import with Schema** from the Top menu.

Element	Description
Schema Name	The name of the schema to import.

Element	Description
Archive File	The archive file to be imported.

A.12.7 Export with Schema Page

This page is used to specify a schema archive for exporting.



To access this page, click **Records** then **Import/Export** then **Export with Schema** from the Top menu.

Element	Description
Schema Name	The name of the schema to export.
Archive Batch	The archive batch file to be exported.

A.13 FOIA and PA Interface Screens

These pages are used to set up the components needed to process requests for information under the Freedom of Information Act (FOIA) and Privacy Act (PA). This section is divided into two subsections:

- "FOIA/PA Processing Screens" on page A-47: these screens are used during the workflow to process a request.
- "FOIA/PA Data Screens" on page A-56: these screens depict forms used to provide supporting documentation for the requests.

This section does not include screen depictions of the workflow used to set up the FOIA and PA process. See the *Oracle Fusion Middleware Application Administrator's Guide for Content Server* for details about workflows.

A.13.1 FOIA/PA Processing Screens

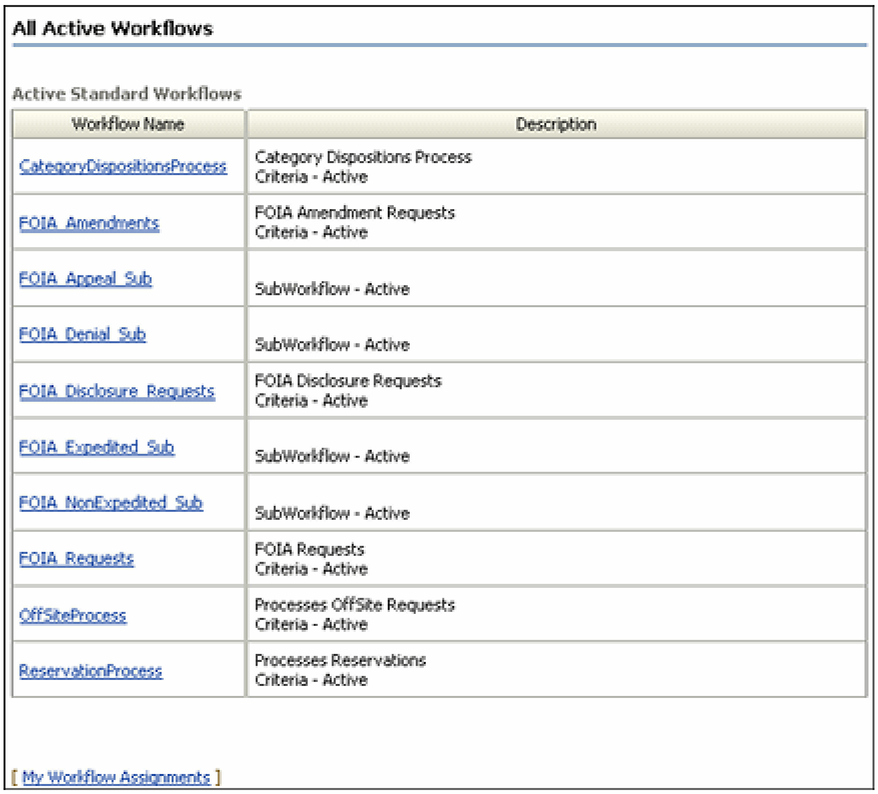
The following screens are used to process FOIA requests in workflows. The following screens are included:

- "Active Workflows Screen" on page A-48
- "Assignments in Queue Screen" on page A-48
- "Amendment Record Form" on page A-49
- "Disclosure Request Form" on page A-50

- "Access Request Form" on page A-50
- "Request Fee Table" on page A-52
- "Workflow Content Page" on page A-53
- "Workflow Review Page" on page A-53
- "Denial Record Form" on page A-54
- "Appeal Request Form" on page A-55
- "Final Result Dialog" on page A-56

A.13.1.1 Active Workflows Screen

This screen shows all workflows that are activated. Not all workflows shown here may be in active use.

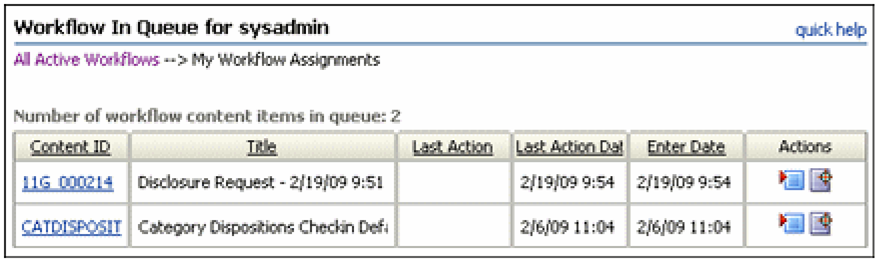


To access this screen, click **Content Management** then **Active Workflows**.

Element	Description
Workflow Name	Activated workflows and sub workflows. This does not imply content is being processed in the workflow, only that the workflow is active and ready to process information.
Description	A description of the workflow, indicating if it is a primary workflow or a sub-workflow.
My Workflow Assignments link	A link to the "Assignments in Queue Screen", listing all current workflow assignments for the logged-in user.

A.13.1.2 Assignments in Queue Screen

This screen displays all workflow assignments for the logged-in user.

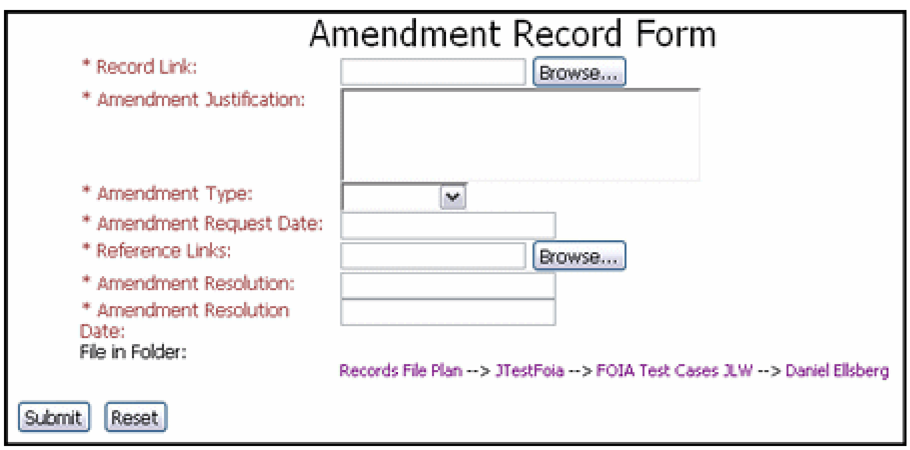


To access this screen, click **Content Management** then **Active Workflows**. Click **My Workflow Assignments**.

Element	Description
Content ID	The content ID of the item in the queue that is assigned to this user for processing.
Title	Title of the item in the queue.
Last Action	The last action for the content item, usually the name of a workflow step.
Last Action Date	The date and time when the last action was taken.
Enter Date	The date the item entered the current workflow step.
Actions	The Action menu containing actions that can be taken for the item and the Workflow Review icon, which displays the "Workflow Review Page".

A.13.1.3 Amendment Record Form

Use this form to initiate the workflow process for a request for amendment to a record.



