Oracle® Fusion Middleware

Setup Guide for Universal Records Management

11*g* Release 1 (11.1.1)

E10640-02

October 2010

ORACLE®

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

E10640-02

Primary Author: Jean Wilson

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

Contents

5 Setting Up Security

6 Additional Security Settings

7 Configuration Options

8 Configuring Physical Content Management

11 Setting up Triggers

A User Interface

B Summary of Security Rights and Roles

Preface

This guide provides instructions to set up 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 the product: This document provides information about installing the software.
- *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:

1.1 About This Guide

This guide provides detailed instructions to set up and administer the product software. In general, it does not contain details about processing information. For example, this guide contains instructions for setting up dispositions (those rules used to manage content life cycles), but it does not contain instructions for processing those dispositions.

Details about processes are contained in either the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* 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 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 installation scenarios. The features available at a 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 installation and 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 in use at your site 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*.

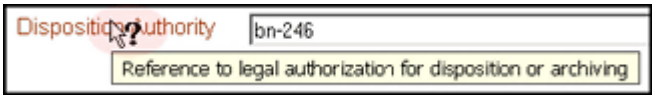
1.4 Using Help

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

1.4.1 Tooltips

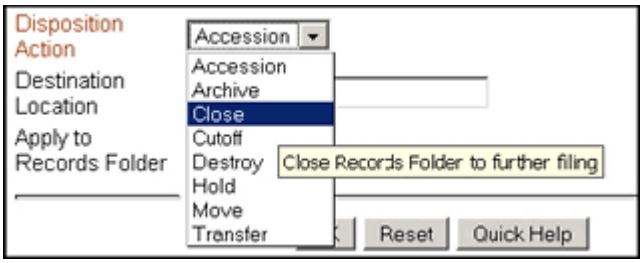
If the mouse cursor is held over a field label in a web browser, context-sensitive information about the field label is displayed. A question mark is displayed, and then the tooltip appears.

Figure 1–1 Field Label Tooltip



When using Netscape or Firefox as a web browser, tooltips for items in options lists are available as well, 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. Your 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. Your 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

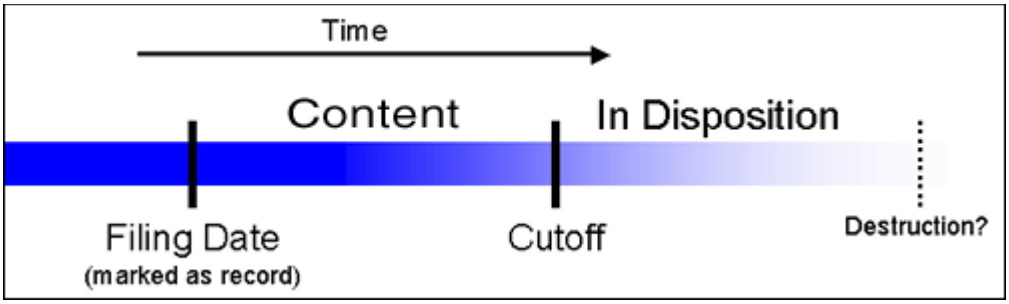
After a retention period, content items are disposed of by authorized people according to the requirements of the organization. Disposition actions can include:

- 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 enables you to manage content, regardless of source or format, in a single, consistent, manageable infrastructure. Managed items are assigned retention schedules and disposition rules which enable you 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 your organization.

Disposition schedules of content in the repository can also be managed, enabling you to schedule 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

Setting Up the Software

This chapter provides details about choices that must be made before setting up a retention system.

It also provides a broad overview of the tasks needed to set up a retention system. Use the information in this chapter as a reference to those tasks that need to be done. For detailed conceptual and reference information pertaining to these tasks, see the other chapters in this guide.

If you are unclear about any of the tasks in this chapter, consult the detailed task information in the later chapters in this guide.

> **Important:** You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

Before setting up the system, review Chapter 2, "Introduction to Records and Retention Management" which provides an essential overview to the concepts and vocabulary used in a retention management system.

Depending on the cache settings for your browser, you may need to either restart your browser or clear the cache settings in order to view changes that are made to the configuration of Oracle URM. For example, if you enable Offsite Storage functionality, you may need to clear the cache settings and restart your browser for the appropriate options to appear on the **Physical** menu. The same is true if you disable functionality in order to remove the options.

This chapter covers the following topics:

Permissions: Specific permissions are required to perform the tasks described here. For details about the required permissions, see the tasks outlined in later chapters of this manual. In general, users with the Record Administrator role should be able to perform the majority of these tasks. For details about rights and roles, see Chapter 5, "Setting Up Security".

3.1 Fusion Middleware Security Considerations

This section describes how to configure your Fusion Middleware product to handle authentication and authorization, and other aspects of application security.

3.1.1 Oracle UCM Security Considerations

Oracle UCM uses the Oracle WebLogic Server user store to manage user names and passwords, so most user management tasks must be performed with the Oracle WebLogic Server user management tools instead of Oracle UCM's User Admin applet. User logins must be created on Oracle WebLogic Server and the default Oracle WebLogic Server users should not be used for Oracle URM.

Oracle UCM and workflow services use Java Platform Security (JPS) and the User and Role API. Oracle Internet Directory stores user and group information. When Oracle UCM uses Oracle Internet Directory, the Oracle Internet Directory Authentication provider must be the first provider listed in the security realm configuration.

If the Oracle Internet Directory Authentication provider is not listed first (for example, it is listed below the Oracle WebLogic Server provider, `DefaultAuthenticator`), then login authentication fails. You can use the Oracle WebLogic Server Administration Console to change the order in which the configured Authentication providers are called.

When you use Oracle Internet Directory, all Oracle UCM administrator and other users must be defined in Oracle Internet Directory.

Oracle UCM assigns an administrator role to users defined in the internal Oracle WebLogic Server user store. This is true regardless of whether Oracle Internet Directory is used or not used. However, if you use Oracle Internet Directory and if the OID Authentication provider is not listed first then any request by Oracle UCM to retrieve the roles of the Oracle WebLogic Server defined administrative users will fail.

See "Managing Security and User Access" in the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for more details about security and user accounts. See the *Oracle Fusion Middleware Application Security Guide* and *Oracle Fusion Middleware Securing Oracle WebLogic Server* for details about LDAP providers.

3.1.2 Oracle URM-WNA Redeployment

For Windows Native Authentication through Kerberos to work with Oracle URM, you must redeploy Oracle URM.

First create then save an .xml file for the Oracle URM domain type that includes the following information. Save the file as urm.xml:

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan
   xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan
```

```
http://xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-plan.xsd"
   global-variables="false">
 <application-name>urm.ear</application-name>
 <variable-definition>
  <variable>
   <name>url-pattern</name>
   <value>/*</value>
  </variable>
  <variable>
   <name>http-only</name>
   <value>false</value>
  </variable>
 </variable-definition>
 <module-override>
  <module-name>urm.war</module-name>
  <module-type>war</module-type>
  <module-descriptor external="false">
   <root-element>web-app</root-element>
   <uri>WEB-INF/web.xml</uri>
   <variable-assignment>
    <name>url-pattern</name>

<xpath>/web-app/security-constraint/[display-name="UCMConstraint"]/web-resource-collection/[web-res
ource-name="idcauth"]/url-pattern</xpath>
    <operation>replace</operation>
   </variable-assignment>
  </module-descriptor>
  <module-descriptor external="false">
   <root-element>weblogic-web-app</root-element>
   <uri>WEB-INF/weblogic.xml</uri>
   <variable-assignment>
    <name>http-only</name>
    <xpath>/weblogic-web-app/session-descriptor/cookie-http-only</xpath>
   </variable-assignment>
  </module-descriptor>
 </module-override>
</deployment-plan>
```

1. As administrator, log in to the Oracle WebLogic Server Administration Console.
2. Click **Deployments** in the Domain Structure navigation tree.
3. Click the **Control** tab then **Next** until you see the Oracle Universal Records Management deployment.
4. Select the checkbox to the left of that deployment.
5. Click **Update**.
6. Under the Deployment Plan Path, select **Change Path**.
7. Navigate to and select the urm.xml file just created.
8. Verify that **Redeploy this application using the following deployment files** is selected.
9. Click **Next**.
10. Click **Finish**.

3.1.3 Configuration for External LDAP Authentication Provider

In almost all cases, you want to reassociate the identity store with an external LDAP server rather than use the default embedded LDAP:

Table 3–1 External LDAP Authentication Provider Documentation

For Information On...	See The Following Guide...
LDAP reassociation	*Installation Guide for Oracle Enterprise Content Management Suite: Section 4.4, Reassociating the Identity Store with an External LDAP Authentication Provider*

3.1.4 Configuration for SSL

You can configure Oracle Fusion Middleware to secure communications between Oracle Fusion Middleware components using SSL, which is an industry standard for securing communications. Oracle Fusion Middleware supports SSL version 3, as well as TLS version 1:

Table 3–2 SSL Documentation

For Information On...	See The Following Guide...
Configuring SSL with Oracle Fusion Middleware: Web Tier, Middle Tier, and Data Tier	*Oracle Fusion Middleware Administration Guide: Chapter 6, SSL Configuration in Oracle Fusion Middleware*
Configuring SSL with Oracle WebLogic Server	*Oracle Fusion Middleware Security Oracle WebLogic Server Guide: Chapter 12, Configuring SSL*

3.1.5 Configuration for Single Sign-On Use

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides a wide range of identity administration and security functions, including several single sign-on options for Fusion Middleware and custom Fusion Middleware applications. OAM is the recommended single sign-on solution for Oracle Fusion Middleware 11g installations.

If your enterprise uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring SSO with Microsoft Clients may also be an option to consider.

The setup required for these SSO solutions is described in the following documents/sections:

Table 3–3 Single Sign-on Documentation

For Information On...	See The Following Guide...
Configuring OAM	*Oracle Fusion Middleware Security Guide: Chapter 10, Configuring Single Sign-On in Oracle Fusion Middleware*
Using Windows Native Authentication for Single Sign-on	*Oracle WebLogic Server Admin Console Help: Configure Authentication and Identify Assertion Providers*

3.1.6 Configuring for Web Services Use

WebLogic Web Services are implemented according to the Web Services for Java EE 1.2 specification, which defines the standard Java EE runtime architecture for implementing Web Services in Java. The specification also describes a standard Java

EE Web Service packaging format, deployment model, and runtime services, all of which are implemented by WebLogic Web Services.

Table 3–4 Web Services Documentation

For Information On...	See The Following Guide...
Apply OWSM security to Web Services	*Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Appendix A: Using Oracle Web Service Security Policies*
Use MTOM with Web Services	*Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Section 2.2: Example of Adding Security to MTOM Web Service*

3.2 Software Configuration

Software configuration should be done before configuring any other aspects of the Oracle URM software. By choosing specific options, specific components are enabled and ready for use.

The following options are available for installation:

- **Minimal**: Enables the minimal amount of functionality and excludes disposition actions and most of the product features. This is the default when the software is enabled.
- **Typical**: Enables all disposition actions and all features except for DoD Configuration, Classified Topics, FOIA/PA tracking (Freedom of Information Act/Privacy Act), and E-mail. This option does enable Physical Content Management (PCM).
- **DoD Baseline**: Enables the features from a Typical installation with the addition of DoD Configuration and E-mail.
- **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 an action is selected, dependent actions are also automatically selected.

The only way to enable FOIA/PA tracking is by using the Custom configuration option. Note that the `INSTALL_SCHEMA_TO_DATA` service must be rerun after the FOIA component is enabled and the browser should be reloaded. See the *Oracle Fusion Middleware Application Administrator's Guide for Content Server* for details about rerunning services. Note that if the FOIA/PA functionality is installed, fast index rebuilds may not be possible. Deselect the **Fast Index Rebuild** option when using FOIA/PA.

Use this procedure to set the software configuration:

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

---

1. Choose **Records** then **Configure** then **Enabled Features** from the Top menu.

   The Enabled Features Page opens.

2. Select the type of configuration to perform. After selection, the feature and disposition options at the bottom of the page appear with the checkbox selected,

indicating which choice is included. If **Custom** is selected, you can choose which features and dispositions to be enabled.

3. Click **Submit**.

Important: You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

After making selections or changing options (for example, switching from Baseline to Classified), restart Oracle UCM. Depending on the search options in use, the index may also need to be rebuilt. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about restarting the system and rebuilding the index from the Repository Manager.

3.3 Retention Setup Checklist

After choosing the features to use, certain options must be configured in order for the system to work properly. If not done, a warning messages appears indicating that the setup is incomplete.

To complete the configuration, click the link in the warning message. The Setup Checklist Page opens. This page shows a series of links to other pages where configuration selections can be made. When done configuring, select the checkbox next to an option to indicate the completed task. Depending on the action, it may be necessary to refresh the frame in order to view the completed tasks.

You can also access the Setup Checklist Page by choosing **Records** then **Configure** then **Setup Checklist** from the Top menu.

You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

Important: If File Store Provider is needed to check in templates for Oracle URM, set up the File Store Provider first and then check in the templates. To install a file store provider, click **Install Default Templates (Category Defaults, Reports, Dashboards, etc.)** on the Setup Checklist Page. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about using File Store Provider.

If the configuration of the system changes (for example, switch from DoD Baseline to Typical) reconfigure the options needed for the level of functionality that is enabled.

The required options include:

- Set configuration variables: Several optional variables can be changed.
- Define default metadata: Some content items are automatically checked in to the repository such as audit entries and screening reports. In order for them to check in properly, choose default metadata for the content. For example, if a DoD installation level is chosen then the default metadata must include the *Cateogry or Folders* metadata field.
- Configure the installation: Before using the system, complete the installation steps outlined in Section 3.2, "Software Configuration."

- Configure the security settings: Determine the appropriate roles, rights, and user permissions to perform certain tasks. For details, see Chapter 5, "Setting Up Security."

The other configuration options on this page can be performed in any order. These options are discussed in the remainder of this chapter.

When finished setting configuration options, click **Submit**. To clear the options selected, click **Reset**.

3.4 Retention Management Options

The following list provides an overview of the steps needed to set up the retention software. The steps should be followed in the order given. For example, you must define triggers and periods before disposition rules, because when you define a category and its disposition rule, you include references to triggers and periods.

This checklist spans multiple sections of this guide. With the table of contents and index, this checklist also serves as a documentation road map for finding the information needed.

Tip: To record your actions while setting up and configuring the system, you may want to configure the audit trail first. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details. All user actions are set to be recorded by default.

Setup tasks include the following topics. Some of these tasks may be optional depending on your organization. The information is provided so you can determine if the step may be useful or not.

- Determine additional security settings. For overview information, see Section 3.5.2, "Classification Security Settings" and for details, see Chapter 6, "Additional Security Settings."
- Configure system settings. For an overview, see Section 3.6, "System-Wide Configuration" and the following sections for details:
  - For financial and accounting information, see Section 7.1.1, "Setting the Fiscal Calendar."
  - To define the time associated with retention or disposition of retained content, see Section 12.2, "Managing Time Periods."
  - To set up any custom fields required, see Section 13.2, "Managing Custom Metadata."
- Set up the retention schedule. For an overview, see Section 3.8, "Setting Up a Retention Schedule" and the following sections for details about configuring the organization of content. This includes:
  - Managing the view of different retention schedule hierarchies. For details, see Section 10.2.1, "Managing a Series."
  - Defining security settings and disposition instructions for that category. For details, see Section 10.3.1, "Managing Retention Categories."
  - Defining folders used in the retention schedule. For details, see Section 10.4.2, "Managing Record Folders."

- Determine how content will be handled. For overview information, see Section 3.9, "Configuring Content Triggers, Dispositions, and Freezes" and the following chapters for details:
  - Using triggers to initiate events affecting content. For details, see Section 11.2, "Managing Triggers."
  - Defining the sequence of actions to be performed on items during their life cycle. For details, see Chapter 14, "Defining Disposition Instructions."
  - Inhibiting disposition processing. For details, see Section 15.1.1, "Managing Freezes."
- Establish relationships between content. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about establishing links between content items.