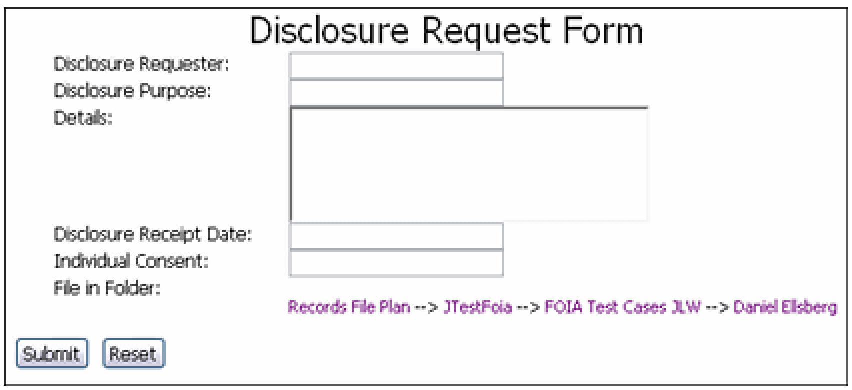
To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Amendment Record Form**.

Element	Description
Record Link	Click the Browse button to search for the record to be amended.
Amendment Justification	A text description of the justification given for the amendment.

Element	Description
Amendment Type	Select the type of amendment: ■ Deletion: a request for deletion of the record(s). ■ Correction: a request for correction of information. ■ Addition: A request for addition of information.
Amendment Request Date	The date the request was received.
Reference Links	Links to record(s) supplied by the requestor as documentary evidence. Click **Browse** to open a search page to search for the records.
Amendment Resolution	A brief statement of how the amendment request was resolved.
Amendment Resolution Date	The date the request was resolved.

A.13.1.4 Disclosure Request Form

Use this form to initiate a workflow for a disclosure request. Note that this is a Disclosure *Request* Form, not a Disclosure Record Form.

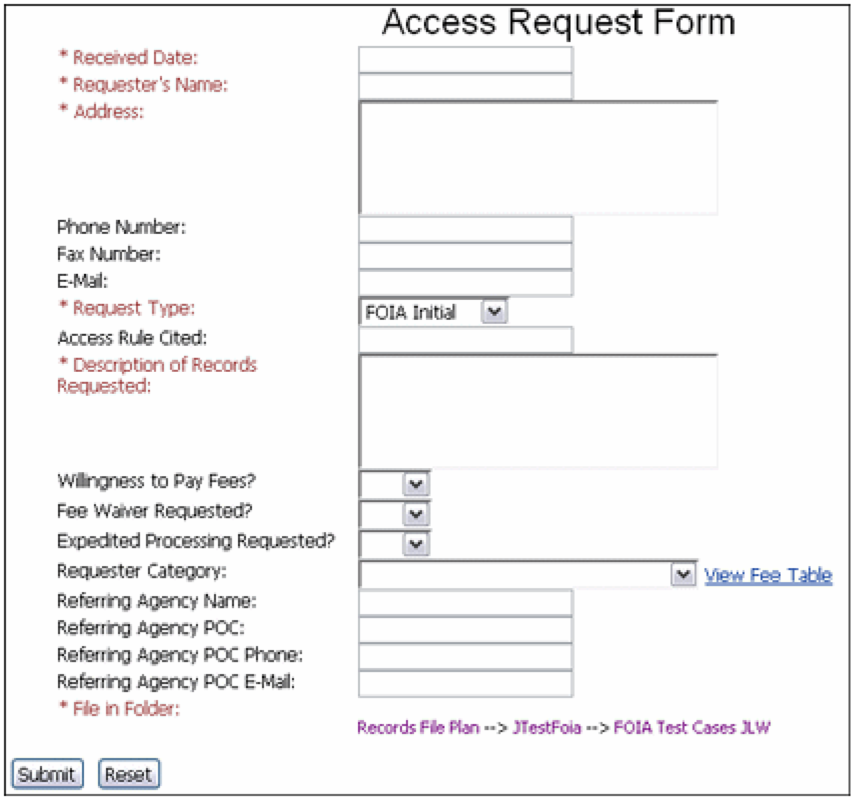


To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Disclosure Request Form**.

Element	Description
Disclosure Requestor	Contact information for the authorized agent requesting the disclosure.
Disclosure Purpose	The use or purpose to which the disclosed information will be put.
Details	Additional details about the requested disclosure.
Disclosure Receipt Date	The date the disclosure request was received.
Individual Consent	Some disclosures require individual consent forms.

A.13.1.5 Access Request Form

Use this form to initiate a workflow to process a request for information.



To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Access Request Form**.

Element	Description
Received Date	The date the request was received.
Requestor's Information	The name, address, phone number, fax number, and email address of the initiator of the request.
Request Type	Select the type of request: ■ FOIA Initial ■ FOIA Referral ■ FOIA Appeal If this is a Privacy Act request, the options are: ■ Privacy Act Review ■ Privacy Act Dispute ■ Privacy Act Disclosure Accounting
Access Rule Cited	The title, date, and version of the rule under which the request was made.
Fee Questions	Choose **Yes** or **No** to indicate if the requestor is willing to pay a processing fee. Required for FOIA requests. Choose **Yes** or **No** to indicate if the requestor is requesting a waiver of fees. Required for FOIA requests.
Expedited Processing Requested	Choose **Yes** or **No** to indicate if the requestor requests expedited processing.

Element	Description
Requestor Category	Required for FOIA requests. Select the category for the requestor. The category chosen will dictate the fee used, as described in the Request Fee Table: ▪ Commercial ▪ Educational ▪ Non-commercial scientific institutions ▪ News Media ▪ All Others ▪ All Others/Privacy Act
Referring Information	If this is a referral, enter the information about the referring agency, point of contact, point of contact phone number, and point of contact email address.
File in Folder	The locator links for the current folder are displayed.

A.13.1.6 Request Fee Table

The fee table indicates the payments associated with the category of requestor on the Access Request Form.

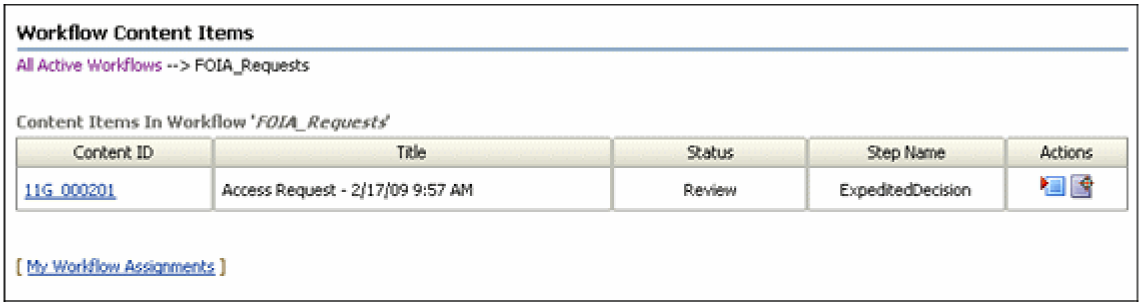
FOIA Fee Table

Requester Type	Fee Specification
Commercial	Requesters should indicate a willingness to pay all search and duplication costs
Educational	Requesters should indicate a willingness to pay duplication costs charges in excess of 100 pages if more than 100 pages are desired. Fees shall be waived or reduced in the public interest if criteria for fee waivers have been met.
Non-commercial scientific institutions	Requesters should indicate a willingness to pay duplication charges in excess of 100 pages if more than 100 pages are desired. Fees shall be waived or reduced in the public interest if criteria for fee waivers have been met.
News Media	Requesters should indicate a willingness to pay duplication charges in excess of 100 pages if more than 100 pages are desired. Fees shall be waived or reduced in the public interest if criteria for fee waivers have been met.
All Others	Requesters should indicate a willingness to pay assessable search and duplication costs if more than two hours of search effort or 100 pages of records are desired.
All Others/Privacy Act	Requests from subjects about themselves will continue to be treated under the fee provisions of the Privacy Act which permit fees only for duplication. Fee waivers or reductions if disclosure of the information is in the public interest

To access this table, click the **View Fee Table** link next to the Requestor Category on the Access Request Form.

A.13.1.7 Workflow Content Page

This page displays items in workflows as well as the stage of the workflow where the item is currently processing.

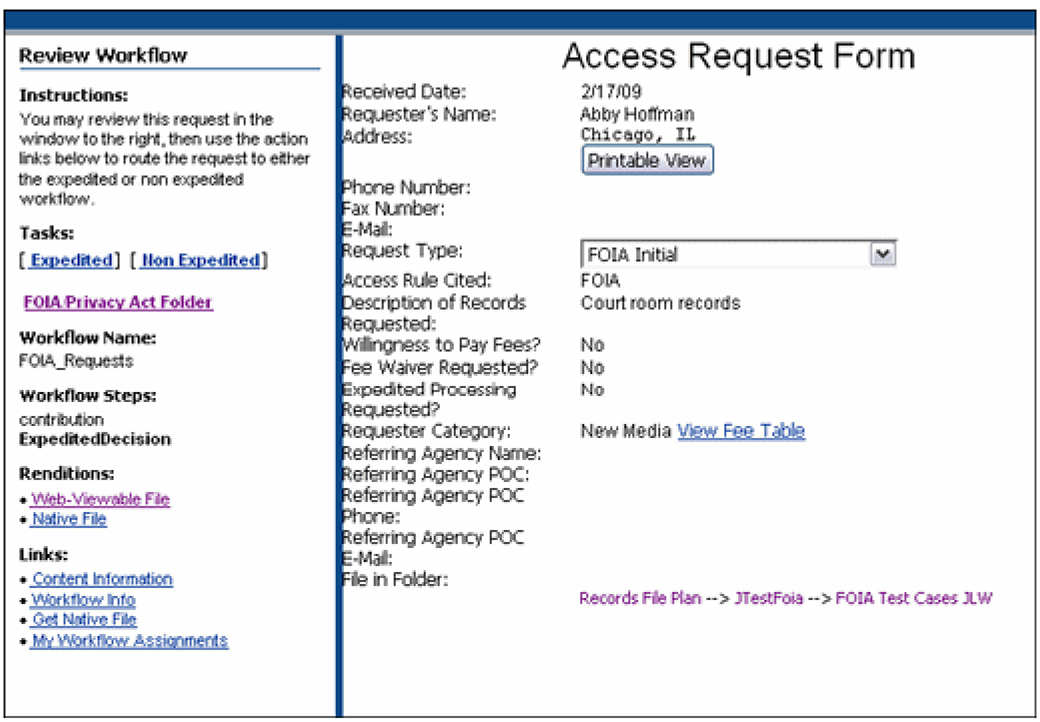


To access this page, click **Content Management** then **Active Workflows** from the Main menu. This page is also displayed whenever an action is taken on the Workflow Review Page.

The Step Name column indicates the stage of the workflow. Note that "ExpeditedDecision" does not imply that an expedited decision has been requested. It is the name of the stage of the workflow.

A.13.1.8 Workflow Review Page

This page displays the current item in the workflow as well as the Review Workflow Pane, where actions can be taken.



To access this page, click the Workflow Review icon next to an item on the Workflow Content Page. The content of this page varies with the type of request and the stage of the workflow when this page was accessed.

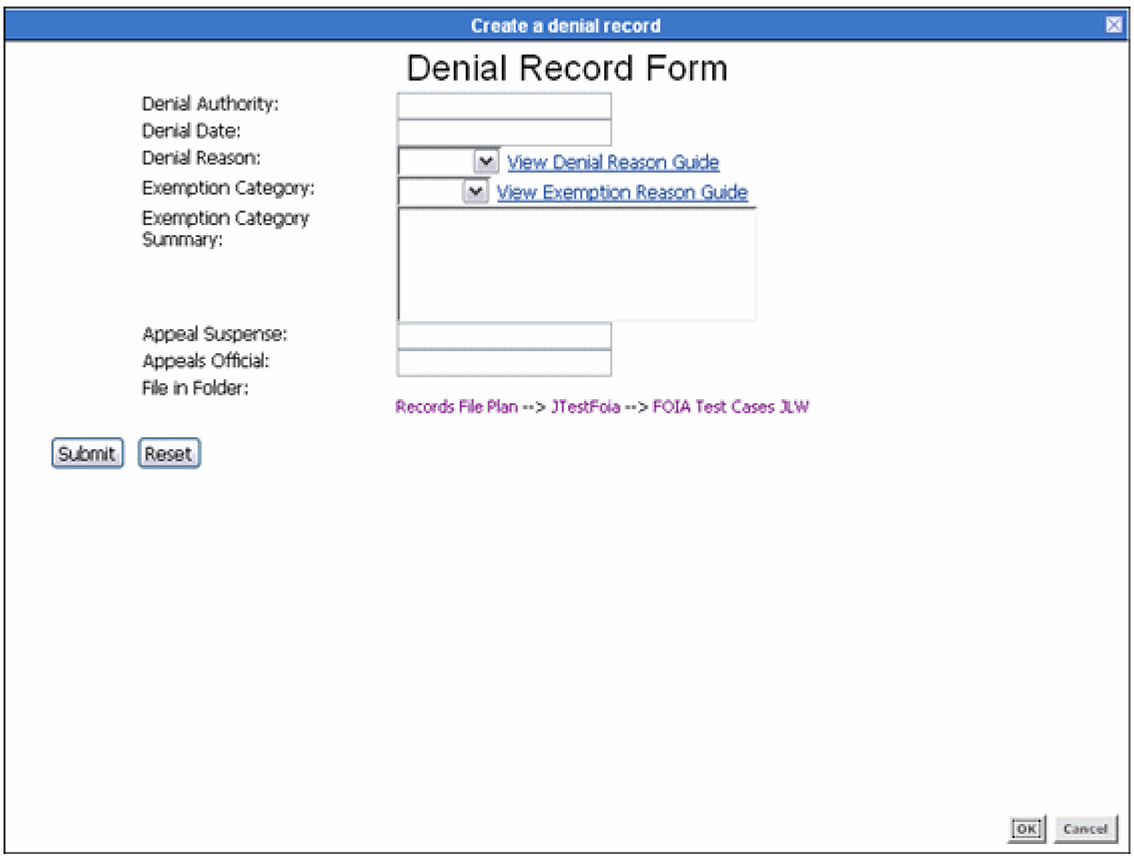
Click the Printable View link on this page to display a popup message showing the address information for the request. Use this to create a mailing label for acknowledgments and other correspondence.

Links in the Review Workflow pane on the left of the screen can be used to initiate actions for the requests. The following links are also available:

- The Content Information Page for the request item.
- The Workflow Information page.
- Get Native File, to retrieve the original request.
- My Workflow Assignments, which displays the Workflow Assignment Page.

A.13.1.9 Denial Record Form

This form is used to initiate a denial of information to a requestor.