Additional tasks discussed in the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* include importing and exporting archives and configuring the audit trail, which tracks activities. In addition, workflows can be created to track requests made under the Freedom of Information Act (FOIA) and Privacy Act (PA) if that software is enabled. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details.

After configuring the software, users with the appropriate rights can file, search, and link content and generate retention schedule reports. For more information, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

The core processing performed by records administrators during the use and maintenance phases of the content life cycle, such as screening and cycling content, is discussed in the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

3.5 Security Overview

Multiple layers of security are available to control access to content. Permissions and privileges are determined by the intersection of all security mechanisms in place. The strictest setting prevails. See Chapter 5, "Setting Up Security" for complete details.

This section discusses the following topics:

- Section 3.5.3, "Security Roles and Definitions"
- Section 3.5.1, "Security Settings"
- Section 3.5.4, "Rights for Roles"
- Section 3.5.2, "Classification Security Settings"

3.5.1 Security Settings

Overall security settings are configured on the Configure Retention Settings Page. The default values on that page are based on the installation level that was chosen. Security preferences set on that page are in addition to those provided with Oracle UCM. PCM security is set using the Oracle URM security measures.

Important: After your production environment is underway, we recommend you do not change the security settings for ACLs or the default Oracle UCM security. Doing so can cause unforeseen consequences.

To configure what security settings are enabled, choose **Records** then **Configure** then **Settings** from the Top menu. The Configure Retention Settings Page opens.

- To use Access Control List Security, select **ACL-based security**.
- To activate the default security, select **Default Content Server security on Categories, Folders, and Triggers**.
- (Required for DOD 5015.2 compliance): To use supplemental markings, select **Supplemental Marking**. For more information, see Section 6.1.1, "Supplemental Markings Details." To make users match all supplemental markings, select **User must match all Supplemental Markings**. To allow a user to match only one supplemental marking, deselect the checkbox.
- To create custom security fields, select **Custom Security Fields**.
- To use classified security, select **Classified Security**. For more information, see Section 6.2.1, "About Records Classification."

When done, click **Submit Update**.

3.5.2 Classification Security Settings

Supplemental markings, classifications, and classification guides provide further security and are used to organize documents that are considered classified, for either government or corporate purposes.

See Chapter 6, "Additional Security Settings" for complete details about additional security settings. This section covers the following topics:

- Section 3.5.2.1, "Supplemental Markings"
- Section 3.5.2.2, "Security Classifications"
- Section 3.5.2.3, "Classification Guides"

3.5.2.1 Supplemental Markings

To disable use of supplemental markings as a security feature, deselect the Supplemental Markings box on the Configure Retention Settings Page and do not assign the markings to users.

When supplemental markings are assigned to users, even if a user has access to a specific record folder, the supplemental marking further restricts access to record folders and content. In circumstances where a record folder or item has multiple supplemental markings, it can be required that a user match all assigned supplemental markings to access the item. When Match All is disabled, if a user matches just one of the multiple supplemental markings, the user can access the object.

Two special supplemental markings, Restricted and Formerly Restricted, can be used to disable the following classification-related metadata fields on the content check-in and metadata update pages:

- Declassify on event
- Declassify on date
- Downgrade instructions
- Downgrade on event
- Downgrade on date

You can enable and disable supplemental markings at any time. To enable markings, select **Supplemental Markings** on the Configure Retention Settings Page. See Chapter 6, "Additional Security Settings" for details.

3.5.2.2 Security Classifications

Security classification can be an additional way to restrict access to content by using supplemental markings and custom security fields.

Several classification features are available to handle and process classified content in accordance with the Chapter 4 requirements of the DoD 5015.2 specification. Several built-in classifications (Top Secret, Secret, and Confidential) are available, but custom classifications can also be created. For details, see Section 6.2.2.2, "Creating or Editing a Custom Security Classification."

Content is either classified, unclassified, or declassified. **Classified** content has an initial classification and a current classification. **Unclassified** content is not and has never been classified. **Declassified** content was formerly classified.

The standard security categories (classification scheme), from highest to lowest, are **Top Secret**, **Secret**, **Confidential**, and **No markings** (that is, unclassified).

Like supplemental markings, classified security can be enabled or disabled at any time. After enabling, custom security classifications can be created. If any additional security classifications are created, indicate the classification place within the marking hierarchy. For further information, see Section 6.2.2.3, "Setting the Order of Security Classifications."

To enable security, select **Classified Security** on the Configure Retention Settings Page. Click **Submit**.

Caution: Disabling classified security puts sensitive classified information at risk of being accessed by unauthorized people. After your classified security is in force, it is recommended that you do not disable it.

3.5.2.3 Classification Guides

Classification guides (and their associated topics) enable convenient implementation of multiple classification schemes. They are used to define default values for classification-related metadata fields on the content check-in page such as:

- Initial Classification: (xInitial Classification)
- Reason(s) for classification: (xClassificationReason)
- Declassify exemption category: (xDeclassifyExemptionCategory)
- Declassify on event: (xDeclassifyOnEventDescription)
- Declassify on date: (xDeclassifyOnDate)

Using classification guides makes checking in classified content easier and more consistent, with similar content having the same classification metadata. Classification guides can be further refined by adding topics within a guide. For complete details, see Section 6.4.2.4, "Creating or Editing a Classification Topic."

3.5.3 Security Roles and Definitions

The following security elements are used to define user roles and permissions:

- Predefined user roles, discussed in detail in Section 5.2, "Roles." Each of these predefined roles comes with a default set of permissions and rights, but these can be modified to suit specific needs. These include the following roles:
  - **rma**, generally assigned to basic users. It allows them to perform basic management tasks. In this documentation, Records User is a term used to designate the person given this role.
  - **rmalocalrecordsofficer**, generally assigned to users who need access to additional functionality (for example, creating triggers or folders, and modifying content attributes). In this documentation, Records Officer is a term used to designate a person given this role. In previous versions of this product, this was the Records Privileged role.
  - **rmaadmin**, generally assigned to administrators who set up and maintain the infrastructure and environment. In this documentation, Records Administrator is a term used to designate the person given this role.
  - **pcmrequestor**, generally assigned to users who have all the permissions assigned to basic users without a PCM role but are also granted additional rights to perform some functions not allowed for basic users (for example, making reservations for physical items). Users with the pcmrequestor role have read and write permissions (RW) for the special RecordsGroup security group. In this documentation, PCM Requestor is a term used to designate a person given this role.
  - **pcmadmin**, generally assigned to administrators who are responsible for setting up and maintaining the physical content management infrastructure and environment. These users have the widest range of rights to perform physical content management tasks (for example, setting up the storage space, editing and deleting reservations, and printing user labels). Users with the PCM Administrator role have read, write, delete, and admin permissions (RWDA) for the special RecordsGroup security group. In this documentation, PCM Administrator is a term used to designate a person given this role.
- **Rights** control access to functions assigned to user roles. The predefined roles have a default set of rights assigned to them, but the rights can be modified to restrict or expand their access to functions. For details, see Section 5.11, "Assigning Rights to User Roles."
- **Security groups** define security on a group of content. This software comes with a predefined security group called RecordsGroup. Users with the predefined Records User or Records Officer roles have read and write permission (RW) to the RecordsGroup security group. Users with the Records Administrator role have read, write, delete, and admin permission (RWDA) to this security group. For details, see Section 5.6, "Security Groups."
- **Access control lists** (ACLs) manage the security model on dispositions (ACLs are an optional feature available during configuration).ACLs can be assigned to folders, triggers, and retention categories. ACLs are used to control user and group access permissions for triggers, categories, and folders. The ACL can be assigned for each category, folder, and trigger that is created. For details, see Section 5.8, "Access Control Lists (ACLs)."

3.5.4 Rights for Roles

Rights define what actions users can perform on content items. To assign rights to user roles, choose **Admin Applets** from the **Administration** menu.

Click the **User Admin** icon and choose **Security** then **Permissions by Role** from the menu. Click the role to review or modify. Click **Edit RMA Rights** then set the appropriate rights by selecting checkboxes on the various tabs. Click **OK** when done.

For details, see Section 5.11, "Assigning Rights to User Roles."

3.6 System-Wide Configuration

This section describes configuration procedures used by administrators to set up the software. Certain configuration procedures described here and in other chapters may also apply to other users if they have been given the appropriate rights. The required rights for each procedure are described in Chapter 7, "Configuration Options," where these procedures are discussed in detail.

The following list highlights several tasks accomplished by using options on the Configure Retention Settings Page. To access that page, choose **Records** then **Configure** then **Settings** from the Top menu. For complete details about all the options, see Section 7.1, "Retention Options."

- Set the fiscal calendar used by the organization for financial and accounting purposes. Specify the start date of the fiscal year once, unless the fiscal start date changes or the start date varies from year to year.
- Configure e-mail notifications sent to users which indicate that items require a review or that a pending disposition event requires attention.
- Enable or disable user-friendly captioning. If disabled, standard DoD 5015 disposition are used on the Disposition Information page and Disposition Rule screen. The DoD screening query language is used in the Criteria boxes of the screening pages.

> **Note:** User-friendly captions are used on most of the screen depictions in this guide.

- Enable supplemental marking security on content, record folders, and users. For more information, see Section 6.1, "Supplemental Markings."
- Enable the classified security feature as required for agencies conforming to the Chapter 4 Classified Records section of DoD 5015.2 specification. This feature can also be used by corporations and other entities who use a classification scheme to designate specific items as important, secret, and so on. When enabled, the Security Classification Fields show on the Configure Retention Settings Page. Deselect this checkbox if it is not required.

3.7 Setting Up Physical Content Management

Several aspects of PCM should be set up in order to use the system. These include:

- Set up the required PCM user roles and rights as discussed in Section 3.5, "Security Overview."
- Configure the PCM environment including chargebacks, customers, and object types. See Chapter 8, "Configuring Physical Content Management".
- Define the storage space environment. See Chapter 9, "Setting Up PCM Storage Space".

- Define disposition rules for physical content, if required. See Chapter 15, "Setting Up Freezes".

See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about setting up barcodes and labels for processing reservations and invoices.

3.8 Setting Up a Retention Schedule

A retention schedule is an organized hierarchy of series, categories, and record folders used to cluster content into similar groups, each with its own retention and disposition characteristics.

This section discusses the tasks involved in setting up a retention schedule. It covers the following topics:

- Section 3.8.1, "Managing a Retention Schedule"
- Section 3.8.1.1, "Creating a Series"
- Section 3.8.1.2, "Creating a Retention Category"
- Section 3.8.1.3, "Creating a Record Folder"

3.8.1 Managing a Retention Schedule

Plan to set up separate retention schedules for those items that require different dispositions. It is simpler to track items when they are sorted into appropriate categories and the category following a disposition.

Content is filed directly into a retention category, and can optionally be filed into a record folder under a retention category. The retention schedule is the top-most series node. The top node is created automatically by the system. The remaining retention schedule objects (series, folder, or category) are created by the Records Administrator.

A series is an optional construct created by the Records Administrator. It does not contain content, but rather is a method of grouping like categories.

A retention category is required, and it contains disposition instructions for processing content. A record folder is optional, and it also organizes content according to common features.

For complete details about planning and implementing a retention schedule, see Chapter 10, "Setting Up a Retention Schedule."

3.8.1.1 Creating a Series

If an organization has many retention categories, setting up some series can assist with managing the view of the retention schedule hierarchies. Series can be nested within each other. Series are also useful for creating work-in-progress retention schedules because series can be hidden from users, which prevents users from filing any items into the hidden series. For details, see Section 10.2.1.1, "Creating or Editing a Series."

3.8.1.2 Creating a Retention Category

A retention category is a retention schedule object with defined security settings and disposition instructions. Retention categories cannot be nested within other retention categories. If ACLs (Access Control List) are on the retention category, the user must also be in the ACL to view or access the retention category.

For details, see Section 10.3.1.1, "Creating or Editing a Retention Category." For detailed instructions about disposition rules and disposition examples, see Chapter 14, "Defining Disposition Instructions."

Retention categories can be created at the root level.

3.8.1.3 Creating a Record Folder

Retained items have different metadata than regular content in the repository and are also associated with a disposition life cycle. A record folder organizes similar items within a retention category.

Multiple record folders can be stored in a category or can be nested within other folders. Record folders inherit disposition rules and security settings from their parent folder or category but can also have their own rules or settings. Supplemental markings can be set on a record folder and on users to further secure the record folder.

Record folders also inherit review information from their parent category. The review information that takes precedence is at the lowest node (the shortest review period prevails), as in the case of nested record folders.

Record folder objects are unique because the folders for temporary retained items are destroyed with the items. The record folders also have a life cycle paralleling that of their content. Record folders must be re-created on a regular basis, a practice that is not typically true of series or categories in the retention schedule.

For complete details about tasks involved in managing record folders, see Section 10.4.2, "Managing Record Folders." Also see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for other record folder task information.

Record folders cannot be created at the root level.

3.9 Configuring Content Triggers, Dispositions, and Freezes

Other retention elements can be configured to help manage content. Triggers are used to initiate the disposition of content in a specified way and at specified periods of time. Freezes can be applied to content as needed. Content can be kept frozen for specified amounts of time.

This section provides an overview of triggers, dispositions and freezes. For complete details, see Chapter 11, "Setting up Triggers,", Chapter 15, "Setting Up Freezes," and Chapter 14, "Defining Disposition Instructions."

This section covers the following topics:

- Section 3.9.1, "Triggers"
- Section 3.9.2, "Dispositions"
- Section 3.9.3, "Freezes"

3.9.1 Triggers

Two types of triggers can initiate disposition processing:

- System derived triggers are built-in triggers based on defined events such as a preceding action, retention period cutoff, or a change in content states.
- Custom triggers can be created by Records Administrators to define specific events. Three types of custom triggers can be defined:

- Global triggers, which occur at a defined time
- Custom direct triggers, which use metadata fields as triggering events
- Custom indirect triggers, which occur on a regular schedule

Custom triggers appear in the Triggering Events list of the Disposition Rules screen. For details about the different trigger types, see Section 11.2.1, "Creating or Editing a Trigger" and Chapter 14, "Defining Disposition Instructions."

3.9.2 Dispositions

Dispositions are predefined actions taken on content, usually for items no longer needed for current business. For details, see Chapter 15, "Setting Up Freezes."

A disposition is defined using instructions. An instruction usually follows this sequence:

```
When a triggering event occurs,
wait a specified rentention period,
then perform a specified disposition action.
```

Instructions are created within retention categories. Child folders and content items inherit dispositions from their parent retention category, but a disposition rule can be applied to a specific record folder only. Use the built-in disposition actions or create custom dispositions.

3.9.2.1 Disposition Types

The following types of dispositions are available:

- An *event disposition* is used if items are eligible for disposition when an event takes place. The event itself acts as a cutoff or closing occurrence.
- A *time disposition* has a fixed retention period and begins with a user-defined file cutoff. The retention period must transpire before the disposition instruction takes action on the content.
- A *time-event disposition* is a disposition instruction that begins with a specified triggering event. After the event has transpired, then the record folder or content item is cut off and the retention period is applied.

3.9.2.2 Triggering Events

A disposition instruction is activated when a triggering event occurs. Events can be split into general categories:

- Those based on a preceding action
- Those based on a content state
- Those based on an indirect trigger
- Those based on a custom trigger

Each category has several different events. For example, content states include the Activated triggering event, the Delete Approved triggering event, Superseded triggering event, No Longer Latest Revision triggering event, and so on.

For a complete list of triggering actions, see Section 14.4, "Triggering Events."

3.9.2.3 Retention Periods

The retention period is the interval of time after the triggering event before a disposition action is performed. Built-in period units are available or custom periods can be created. For details, see Section 12.2.1, "Creating or Editing a Custom Time Period."

3.9.2.4 Disposition Actions

A disposition action defines what happens after Triggering Events occur and Retention Periods, if any, have passed. Several built-in disposition actions are available or custom dispositions can be created.

Important: The software does not perform the disposition action itself; rather, it sends an e-mail notification to the person responsible for carrying out the action.

Actions can be separated into several categories:

- General Actions: These include archive, cutoff, delete old revisions, no action, and so on.
- Content Actions: These include Delete Previous Revision, Delete Revision, and so on.
- Record Actions: These include Accession, Destroy, Expire, and so on.
- Classified Actions: These include declassify, upgrade, or downgrade classification.

3.9.2.5 Disposition Rules

After configuring the types of dispositions, establish the rules used by the dispositions when evaluating content. Rules apply to all content and record folders in a category by default. A disposition rule that applies only to a specific record folder can also be created. For details about different types of rules, see Section 14.10, "Disposition Examples."

3.9.3 Freezes

Freezing content or a record folder inhibits disposition processing. In addition, metadata for the folder or item is also frozen.

You can predefine freeze types to better control the freeze/hold process. For details, see Chapter 15, "Setting Up Freezes."

4

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 glossary at the end of this book.

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.

4.1 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.

4.1.1 Configuring the System

Use the **Records** menu in the Top menu to access most aspects of Oracle URM. The exact menu options any user sees depend on the rights assigned to that user. 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 "Assigning Rights to User Roles" on page 5-18.

You can frequently perform actions from several different locations. For example, you can create a series within a series by clicking **Create Series** from the Page menu on the Series Information Page. Or you can click **Create Series** from the **Action** menu of a series listed on the Retention Schedule page. This documentation describes the most commonly used method of accessing tasks.

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

- **Rights**: Used to view a user's 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 a 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.
- **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 Adapters) where content is retained or tracked.

4.1.2 Configuring Reports

Use the Configure Reports Management Page to set up reports for retention tasks such as freezes, screening, and labels. Default reports can be used or custom 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 the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about reports and their configuration.

4.1.3 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 also allows the addition 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.

4.2 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 allowing access to information pages for folders, 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.

4.3 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, customizing what users will see. Additional options may appear depending on profiles created at the site and the choices made during configuration.

These menu options can be used to help quickly narrow down 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.

The options on this menu help a user narrow a search by selecting new fields from those already selected, or to save the search under a file name for use later. See the *Oracle Fusion Middleware User's Guide for Content Server* for more details about searching and saving query results.

See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about creating and using profiles.

5

Setting Up Security

Multiple layers and types of security are available in Oracle URM, including roles, rights, security groups, and access control lists. As with the standard Oracle UCM security model, the final determination of permissions and privileges is determined by the intersection of all security mechanisms in place.

Access control lists and supplemental markings are required for compliance with the DoD 5015.2 specification. Classification levels are required for compliance with Chapter 4 of DoD 5015.2. Custom security fields can be created and additional security added to individual fields. See Chapter 6, "Additional Security Settings" for details.

You can also use the accounts security model in addition to the options provided by the system. For more information about the account security model, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*. See "Fusion Middleware Security Considerations" on page 3-2 for details about user roles, accounts, and permission considerations.

This section covers the following topics:

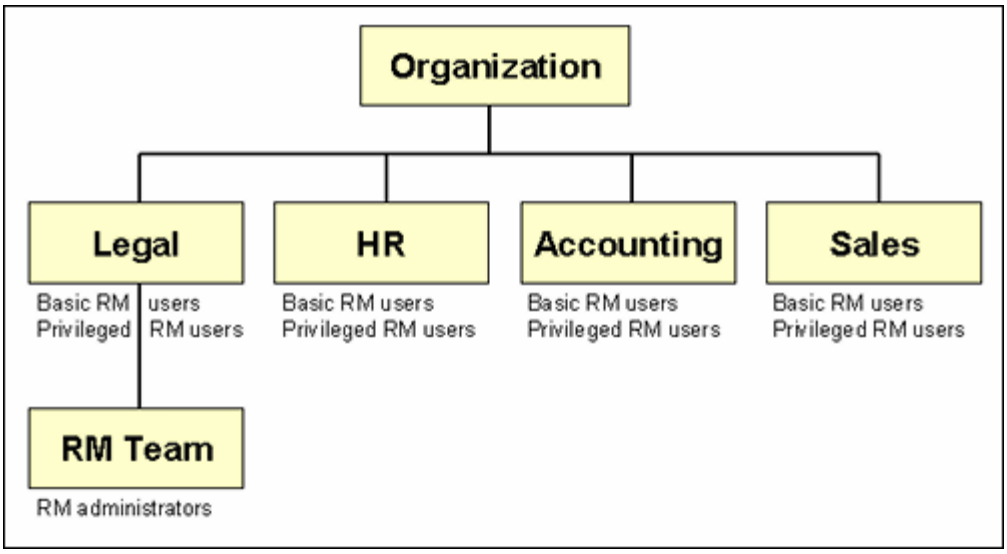
Concepts

Tasks

5.1 Retention Management in an Organization

The figure below shows a typical retention management structure in an organization.

Figure 5–1 Typical Retention Management Organization



Most people in the various departments of an organization can file content or check in content items, search for items, and view them. These are basic Records Users.

A much smaller group of people ("privileged users") is typically granted rights to perform some additional functions not allowed for basic users (for example, altering classifications or creating triggers or retention schedules). These are people with the Records Officer right.

A very limited number of people are administrators, who are typically responsible for setting up and maintaining the management infrastructure. Records Administrators have the widest range of rights to perform management tasks. For example, they can usually perform *all* and disposition actions, including those assigned to others. The administrators are often in the legal department of an organization, which can drive the efforts for effective and efficient management.

The software comes with predefined management roles called 'rma', 'rmalocalrecordsofficer', and 'rmaadmin', designated in the documentation as Records User, Records Officer, and Records Administrator. Each of these standard roles provides a default set of permissions and rights, which coincide with the typical responsibilities of basic users, privileged users, and administrators, respectively. However, these roles can easily be modified to suit specific management needs. New roles can be created with assigned management rights or different management rights can be given to existing roles.

Users without specific rights can still apply life cycles to content items.

Important: Record management consists of more than just software. You also need to have the appropriate organizational structures and policies in place in your organization.

5.2 Roles

The system comes with predefined user roles, discussed in detail in "Security Groups" on page 5-15:

- **rma** (denoted as "Records User" in this documentation): This role is generally assigned to basic users and allows them to perform basic management tasks. Users

with this role have read permission (R) to the Public security group, and read and write permission (RW) to the special Record Group security group.

- **rmalocalrecordsofficer** (denoted by "Records Officer" in this documentation): This role is generally assigned to "privileged" users, who have all the permissions assigned to basic users (‘rma’ role) but are also granted rights to perform additional functions (for example, creating triggers or folders, and modifying content attributes).

  Users with the this role have read permission (R) to the Public security group, and read and write permission (RW) to the special Records Group security group.

- **rmaadmin** (denoted by "Records Administrator" in this documentation): This role is generally assigned to administrators who are responsible for setting up and maintaining the management infrastructure and environment.

  These users have the widest range of rights to perform management tasks (for example, defining users in this role to have read permission (R) to the Public security group, and read, write, delete, and write permission (RWDA) to the special Records Group security group). The Records Administrator can create variations to provide a fine level of granularity in security. In this documentation, only the default roles or Records Administrator, Records Officer, or Records User are discussed.

If Physical Content Management is enabled, the following roles are also available:

- **pcmrequestor** (denoted by "PCM Requestor" in this documentation): This role is generally assigned to users who have all the permissions assigned to basic users without a PCM role but are also granted additional rights to perform some functions not allowed for basic users (for example, making reservations for physical items). Users with the 'pcmrequestor' role have read and write permissions (RW) for the special RecordsGroup security group.
- **pcmadmin** (denoted by "PCM Administrator" in this documentation): This role is generally assigned to administrators who are responsible for setting up and maintaining the physical content management infrastructure and environment. These users have the widest range of rights to perform physical content management tasks (for example, setting up the storage space, editing and deleting reservations, and printing user labels). Users with the 'pcmadmin' role have read, write, delete, and admin permissions (RWDA) for the special RecordsGroup security group.

  The PCM Administrator can create variations to provide a fine level of granularity in security. In this documentation, only the default roles or PCM Administrator or PCM Requestor are discussed.

  If users have no PCM role assigned to them, they can still search for physical items.

Note that Physical Content Management is treated as an ’external’ source, just as an adapter is treated. Therefore, if Physical Content Management is enabled, two additional roles are created. Those roles are not discussed in this documentation because the tasks associated with those roles are not discussed here but should be discussed in the appropriate adapter documentation.

- **ermrequestor**: This role is generally assigned to users who can read, edit, or create content on the external source.
- **ermadmin**: This role is generally assigned to administrators who can read, edit or delete content on the external source.

Each of these predefined roles comes with a default set of permissions and rights, but these can be modified to suit specific needs. New roles and management rights can be created. This functionality enables provides the opportunity for a very granular security model.

Role permissions are additive, just as in Oracle UCM. If your organization uses accounts, the accounts are a hierarchical overlay to your current security model.

Access to the majority of functions is controlled by rights assigned to user roles. The predefined management roles each have a default set of rights assigned to them, but the roles can easily be modified to restrict or expand their access to management functions (see "Assigning Rights to User Roles" on page 5-18 for details).

To see what roles are assigned to a user, click the user name in the top upper right corner of the screen. The roles assigned to the logged-in user are displayed at the top of the User Profile information.

To see rights assigned to the logged-in user, click **Records** then **Rights** from the Top menu. The Assigned Rights Page is displayed. This screen shows the rights assigned to the current user for the enabled components. To view details about each component, click the **Show** link for that component.

To view details about all rights, click the **Show All Rights** link at the top of the screen. To hide rights again, click the **Hide** link in the component section or at the top of the screen.

For information about adding new roles and assigning roles to users, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

5.3 Tasks and Default Rights for Roles

If the Related Content component is enabled, the Record.CreateLink and Record.Unlink rights are set by default for users.

The ability to browse and view the retention schedule not only depends on assigned rights, but also on any other applied security features, such as supplemental markings and access control lists (ACLs). See Chapter 10, "Setting Up a Retention Schedule" for details about retention schedules. See Chapter 6, "Additional Security Settings" and "Access Control Lists (ACLs)" on page 5-16 for further details.

The following sections give more detailed information about common tasks that can be performed and the rights required to perform each task. See each designated chapter for further details about the specific permissions required for individual tasks.

See Appendix B, "Summary of Security Rights and Roles" for this information presented in tabular form.

Important: This section describes the default configuration. The security model is highly customizable, which means it can be modified to suit the needs of your specific environment.

5.3.1 Trigger Tasks and Defaults for Predefined RM Roles

For more information about triggers, see Chapter 11, "Setting up Triggers".

- To **view information** about triggers, the Admin.Triggers right or the Admin.RecordManager right is required. These rights are assigned by default to the Records Officer and Records Administrator roles.

- To **create a trigger** or **edit a trigger**, the Admin.RecordManager right is required to perform these tasks. This right is assigned by default to the Records Officer and Records Administrator roles.
- To **delete a trigger**, the Admin.Triggers right *and* Delete permission for the trigger's security group is required. This right is assigned by default to the Records Officer (delete permission not granted by default) and Records Administrator roles.

5.3.2 Time Period Tasks and Defaults for Predefined Roles

For more information, see Chapter 12, "Configuring Time Periods".

- To **view information** about time periods, the Admin.Triggers or Admin.RecordManager is required. These rights are assigned by default to the Records Officer and Records Administrator roles.
- To **create**, **edit**, or **delete** a time period, the RM Admin.RecordManager right is required. This right is assigned by default to the Records Administrator role.

5.3.3 Supplemental Markings Tasks and Defaults for Predefined Roles

For more details, see Chapter 6, "Additional Security Settings".

- To **view information** about supplemental markings, the Admin.Triggers or Admin.RecordManager right is required. These rights are assigned by default to the Records Officer and Records Administrator roles.
- To **create**, **enable**, **disable**, **edit**, or **delete** a supplemental marking, the Admin.RecordManager right is required. This right is assigned by default to the Records Administrator role.

5.3.4 Security Classifications Tasks and Defaults for Predefined Roles

For more information, see Chapter 6, "Additional Security Settings".

The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform the following tasks involving classification. These rights are assigned by default to the Records Administrator role.

- **Enable** security classification
- **Disable** security classification
- **Create** security classifications
- **Edit** security classifications
- **Delete** security classifications
- **Reorder** security classifications

5.3.5 Classification Guides Tasks and Defaults for Predefined Roles

For more information, see "Classification Guides" on page 6-24

The Admin.ClassificationGuide right is required to perform these tasks involving classification guides. This right is assigned by default to the Records Administrator role.

- **View information** about classification *guides*
- **Create** classification *guides*

- **Edit** classification *guides*
- **Delete** classification *guides*
- **View** information about classification *topics*
- **Create** classification *topics*
- **Edit** classification *topics*
- **Delete** classification *topics*

5.3.6 Custom Security Tasks and Defaults for Predefined Roles

For more information, see Chapter 6, "Additional Security Settings".

- To **view information** about custom security fields, the Admin.Triggers or Admin.RecordManager right is required. These rights are assigned by default to the Records Officer and Records Administrator roles.
- To **create**, **enable**, **disable**, **edit**, or **delete** a custom security field, the Admin.RecordManager right is required. This right is assigned by default to the Records Administrator role.

5.3.7 Custom Category or Folder Metadata Tasks and Defaults for Predefined Roles

For more information, see Chapter 13, "Creating Custom Metadata".

The Admin.RecordManager right is required to perform these tasks involving custom category or folder metadata. This right is assigned by default to the Records Administrator role.

- **Create** a custom category or folder metadata field
- **Edit** a custom category or folder metadata field
- **Delete** a custom category or folder metadata field

5.3.8 Freezes Tasks and Defaults for Predefined Roles

For more information, see Chapter 15, "Setting Up Freezes".

The Admin.RecordManager right is required to perform these tasks involving freezes. This right is assigned by default to the Records Administrator role.

- **View information** about freezes.
- **Create** a freeze.
- **Edit** freezes.
- **Send e-mail notifications** about freezes.
- To **delete a freeze**, the Admin.RecordManager right *and* Delete permission for the freeze's security group is required. This right is assigned by default to the Records Administrator role.

5.3.9 Series Tasks and Defaults for Predefined Roles

For more information, see "Using a Series" on page 10-10.

- To **browse/view information** about series, the Series.Read right is required. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.

- To **create** a series, the RM Series.Create right is required. This right is assigned by default to the Records Administrator role.
- To **edit** a series, the RM Series.Edit right is required. This right is assigned by default to the Records Administrator role.
- To **hide** or **unhide** a series, the RM Series.Hide/Unhide right is required. This right is assigned by default to the Records Administrator role.
- To **move** a series, the RM Series.Move right is required. This right is assigned by default to the Records Administrator role.
- To **delete** a series, the RM Series.Delete right is required. This right is assigned by default to the Records Administrator role.

5.3.10 Retention Category Tasks and Defaults for Predefined Roles

For more information, see "Retention Categories" on page 10-13.

- To **browse/view information** about a category, the Category.Read right is required. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.
- To **create** a category, the RM Category.Create right is required. This right is assigned by default to the Records Administrator role.
- To **edit** a category, the RM Category.Edit right is required. This right is assigned by default to the Records Administrator role.
- To **edit review information** for a category, the RM Category.EditReview right is required. This right is assigned by default to the Records Administrator role.
- To **move** a category, the RM Category.Move right is required. This right is assigned by default to the Records Administrator role.
- To **delete** a category, the RM Category.Delete right is required. This right is assigned by default to the Records Administrator role.
- To **apply/reapply disposition rules** to specific/all content in a retention category, the RM Category.Edit right is required. This right is assigned by default to the Records Administrator role.

5.3.11 Folder Tasks and Defaults for Predefined Roles

For more information, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The Folder.Read right is required to perform these tasks involving folders. These rights are assigned by default to all Records roles.

- **Browse and view information** about record folders.
- **View the life cycle** of a record folder.
- **View the review history** of a record folder.
- **View the metadata history** of a record folder.

The following tasks can be performed for record folders:

- To **create** a folder, the Folder.Create right is required. It is assigned by default to the Records Officer and Records Administrator roles.
- To **edit** a folder (if the user is the author of that folder), the Folder.EditIfAuthor right is required. It is assigned by default to the Records Officer role.

- To **edit the review information** of a record folder, the Folder.EditReview right is required. It is assigned by default to the Records Officer and Records Administrator roles.
- To **delete** a record folder, the Folder.Delete right is required. It is assigned by default to the Records Officer and Records Administrator roles.
- To **close/unclose** a folder, the Folder.Open/Close right is required. It is assigned by default to the Records Officer and Records Administrator roles.
- To **freeze/unfreeze** a folder, the Folder.Freeze/Unfreeze right is required. This right is assigned by default to the Records Administrator role.
- To **undo the cutoff** of a folder, the Folder.UndoCutoff right is required. This right is assigned by default to the Records Administrator role.
- To **review a folder**, the Admin.PerformPendingReviews right is required.It is assigned by default to the Records Officer and Records Administrator roles.

The Folder.Edit right is required to perform these tasks involving folders. This right is assigned by default to the Records Administrator role.

- **Edit** a folder (if the user is not the author of that folder).
- **Move** a record folder
- **Cancel** a record folder
- **Expire** a record folder
- **Rescind** a record folder
- Make a record folder **obsolete**
- **Undo the obsolete status** of a record folder

The Category.Edit right is required to perform these tasks involving folders. This right is assigned by default to the Records Administrator role.

- **Apply a disposition rule** to a **specific** record folder
- **Apply a disposition rule** to all record folders

5.3.12 Archive Tasks and Defaults for Predefined Roles

For more information about archiving, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The Admin.RetentionSchedulesArchive and other rights for specific items in the import or export are required to **import or export an archive**. This right is assigned by default to the Records Administrator role.

5.3.13 Screening Tasks and Defaults for Predefined Roles

For more information about screening, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The Admin.Screening right is required to perform these tasks involving screening. This right is assigned by default to the Records Administrator role.

- **Enable/disable** advanced screening
- **Screen retention categories**
- **Screen record folders**

- **Screen content**

The Admin.RecordManager right is required to **enable/disable user-friendly screening** captions. This right is assigned by default to the Records Administrator role.

5.3.14 Audit Trail Tasks and Defaults for Predefined Roles

For more information about using the audit trail, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The Admin.Audit right is required to perform these tasks involving audit trails. This right is assigned by default to the Records Administrator role.

- **Configure** the audit trail
- **Generate and view** an audit trail
- **Search with** audit trails
- **Set default metadata** for checking in audit trails
- **Check in and archive** audit trails (with the addition of Admin.RecordManager right)
- **Search** archived audit trails

The Admin.SelectMeta right is required to **select what metadata fields to include** in the audit trail. This right is assigned by default to the Records Administrator role.

5.3.15 Disposition Tasks and Defaults for Predefined Roles

For more information about disposition tasks, see Chapter 14, "Defining Disposition Instructions".

The following rights are assigned by default to the Records Administrator role.

- To **view disposition information**, the Category.Read right is required.
- To **enable/disable user-friendly disposition captions**, the Admin.RecordManager right is required.
- To **create** disposition rules, the Category.Create right is required.
- To **edit** disposition rules, the Category.Edit right is required.
- To **delete** disposition rules, the Category.Delete right is required.

5.3.16 Link Tasks and Defaults for Predefined Roles

For more information about linking and link types, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

The Admin.ConfigureLinkTypes right is required to perform these tasks involving links. This right is assigned by default to the Records Administrator role.

- **Add** custom link types
- **Edit** custom link types
- **Delete** custom link types

To **create or remove links** between content items, the Record.CreateLink or Record.Unlink right is required. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.

5.3.17 Default Report Tasks and Defaults for Predefined Roles

For more information about reports, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* .

The Admin.Reports right is required to perform these tasks. This right is assigned by default to the Records Administrator role.