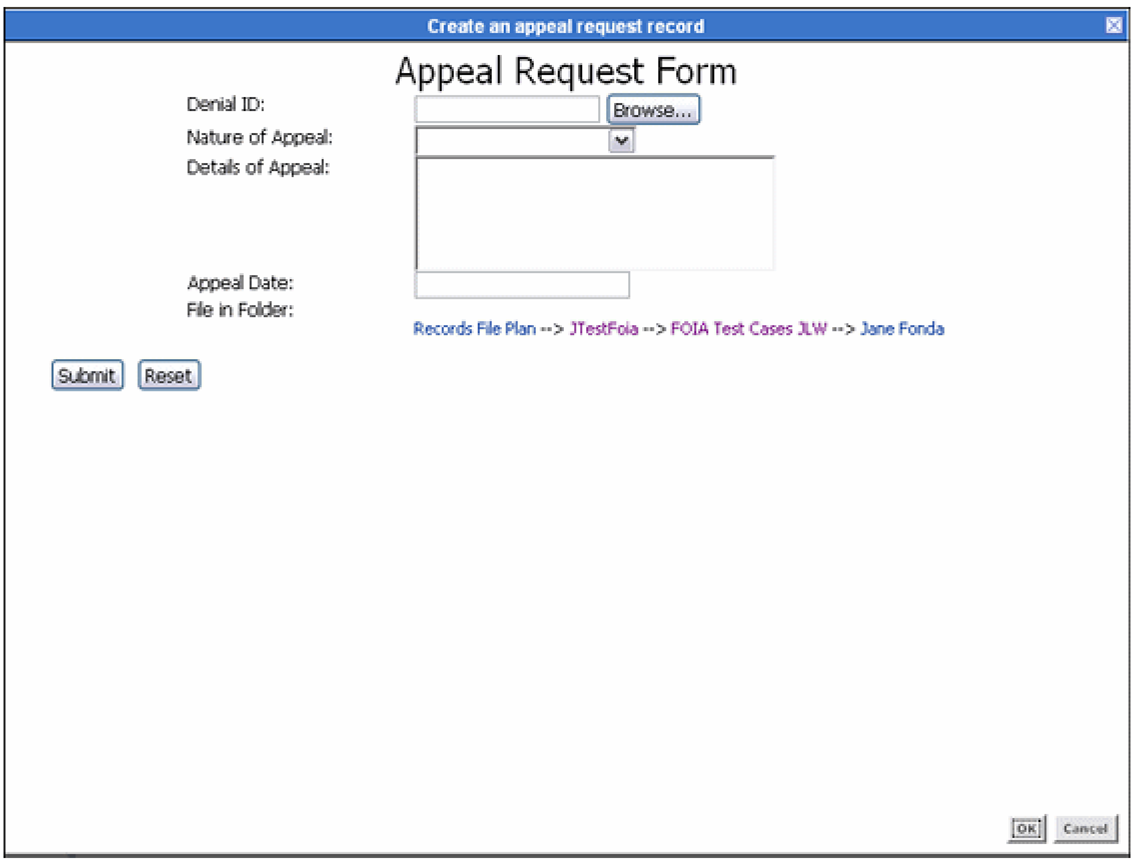
To access this form, click **Recommend Denial - Existing Record** or **Recommend Denial - New Form** on the Workflow Review Pane on the Workflow Review Page.

Element	Description
Denial Authority	The name, title, position, signature or electronic signature of the designated denial authority.
Denial Date	The date the denial was initiated.
Denial Reason	Select the reason for denial from the list. Click **View Denial Reason Guide** for a list of denial reasons and descriptions.

Element	Description
Exemption Category	If an exemption is warranted, choose the category from the list. Click **View Exemption Reason Guide** for a list of exemptions and descriptions.
Exemption Category Summary	If needed, enter a summary of the exemption decision.
Appeal Suspense	The suspense duration for the denial. Currently set at 60 calendar days according to DoD 5015.2 specifications.
Appeals Officer	Name, title, position, signature, or electronic signature of the designated authority.
File in Folder	The locator links for the current folder are displayed.

A.13.1.10 Appeal Request Form

This form is used to start an appeal when a FOIA or PA request is denied.



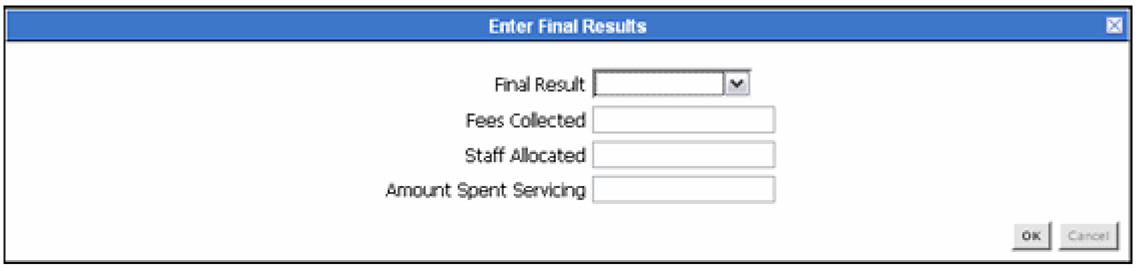
To access this form, click **Appeal Received - New Form** in the Review Workflow pane on the Workflow Review Page. Appeals are always linked to denials.

Element	Description
Denial ID	Click **Browse** to search for and link to the denial record being appealed. The ID of the request is inserted and this appeal will then be associated with it.

Element	Description
Nature of Appeal	Choose from the following options: ■ Review ■ Dispute ■ Disclosure Accounting
Details of Appeal	Further details about the appeal.
Appeal Date	The date the appeal was received.

A.13.1.11 Final Result Dialog

This dialog is used to collect request processing information for reports.



This dialog is displayed when a request workflow completes, either after the request is serviced or if the request for information is denied.

Element	Description
Final Result	Choose a result from the list. Options include: ■ Granted in Full ■ Denied in Part ■ Denied in Full ■ Other Reason
Fees Collected	Enter a decimal amount, excluding the dollar sign.
Staff Allocated	Enter an integer indicating the number of people who were allocated to service the request.
Amount Spent Servicing	Enter the total amount spent to service the request.

A.13.2 FOIA/PA Data Screens

These screens are used to provide details about the requests processed in Oracle URM. Depending on the type of request, a variety of forms are used. For complete details about these forms and when they are used, see the DoD 5015.2 specification.

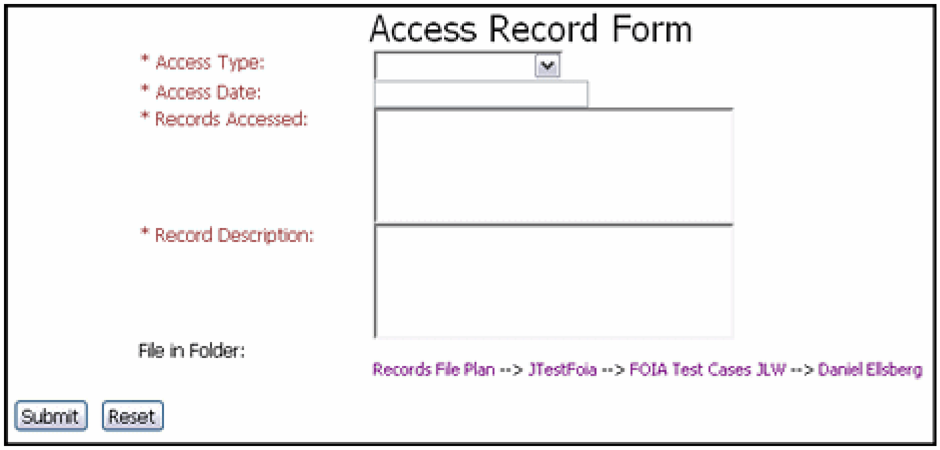
The following forms are described here:

- "Access Record Form" on page A-57
- "Accounting Record Form" on page A-57
- "Disclosure Record Form" on page A-58
- "Dispute Record Form" on page A-60
- "Exemption Record Form" on page A-61

- "Matching Program Records Form" on page A-62
- "Privacy Act File" on page A-62
- "System of Records Form" on page A-63

A.13.2.1 Access Record Form

Use this form to document the collection of records for an access request.

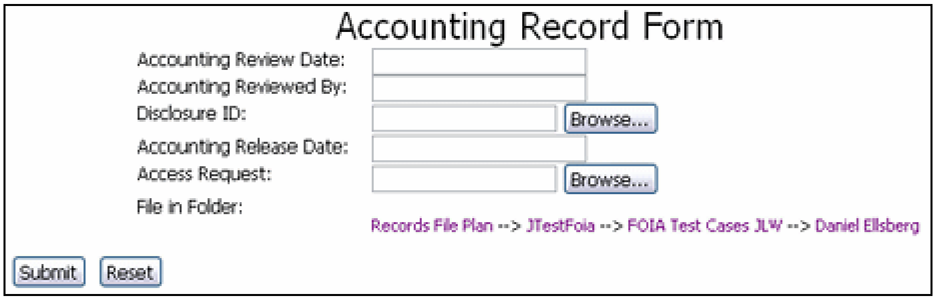


To access this form, click **Create** then **FOIA Requests** or **Privacy Acts Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then click **Access Record Form**.

Element	Description
Access Type	Choose from the following options that describe how the records are gathered for the request: ▪ In Person ▪ By Authorized Agent ▪ By Mail ▪ By FAX ▪ By Email ▪ Via Internet
Access Date	The date the records were accessed: ▪ In person: the date the person visited ▪ By Mail or By FAX: the date the package was sent ▪ By Email: the date the email was sent ▪ via Internet: the timestamp on the retrieval
Records Accessed	A listing of records accessed by or provided to the individual.
Record Description	A summary of the record state (original, redacted, summary, etc.)
File in Folder	The locator links for the current folder are displayed.

A.13.2.2 Accounting Record Form

Use this form to track disclosures of information from the System of Records (SOR). This form is linked to disclosures in review.



Accounting Record Form

Accounting Review Date:

Accounting Reviewed By:

Disclosure ID: Browse...

Accounting Release Date:

Access Request: Browse...

File in Folder: Records File Plan --> JTestFoia --> FOIA Test Cases JLW --> Daniel Ellsberg

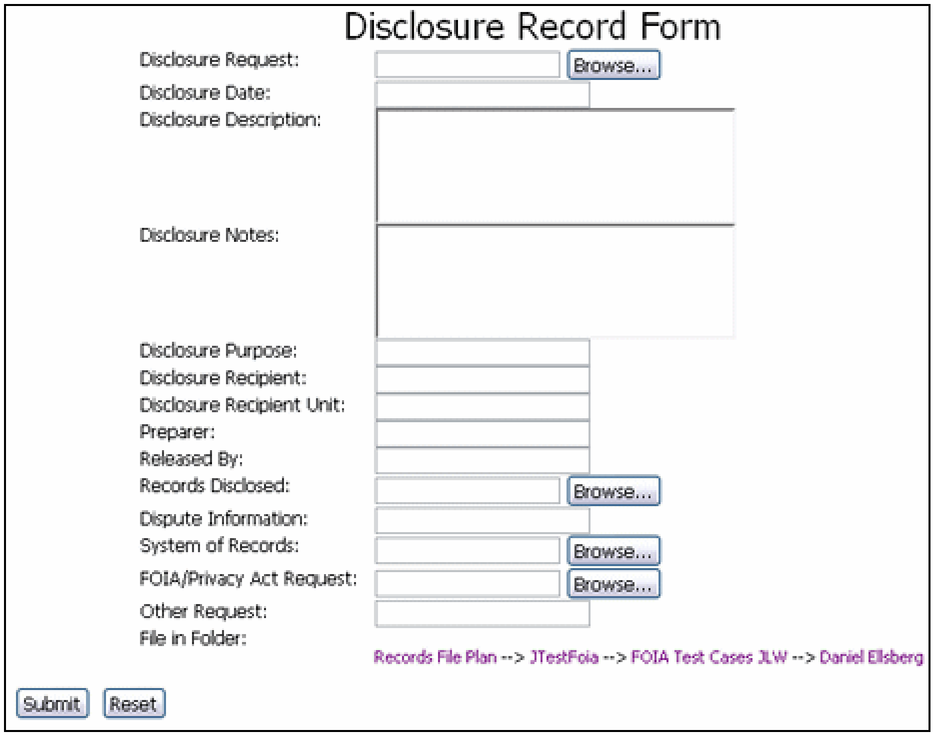
Submit Reset

To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then click **Accounting Record Form**.

Element	Description
Accounting Review Date	The date the disclosure was reviewed.
Accounting Reviewed By	The name and contact information for the person conducting the review.
Disclosure ID	Enter the disclosure ID or click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
Accounting Release Date	The date accounting was released to the individuals involved.
Access Request	Click **Browse** to link to the original access request. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
File in Folder	The locator links for the current folder are displayed.

A.13.2.3 Disclosure Record Form

Use this form to create a record of disclosure.



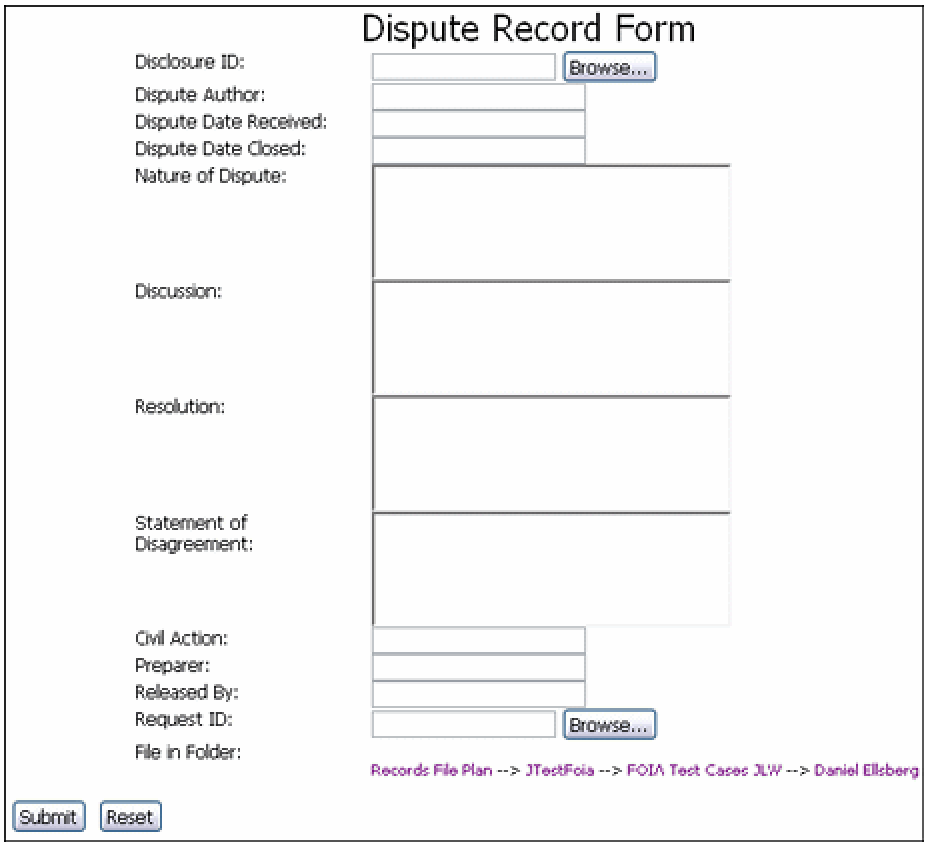
To access this form, click **Create** then **FOIA Requests** then **Disclosure Record Form** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then click **Disclosure Record Form**.