- Create a **user/group** report
- Create a **role** report
- Create a **group** report

5.3.18 Content Management Tasks and Defaults for Predefined Roles

For more information about managing content, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The Record.Read right is required to perform these tasks. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.

- **Download** an item for viewing
- **Search** for content items
- **View information** about a content item
- **View the life cycle** of a content item
- **View the review history** of a content item
- **View the metadata history** of a content item
- **View the classification history** of a content item

The Record.Edit right is required to perform these tasks involving content. This right is assigned by default to the Records Officer and Records Administrator roles.

- **Review the classification** of a content item
- **Cancel** a content item
- **Expire** a content item
- **Rescind** a content item
- Make a content item **obsolete**
- **Undo the obsolete status** of a content item
- **Remove a supplemental marking** from a content item
- **Move** an item to another category or folder.

The following rights are required to perform the following tasks:

- To **edit metadata before a cutoff**, the Record.UndoCutoff right is required. Users can edit metadata for content items after cutoff and before cutoff. It is assigned by default to the Records Administrator role.
- To **upgrade or downgrade the security classification** of an item, the Record.Upgrade/Downgrade right is required. It is assigned by default to the Records Officer and Records Administrator roles.
- To **review** a content item, the Admin.PerformPendingReviews right is required. This right is assigned by default to the Records Officer, Records User and Records Administrator roles.

- To **undo the cutoff** of a content item, the Record.UndoCutoff right is required. It is assigned by default to the Records Administrator role.
- To **undo the status** of a content item, the Record.UndoRecord right is required. It is assigned by default to the Records Administrator role.
- To **edit the review information** for a content item, the Record.EditReview right is required. This right is assigned by default to the Records Officer, Records User, and Records Administrator roles.
- To **delete the metadata history** of a content item, the Record.DeleteHistoryFile right is required. This right is assigned by default to the Records Officer and Records Administrator roles.
- To **create** or check in a content item, the Record.Create right is required. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.
- To **link or unlink** content items, the Record.CreateLink or Record.Unlink right is required. This right is assigned by default to the Records User, Records Officer, and Records Administrator roles.
- To **delete** a content item, the Record.Delete right is required. This right is assigned by default to the Records Administrator role.
- To **freeze or unfreeze** a content item, the Record.Freeze/Unfreeze right is required. This right is assigned by default to the Records Administrator role.

5.3.19 Customization Tasks

The Rma.Admin.Customization right is required to perform the following tasks. This right is not assigned by default to any role. A detailed knowledge of services and their uses is required to perform these tasks. See Appendix C, "Customizing Your System" for more details.

- **Define custom dispositions**
- **Define custom barcode actions**
- **Define custom reports**

5.3.20 Other Common Tasks

The Admin.RecordManager right is required for these tasks. This right is assigned by default to the Records Administrator role.

- **Set the fiscal calendar**
- **Perform disposition actions** (processing events)
- **Specify the default recipient(s)** for notifications

5.4 Common Physical Content Management Tasks and Roles

Access to the majority of Physical Content Management (PCM) functions is controlled by rights assigned to Oracle UCM or Oracle URM roles. The two predefined physical content management roles (PCM Requestor and PCM Administrator) each have a default set of rights assigned to them, but the roles can easily be modified to restrict or expand their access to physical content management functions. New roles can be created with specific physical content management rights assigned to them.

5.4.1 Storage Space Tasks and Defaults for Predefined Roles

For more information about storage, see Chapter 9, "Setting Up PCM Storage Space".

The following rights are required to perform the following tasks:

- To **view information about storage locations**, the PCM.Storage.Read right is required. It is assigned by default to the PCM Requestor and PCM Administrator roles.
- To **create individual storage locations**, the PCM.Storage.Create right is required. This right is assigned by default to the PCM Administrator role.
- To **create storage locations in batches**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.
- To **edit storage locations**, the PCM.Storage.Edit right is required. This right is assigned by default to the PCM Administrator role.
- To **delete storage locations**, the PCM.Storage Delete right is required. This right is assigned by default to the PCM Administrator role.
- To **reserve storage locations**, the PCM.Storage.Reserve right is required. This right is assigned by default to the PCM Requestor and PCM Administrator roles.
- To **block storage locations**, the PCM.Storage.Block right is required. This right is assigned by default to the PCM Administrator role.
- To **print labels for storage locations**, the PCM.Admin.PrintLabel right is required. This right is assigned by default to the PCM Administrator role.
- To **import batch-created storage hierarchy**, the Admin.RetentionScheduleArchive right is required. This right is not assigned by default to any predefined role.

5.4.2 Reservation Tasks and Defaults for Predefined Roles

For more information about reservations, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights are required to perform the following tasks:

- To **view reservation information about physical items**, the PCM.Reservation.Read right is required. This right is assigned by default to the PCM Requestor and PCM Administrator roles.
- To **create a reservation request**, the PCM.Reservation.Create right is required. This right is assigned by default to the PCM Requestor and PCM Administrator roles.
- To **edit a reservation request**, the PCM.Reservation.Edit right is required. This right is assigned by default to the PCM Administrator role.
- To **delete a reservation request**, the PCM.Reservation.Delete right is required. This right is assigned by default to the PCM Administrator role.
- To **process a reservation request**, the PCM.Reservation.Process right is required. This right is assigned by default to the PCM Administrator role.
- To **run request reports**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.
- To **configure default metadata for reservations**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.

5.4.3 Physical Item Tasks and Defaults for Predefined Roles

For more information about physical items, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights are required to perform the following tasks:

- To **view information about physical items**, the PCM.Physical.Read right and PCM.Storage.Read rights are required. These rights are assigned by default to the PCM Requestor and PCM Administrator roles.
- To **create (check in) physical items**, the PCM.Physical.Create and PCM.Storage.Read rights are required. These rights are assigned by default to PCM Requestor and PCM Administrator roles.
- To **edit physical items**, the PCM.Physical.Edit and PCM.Storage.Read rights are required. These rights are assigned by default to PCM Requestor and PCM Administrator roles.
- To **move physical items**, the PCM.Physical.Edit, PCM.Physical.Move, and PCM.Storage.Read rights are required. These rights are assigned by default to the PCM Administrator role.
- To **delete physical items**, the PCM.Physical.Delete and PCM.Storage.Read rights are required. These rights are assigned by default to the PCM Administrator role.
- To **search for physical items**, the PCM.Physical.Read and PCM.Storage.Read rights are required. These rights are assigned by default to the PCM Requestor and PCM Administrator roles.
- To **print labels for physical items**, the PCM.Admin.PrintLabel right is required. This right is assigned by default to the PCM Administrator role.
- To **freeze or unfreeze physical items**, the Record.Freeze/Unfreeze right is required. This right is not assigned by default to any role.
- To **manually override external freeze errors**, the Admin.PerformActions right is required. This right is not assigned by default to any role.
- To **screen for physical items**, the Admin.Screening right is required. This right is not assigned by default to any role.

5.4.4 Location, Object, and Media Types Tasks and Defaults for Predefined Roles

For more information about locations, objects, and media, see Chapter 8, "Configuring Physical Content Management".

The following rights are required to perform the following tasks:

- To **set up location types**, the PCM.Admin.Manager and PCM.Admin.LocationTypes rights are required. These rights are assigned by default to the PCM Administrator role.
- To **set up object types**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.
- To **set up media types**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.
- To **set up custom metadata fields**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.

5.4.5 Chargeback Tasks and Defaults for Predefined Roles

For more information about chargebacks, see Chapter 8, "Configuring Physical Content Management" and the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights are required to perform the following tasks:

- To **set up chargeback types, payment types, and customers**, the PCM.Admin.Manager and CBC.ChargeBacks.Admin rights are required. These rights are assigned by default to the PCM Administrator role.
- To **view information on chargeback-related items (transactions, invoices, and so on)**, the PCM.Admin.Manager, CBC.ChargeBacks.Admin, and CBC.ChargeBacks.Read rights are required. These rights are assigned by default to the PCM Administrator role.
- To **create chargeback-related items (transactions, invoices, and so on)**, the PCM.Admin.Manager, CBC.ChargeBacks.Admin, and CBC.ChargeBacks.Read rights are required. These rights are assigned by default to the PCM Administrator role.
- To **edit chargeback-related items (transactions, invoices, and so on)**, the PCM.Admin.Manager, CBC.ChargeBacks.Admin, and CBC.ChargeBacks.Edit rights are required. These rights are assigned by default to the PCM Administrator role.
- To **delete chargeback-related items (transactions, invoices, and so on)**, the PCM.Admin.Manager, CBC.ChargeBacks.Admin, and CBC.ChargeBacks.Delete rights are required. These rights are assigned by default to the PCM Administrator role.
- To **screen for charges**, the PCM.Admin.Manager and CBC.ChargeBacks.Admin rights are required. These rights are assigned by default to the PCM Administrator role.
- To **browse invoices**, the PCM.Admin.Manager and CBC.ChargeBacks.Admin rights are required. These rights are assigned by default to the PCM Administrator role.
- To **print invoices**, the PCM.Admin.Manager and CBC.ChargeBacks.PrintInvoice rights are required. These rights are assigned by default to the PCM Administrator role.
- To **adjust invoices (for example, to manually change invoice amounts)**, the PCM.Admin.Manager and CBC.ChargeBacks.Adjust rights are required. These rights are not assigned by default to any role.

5.4.6 Barcode and Label Tasks and Defaults for Predefined Roles

For more information about barcodes, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights are required to perform the following tasks:

- To **process barcode files**, the PCM.Barcode.Process right is required. This right is assigned by default to the PCM Administrator role.
- To **print labels for users**, the PCM.Admin.PrintLabel right is required. This right is assigned by default to the PCM Administrator role.
- To **print storage location labels**, the PCM.Admin.PrintLabel right is required. This right is assigned by default to the PCM Administrator role.

- To **print physical location labels**, the PCM.Admin.PrintLabel right is required. This right is assigned by default to the PCM Administrator role.

5.4.7 Additional PCM Administrative Tasks and Defaults for Predefined Roles

For more information about PCM administration, see Chapter 8, "Configuring Physical Content Management".

The following rights are required to perform the following tasks:

- To **configure the environment**, including enabling or disabling the use of Offsite Storage, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.
- To **run batch services**, the PCM.Admin.Manager right is required. This right is assigned by default to the PCM Administrator role.

5.5 External Source Management Tasks and Roles

The following tasks and roles are used when managing external sources (adapters).

5.5.1 External Source Tasks and Defaults for Predefined Roles

For more information about adapters, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights are required to perform the following tasks:

- To **read external items**, the ECM.External.Read right is required. This right is assigned by default to the ERM Requestor and ERM Administrator roles.
- To **create an external item**, the ECM.External.Create right is required. This right is assigned by default to the ERM Requestor and ERM Administrator roles.
- To **edit an external item**, the ECM.External.Edit right is required. This right is assigned by default to the ERM Administrator role.
- To **delete an external item**, the ECM.External.Delete right is required. This right is assigned by default to the ERM Administrator role.
- To **perform administrative functions involving the external source**, the ECM.External.Admin right is required. This right is assigned by default to the ERM Administrator role.

5.6 Security Groups

A security group defines security for a group of content. Oracle URM is shipped with a predefined security group called "RecordsGroup." This group defines security for a group of content designated as that being tracked and/or retained.

Users with the predefined Records User, Records Officer, or Records Administrator roles have read and write permission (RW) to the RecordsGroup security group. Users with the Records Administrator role have read, write, delete, and admin permission (RWDA) to this security group.

Note: Even though the default Records User and Records Officer roles appear to be identical, they are not. The default Records Officer role has subadministrator access to certain administrator functions that the default Records User role does not (for example, creating triggers and folders). For details about rights that can be assigned to roles, see "Tasks and Default Rights for Roles" on page 5-4.

5.7 Aliases

When the product software is enabled, several aliases are created to help administrators manage large groups of people. Although the aliases are created, no default users are added to those groups. An administrator should add users as needed to the following alias lists:

- OffSiteRequestReviewGroup
- ReservationGroup
- DispositionReviewGroup

Several default aliases are also created if the FOIA/PA functionality is enabled. Default users are added to those alias lists but the users themselves are not created automatically. An administrator will need to create those users and assign appropriate permissions to them:

- FOIAOfficers
- FOIAProcessors
- FOIASpecialists
- JAG

5.8 Access Control Lists (ACLs)

Important: Enabling or disabling ACLs affects existing ACL settings system-wide. For example, if ACLs are enabled in Oracle UCM and Oracle URM is configured to one of the DoD settings (which re-enables ACLs), the Oracle UCM ACLs are overridden. And if the **Typical** or **Minimal** Oracle URM settings are used, ACLs are disabled because ACL-based security is not enabled by default for those options. It is enabled by default for the **DoD** options.

Access control lists (ACLs) are intended to manage the security for dispositions. ACLs can be assigned to the following retention schedule components:

- triggers
- retention categories
- record folders

ACLs can be used to control user and group access permissions for triggers, categories, and record folders. ACLs can be assigned for each category, folder, and trigger.

Be aware that searching for items takes more time when using ACLs because the permissions are checked on all parent folders and categories.

If not required, consider disabling ACLs for faster search retrieval performance. The default security, custom security fields, and supplemental markings provide excellent security.

5.8.1 Setting ACLs During Software Use

ACLs for individual users and groups and aliases can be adjusted while setting up elements of Oracle URM. Not all procedures allow the setting of all three types of permissions. The following procedure can be followed to adjust ACLs regardless of which type of permission are being set (user, group, or alias).

1. In the Group, User, or alias permission section of the Access Control Edit Section of the page in use, begin typing the user name of the person to add. A list appears and the user can be selected. Or type two asterisks (**) in the name field or group field. A list of users and groups appears.
2. Scroll to the name to use and click **Add User**, **Add Alias** or **Add**.
3. To the right of the displayed name is a grouping of permissions. Click on a permission to add or remove it.
4. To remove a user or group from the permissions box, click the **X** next to the name.

5.9 Security Matrix

The table below shows a matrix of content and retention schedule components, and the corresponding permissions for each predefined role. Supplemental markings have the most restrictive access capabilities. See Chapter 6, "Additional Security Settings" for details.

Objects and Retention Schedule Components	Subject to Additional Security of Type	Records User (rma)	Records Officer (recordsofficer)	Records Administrator (rmaadmin)
Content Items	Rights; supplemental markings; custom security field; ACLs	RW	RW	RWDA
Folders	Rights; supplemental markings; ACLs	R	RWD	RWD
Categories	Rights; supplemental markings; ACLs	R	R	RWD
Series	Rights	R	R	RWD
Triggers	Rights; ACLs		RW RWD permission required to delete triggers.	RWDA Only custom triggers can be deleted.
Periods	Rights		R	RWD Only custom periods can be deleted.
Supplemental markings	Rights			RWD
Classification guides	Rights			RWD

5.10 Setting Security Preferences

Security preferences are set on the Configure Retention Settings Page. The security preferences set on that page are in addition to those provided with Oracle UCM. The available security depends on what type of installation was chosen (for example, Minimal or a DoD setting).

Important: After your production environment is underway, it is recommended that you do not change the security settings for ACLs or the default security.

To configure security settings, complete the following steps:

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

   The Configure Retention Settings Page is displayed. If necessary, click the plus icon (+) to expand the Security section on the page.

2. (Optional based on the security model): To make use of Access Control List Security, click the **ACL-based security** box.

3. (Recommended): To activate the default security inherent in Universal Content Management for extra security on categories, folders, and triggers, click the **Default Content Server security on Categories, Folders, and Triggers** box. To not set the additional security, clear the box.

4. (Required for DOD 5015.2 compliance): To use supplemental markings, click the **Supplemental Marking** box.

5. (Optional based on the security model): To make users match all supplemental markings on a record folder, click the **User must match all Supplemental Markings** box. This is the most restrictive setting for supplemental markings. To allow a user to match only one supplemental marking to a folder to access its content or a content item (in the case of multiple supplemental markings), clear the box. For more information, see "Supplemental Markings Details" on page 6-2.

6. (Optional): To create custom security fields at the content field level to further restrict users, click the **Custom Security Fields** box. To not use custom security fields, clear the box.

7. (Optional): To use classified security, click the **Classified Security** box. To not use classified security fields, clear the box. For more information, see "About Records Classification" on page 6-9.

8. Click **Submit Update**. A message is displayed saying the settings have been configured successfully.

5.11 Assigning Rights to User Roles

The system is shipped with several predefined roles. Each of these roles has several default rights, which define what users with that role are allowed to do. For further details about roles and their default rights, see "Tasks and Default Rights for Roles" on page 5-4 and "Common Physical Content Management Tasks and Roles" on page 5-11.

5.11.1 Setting Rights for Roles

Rights define what actions users are allowed to perform. To assign rights to user roles, complete the following steps:

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. Choose **Security** then **Permissions by Role** from the menu.

4. Select the role to review or modify. Click **Edit RMA Rights** or **Edit ECM Rights** for PCM.

   The appropriate Edit Rights Page is displayed.

5. Set the rights by selecting or clearing the boxes on the various tabs.

6. Click **OK** when done.

7. Click **Close** to exit the Permissions by Role screen.

5.12 Default Rights for Roles

This section describes the features of the Edit Rights screen, and the default rights for each of the predefined roles.

Some of the rights are interconnected. Enabling or disabling certain options automatically enables or disables other options. For example, if you disable the Record.Create option on the Record tab, some of the other options on that tab are disabled as well. Conversely, if you enable the Category.Create option on the Category tab and the Category.Read option is not yet enabled, it will be enabled automatically.

5.12.1 The Series Tab

For more information, see "Using a Series" on page 10-10.

The following rights appear on the Series tab of the Edit Rights Page:

- **Read**: allows the user to view information about a series. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role.

- **Create**: allows the user to create a series.
- **Delete**: allows the user to delete a series.
- **Move**: allows the user to move a series.
- **Edit**: allows the user to edit a series.
- **Hide/Unhide**: allows the user hide and unhide a series.

5.12.2 The Category Tab

For more information, see "Retention Categories" on page 10-13.

The following rights appear on the Category tab of the Edit Rights Page.

- **Read**: allows the user to view information about a retention category. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role:

- **Create**: allows the user to create a retention category.

- **Delete**: allows a user to delete a retention category.
- **Move**: allows a user to move a retention category.
- **Edit**: allows a user to edit a retention category.
- **Edit Review**: allows a user to edit a retention category that is subject to review.

5.12.3 Folder Tab

For more information about folders, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

The following rights appear on the Folder tab of the Edit Rights Page:

- **Read**: allows the user to view information about a folder. It is assigned by default to the Records User, Records Officer, and Records Administrator roles.
- **EditIfAuthor**: allows a user to edit a folder, but only if the user is the author of that folder. It is not assigned by default to any role.

The following rights are assigned by default to the Records Officer and Records Administrator roles:

- **Create**: allows a user to create a folder.
- **Open/Close**: allows a user to open or close a folder.
- **Edit Review**: allows a user to edit a folder that is subject to review.
- **Move**: allows a user to move a folder.

The following rights are assigned by default to the Records Administrator role:

- **Edit**: allows a user to edit a folder, even if the user is not the author of that folder.
- **UndoCutoff**: allows a user to undo the cutoff of a folder.
- **Delete**: allows a user to delete a folder.
- **Freeze/Unfreeze**: allows a user to freeze and unfreeze a folder.

5.12.4 Record Tab

The following rights appear on the Record tab of the Edit Rights Page. These rights are assigned by default to the Records User, Records Officer, and Records Administrator roles:

- **Read**: allows the user to view information about an item.
- **CreateLink**: allows the user to link content items. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details.
- **Create**: allows a user to create content or check it in to the retention schedule. For details, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*.
- **Unlink**: allows a user to unlink content. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details.

The following rights are assigned by default to the Records Officer, Records User, and Records Administrator roles:

- **Edit**: allows the user to edit content, including moving, canceling, expiring, rescinding, making obsolete, and reviewing.
- **EditReview**: allows a user to edit content that is subject to review.

- **DeleteHistoryFile**: allows a user to delete the metadata history file of content. This box is only available if the 'Classified Security' option has been enabled.
- **Upgrade/Downgrade**: allows a user to upgrade and downgrade the security classification of content. This box is only available if the 'Classified Security' option has been enabled on the Configure Retention Settings Page.

The following rights are assigned by default to the Records Administrator role:

- **UndoCutoff**: allows a user to undo the cutoff of an item.
- **Delete**: allows a user to delete content within the retention schedule.
- **Freeze/Unfreeze**: allows a user to freeze and unfreeze content.
- **UndoRecord**: allows a user to undo the status of content.

5.12.5 Admin Tab

The following rights appear on the Admin tab of the Edit Rights Page.

- **PerformPendingReviews**: allows a user to perform pending reviews. This right is assigned by default to the Records Officer, Records User, and Records Administrator roles. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for more details.
- **PrivilegedEnvironment**: allows a user to set the declassification time frame (see "Setting the Declassification Time Frame" on page 6-14). This right is assigned by default to the Records Officer and Records Administrator roles. This box is only available if the 'Classified Security' option has been enabled on the Configure Retention Settings Page.
- **ClassificationGuide**: allows a user to work with classification guides. This right is assigned by default to the Records Officer and Records Administrator roles.
- **Triggers**: allows the user to work with global triggers, custom direct triggers, and indirect triggers. See Chapter 11, "Setting up Triggers". To delete a trigger, Delete permission (D) for the trigger's security group is also required. This right is assigned by default to the Records Officer and Records Administrator roles.