Element	Description
Disclosure Request	Enter the disclosure ID or NARA transfer identifier or click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
Disclosure Date	The name, address, phone number, fax number, and email address of the initiator of the request.
Disclosure Description	A description of the information released. This may also include links to the actual records disclosed.
Disclosure Purpose	The reason for the disclosure.
Disclosure Recipient	The name of the recipient of the disclosed records.
Disclosure Recipient Unit	The organization receiving the disclosed records.
Disclosure Notes	A discussion of deletions or changes to the disclosed records. This may include other information that is pertinent to the disclosure.
Preparer	The identification of the person responsible for preparing the disclosure.
Released By	The identification of the person responsible for releasing the disclosure.
Records Disclosed	A link to the records disclosed. Click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
Dispute Information	Indicate if the disclosed information has been corrected or disputed.

Element	Description
Request Type	If linked to a FOIA request or Privacy Act request, click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**. If used for another type of request (such as court order, subpoena, and so on) indicate that type in the **Other Request** field.

A.13.2.4 Dispute Record Form

Use this form to add details about disputed records.



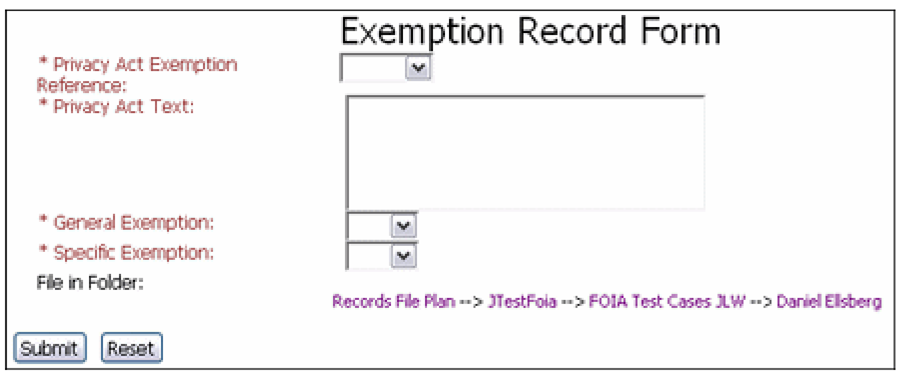
To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then **Dispute Record Form**.

Element	Description
Disclosure ID	A link to the disclosure record. Click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
Dispute Author	The name of the person initializing the dispute.
Dispute Date Received	The date the organization received the dispute.
Dispute Date Closed	The date of the final action on the dispute.
Nature of Dispute	A summary of the dispute allegations.

Element	Description
Discussion	A discussion of the dispute allegations.
Resolution	A discussion of the final resolution of the dispute.
Statement of Disagreement	This is required if the dispute author provides a statement.
Civil Action	This is required if a civil action arises from the dispute.
Preparer	The identification of the person preparing the disclosure or the individual access response that led to the dispute. Required if the dispute is related to a disclosure.
Released By	The identification of the person approving the disclosure or the individual access response. Required if the dispute is related to a disclosure.
Request ID	A link to the original access request. This is required if the dispute is related to a disclosure or individual access response. Click **Browse**. A search screen is displayed. Enter the metadata for searching or click **Search** to return all items. Click the checkbox of the item to use for linking then click **OK**.
File in Folder	The locator links for the current folder are displayed.

A.13.2.5 Exemption Record Form

Use this form to detail information about an exemption request.

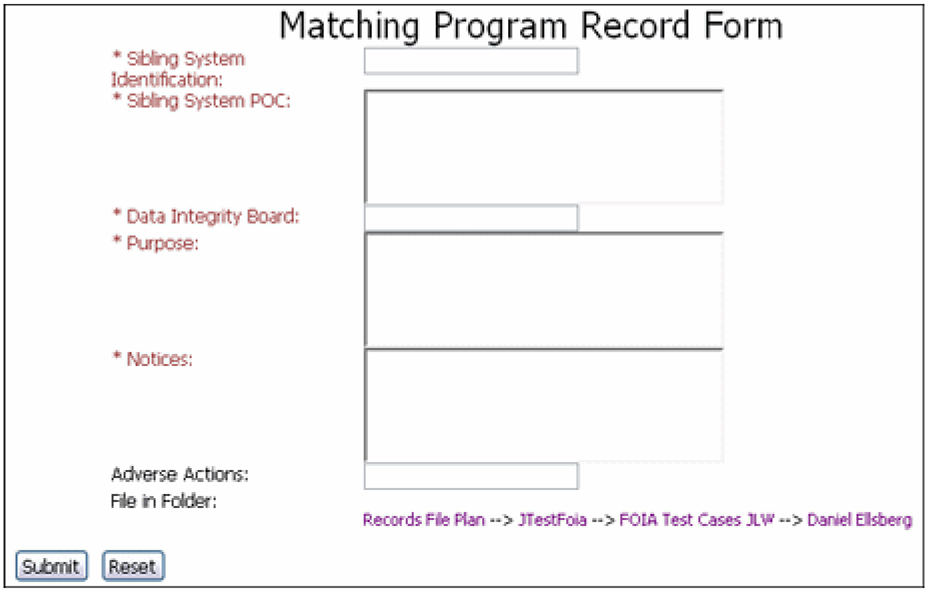


To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then **Exemption Record Form**.

Element	Description
Privacy Act Exemption Reference	Choose the reference in the Privacy Act that allows the exemption.
Privacy Act Text	The text which matches the chosen reference is inserted. Optional text can be added.
General Exemption	Select **Yes** or **No** to indicate if this is a general exemption.
Specific Exemption	Select **Yes** or **No** to indicate if this is a specific exemption.
File in Folder	The locator links for the current folder are displayed.

A.13.2.6 Matching Program Records Form

Use this form to add information about records that will be cross-matched.



To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then **Matching Program Record Form**. See the DoD 5015.2 specification for details about this form.

Element	Description
Sibling System Identification	The system name or identifier of systems with which the information will be cross-matched.
Sibling System POC	The point of contact for the matching system.
Data Integrity Board	The name of the board verifying the match.
Purpose	The purpose of the matching program.
Notices	Any notices associated with this form.
Adverse Actions	Any adverse actions associated with this form.
File in Folder	The locator links for the current folder are displayed.