- **ShareFavorites**: allows users to share the contents of their Favorites list with other users. This right is assigned by default to the Records Officer and Records Administrator roles.

The following rights are assigned by default to the Records Administrator role:

- **RecordManager**: allows a user to configure several settings and also set up and administer periods, supplemental markings, security classifications, custom security fields, custom category and folder metadata fields, classification guides and freezes.
- **Screening**: allows a user to screen retention categories, folders, and content.
- **PerformActions**: allows a user to process content assignments.
- **SelectMeta**: allows a user to specify metadata fields to be audited.
- **Reports**: allows a user to generate user and group reports.
- **RetentionScheduleArchive**: allows a user to import and export a retention schedule archive.
- **SelectAuthor**: allows a user to select a different filer (author) for a category than him/herself.

- **Audit**: allows a user to work with audit trials.
- **ConfigureLinkTypes**: allows a user to manage custom content links.
- **AllowDispositionUpgrade/Downgrade**: allows a user to perform upgrade and downgrade classification actions.

See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for more details about screening, creating reports, audits, archives, and configuring link types.

The following rights **are not assigned** by default to any role.

- **NoPostFilterSearch**: allows users to unfilter search results. The results include content the user has no access to based on security classifications, supplemental markings, custom security fields, and ACLs. If the user has no access to a content item in the search results, clicking on it results in an "access denied" error. By enabling this option, search queries are executed much faster because no complex post-filtering must be performed.

  Users with this right can still only access content items they have been explicitly granted access privileges to based on security groups and accounts. They will *see* other results in the search results list, but cannot access them. However, they will see some metadata information about the content item (for example, their title), which may interfere with an organization's security model.

- **NoSecurity**: allows users to become "immune" to security classifications, supplemental markings, custom security fields, and ACLs. Their access to content is unrestricted by these security features. In addition, this option turns off search post-filtering, so search results include content the user has not been explicitly granted access to. For example, a user would have access to content marked as "Top Secret" even if that security classification has not been assigned to the user. This right can be used to give sysadmins the privilege to access every content item in the system.

  Access to content items continues to be restricted by security groups and accounts.

- **CustomDispositionActions**: allows users to define custom disposition actions or to delete any disposition action. See Appendix C, "Customizing Your System" for details.

- **SecurityClassifications**: *new installs only.* If enabled (with the Admin.RecordManager option), the user is allowed to set up security classification levels. See "Security Classifications" on page 6-8. This box is only available if the 'Classified Security' option has been enabled.

- **GetAllFilePlan**: allows a user to get all series, categories, and folders when the GET_FILE_PLAN_ALL service is called. Without this right, inaccessible objects are excluded. The service is typically used by Oracle URM Adapters.

Important: When a user has Admin permission to a security group but does not have the Admin.SelectAuthor right, the user is still able to select an author at checkin. The Admin.SelectAuthor right is used only to add that functionality to a user who does not have Admin permission to a group.

5.12.6 CBC Tab

Chargebacks are used with Physical Content Management, which is only available when that software is enabled.

The following rights are assigned by default to the PCM Administrator role:

- **ChargeBacks.Read**: allows the user to view information about chargeback-related items (transactions, invoices, and so on).
- **ChargeBacks.Create**: allows a user to create chargeback-related items.
- **ChargeBacks.Edit**: allows a user to edit chargeback-related items.
- **ChargeBacks.Delete**: allows users to delete chargeback-related items.
- **ChargeBacks.PrintInvoices**: allows users to print invoices.
- **ChargeBacks.MarkPaid**: allows users to mark invoices as paid.
- **ChargeBacks.Adjust**: allows users to manually adjust invoices.
- **ChargeBacks.Admin**: allows users to perform administrative tasks such as define new payment types, define customers, and so on.

5.12.7 PCM Tab

The following rights are assigned by default to the PCM Requestor and PCM Administrator roles:

- **Physical.Read**: allows the user to view information about physical items.
- **Physical.Create**: allows a user to create physical items.
- **Physical.Edit**: allows a user to edit physical items.
- **Storage.Read**: allows users to view information about a storage location.
- **Storage.Reserve**: allows users to reserve a storage location.
- **Reservation.Read**: allows users to view information about reservations.
- **Reservation.Create**: allows users to create reservations.
- **Reservation.Edit**: allows users to alter reservations.

The following rights are assigned by default to the PCM Administrator role only:

- **Physical.Move**: allows users to move a physical item (change the location)
- **Physical.Delete**: allows users to delete physical items.
- **Storage.Create**: allows users to create new storage.
- **Storage.Edit**: allows users to edit an existing storage location.
- **Storage.Delete**: allows users to delete a storage location.
- **Storage.Block**: allows users to block or unblock a storage location.
- **Reservation.Delete**: allows users to delete reservations.
- **Reservation.Process**: allows users to process reservations by modifying the status of request items.
- **Barcode.Process**: allows users to process barcode files.
- **Admin.Manager**: allows a user to access all of PCM's administrative functions.
- **Admin.Location.Types**: allows users to configure location types, providing the user also has the Admin.Manager right.
- **Admin.PrintLabel**: allows users to generate labels for users, locations, and physical items.

5.12.8 ECM Tab

The following rights are assigned by default to the ERM Requestor and ERM Administrator roles:

- **External.Read**: allows the user to view information about external items.
- **External.Create**: allows a user to create external items.
- **External.Edit**: allows a user to edit external items.

The following rights are assigned by default to the ERM Administrator role only:

- **External.Delete**: allows users to delete external items.
- **External.Admin**: allows users to perform administrative tasks.

5.13 Specifying PCM Barcode Values for Users

Barcodes are used with Physical Content Management, which is only available when that software is enabled.

By default, the barcode value for a user consists of a user's login name in all upper-case letters, for example 'JSMITH' or 'MJONES'. If you do not want to use the login name of a user as the barcode value, use the User Admin utility to specify a different value for the user.

This is especially useful for login names containing characters other than the basic letters (a-z, A-Z) or numbers (0-9) (for example, accented letters such as 'kmüller'). By default, the barcode values generated for such users include hexadecimal representations of the accented letters (for example, 'KMC39CLLER'). To avoid this behavior set specific barcode values for these users (for example, 'KMULLER'), which are then used rather than the (converted) user login names.

You can run the `Update Users with no Barcode` batch service to automatically set the barcode values for all users who currently do not have a barcode value. This is useful for users who are already in the system before Physical Content Management was enabled. The barcode values are set in accordance with the rules above.

To manually set a specific barcode value for a user, complete the following steps:

1. Log in as an administrator.
2. Click **Administration** then click **Admin Applets**.
3. Click the **User Admin** icon.

   The User Admin utility is started.
4. On the **Users** tab, select the user whose barcode value should be set and click **Edit**.

   The Edit User dialog is displayed.
5. In the **Barcode** field, specify a unique value for the user. This value will be used in the barcode label for the user rather than the user's login name (in all upper-case letters) as specified in the Name field.

   The specified value must be unique for each user in the system. An error message will be displayed if a value is used that is not unique.

   Do not use any accented letters in the barcode value (an error message is displayed if you try). Also, any lower-case letters are automatically converted to upper case after clicking **OK**.
6. Click **OK** when finished.

7. Close the User Admin utility.

6

Additional Security Settings

This section describes how to use the classification, classification guides, and supplemental marking functions to provide additional security. It covers the following topics:

Concepts

Tasks

Examples

6.1 Supplemental Markings

Supplemental markings can be assigned to content and record folders to clarify document handling in addition to standard document classification. For example, you can add supplemental markings such as "Restricted Data" or "Originator Controlled." Or you can use supplemental markings in collaboration projects. Only people with specific markings will be able to access a group of content. Supplemental markings can be set at both the record folder and the content level.

This section covers the following topics:

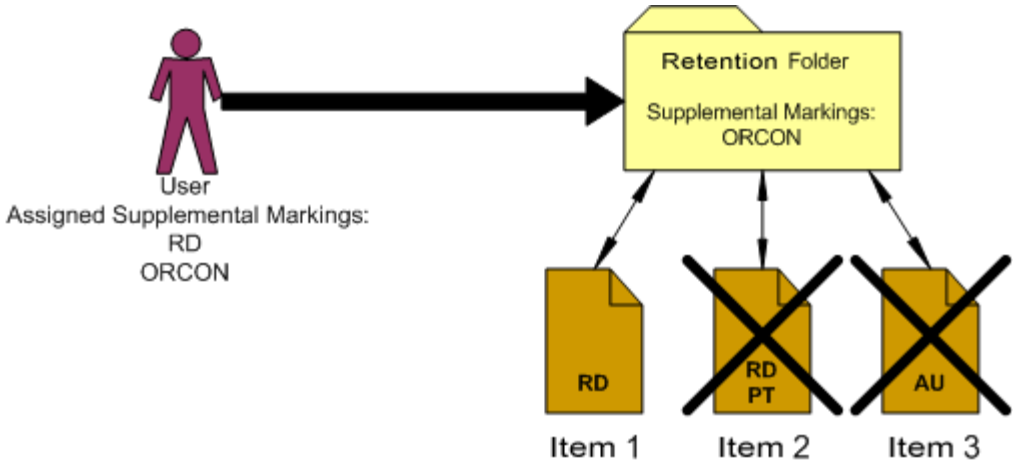
6.1.1 Supplemental Markings Details

In addition to using supplemental markings as a means of clarifying document handling, supplemental markings can be used as a security feature to further restrict users from accessing record folders and content.

To disable the use of supplemental markings as a security feature, clear the *Supplemental Markings* box on the Configure Retention Settings Page and do not assign the markings to users.

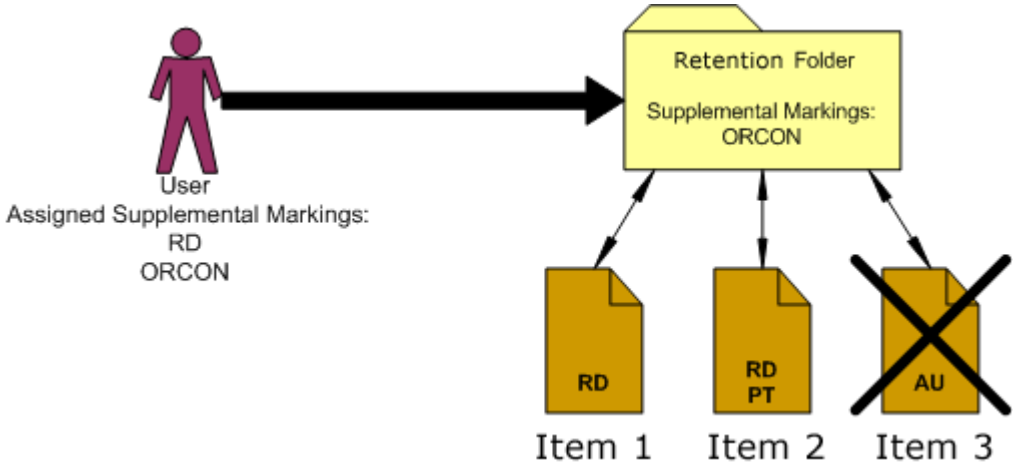
When supplemental markings are assigned to users, even if a user has access to a specific record folder, the supplemental marking further restricts access to folders and content. In circumstances where a folder or content has multiple supplemental markings, it can be required that a user match all assigned supplemental markings to access an item or record folder. When 'match all' is disabled, if a user matches just one of the multiple supplemental markings, the user can access the content or record folder object.

Figure 6–1 User Must Match All Supplemental Markings



For example, in the diagram above, the user is assigned the supplemental markings "RD" and "ORCON." The folder is marked with "ORCON," therefore the user can access the folder. The content within the folders are assigned one or more of the markings, "RD," "PT," and "AU." If the security configuration for supplemental markings is set to force the user to match *all* supplemental markings, then the user can access the folder marked "ORCON" and its child "Item 1" marked with the supplemental marking "RD." Because the user has not been assigned the supplemental marking "PT" or "AU", the user cannot access "Item 2," which has the multiple markings "RD" and "PT," nor can the user access "Item 3" with the marking "AU."

Figure 6–2 User Must Match at Least One Supplemental Marking



If the supplemental marking security configuration is not forcing a user to match all markings, then the user can now access Item 2, because the user matches at least one marking "RD" on the Item 2. Because the user has not been assigned the supplemental marking "AU," the user still cannot access Item 3, which has the supplemental marking "AU." The user would have to be assigned the supplemental marking "AU" in the User Admin application to access the item.

Supplemental markings are *not* inherited by record folders or content. Markings are checked at every folder and item level. Supplemental markings do not have any permissions hierarchy. All markings have equal permissions: access granted or access denied to users. In contrast, the classified security does have a hierarchy to its

classification levels. For further information, see "Classified Records Security Hierarchy" on page 6-10.

Two special supplemental markings, *Restricted* and *Formerly Restricted*, can be used to disable the following classification-related metadata fields on the content check-in and metadata update pages:

- Declassify on event
- Declassify on date
- Downgrade instructions
- Downgrade on event
- Downgrade on date

To work with supplemental markings, you must have one of the following rights:

- **Admin.Triggers**: This right enables you to view information about supplemental markings.
- **Admin.RecordManager**: In addition to viewing information about supplemental markings, this right also enables you to create (add), edit, and delete supplemental markings.

Optionally, the following right may be useful for working with supplemental markings:

- **Record.Edit**: This right is required to use metadata disabling based on supplemental markings.

Permissions: Oracle UCM administrative permissions are required to perform this action.

6.1.2 Managing Supplemental Markings

The following procedures are followed when managing supplemental markings:

- "Enabling or Disabling Supplemental Markings" on page 6-4
- "Creating or Editing a Supplemental Marking" on page 6-5
- "Viewing Supplemental Marking Information and References" on page 6-6
- "Deleting a Supplemental Marking" on page 6-6
- "Assign or Remove User Supplemental Markings" on page 6-7
- "Using Restricted and Formerly Restricted Supplemental Markings" on page 6-8

6.1.2.1 Enabling or Disabling Supplemental Markings

You can enable and disable supplemental markings at any time. Enabling supplemental markings enforces the markings assigned to any users attempting to access marked items and record folders.

Disabling supplemental markings means the security provided by the markings is not in force; however, the supplemental markings can still be used generically as document handling instructions.

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

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

   The Configure Retention Settings Page is displayed. Expand the Security section if needed.

2. Enable the **Supplemental Markings** box.

3. (Optional) To force a user to match **all** supplemental markings assigned to an item or record folder before granting access, click the **User must match all Supplemental Markings** box. To allow access if the user has at least one of the markings, leave the box unchecked.

4. Click **Submit**. The 'successful configuration' message is displayed.

To disable supplemental markings, clear the **Supplemental Markings** box and the **User must match all supplemental markings** box. Click **Submit**. A configuration successful message is displayed. Supplemental markings are now disabled and the Supplemental Marking selection field is hidden from view.

6.1.2.2 Creating or Editing a Supplemental Marking

You can create supplemental markings only if they are enabled. See "Enabling or Disabling Supplemental Markings" on page 6-4 for details.

After creating a supplemental marking, it is available for applying to content, record folders, and users.

When editing an existing supplemental marking, its description can be modified but not its name.

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

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Supplemental Markings**.

   The Configure Supplemental Markings Page is displayed.

2. Click **Add**.

   The Create or Edit Supplemental Marking Page is displayed.

3. Enter a unique supplemental marking with a maximum of 30 characters in the **Supplemental Marking** text box.

4. Enter a description of the marking with a maximum of 30 characters in the **Brief Description** text box.

5. Click **Create**.

6. The Supplemental Marking Information Page is displayed with a message indicating the creation was successful. Use that page to edit or delete the marking, or view references to the marking.

7. Click **OK** when done.

To edit an existing supplemental marking, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Supplemental Markings**.

   The Configure Supplemental Markings Page is displayed.

2. You can edit the marking in one of two ways:

   - Click **Edit Marking** from the item's **Action** menu. The Create or Edit Supplemental Marking Page is displayed.
   - Click the name of the marking to edit. The Supplemental Marking Information Page is displayed. Click **Edit** on this page. The Create or Edit Supplemental Marking Page is displayed.

3. Make the changes and click **Submit Update.** The Supplemental Marking Information Page is displayed with a message indicating the creation was successful. Use this page to edit or delete the marking, or view references to the marking.

4. Click **OK** when done.

6.1.2.3 Viewing Supplemental Marking Information and References

---

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform these actions. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role.

---

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Supplemental Markings**.

   The Configure Supplemental Markings Page is displayed.

2. Click the name of the marking with information to view.

3. The Supplemental Marking Information Page is displayed. Use the page to edit or delete the marking, or view references to the marking.

4. Click **OK** when done.

6.1.2.4 Deleting a Supplemental Marking

You can delete supplemental markings regardless of whether markings are enabled. A supplemental marking cannot be deleted until any references to the marking in content or record folders is removed. The marking must also be manually removed from any assignments to users.

If a user attempts to delete a supplemental marking currently in use, a message is displayed stating the marking is in use by users (the marking is assigned to users and must be removed), by record folders, or by a content item. The marking must then be removed from the user, folder, or item before proceeding.

To remove the marking from any option lists, the schema must be republished after deleting the marking. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about publishing schema.

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 **Security** then **Supplemental Markings**.

   The Configure Supplemental Markings Page is displayed.

2. Click **Delete** from the item's **Action** menu. To delete multiple markings, click the checkbox next to the marking name and click **Delete** in the Table menu. A marking can also be deleted when viewing the marking's Supplemental Marking Information Page.

3. A message indicates the deletion was successful.

4. Click **OK**.

Tip: You can search for supplemental markings from the Search page. Select the marking to search for from the Supplemental Markings list on the Search page. Use the search results to see which objects have the marking in use. You can also use screening folders to quickly isolate and sort objects by supplemental markings. For further information, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

6.1.2.5 Assign or Remove User Supplemental Markings

Permissions: Administrator privileges in Oracle UCM are required to perform this action.

Before assigning markings to users, make sure you have enabled supplemental markings, created the markings, assigned supplemental markings to record folders and retained content, and assigned roles to the users. For the most strict supplemental marking security, you can also force a user to pass all supplemental markings to access an item or record folder.

You may want to remove access from a user who is no longer authorized for a supplemental marking, or to delete a supplemental marking no longer in use. You must remove any references to a supplemental marking before you can delete it.

To disable use of supplemental markings as a security feature, do not assign the markings to users.

1. Click **Admin Applets** from the **Administration** menu.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Info tab on the Edit User page is displayed.

4. In the **Supplemental Markings** field, select the markings to which the user should have access. Click the options list arrow, and highlight the marking. Multple markings can be assigned to a user.

5. Click **OK**. Repeat the process for each user who needs markings.
6. Restart the Content Server.

To remove a supplemental marking from a user, complete the following steps:

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.
2. Click the **User Admin** icon.

   The User Admin utility starts.
3. On the Users tab, select the user in the Users list, and click **Edit**. The Info tab on the Edit User page is displayed.
4. In the **Supplemental Markings** field, delete a marking by editing the text in the **Supplemental Markings** text box. Use the delete or backspace key to remove the marking.

   Caution: Be careful when editing text in this field. Each supplemental marking must have a comma and a space between markings, or an "access denied" error occurs when trying to access content with multiple markings and 'match all markings' is enabled.
5. Click **OK**. Repeat for each user who has a marking to be removed.
6. Restart the Content Server. For more information about restarting, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

6.1.2.6 Using Restricted and Formerly Restricted Supplemental Markings

Restricted Data and *Formerly Restricted Data* are supplemental markings shipped with the product. Those markings can be used alone or in combination with other markings to disable classified metadata fields on the content check-in and metadata update forms:

1. Enable supplemental markings (see "Enabling or Disabling Supplemental Markings" on page 6-4).
2. Click *Restricted Data* or *Formerly Restricted Data* as the supplemental marking.
3. Restart the Content Server.

6.2 Security Classifications

The classification of content is the process of identifying and safeguarding content requiring protection against unauthorized disclosure, for example, because it contains information sensitive to the national security of the United States or sensitive to the stability of a company.

Classification can be an additional way to restrict access when used with supplemental markings and custom security fields. Classification markings are at the content level only, unlike supplemental markings, which are at the content or record folder level.

This section discusses the following topics:

6.2.1 About Records Classification

Oracle URM offers several features specifically geared to handling and processing classified content in accordance with the Chapter 4 requirements of the DoD 5015.2 specification. This functionality must be enabled for use (see "Enabling or Disabling Classified Security" on page 6-11).

A content item is marked as a classified using a classification specifying the security level of the item. Several built-in classifications ("Top Secret," "Secret," and "Confidential") are available, but custom classifications can be created (see "Creating or Editing a Custom Security Classification" on page 6-12).

Content is either classified, unclassified, or declassified:

- **Classified** content has an initial classification and a current classification. The initial classification is specified when the item is first filed. All changes to classification are tracked in the audit logs in the Record History reports.
- **Unclassified** content is not and has never been classified.
- **Declassified** content was formerly classified. When an item is filed and classified, it typically must be declassified within a ten year period. Any exceptions to this must be given an exemption category. When a declassify date exceeds the ten year period after the publication (filing) date, an alert reminds the user to enter an exemption category for the item.

6.2.1.1 Classification Levels

The standard security categories (classification scheme), from highest to lowest, are as follows:

1. Top Secret
2. Secret
3. Confidential
4. No markings (unclassified)

When using security classification for corporate use only (that is, if you are not concerned with DoD compliance), these terms can be defined as necessary for the organization's infrastructure. For example, "Top Secret" may apply to that content which is critical to the operation of your company and should never be deleted, while "Confidential" may apply to content which must be kept limited to a specific group of individuals, such as Human Resource representatives or members of your accounting team.

Custom classifications can also be defined. See "Creating or Editing a Custom Security Classification" on page 6-12.

The following descriptions are applicable for those companies which are using the Oracle URM product for DoD compliance.

Figure 6–3 Classified Hierarchy

6.2.1.1.1 Top Secret If complying with DoD Section 1508, the Top Secret classification (according to Executive Order 12958) is "applied to information, the unauthorized disclosure of which could be expected to cause **exceptionally grave damage** to the national security that the original classification authority is able to identify or describe."

If complying with DoD Section 1508, only the President of the United States has the authority to classify content as Top Secret, pursuant to the Executive Order 12958. For further details, access the following link:

http://www.fas.org/sgp/clinton/eo12958.html

6.2.1.1.2 Secret According to EO 12958, the Secret classification level is "applied to information, the unauthorized disclosure of which could be expected to cause **serious damage** to the national security that the original classification authority is able to identify or describe."

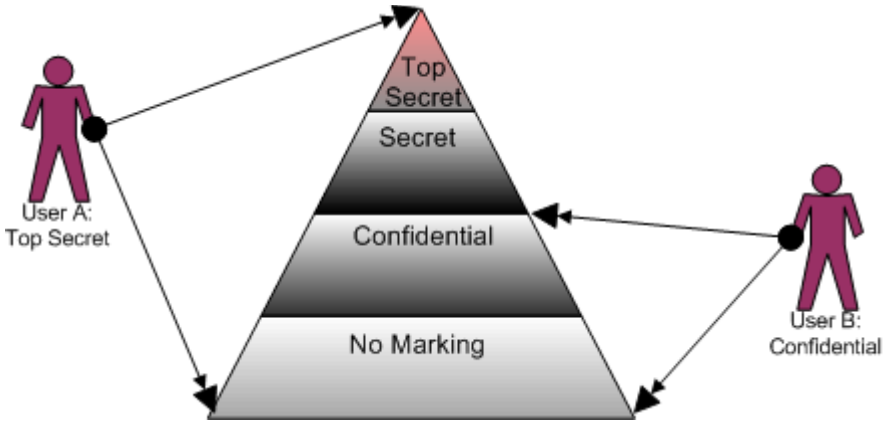
6.2.1.1.3 Confidential According to EO 12958, the Secret classification level is "applied to information, the unauthorized disclosure of which could be expected to cause **damage** to the national security that the original classification authority is able to identify or describe."

6.2.1.2 Classified Records Security Hierarchy

Every retention user has access to unclassified content, provided all other security criteria are met (such as supplemental markings, right, roles, and so on).

A user who has access to Top Secret classification has access to all lower classifications as well, as shown for User A in the figure below. User B has access to Confidential content and unclassified content.

Figure 6–4 Hierarchical User Access



6.2.2 Managing Classified Security

The following tasks are included in managing classifications:

- "Enabling or Disabling Classified Security" on page 6-11
- "Creating or Editing a Custom Security Classification" on page 6-12
- "Setting the Order of Security Classifications" on page 6-13
- "Deleting a Security Classification" on page 6-14
- "Setting the Declassification Time Frame" on page 6-14
- "Assigning a Classification to a User" on page 6-15
- "Changing a User's Classification" on page 6-16
- "Removing a User's Classification" on page 6-16

6.2.2.1 Enabling or Disabling Classified Security

You can enable and disable classified security at any time. Enabling classified security enforces the security classifications assigned to users who attempt to access classified data.

After enabling classified security, create any custom security classifications required by the organization. If additional security classifications are created, make sure to indicate the classification's place within the marking hierarchy. For further information, see "Setting the Order of Security Classifications" on page 6-13.

> **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** then **Settings** from the Top menu.

   The Configure Retention Settings Page is displayed. If necessary, expand the Security section.

2. Enable the **Classified Security** box.

3. Click **Submit**. A message is displayed stating the configuration was updated successfully.

Caution: Disabling classified security puts sensitive classified items at risk of being accessed by unauthorized people. After your classified security is in force, it is recommended that you do not disable it.

To disable classified security, complete the following steps:

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

   The Configure Retention Settings Page is displayed.

2. Clear the **Classified Security** box.

3. Click **Submit**. A message is displayed stating the configuration was updated successfully. Classified security is now disabled and the security classification selection field is hidden from view on the content check-in form.

6.2.2.2 Creating or Editing a Custom Security Classification

Use this procedure to create a new security classification. After creating a custom classification, indicate its order in the hierarchy. If not done, the security classification is ignored. For further information, see "Setting the Order of Security Classifications" on page 6-13.

Security classifications can be created only if the classified security feature has been enabled (see "Enabling or Disabling Classified Security" on page 6-11).

When editing an existing security classification, the description can be modified but not its name.

Permissions: The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform these actions. These rights are assigned by default to the Records Administrator role.

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

   The Configure Security Classification Page is displayed.

2. Click **Add**.

   The Create or Edit Security Classification Page is displayed.

3. Enter a unique classification up to 30 characters in the **Security Classification** text box.

4. Enter a description up to a maximum of 30 characters in the **Brief Description** text box.

5. Click **Create**. A message indicates creating the classification was successful.

6. Click **OK**. The Configure Security Classification Page is displayed with the new classification in the list. A user must be assigned the classification level or a higher level to be able to view the security classification level. Make sure to indicate the placement of the new classification in the hierarchy. For further information, see "Setting the Order of Security Classifications" on page 6-13.

Permissions: When editing a classification, you must also be assigned the highest security level to view all of the available classifications for editing.

To edit an existing security classification, complete the following steps:

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

   The Configure Security Classification Page is displayed.

2. Click the **Edit** icon (a pencil) next to the classification to edit.

   The Create or Edit Security Classification Page is displayed.

3. Make any changes in the **Brief Description** text box, and click **Submit Update.** A message is displayed stating the security classification was updated successfully.

4. Click **OK**.

6.2.2.3 Setting the Order of Security Classifications

Prerequisites

- Create any custom security classifications that are required. See "Creating or Editing a Custom Security Classification" on page 6-12.
- Assign yourself the highest classification level so you can view and reorder all levels. See "Changing a User's Classification" on page 6-16.

Permissions: The Admin.RecordManager and Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also have the specific security classification level assigned to you to view or work with it.

Use this procedure to indicate the order of the security classifications within the security classification hierarchy. If only the built-in security classifications are used in their default order, this procedure is not needed.

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

   The Configure Security Classification Page is displayed.

2. Use the up arrow (and down arrow) to move a selected security classification up or down in the classification hierarchy. The highest classification should be at the top of the list and the lowest at the bottom.

   Important: The last item in the list will be unclassified regardless of the name you assign to it. Make sure you have a "classification" in your hierarchy that you intend to be unclassified.

3. Click **Submit Update**. A message is displayed stating the configuration was updated successfully.

6.2.2.4 Deleting a Security Classification

A classification cannot be deleted until any references to the classification in content are removed (see "Viewing Security Classification References" on page 6-15). Security classification assignments must also be manually removed from users (see "Removing a User's Classification" on page 6-16). If you attempt to delete a security classification still in use, a message is displayed stating the classification is in use by users (it is assigned to users and must be removed) or by content.

Search for security classifications from the Search page. Use the search results to see which items have the classification in use. Screening can also be used to quickly isolate content. For further information, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also be assigned the highest security level to view all of the available classifications for deleting.

---

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

   The Configure Security Classification Page is displayed.

2. Click the Delete icon (a red X) next to the classification to delete.
3. A message is displayed stating the security classification was deleted successfully.
4. Click **OK**.

6.2.2.5 Setting the Declassification Time Frame

Classified items are automatically declassified after 25 years unless they were exempted from declassification. When an item is declassified, the Declassify On Date field is compared to the Publication Date, and if the retention period for classification status exceeds ten years, an alert is presented to the user.

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

---

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

   The Configure Retention Settings Page is displayed. If necessary, expand the Security section.

2. In the "Maximum years before declassifying" field, enter the number of years after which items will be declassified (the default is 25). If this field is not available, the Admin.PrivilegedEnvironment right is not assigned to the user viewing the page.

   f this field is set to 0 and auto-computation of declassification dates is chosen, any classified items currently in the system are set to declassified.

3. Click **Submit Update**. A message is displayed stating the configuration was successful.
4. Click **OK**.

6.2.2.6 Viewing Security Classification References

Use this procedure to view references to a security classification (those disposition rules which use the security classification in their definitions).

> **Permissions:** The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to perform this action. These rights are assigned by default to the Records Administrator role. You must also be assigned the highest security level to view all of the available classifications for viewing.

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

   The Configure Security Classification Page is displayed.

2. Select the security classification to view, and click the **Info icon.**

   The Security Classification Information Page is displayed.

3. Click **Reference** from the Page menu.

   The Security Classification References Page is displayed

   This page shows all users and content assigned to the selected security classification level. If any of the content links are clicked, the associated content information page for that item is displayed.

6.2.2.7 Assigning a Classification to a User

You can assign security classifications only if the classified security feature has been enabled (see "Enabling or Disabling Classified Security" on page 6-11).

> **Permissions:** Administrator privileges in Oracle UCM ('sysadmin' permissions) are required to assign user access to classifications. Your own assigned classification level must also be at least the level being assigned to users. For example, if you are assigned the classification level 'Secret', you cannot assign the classification level 'Top Secret' to users.

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User page is displayed.

4. Make sure the Info tab is active.

5. In the **Security Classification** field, select the maximum security level the user should have access to from the option list available on the pull-down menu.

6. Click **OK**. Repeat the process for each user.

Note the following considerations:

- If a user is not assigned any security classification, the user cannot pick an initial classification while checking in a content item. Because specifying the initial classification is mandatory, the user cannot check the item into the repository.
- It is recommended that the highest security classification be assigned to the Records Administrator and overall administrator. This allows them to perform all classification-related tasks (for example, on behalf of someone who must downgrade or declassify an item but does not have the required classification privileges).

6.2.2.8 Changing a User's Classification

The assigned security classification of users determines what items they can access.

> **Permissions:** Administrator privileges in Oracle UCM are required to perform this action. Your own assigned classification level must also be at least the level being accessed.

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User page is displayed.
4. Make sure the Info tab is active.
5. In the **Security Classification** field, select the new maximum security level the user should have access to. Click the options list arrow, and click the classification needed.
6. Click **OK**.

6.2.2.9 Removing a User's Classification

You may want to remove access from a user who is no longer authorized for a classification or to delete a classification no longer in use. Remove any references to a classification before deletion it.

> **Permissions:** Administrator privileges in Oracle UCM are required to perform this action. Your own assigned classification level must also be at least the level being accessed.

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. On the Users tab, select the user in the Users list, and click **Edit**. The Edit User page is displayed.
4. Make sure the Info tab is active.

5. In the **Security Classification** field, delete the current security level (using the keyboard or by selecting the blank line from list).
6. Click **OK**.

6.3 Custom Security

Custom security is optional and are another layer of security in addition to supplemental markings (see "Supplemental Markings" on page 6-2).

Two types of custom security are available:

- Simple custom security fields, where custom field are configured to be matched by a user rather than a designated supplemental marking. This is called *custom supplemental markings* in the DoD 5015 standard,
- Advanced custom security, where security is applied to fields that use option lists. Security can be applied to individual items in the option list.

Unlike supplemental markings, custom security is enforced at the item level. Supplemental markings are enforced at both the record folder and the item level.

This section covers the following topics:

6.3.1 About Custom Security

To work with custom security, you need to have one of the following rights:

- **Admin.Triggers**: This right enables you to view information.
- **Admin.RecordManager**: In addition to viewing information, this right also enables you to create (add), edit, and delete custom security.

A *simple custom security field* pairs a custom content field with a custom user field. For example, you can create a custom security field such as "Project Name." Users must be assigned the appropriate project name or names to access or view an item assigned with custom security. If the "match all" setting is enabled, a user must be assigned to all the same projects as an item is assigned to for the user to access an item with multiple project assignments. If a user does not match all project names, the user cannot access an item.

You can opt to select the "match all" feature for custom security fields just as you can with supplemental markings. Content is then checked in with one or more custom security field options, such as a particular project name, assigned to the content.

For instance, "user1" is assigned project name "Pangea" only. The user named "user2" is assigned both project name "Pangea" and "Tectonic." If content is checked in with multiple field options assigned (for example, "Pangea" and "Tectonic"), then only a user with all project names assigned (user2) can access that content. If the "match all" setting is disabled, then a user only must match one field option to access an item.

Advanced custom security also limits access to content items. However, advanced security can also restrict access based on aliases as well as individual users. This type of security assigns security at the *item* level for option lists. When using this type of security, the only metadata that can be used is that which has an option list associated

with it. Access can then be restricted to individual items in the option list by limiting which accounts, which users, or which aliases of users can access specific options.

6.3.2 Managing Custom Security

The following tasks are often performed when managing custom security:

- "Enabling or Disabling Custom Security Usage" on page 6-18
- "Creating or Editing a Simple Custom Security Field" on page 6-18
- "Adding or Editing Advanced Security" on page 6-19
- Viewing Simple Custom Security Field Information
- Deleting a Simple Custom Security Field (Simple)

6.3.2.1 Enabling or Disabling Custom Security Usage

Use this procedure to enable the custom security feature. It can be enabled or disabled at any time.

Permissions: The Admin.RecordManager right is required to enable custom security. This right is assigned by default to the Records Administrator role.

---

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

   The Configure Retention Settings Page is displayed. Expand the Security section if needed.

2. Click the **Custom Security** box.
3. Click **Submit Update**. A message is displayed saying the configuration was successful.
4. Click **OK**.

To disable the feature, clear the **Custom Security** box.

6.3.2.2 Creating or Editing a Simple Custom Security Field

Use this procedure to create a new simple custom security field.

Important: Make sure you have defined the custom field for the items in the Configuration Manager utility, and the custom field for the users in the User Admin utility before performing this task. See "Simple Custom Security Field Example" on page 6-21 for a step-by-step sample of setting up a simple custom security field.

You can create custom security fields only if the custom security field feature has been enabled (see "Enabling or Disabling Custom Security Usage" on page 6-18).

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

---

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

   The Configure Custom Security Page is displayed.

2. In the Custom Security Field area, click **Add**.

   The Create or Edit Simple Custom Security Field Page is displayed.

3. Enter a name for the field in the **Custom Security Field** text box.
4. Select the document metadata name for the content field from the **Content Field** list.
5. Select the metadata name of the user field from the **User Field** list.
6. (Optional) Click the **Match all** box to force the user entries to match **all** content field entries. Leave this box cleared to allow only one content field to match the user field.
7. Click **Create**. The successfully created custom security field message is displayed.
8. Click **OK**.

To edit an existing custom security field, complete the following steps:

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

   The Configure Custom Security Page is displayed.

2. Click **Edit Field** from the field's **Actions** menu.
3. Make the necessary edits:
   a. Select the name of the metadata field from the **Content Field** list.
   b. Select the name of the user metadata field in the **User Field** list.
   c. Select or clear the **Match all** box.
4. Click **Submit Update**. A message indicates the update was successful.
5. Click **OK**.

6.3.2.3 Adding or Editing Advanced Security

Use this procedure to add advanced security to an existing field. The field used must be one which has an option list associated with it.

You can add custom security only if the custom security feature is enabled (see "Enabling or Disabling Custom Security Usage" on page 6-18).

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

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

   The Configure Custom Security Page is displayed. If necessary, click the Advanced Custom Security tab to display that page.

2. Click **Add**.

   The Select Security Dialog is displayed.

3. Select a field from the list. Note that only fields with option lists are available for selection.
4. Click **OK**.

   The Advanced Custom Security Option Page is displayed showing the option items associated with the field that was chosen.
5. Click the Actions menu for the option item which needs security. Click **Edit Security**.

   The Select Security Dialog is displayed.
6. Select users or aliases who will have access to content items with that individual option list value. See "Setting ACLs During Software Use" on page 5-17 for details about choosing users or aliases.
7. If needed, select a security group from the list.
8. The Advanced Custom Security Option Page is re-displayed, showing the selections just made.

To alter custom security for a field (including removing the security), complete the following steps:

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

   The Configure Custom Security Page is displayed.
2. In the Advanced Custom Security area, click **Edit Security** on the Actions menu of the option item. To remove security for the option item, click **Remove Security** on the Actions menu of the option item.

   When editing, the Advanced Custom Security Dialog is displayed.
3. Select a field from the list. Note that only fields with option lists are available for selection.
4. Click **OK**.

   The Advanced Custom Security Option Page is displayed showing the option items associated with the field that was chosen.
5. Click the Actions menu for the option item which needs security. Click **Edit Security**.

   The Select Security Dialog is displayed.
6. Select users or aliases who will have access to content items with that individual option list value. See "Setting ACLs During Software Use" on page 5-17 for details about choosing users or aliases.
7. If needed, select a security group from the list.
8. The Advanced Custom Security Option Page is re-displayed, showing the selections just made. The security is now in place.

6.3.2.4 Viewing Simple Custom Security Field Information

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role.

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

   The Configure Custom Security Page is displayed.

2. In the custom field area, click the field to view.

   The Custom Security Field Information Page is displayed.

3. Click **OK** when done.

6.3.2.5 Deleting a Simple Custom Security Field (Simple)

You can delete a custom security field without having to remove references to it by users and content, unlike supplemental markings and security classifications.

Permissions: The Admin.RecordManager right is required to delete a custom security field. This right is assigned by default to the Records Administrator role.

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

   The Configure Custom Security Page is displayed.

2. Click **Delete** from the item's **Actions** menu. To delete multiple fields, select the checkbox next to the field name and click **Delete** in the Table menu. A field can also be deleted when viewing the field's Custom Security Field Information Page.

3. A message displays, indicating the deletion was successful.

4. Click **OK**.

6.3.3 Simple Custom Security Field Example

This example gives step-by-step instructions for setting up a custom security field called "Project Name." It includes the following processes:

1. Create the Custom Security Field in Configuration Manager.
2. Create the Custom Security Field in User Admin. Oracle UCM assigns the "u" prefix. Assign the field options to the user.
3. Rebuild the Content Server search index, and restart the server. Complete instructions are in the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.
4. Create the Custom Security Field using the exact field names defined in the Oracle UCM utilities.

After the custom security field is set up, test the field by checking in and accessing items assigned field options. See Verify the Custom Security Field.

6.3.3.1 Create the Custom Security Field in Configuration Manager

This portion of the example creates the custom security field as a document field within the Configuration Manager utility. The field will be available for use on the check-in form.

1. Click **Admin Applets** from the **Administration** menu on the left.

   The Administration Applets for the server are displayed.

2. Click the **Configuration Manager** icon.

   The Configuration Manager utility starts.

3. Click the **Information Fields** tab.

4. Click **Add**.

   The Add Custom Info Field page is displayed.

5. Type `ProjectName`, and click **OK**. The Add Custom Info Field page is displayed. Specify the field attributes:

   a. In the **Field Caption** text box, enter a space between any compound words (in the above example, "Project" and "Name") so the field label displays properly.

   b. In the **Field Type** list, click **Long Text**.

   c. Click the **Enable Options List** box. The Configure button becomes enabled. Click this button.

   d. The Configure Option List page opens. In the **Options List Type**, click the **Edit and Multiselect List** option.

   e. Click **Edit** next to **Use Option List**. The Option List page is displayed.

   f. In the options list, type `Pangea`. Press Enter for a carriage return, then type `Tectonic`. Click **OK** three times.

6. Click **Update Database Design**.

6.3.3.2 Create the Custom Security Field in User Admin

This portion of the example creates the custom security field as an information field called "Project Name" within the User Admin utility.

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets for the server are displayed.

2. Click the **User Admin** icon.

   The User Admin utility starts.

3. Open the **Information Fields** tab.

4. Click **Add**.

   The Add Custom Info Field page is displayed.

5. Type `ProjectName` and click **OK**. The Add Metadata Field page is displayed. Specify the field attributes:

   a. In the **Field Caption** text box, enter a space between any compound words (as in the example, "Project" and "Name") so the field label displays properly.

   b. In the **Field Type** list, click **Long Text**.

c. Click the **Enable Options List** box. The Options List Settings tab becomes enabled.

d. In the **Options List Type**, click the **Edit and Multiselect List** option.

e. Click **Edit**. The Option List page is displayed.

f. In the options list, type `Pangea`. Press Enter for a carriage return, and then type `Tectonic`. Click **OK twice**.

6. Click **Update Database Design**.

7. Click the **Users** tab. Create a uesr named 'user1' then select that name and click **Edit**. The Edit User "user1" page is displayed.

   a. In the Project Name list, click the down arrow, and click the project name "Pangea" from the list. Repeat for "Tectonic." You now have a comma-separated list of project names assigned to user1.

   b. Click **OK**.

8. Restart the Content Server.

6.3.3.3 Create the Custom Security Field

This portion of the example creates the custom security field. Make sure the Custom Security Field option is enabled in the Configure Retention Settings Page, and you have defined the document and user fields in the appropriate administration utilities.

1. Click **Configure** then **Custom Security Fields** from the Configure Retention Settings Page.

2. On the Configure Custom Security Page, click **Add**.

   The Create or Edit Simple Custom Security Field Page is displayed.

3. In the **Custom Security Field** text box, type `Project Name`.

4. From the **Content Field** list, click **ProjectName**.

5. From the **User Field** list, click **ProjectName**.

6. Click the **Match all** box to force a user to match all content field entries. This is the strictest setting. If a user is not assigned all project names assigned to an item, the user cannot access that item.

7. Click **Create**.

6.3.3.4 Verify the Custom Security Field

This portion of the example demonstrates how the custom security field restricts access.

- Log in as *user1* and check in an item with both "Pangea" and "Tectonic" selected as project names in the check-in form. Search for the item you just checked in as *user1*. The search should be successful.

- Now log in as a new user without any custom field assignments. Attempt to access the item user1 just checked in. The attempt to view the item should not be successful because the new user does not have any assigned field options.

- Log in as an administrator and assign the new user the field option "Pangea." Disable the **Match all** option for the custom security field. Log in as the new user and attempt to access the item with "Pangea" and "Tectonic" assigned as the project name. The access should now be successful because only one field list option has to match, and the user is assigned the appropriate field list option.

6.4 Classification Guides

Note: Classification guides can be set up only if the ClassifiedEnhancements component is enabled.

Classification guides are used to facilitate the proper and uniform derivative classification of information. Specifically, Executive Order 12958 defines "derivative classification" as incorporating, paraphrasing, restating or generating in new form information already classified, and marking the newly developed material consistent with the classification markings applying to the source information.

Classification guides are not the same as classifying a piece of content with a setting such as Top Secret, and so on. Guides are separate from classifications.