A.13.2.7 Privacy Act File

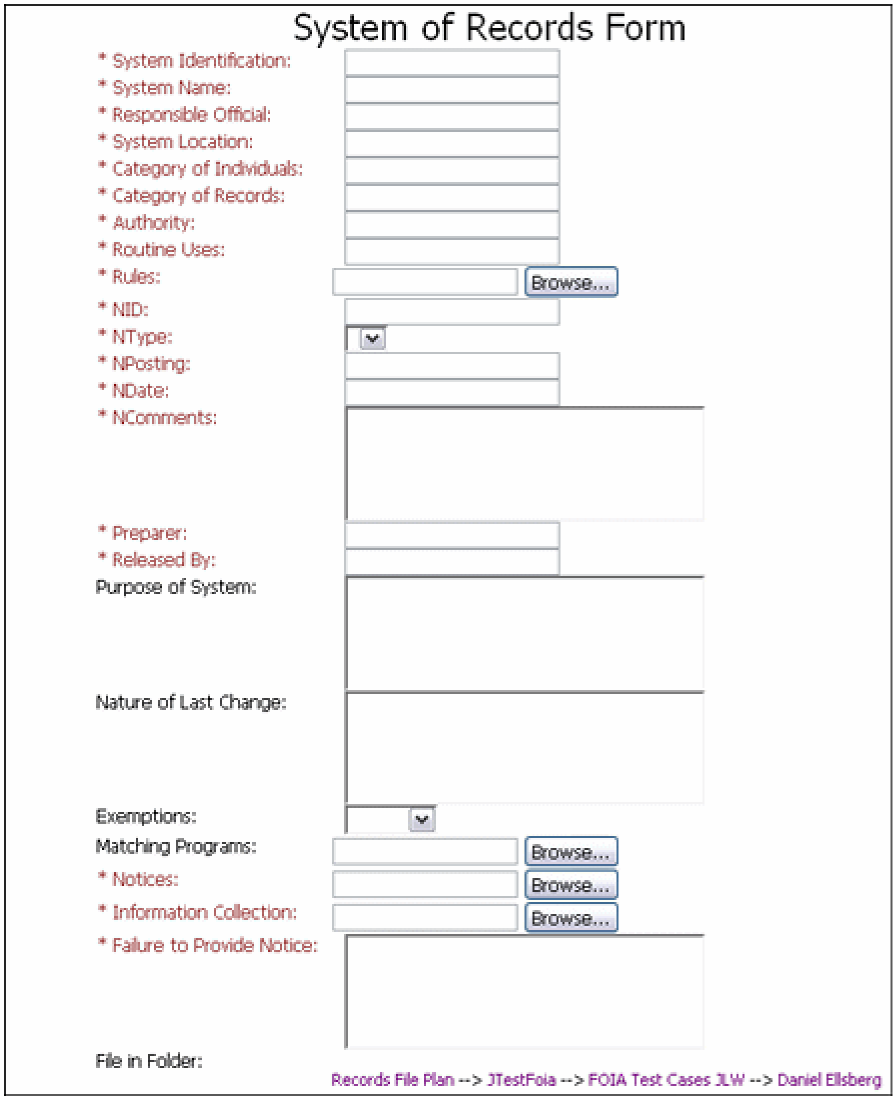
Use this form to create a privacy act case file.

To access this form, click **Create** then **FOIA Requests** then **Access Request Form** from the Action menu of a folder used to store FOIA or PA information. Click **Other** then **Privacy Act File**. See the DoD 5015.2 specification for details about this form.

Element	Description
File ID	The privacy act file ID. Enter a maximum of 21 alphanumeric characters.
File Name	The file name. Enter a maximum of 55 alphanumeric characters.
File in Folder	The locator links for the current folder are displayed.

A.13.2.8 System of Records Form

This screen is used to prepare the systems of record (SOR) components.



To access this form, click **Create** then **FOIA Requests** or **Privacy Act Requests** from the Action menu of a folder used to store FOIA or PA information. Click Other then **System of Records Form**. See the DoD 5015.2 specification for details about the sections of the specification pertaining to this form.

Element	Description
System Identification	The system identified. Enter a maximum of 21 alphanumeric characters.

Element	Description
System Name	The name of the system used. Enter a maximum of 55 alphanumeric characters.
Responsible Official	The title and business address of the responsible agency official.
System Location	The addresses of each location where the system or segment of the system is maintained. Classified addresses are not listed but the classification of a system should be noted.
Category of Individuals	A description of the specific categories of individuals to whom the records pertain.
Category of Records	Clear descriptions of the types of records maintained in the system.
Authority	Links to authority records.
Routine Uses	A description about how the information will be used. Examples include Law Enforcement, Taxing Authorities, or Congressional Inquiry. See the DoD 5015.2 specification for more details.
Rules	The name of the documentation providing the access rules. Click **Browse**. A search screen is displayed. Enter metadata to search for the document then click **Search**. A list of search results is displayed. Click the checkbox of the item to use and click **OK**.
NID	The notice identifier.
NType	Choose the type from the list Options include New, Alteration, Amendment or Deletion.
NPosting	The date and volume of the Federal Register.
NDate	The date the notice was published in the Federal Register.
NComments	Any comments about unique circumstances of this notice.
Preparer	The author or preparer of the System of Record Notification (SORN).
Released By	The name of the person responsible for ensuring the publication of the SORN.
Purpose of System	A brief discussion of the system purpose. This is required for new systems.
Nature of Last Change	A discussion of changes to the purpose or use of the system. This includes deletions. This is required for altered systems.
Exemptions	Choose the section reference of the exemption. Required if exemptions apply. See the DoD 5015.2 specification for details about exemptions regarding classifications.
Matching Programs	Links to matching program records or descriptions. This is required if SOR participates in one or more matching programs. Click **Browse**. A search screen is displayed. Enter metadata to search for the document then click **Search**. A list of search results is displayed. Click the checkbox of the item to use and click **OK**.
Notices	Links to or from notices about this SOR. Click **Browse**. A search screen is displayed. Enter metadata to search for the document then click **Search**. A list of search results is displayed. Click the checkbox of the item to use and click **OK**.
Information Collection	Identify or links to form(s) used to collect the personal information stored in the system.
Failure to Provide Notice	A description of the reason for a failure to provide notice.
File in Folder	The locator links for the current folder are displayed.

A.14 Federated Search and Freeze Screens

The following screens are used when performing Federated searches and freezes.

- "Federated Query Builder Page" on page A-65
- "Federated Searches List Page" on page A-66
- "Federated Search Details Page" on page A-67
- "Federated Search Results Page" on page A-67

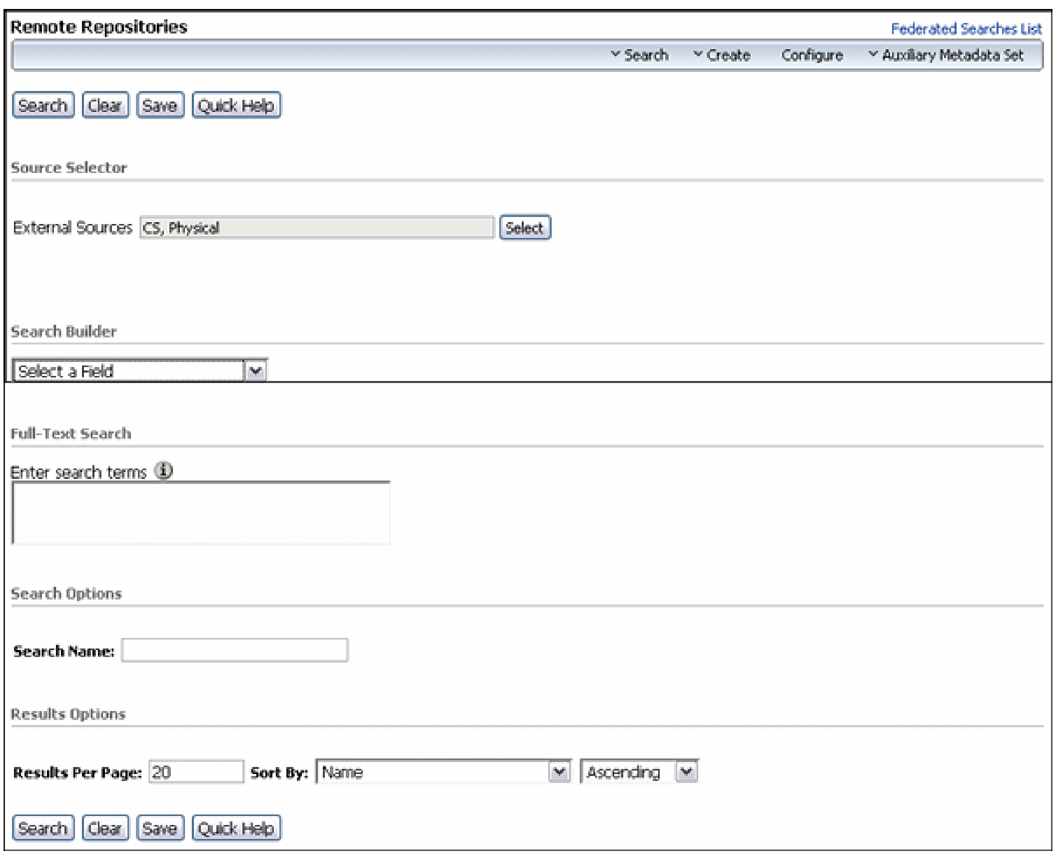
A.14.1 Federated Search Pages

The following pages are used to schedule Federated searches.

- "Federated Query Builder Page" on page A-65
- "Federated Searches List Page" on page A-66
- "Federated Search Details Page" on page A-67

A.14.1.1 Federated Query Builder Page

This screen is used to build a query for a Federated search.



To access this screen, click **Search** then **Global Search** from the Top menu. Choose the type of search to perform. A similar screen is used for all three types of searches: Central Catalog, Remote Repository, and SES Search.

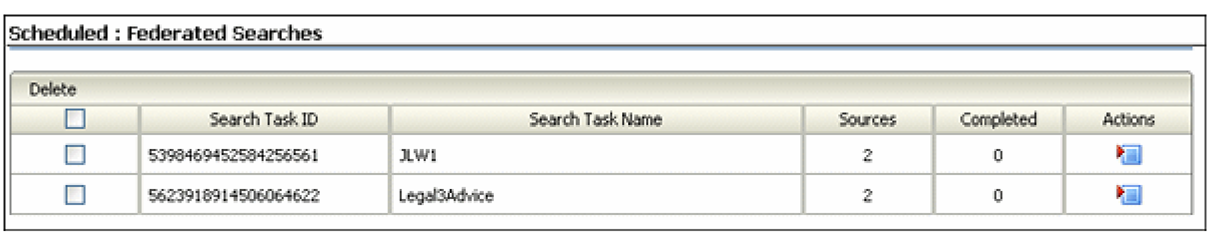
When using a Remote Repository search, an **Include Content** checkbox is available, used to retrieve copies of the content that match the search criteria. Do not click this box unless search results are certain. Returning a copy of the data takes long and uses space. Fine tune the query first and verify what items will be returned before actually retrieving the content.

Click the **Federated Searches List** link to see a list of a previously scheduled searches.

Element	Description
External Sources	The repositories to be used in the search. Searches are not performed immediately. If an external repository has been chosen, the adapter will schedule the search using its previously established configuration parameters. If local repositories on the Oracle URM server are chosen in this field, they will be searched during regularly scheduled search batches, scheduled by default for midnight.
Search Builder	A pull-down menu containing all fields available for searching. The fields displayed are those in use on the Oracle URM server. These fields should be mapped to those on remote repositories in order to assure correct retrieval. When a field is selected, additional search options appear, allowing a user to match the field to a specific value. See the *Oracle Fusion Middleware User's Guide for Content Server* for details about using the Query Builder tool.
Full-text Search	Area used to enter terms for searching. Not all remote repositories will be configured for full-text searching. If using this option, make sure the repositories selected for searching allow this type of search.
Search Name	A name for the search. Federated Searches are performed by adapters and thus conform to an adapter schedule. A meaningful search name will help track the progress of the search.
Results section	Selects the number of results per page. Default: 20.
Sort By attribute list	Selects one or more attributes by which to sort the results. The list contains all of the screening criteria options.
Sort order list	Specifies the sort order of the screening results: ■ **Descending**: (**default**) Sorts alphabetical results in Z-A order, numeric results in 9-0 order and date results in newest to oldest order. ■ **Ascending**: Sorts alphabetical results in A-Z order, numeric results in 0-9 order, and date results in oldest to newest order.
Save button	Prompts the user to save the query under a query name. Once saved, the query is available in the **My Saved Query** section of the **My Content Server** menu.

A.14.1.2 Federated Searches List Page

This page displays a list of all scheduled searches and their progress.

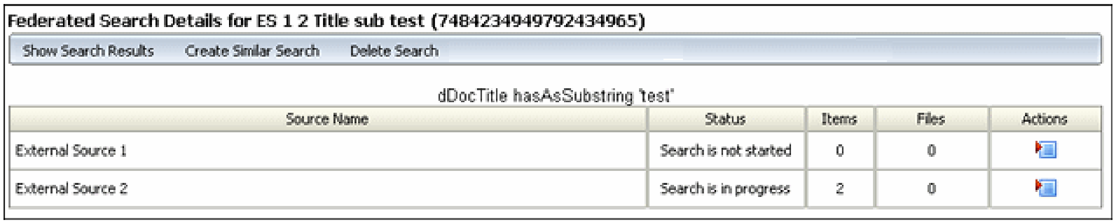


To access this page, click **Federated Searches List** from the Federated Query Builder Page or by clicking **Records** then **Scheduled** then **Federated Searches**.

Element	Description
Search Task ID	An assigned ID for the scheduled search.
Search Task Name	The name given to the search on the Federated Query Builder Page.
Sources	The number of sources chosen for the search.

A.14.1.3 Federated Search Details Page

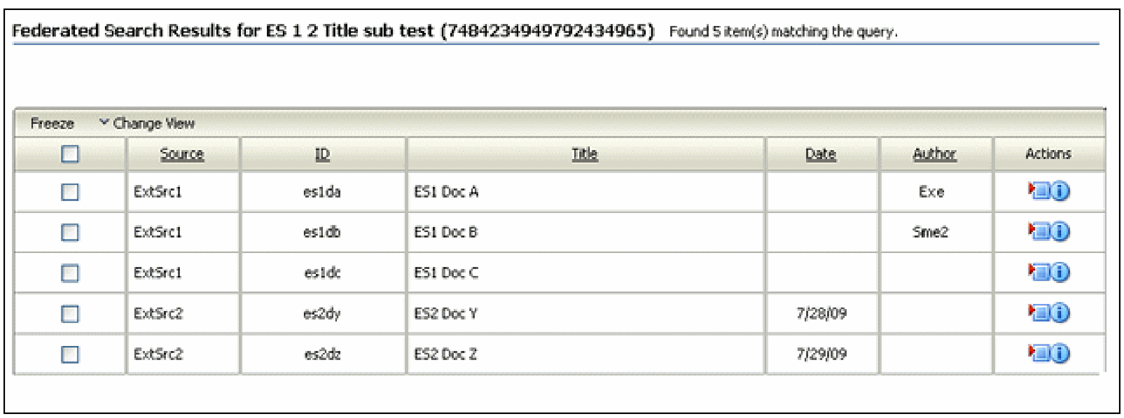
This page shows the details of a scheduled search.



To access this page, click **Show Search Details** from the **Action** menu of a search on the Federated Searches List Page.

A.14.1.4 Federated Search Results Page

This page shows the results of a search.



To access this page, click **Show Search Results** from the **Action** menu of a search on the Federated Searches List Page

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W