This section covers the following topics:

6.4.1 About Classification Guides

Classification guides (and their associated topics) enable convenient implementation of multiple classification schemes.

They are used to define default values for the following classification-related metadata fields on the content check-in page:

- **Initial Classification** (xInitialClassification)
- **Reason(s) for classification** (xClassificationReason)
- **Declassify exemption category** (xDeclassifyExemptionCategory)
- **Declassify on event** (xDeclassifyOnEventDescription)
- **Declassify on date** (xDeclassifyOnDate)

This makes checking in classified content easier and more consistent, with similar content having the same classification metadata. The Records Administrator can define multiple classification guides. Each classification guide consists of one or more topics, which provide a further level of detail for grouping classified content.

The default metadata field values associated with a classification topic are suggestions only; they can be overridden. Classification guides can be set up only if the ClassifiedEnhancements component is enabled.

6.4.2 Managing Classification Guides

The following tasks are performed when managing classification guides:

- Creating or Editing a Classification Guide
- Deleting a Classification Guide
- Viewing Classification Guide Information
- Creating or Editing a Classification Topic
- Editing Classification Topic Settings
- Deleting a Classification Topic

6.4.2.1 Creating or Editing a Classification Guide

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

1. Click **Records** then **Configure** from the Top menu. Click **Security** then **Classification Guide**.

   The Configure Classification Guide Page is displayed.

2. Click **Add**.

   The Create or Edit Classification Guide Page is displayed.

3. Provide a guide ID and a guide name (description), and click **Create**.

   A "Successfully created classification guide" page is displayed showing the identifier and name of the newly created classification guide. The page also includes an **Actions** menu, where current classification guides can be edited or deleted or add topics added to it. See "Creating or Editing a Classification Topic" on page 6-26.

4. Click **OK** to return to the Configure Classification Guide Page).

Use this procedure to edit a classification guide:

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. Select a classification guide to edit from the list and click **Info**.

   The Classification Guide Information Page is displayed.

3. Click **Edit** then click **Edit Classification Guide** from the Page menu.

   The Create or Edit Classification Guide Page is displayed.

4. Change the classification guide name as required. The guide ID cannot be modified. Click **Submit Update** when done.

   A "Successfully updated classification guide" page is displayed showing the identifier and modified name of the classification guide. The page also includes a menu where the current classification guide can be edited or deleted or have topics added to it. See "Creating or Editing a Classification Topic" on page 6-26.

5. Click **OK** to return to the Configure Classification Guide page.

6.4.2.2 Deleting a Classification Guide

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. Select the classification guide to delete from the menu and click **Delete**.

   The classification guide is deleted.

3. Click **OK** to return to the Configure Classification Guide Page.

6.4.2.3 Viewing Classification Guide Information

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. Select the classification guide whose information to view from the menu and click **Info**.

   The Configure Classification Guide Page is displayed.

   The page shows the identifier and name of the selected classification guide. The page also includes a menu where the current classification topic can be edited or deleted or have topics added to it See "Creating or Editing a Classification Topic" on page 6-26.

3. Click **OK** to return to the Configure Classification Guide Page.

6.4.2.4 Creating or Editing a Classification Topic

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. Select the classification guide in the list to create the topic for, and click **Info**.

   The Configure Classification Guide Page is displayed.

3. From the Page menu, click **Edit** then click **Configure Topics**.

   The Administer Classification Topic Page is displayed.

4. Click **Add**.

5. The Create or Edit Classification Topic Page is displayed.

6. Provide a name and description for the classification topic, and click **Create** when done.

7. The Configure Topic Settings Page is displayed.

   Provide default values for each of the metadata fields, and click **Submit Update** when done.

Use this procedure to edit an existing classification topic:

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. In the list, select the classification guide to edit and click **Info**.

   The Classification Guide Information Page is displayed.

3. From the **Actions** menu, choose **Configure Topics**.

   The Administer Classification Topic Page is displayed.

4. From the **Topic Name** list, select the classification topic to edit, and click **Info**.

   The Classification Topic Information Page is displayed.

5. From the **Actions** menu, choose **Edit**.

6. Edit the description for the classification topic, and click **Submit Update** when done.

   A "Successfully updated classification topic" page is displayed.

7. Click **OK** to return to the Administer Classification Topic Page.

6.4.2.5 Editing Classification Topic Settings

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. From the list select the classification guide to edit topic settings for, and click **Info**.

   The Classification Guide Information Page is displayed.

3. From the **Actions** menu, choose **Configure Topics**.

   The Administer Classification Topic Page is displayed.

4. From the **Topic Name** list, select the classification topic whose settings to edit, and click **Info**.

   The Classification Topic Information Page is displayed.

5. From the Page menu, choose **Edit** then **Edit Topic Settings**.

6. Modify the default metadata field values as required, and click **Submit Update** when done.

   The Edited Topic Settings page is displayed.

7. Click **OK** to return to the Administer Classification Topic Page.

6.4.2.6 Deleting a Classification Topic

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. In the list select the classification guide whose topic to delete, and click **Info**.

   The Classification Guide Information Page is displayed.

3. From the Page menu, choose **Configure Topics**.

   The Administer Classification Topic Page is displayed.

4. From the **Topic Name** list, select the classification topic to delete, and click **Delete**.

   A message is displayed stating the classification topic was successfully deleted.

5. Click **OK** to return to the Administer Classification Topic Page.

6.4.2.7 Viewing Classification Topic Information

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

1. Click **Configure** then **Classification** then **Configure Classification Guide** from the Configure Retention Settings Page.

   The Configure Classification Guide Page is displayed.

2. In the list, select the classification guide whose topic information is to be viewed, and click **Info**.

   The Classification Guide Information Page is displayed.

3. From the Page menu, choose **Edit** then choose **Configure Topics**.

   The Administer Classification Topic Page is displayed.

4. From the **Topic Name** list, select the classification topic to view, and click **Info**.

   The Classification Topic Information Page is displayed.

5. Click **OK** to return to the Administer Classification Topic Page.

7

Configuration Options

This chapter contains information for administrators who are responsible for configuring the system, usually those with the Records Administrator role. Certain configuration procedures described here and in other chapters may also apply to other users if they have been given the appropriate rights. The required rights are noted for each procedure.

This chapter covers the following topics:

7.1 Retention Options

Several system-wide configuration settings are specified on the Configure Retention Settings Page. This chapter discusses the following specific configuration screens and tasks. Other configuration options are discussed in the remaining chapters of this book.

Most of these options can be set by selecting the checkbox next to the option. For details about each option, see "Configure Retention Settings Page" on page A-6. Other options which require further configuration are discussed later in this section.

General configuration choices are available by clicking **Records** then **Configure** from the Top menu. Click **Settings** to display the Configure Retention Settings Page.

General options:

- Start of fiscal calendar: sets the start date for the calendar used for fiscal accounting. See "Setting the Fiscal Calendar" on page 7-3 for details.
- Archive Meta Data Format: sets the storage file format for metadata of items in a disposition bundle.
- Log Metadata Changes: enables tracking of item-level metadata changes.
- Disable life cycle updates: stops the updating of disposition dates and review date computation.
- Enable Report Exclude Search Options: enables an option that allows a user to exclude reports from searches.

Record Definition options:

- Always restrict revisions/Never restrict revisions: allows revisions of content items or prevents revisions.
- Always restrict deletions/Never restrict deletions: allows deletions of content items or prevents deletions.
- Always restrict edits/Never restrict edits: allows edits of content or prevents content editing.
- Display record icon when: indicates when a record icon should be displayed. Options include when editing, deleting, or revisioning of content is restricted or any combination of those actions. The appearance of the record icon can also be disabled. The icon can assist users to determine the status of content (that is, if it is considered a record for tracking purposes).

Security options:

- ACL-based security: enables security based on access control lists.
- Default Content Server security on Retention Schedule objects: enables default security on categories, folders, and triggers.
- Supplemental Markings: enables supplemental marking security on retention objects.
- User must match all supplemental markings: forces a user to match all markings to access an item.
- Custom security fields: enables the ability to create custom security fields.
- Classified security: enables classified security features (required for conformance to the Chapter 4 Classified Records section of the DoD 5015.2 specification).

Notification options:

- Do not notify authors: prevents e-mail notifications to be sent for pending events, reviews, and the Notify Authors disposition action.

Scheduling options:

- Only allow scheduled screening: prevents users from starting screenings manually by hiding the "Search" button on the screening page.

User interface options:

- User-friendly disposition: enables user-friendly language for disposition rules and processing.
- Show export date: enables users to export items that changed since a specific date.
- Use Page Navigation: displays more elaborate page navigation controls on screening results lists and record folder lists.
- Paginate Navigation Tree: displays the retention schedule in the Browse Content menu as a tree-like structure when using the Trays layout. If more than 20 items are available for viewing, an option appears to view the next 20 items in the structure.

DoD Configuration options:

- Enable custom scripting: allows creation of custom scripts for security or for notifications.

Classified topic options:

- Run auto computation of declassification date: compute the declassification date for classified objects.
- Maximum years before declassifying: sets the number of years after which content is declassified.

7.1.1 Setting the Fiscal Calendar

The fiscal calendar is the calendar used by an organization for financial and accounting purposes. A fiscal year may coincide with a calendar year (that is, run from January 1 to December 31), but it does not need to.

Specify the start date of the fiscal year once, unless the organization changes the fiscal start date or the start date varies from year to year. The fiscal start date may need to be set manually each year if your organization has a unique fiscal calendar start, such as the first Monday of each year, for example, because a date does not fall on the same weekday each year.

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

To set the fiscal calendar start date, complete the following steps:

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

   The Configure Retention Settings Page is displayed.

2. Specify the date the fiscal year begins for the organization in the **Start of Fiscal Calendar** box. To enter a date, enter the starting date and select the month from the list. For example, if your organization starts its fiscal calendar on April 1, type 1 and select April from the list of months.

3. Click **Submit Update**.

   A message is displayed saying the configuration was successful.

4. Click **OK**.

7.1.2 Setting Performance Monitoring

You can enable performance monitoring 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.

For details about using performance monitoring, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

7.2 PCM Options

Some general configuration options for Physical Content Management are available on the Configure Physical Settings Page. This is similar to the Configure Retention Settings Page where a series of options are used to determine system functionality.

To access this page, click **Physical** then **Configure** then **Settings** from the Top menu. Other configuration options are available on the **Configure** menu, such as setting up chargebacks, invoices, and other aspects of Physical Content Management.

Other chapters in this guide discuss how to configure components to use for Physical Content Management. See Chapter 8, "Configuring Physical Content Management" and Chapter 9, "Setting Up PCM Storage Space" for details and see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for additional information

The following options appear on the Configure Physical Settings Page:

- Default Transfer Method: specifies the default transfer method (copy, fax, mail, and so on).
- Default Request Priority: specifies the default priority to be used for reservations (no priority, rush, this week, and so on).
- Default Checkout Period (days): specifies the number of days a reserved physical item can be checked out.
- Delete completed requests: specifies if completed reservation requests are automatically deleted after a specified number of days.
- Request history period (days): the maximum number of days a reservation request is stored in history.
- Check in internal content item for reservation workflow: specifies if a new internal content item should be checked in when a reservation request is made.
- Do not notify users when checked-out items are overdue: specifies that users with late items receive an e-mail notification.
- Allow reservation requestors to modify/delete their reservations: specifies if users who create a reservation request can modify or delete their open requests.
- Automatically update request waiting list: specifies if waiting lists for requests are updated automatically.
- Show batch services: specifies if batch services are available in the External Content menu.
- Enable offsite functionality: specifies if the storage of content offsite is enabled. When this is enabled, new metadata fields are added to the system as well as the Offsite security group.

7.3 Setting Up Workflows

Important: Workflow creation is only needed to enable category disposition approval processing, reservation processing, or offsite request processing. If you do not need that functionality, you do not need to set up any workflows.

Workflows are used to specify how content is routed for review, approval, and release to the system. A criteria workflow is used for content that enters the review process automatically, based on metadata matching predefined criteria. A basic workflow is one used to process specific content items.

Three specific criteria workflows must be set up in order for the following functionality to work:

- **Category Disposition Approval Processing**: set up to route category dispositions for review and approval.
- **Reservation Processing**: set up to route reservation requests for physical content for processing.
- **Offsite Processing**: set up to process requests for offsite storage of items.

A workflow is composed of several steps which route the content to groups of people in an alias list. It can be customized to exit when completed, branch content depending on certain conditions, and use variables to designate unknown users.

After a workflow is enabled, it goes through several specific stages:

- When a content item is approved by the minimum number of reviewers for a particular step, it goes to the next step in the workflow.
- If the step is defined with 0 approvals required, the reviewers are notified, but the content goes to the next step automatically. This is useful to ensure that the proper people are aware that an item is in the workflow process.
- If any reviewer rejects the content, it goes back to the most recent Review/Edit Revision or Review/New Revision step. If there is no such step, the content goes back to the original author.
- Depending on how the edit criteria is defined, the most recent Review/Edit Revision or Review/New Revision step may result in a new revision or an updated revision.
- A revision may be released to the system:
  - After it exits the workflow: When content is approved at the last step in the workflow, the content item is released to the system.
  - Before it exits the workflow: When you set up a side effect that releases a document from edit state, the document is available for indexing, searching, and archiving. This is useful primarily for business routing that doesn't require publishing to the web, for example an expense report.
- Generally, if a Basic workflow contains multiple content items, none of them will be released to the system until all of the items have been released from completion of the workflow. However, if a content item is released from edit state as a side effect, that content item can be released without waiting for all items in the Basic workflow.

Workflows are discussed in detail in the *Oracle Fusion Middleware Application Administrator's Guide for Content Server*. This section describes only the information needed to establish the three workflows necessary for Oracle URM.

7.3.1 Workflow Prerequisites and Process

The following steps briefly explain the Criteria workflow process and some of the tasks that should be performed before setting up the workflow:

1. A user with Workflow rights sets up the Criteria workflow by defining the following:
   - **Security groups**: the RecordsGroup, Reservation and Offsite security groups are required.
   - **Metadata fields and values**: these fields are set up at installation (for example, *OffsiteRequest*.)

- **Review steps** and **reviewers** for each step: it is good practice to discuss workflows with the people involved so they are aware of the responsibilities they will have in the process.
- If a group of people need to be included in an **alias** that should be created ahead of time. The following alias lists are needed:
  - *Disposition Reviewers*: those people who will review disposition criteria. Suggested name: DispositionReviewGroup.
  - *Reservation Reviewers*: those people who can approve reservation requests. Suggested name: ReservationGroup.
  - *Offsite Request Reviewers*: those people who review requests for offsite storage. Suggested name: OffSiteRequestReviewGroup.

  See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about adding aliases and adding users to alias groups.

2. A user with Workflow rights starts the Criteria workflow by enabling it.
3. When content is checked in with the defined security group and metadata field value, the content enters the workflow.
4. Reviewers for the first step are notified by e-mail that the revision is ready for review.
5. The reviewers approve or reject the revision.
   - If the step is a reviewer/contributor step, the reviewers can check out the revision, edit it, and check it back in before approving it. For example, administrators may need to alter a reservation request.
   - If a user rejects the revision, the workflow returns to the previous contribution step, and the users for that step are notified by e-mail.
   - When the minimum number of users have approved the revision, it goes to next step. (If the minimum number of approvals is 0, the revision moves to the next step automatically.)
6. When all steps are complete, the revision is released to the system.

7.3.2 Creating Oracle URM Workflows

Permissions: The Rights.Apps.Workflow right is required to perform this task. This right is **not assigned by default** to any role. It must be assigned to a role before a workflow can be created.

This section details the specific requirements for the three workflows needed for Oracle URM functionality.

7.3.2.1 Category Dispositions Workflow

The Category Disposition Workflow is used to approve the disposition rules on a category before the rules are enacted.

1. Click **Administration** then **Admin Applets** from the Main menu.

   The Administration Applets Page is displayed.
2. Click **Workflow Admin**.

The Workflow Admin dialog is displayed.

3. Click the **Criteria** tab. Click **Add**.

   The New Criteria Workflow dialog is displayed.

4. Enter the following information:

   - **Workflow name**: *CategoryDispositionsProcess*
   - **Description**: *Category Disposition Processing*
   - **Security Group**: select *RecordsGroup* from the dropdown list
   - **Original Author Edit Rule**: select *Edit Revisio*n
   - **Has Criteria Definition**: click this checkbox
   - **Field**: select *Type* from the dropdown list
   - **Operator**: this should say "Matches"
   - **Value**: select *RetentionCategory* from the dropdown list

   Click **OK** when done. The Workflow Admin dialog is redisplayed.

5. In the Criteria portion of the dialog, in the Steps section, click **Add**.

   The Add New Step dialog is displayed.

6. Enter the following information:

   - **Step name**: *CategoryDispositionsReview*
   - **Description**: *Review Category Dispositions*
   - **Users can review and edit (replace) the current revision**: check this box
   - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will be reviewing dispositions and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, click the checkbox for **All Reviewers**.

7. Click **OK**. The Workflow Admin dialog is redisplayed.

8. Click **Enable** to start the workflow.

7.3.2.2 Reservation Processing Workflow

The Reservation workflow is used to process reservation requests for physical items.

1. Click **Administration** then **Admin Applets** from the Main menu.

   The Administration Applets Page is displayed.

2. Click **Workflow Admin**.

   The Workflow Admin dialog is displayed.

3. Click the **Criteria** tab. Click **Add**.

   The New Criteria Workflow dialog is displayed.

4. Enter the following information:

   - **Workflow name**: *ReservationProcess*
   - **Description**: *Processes reservations*
   - **Security Group**: select *Reservation* from the dropdown list

- **Original Author Edit Rule**: select *Edit Revision*
- **Has Criteria Definition**: click this checkbox
- **Field**: select *Type* from the dropdown list
- **Operator**: this should say "Matches"
- **Value**: select *Request* from the dropdown list

Click **OK** when done. The Workflow Admin dialog is redisplayed.

5. In the Criteria portion of the dialog, in the Steps section, click **Add**.

   The Add New Step dialog is displayed.

6. Enter the following information for the first step:
   - **Step name**: *RequestReview*
   - **Description**: Review Request
   - **Users can review and edit (replace) the current revision**: check this box
   - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will be reviewing reservation requests and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, click the checkbox for **At Least This Many Reviewers** and enter 1 for the value.
   - Click **OK**. The Workflow Admin dialog is redisplayed.
7. In the Criteria portion of the dialog, in the Steps section, click **Add**.

   The Add New Step dialog is displayed.

8. Enter the following information for the second step:
   - **Step name**: *RequestComplete*
   - **Description**: *Complete the request*
   - **Users can review the current revision**: check this box
   - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will be completing the reservation requests and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, click the checkbox for **At Least This Many Reviewers** and enter 0 for the value.
   - Click the **Events** tab.
     - Click **Edit** in the Entry section. Click the **Custom** tab then click the **Custom Script Evaluation** checkbox. Enter the following code

       ```
       <$wfSet("wfJumpName", "complete")$>
       <$wfSet("wfJumpEntryNotifyOff", "1")$>
       ```

       Click **OK**.

     - Click **Edit** in the Update section. Click the **Custom** tab then click the **Custom Script Evaluation** checkbox. Enter the following code:

       ```
       <$if parseDate(dOutDate) < parseDate(dateCurrent(1))$>
       <$wfSet("wfJumpName", "complete_update")$>
       <$wfSet("wfJumpTargetStep", wfCurrentStep(10))$>
       <$wfSet("wfJumpEntryNotifyOff", "1")$>
       <$endif$>
       ```

Click **OK**.

9. Click **OK**. The Workflow Admin dialog is redisplayed.
10. Click **Enable** to start the workflow.

7.3.2.3 Offsite Storage Workflow

The Offsite Storage workflow is used to process requests to store physical items offsite.

1. Click **Administration** then **Admin Applets** from the Main menu.

   The Administration Applets Page is displayed.
2. Click **Workflow Admin**.

   The Workflow Admin dialog is displayed.
3. Click the **Criteria** tab. Click **Add**.

   The New Criteria Workflow dialog is displayed.
4. Enter the following information:
   - **Workflow name**: *OffsiteProcess*
   - **Description**: *Processes Offsite Requests*
   - **Security Group**: select *Offsite* from the dropdown list
   - **Original Author Edit Rule**: select *Edit Revision*
   - **Has Criteria Definition**: click this checkbox
   - **Field**: select *Type* from the dropdown list
   - **Operator**: this should say "Matches"
   - **Value**: select *Offsiterequest* from the dropdown list

   Click **OK** when done. The Workflow Admin dialog is redisplayed.
5. In the Criteria portion of the dialog, in the Steps section, click **Add**.

   The Add New Step dialog is displayed.
6. Enter the following information for the first step:
   - **Step name**: *OffsiteRequestReview*
   - **Description**: Review Offsite Request
   - **Users can review and edit (replace) the current revision**: check this box
   - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will be reviewing reservation requests and click **OK**.
   - Click the **Exit Condition** tab. In the Required Approvers portion, click the checkbox for **At Least This Many Reviewers** and enter 1 for the value.
7. Click **OK**. The Workflow Admin dialog is redisplayed.
8. Click **Enable** to start the workflow.

7.4 Configuration with Desktop Integration Suite

When using Oracle DIS with Oracle URM with the DoD compliance component enabled, users may not be able to check in files by copying and pasting or by dragging and dropping them into contribution folders. DoD compliance requires that the

Category or Folder fields be required during checkin, which means an item cannot be checked in if the field is empty.

Because copying and pasting or dragging and dropping into a folder often doesn't require any additional user interaction, the checkin won't complete successfully unless the administrator configures Oracle URM to enable such checkins.

Several workarounds for this issue are available:

- Set default metadata for the folders by selecting the category and folder from the available selections
- Set default metadata for users by creating a global rule when setting up profiles.
- Change the configuration of the system by setting the `dodSkipCatFolderRequirement` variable.

7.5 Configuration Variables

Several configuration variables are available that can be included (or modified) in a configuration file to change the behavior or interface of the software.

In addition to the configuration variables described here, flags in the rma_email_environment.cfg file can be set to determine which fields can be edited during events such as checkin and update for e-mail content. The flags are a double-colon-separated list.

The following section describes some of the more commonly used configuration variables.

- "RmaAllowKeepOrDestroyMetadataOption" on page 7-14

7.5.1 UieHideSearchCheckboxes

Use this configuration variable to show or hide the metadata field boxes on the search page, which limit the number of metadata fields initially shown on the page.

- `UieHideSearchCheckboxes=true`: The metadata field boxes are not shown on the search page.
- `UieHideSearchCheckboxes=false`: The metadata field boxes are shown on the search page.

The default setting is `TRUE`, so the metadata field boxes are not displayed.

Restart the Content Server for this setting to take effect.

7.5.2 RmaNotifyDispReviewerAndCatAuthor

By default, when events are triggered by a disposition rule, both the specified notification reviewer and the original category author receive e-mail notifications about the event. Use this configuration variable to control who is notified.

- `RmaNotifyDispReviewerAndCatAuthor=true`: Both the specified notification reviewer and the category author receive e-mail notifications.
- `RmaNotifyDispReviewerAndCatAuthor=false`: Only the category author receives e-mail notifications.

The default setting is `TRUE`, so both the specified notification reviewer and the category author receive e-mail notifications.

Restart the Content Server for this setting to take effect.

7.5.3 RmaNotifyReviewerAndAlternateReviewer

Users can select an alternate user to perform review actions and process assigned disposition events (for example, if they are out of the office for some time). By default, only the alternative reviewer receive e-mail notifications about the action.You can use this configuration variable to control who is notified.

- `RmaNotifyReviewerAndAlternateReviewer=true`: Both the specified alternative reviewer and the original user receive e-mail notifications.
- Default: `RmaNotifyReviewerAndAlternateReviewer=false`: Only the alternative reviewer receives e-mail notifications.

The default setting is `FALSE`.

Restart the Content Server for this setting to take effect.

7.5.4 RecordsManagementNumberOverwriteOnDelete

Use this configuration variable to set the number of disk scrubbing passes used for a destroy action.

- `RecordsManagementNumberOverwriteOnDelete=`*Number:* Where *Number* is the number of passes.

The default number of scrubbing passes is 2.

Restart the Content Server for this setting to take effect.

7.5.5 RMAHideExternalFieldsFromSearchInfo

Use this configuration variable to hide external fields on the Search and Info pages. The default setting is TRUE, meaning External fields are hidden on those screens.

- `RMAHideExternalFieldsFromSearchInfo=true`: This hides the external fields on the Search and Info pages.
- `RMAHideExternalFieldsFromSearchInfo=false`: This displays the external fields on the Search and Info pages.

Restart the Content Server for this setting to take effect.

7.5.6 RMAHideExternalFieldsFromCheckInUpdate

Use this configuration variable to hide external fields on the Checkin and Update pages. The default setting is `TRUE`, meaning External fields are hidden on those screens.

- `RMAHideExternalFieldsFromCheckInUpdate=true`: This hides the external fields on the Checkin and Update pages.
- `RMAHideExternalFieldsFromSearchInfo=false`: This displays the external fields on the Checkin and Update pages.

Restart the Content Server for this variable to take effect.

7.5.7 AllowRetentionPeriodWithoutCutoff

This variable specifies retention periods for triggers. To use this functionality, add this variable to the records_management_environments.cfg file.

- `AllowRetentionPeriodWithoutCutoff=true`: retention periods for triggers for content is enabled. Default.
- `AllowRetentionPeriodWithoutCutoff=false`: retention periods are disabled.

Restart the Content Server for this variable to take effect.

7.5.8 RmaAddDocWhereClauseForScreening

This variable allows users with the Records Administrator role to screen for frozen items to which they do not have access (using ACLs) on the screening page or on the Freeze Information Page.

- `RmaAddDocWhereClauseForScreening=false`: frozen items can be screened. Default.
- `RmaAddDocWhereClauseForScreening=true`: frozen items cannot be screened.

The default is `FALSE`.

Restart the Content Server for this setting to take effect.

7.5.9 RecordsManagementDenyAuthorFreePassOn RMSecurity

This variable allows the author of content to delete content they authored regardless of the user's security settings.

- `RecordsManagementDenyAuthorFreePassOnRMSecurity=TRUE`: Authors are not allowed to delete content they authored.

- `RecordsManagementDenyAuthorFreePassOnRMSecurity=FALSE`: Authors are allowed to delete content they authored.

The default is `FALSE`.

Restart the Content Server for this setting to take effect.

7.5.10 HideVitalReview

This variable hides the Subject to Review related fields.

- `HideVitalReview=true`: Subject to Review fields are hidden.
- `HideVitalReview=false`: Subject to Review fields are revealed.

Restart the Content Server for this setting to take effect.

7.5.11 RmaEnableWebdavPropPatchOnExport

This variable enables WebDAV support of a PropPatch method to assign metadata values to a file that has been uploaded to a WebDAV server.

- `RmaEnableWebdavPropPatchOnExport=true`: Enables the PropPatch method.
- `RmaEnableWebDavPropPatchOnExport=false`: The method is not enabled.

Restart the Content Server for this setting to take effect.

7.5.12 SimpleProfilesEnabled

This variable enables the Simple Profile functionality.

- `IsSimpleProfilesEnabled:=true`: Enables Simple Profile functionality.
- `IsSimpleProfilesEnabled=false`: Disables Simple Profile functionality.

Restart the Content Server for this setting to take effect.

7.5.13 RmaEnableFixedClone

This variable enables the fixed clone functionality which allows the create of record clones of content revisions.

- `RmaEnableFixedClones=true`: Enabled fixed clone functionality.
- `RmaEnableFixedClones=false`: Disables fixed clone functionality.

Restart the Content Server for this setting to take effect.

7.5.14 RmaFixedClonesTitleSuffix

This variable is used to set the suffix that is automatically appended to a fixed clone content item.

Default: `RmaFixedClonesTitleSuffix=(fixed clone)`

Restart the Content Server for this setting to take effect.

7.5.15 ShowContentForStorageBrowse

This variable is used to show content items in the storage browse screens.

- `ShowContentForStorageBrowse=true`: Displays content items in the storage browse screens.

- `ShowContentForStorageBrowse=false`: Hides content items in the storage browse screens.

Restart the Content Server for this setting to take effect.

7.5.16 RmaFilePlanVolumePrefix and RmaFilePlanVolumeSuffix

These variables are used to define the naming convention for volumes. The usual convention is `prefix+timestamp+suffix`. Use these variables to define the prefix and suffix. If neither is define, a prefix of `volume_` is used by default.

- `RmaFilePlanVolumePrefix=`*value*: Sets the prefix used to *value*.
- `RmaFilePlanVolumeSuffix=`*value*: Sets the suffix used to *value*.

Restart the Content Server for this setting to take effect.

7.5.17 RmaEnableFilePlan

This variable enables File Plan folder structure functionality.

- (default) `RmaEnableFilePlan=false`: Disables the folder structure used with MoReq2 file plans.
- `RmaEnableFilePlan=true`: Enables folder structure for use with MoReq2 file plans.

Restart the Content Server for this setting to take effect.

7.5.18 RmaEnablePostFilterOnScreening

This variable enables additional security on screening results. If a user does not have appropriate security for an item in a screening result list, that item is hidden from view.

- Default: `RmaEnablePostFilterOnScreening=true`: Enable filtering on screening results.
- `RmaEnablePostFilterOnScreening=false`: Disables additional security on screening results.

Restart the Content Server for this setting to take effect.

7.5.19 dodSkipCatFolderRequirement

This variable allows an item to be checked in without specifying a category or folder for the checkin. If a DoD configuration is in use, this will cause non-conformance with DoD regulations.

- Default: `dodSkipCatFolderRequirement=true`: Items must be checked in with a category or folder specified.
- `dodSkipCatFolderRequirement=false`: Items may be checked in without specifying a category or folder.

Restart the Content Server for this setting to take effect.

7.5.20 RmaAllowKeepOrDestroyMetadataOption

This variable allows the option to keep or detroy metadata when using the following disposition actions: Delete All Revisions, Accession, Archive, Move, and Transfer. See "Disposition Actions" on page 14-6 for details.

- `RmaAllowKeepOrDestroyMetadataOption=true`: Enables the user of the keep/destroy option.
- `RmaAllowKeepOrDestroyMetadataOption=false`: Disables the use of this option.

Restart the Content Server for this setting to take effect.

8

Configuring Physical Content Management

This chapter is for content administrators who are responsible for configuring Physical Content Management (generally those with the PCM Administrator ('pcmadmin') role). This functionality is only available if PCM has been enabled. It is enabled by default for all levels except the Minimal level.

This chapter covers the following topics:

Concepts

Tasks

Examples

8.1 About Physical Content Management

PCM is used to manage physical records and content that are not stored in the repository in electronic form (for example, physical media such as compact disks). All items, both internal and external, regardless of their source or format are managed using a single user interface. The same retention schedule can be used for both electronic (internal) and physical (external) content.

With PCM the storage location and retention schedules of the physical items can be tracked. This is done by using several key features:

- **Space management**: defines how items will be stored, from the largest storage area (warehouse layouts) to fine details (cases, shelves, bins).
- **Circulation services**: sets up reservations for handling requests for items, checking them out to users and tracking the space used and available space.
- **Chargeback services**: defines costs for storage services or other actions performed on physical items. These costs can then be invoiced to defined customers.
- **Barcode processing**: defines barcodes for customers and for storage locations, enabling quick processing of reservations, storage, and invoicing information. Barcode data can be uploaded automatically into PCM or can be entered manually.
- **Label creation and printing**: in conjunction with barcodes, can be used to create barcode labels to be used with items, storage, and customers.
- **Retention management**: sets up retention schedules for external items and freezes them, sends email for pending events, or performs periodic reviews of storage and items.

In addition to storing items locally, offsite storage capabilities can be set up to move archive content to a different location. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about setting up offsite storage.

The following list describes the tasks needed to set up a PCM environment.

- **Establish the required user roles and rights**. See Chapter 5, "Setting Up Security" for details.
- **Configure chargeback processing**, which includes defining payment types (credit, cash, and so on), charge types (billable events), and customers (organizations or users who are billed for services). See "Configuring Chargeback Processing" on page 8-3 for details.
- **Configure location types**, which define the locations that hold physical content. Location types can include warehouses, rooms, bays, shelves, and other storage areas. See "Configuring Location Types" on page 8-3 for details.
- **Configure object types**, which define the kinds of items stored in the locations. A storage location can hold a specific kind of object, and if a user attempts to store an object in an incorrect location, an error occurs. See "Configuring Object Types" on page 8-7 for details.
- **Configure media types**, which define what kinds of media are associated with objects. For example, 'optical' is a type of object and it can have several different media types: mixed, CD, Disc, or DVD. See "Configuring Media Types" on page 8-9 for more details.
- **Configure default reservation information**. Default metadata values can be set for reservations and for items that will be stored offsite (as discussed in the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*). See

"Configuring Default Metadata Values: Offsite and Reservations" on page 8-12 for details.

- **Create barcode labels for content, storage and users**. Default values are provided for users but barcode labels can also be designed. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about creating and editing labels.
- **Define your storage space environment**. After defining location, object, and media *types*, assign relationships in the storage space to those types. See Chapter 9, "Setting Up PCM Storage Space" for details about this process.
- **Create disposition rules for physical content** (if required). This is similar to creating rules for non-physical content. That process is discussed in Chapter 10, "Setting Up a Retention Schedule", Chapter 14, "Defining Disposition Instructions", and Chapter 15, "Setting Up Freezes".

8.2 Configuring Chargeback Processing

Chargebacks are fees charged to people or businesses for the use of storage facilities or actions performed on physical items in the storage facilities. The Physical Content Management functionality can be used to generate invoices for the storage, use, reservation, and destruction of the managed content. These invoices can then be sent to the internal or external customers in accordance with the applicable business procedures.

Depending on rights and roles assigned, users or administrators can set up chargebacks and customers. See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about configuring chargebacks and customers.

8.3 Configuring Location Types

Permissions: The PCM.Admin.Manager right is required to set up location types. This right is assigned by default to the PCM Administrator role.

Location types are used in the definition of the storage space holding the physical content. They represent the hierarchy of storage units where items can be stored. The Physical Content Management functionality uses the location types and their defined hierarchy to keep track of the locations of the managed external physical content. Reordering location types does not affect any existing storage locations.

8.3.1 Predefined Location Types

The out-of-the-box Physical Content Management functionality comes with the following six predefined location types (in hierarchical order), with their standard icons for the default Trays layout:

Predefined Location Types	Icon (large)	Allows Storage of Content (Default)
Warehouse		No

Predefined Location Types	Icon (large)	Allows Storage of Content (Default)
Room		No
Row		No
Bay		No
Shelf		No
Position		Yes

These are the default settings, which can be modified. Storage of content applies to a particular level only, not to any lower levels. For example, in the default hierarchy shelves have several positions, each of which can hold content items, but no content items can be directly assigned to the shelf level (only to the positions on a shelf). The location type 'Shelf' cannot store content, whereas the type 'Position' can.

These predefined location types are hierarchical: a warehouse consists of one or more rooms, a room consists of one or more rows, a row consists of one or more bays, and so on.

8.3.2 Location Type Icons

Each defined location type can be assigned an icon used to indicate the location type of storage locations. The icons are located in /weblayout/ resources/layouts/*Layout_Name*/*Skin_Name*/Pcm_Icons, and come in three varieties:

- *Name*_lg.gif: This is the large variety of the icon (32x32 pixels), used in the thumbnail view of the exploring pages.
- *Name*_sm_closed.gif: This is the small variety of the icon (16x16 pixels) used to indicate the location types of storage locations in the storage space tree view. This appears in the Trays layout when the child tree below the storage location is collapsed or when there are no child storage locations.
- *Name*_sm_open.gif: This is the small variety of the icon (16x16 pixels) used to indicate the location types of storage locations in the storage space hierarchy when the child tree below the storage location is opened.

The open and closed icons for the predefined location types are identical, but they do not need to be.

8.3.2.1 Adding Customized Icons

Customized icon files can be added to the image selection list for location types by copying three gif files with the above naming pattern) for each icon to the appropriate Pcm_Icons directories. For example, you could create icon files called Storage_archive_lg.gif (32x32 pixels), Storage_archive_sm_open.gif (16x16 pixels), and Storage_archive_sm_closed.gif (16x16 pixels), and copy these to the previously mentioned directory to make them available in the default Trays layout.

If icons were created in a previous version of this software they are not automatically transferred during an upgrade. They must be copied after upgrading.]

8.3.3 Creating or Editing a Location Type

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Use this procedure to create a new location type to be used in the definition of the storage space environment. The following information is a general navigational procedure. To view a specific example of creating a custom metadata field, see "Example: Creating a Location Type" on page 8-6

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

   The Configure Location Types Page is displayed.

2. Click **Add**.

   The Create or Edit Location Type Page is displayed.

3. Specify the properties of the location type and click **OK**.

   The new location type is now added to the bottom of the list on the Configure Location Types Page. If required, use the up and down arrows to move the new location type to its new position in the location type hierarchy.

To modify a location type, select the type to edit in the list and click **Edit** from the **Action** menu. Modify the properties as required and click **OK** when finished.

8.3.4 Viewing Location Type Information

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Use this procedure to view information about an existing location type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

   The Configure Location Types Page is displayed.

2. Select the location type and click the **Info** icon.

   The Location Type Information Page is displayed. When done viewing information, click **OK**.

8.3.5 Deleting a Location Type

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Use this procedure to delete an existing location type. Note that this does not delete the location. It deletes the location type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

   The Configure Location Types Page is displayed.

2. Select the location type to delete and click the **Info** icon.

   The Location Type Information Page is displayed. Choose **Delete** on the Page menu.

8.3.6 Reordering Location Types

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Use this procedure to change the hierarchical order of the defined location types.

Important: Reordering location types does not affect existing storage locations. You must remove the existing storage locations and rebuild the storage environment if you want it to match the reordered location types.

---

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

   The Configure Location Types Page is displayed.

2. Use the up and down arrows to move location types to the new level in the hierarchy.

3. Repeat this step for every location type to move until the new storage hierarchy is achieved.

4. When finished, click **Submit Update**.

   A message is displayed saying the location types were configured successfully.

5. Click **OK** to return to the Configure Location Types Page.

8.3.7 Example: Creating a Location Type

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this example. These rights are assigned by default to the PCM Administrator role.

This example creates a location type called "Box," located at the bottom level of the storage level hierarchy (below "Position"). Therefore, each position contains one or more boxes, each of which can contain a maximum of five physical content items.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

The Configure Location Types Page is displayed.

2. Click **Add**.

   The Create or Edit Location Type Page is displayed.

3. In the **Location Type ID** field, type `Archive`.
4. In the **Name** field, type `Box`.
5. In the **Description** field, type a description of the location type (optional).
6. In the **Tooltip** field, type a tooltip for the location type (optional).
7. Make sure the **Allow storage of content (default)** box is selected, and enter `5` in the **Content Items Allowed** field.
8. In the **Images** list, choose the storage_box_lg.gif icon image. This image is used to indicate the location type of storage locations in the Browse Storage tree in the Trays layout.
9. Click **OK**.

   A message is displayed saying the location type was created successfully, along with the properties of the newly created location type.

10. Click **OK**.

    The Configure Location Types Page is displayed with the new location type "Box" added to the bottom of the list of location types.

8.4 Configuring Object Types

Object types define the types of items storage locations can hold. The out-of-the-box Physical Content Management functionality comes with several predefined object types, but new types can be created.

When creating a physical item, specify its object type. If you select an object type that is not allowed for the assigned storage location, an error message is displayed and you cannot check in the physical item.

Object types can hold other object types. For example, the predefined Box object type can hold the following predefined object types: Folder, Optical, Micro, Document, and Tape. Relationships between object types are defined on the Edit Object Type Relationships Page.

8.4.1 Predefined Object Types

The out-of-the-box Physical Content Management functionality comes with the following predefined object types:

- All (any of the predefined object types, including custom types). Note that an "All" object type cannot be assigned to a physical item in this version of the software.
- Box
- Document
- Folder
- Micro
- Optical
- Tape

You can further specify what a storage location can hold using media types (see "Configuring Media Types" on page 8-9).

You do not need to specify an object type when creating a storage location. The storage location can then hold any type of content. If you do select an object type, and you attempt to assign a physical item of a different object type to the storage location, an error message is displayed and you cannot check in the physical item.

8.4.2 Creating or Editing an Object Type

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to create a new object type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**.

   The Configure Object Types Page is displayed.

2. Click **Add** in the Object Types Table area.

   The Create or Edit Object Type Page is displayed.

3. Specify the properties of the object type and click **Create**.

   A page is displayed confirming the object type was created successfully.

4. Click **OK**.

The new object type is now added to the list of object types on the Configure Object Types Page and can be selected on the Create or Edit Physical Item page.

To edit an object type, click **Edit Object Type** from the item's **Action** menu.

8.4.3 Viewing Object Type Information

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to view information about an existing object type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**.

   The Configure Object Types Page is displayed.

2. In the list of existing object types, select the object type and click the **Info** icon.

3. When finished, click **OK** to return to the Configure Object Types Page.

8.4.4 Deleting an Object Type

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to delete an existing object type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**.

   The Configure Object Types Page is displayed.

2. In the list of existing object types, click **Delete Object Type** from the **Action** menu for the object. To delete multiple types, click the checkbox for the type then click **Delete** in the Table menu.

   The object type is deleted, and a message to that effect is displayed.

3. Click **OK** to return to the Configure Object Types Page.

8.4.5 Editing Object Type Relationships

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to edit the relationship between an object type and the other defined object types.

To edit object type relationships, complete the following steps:

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**.

   The Configure Object Types Page is displayed.

2. In the list of existing object types, select the item to edit and click **Edit Object Type Relationships** in the **Action** menu.

   The Edit Object Type Relationships Page is displayed).

3. Make sure the Assigned Object Types box contains all object types that can be contained within the current object type. If not, select the appropriate item in the Unassigned Object Types box and click **Add** to move it to the Assigned Object Types box.

4. Click **Submit Update** when finished.

   The object type relationships are updated, and the Object Type Information Page is displayed again with updated values for the **Object Type Hold** field.

8.5 Configuring Media Types

Media types are an extension to object types (see "Configuring Object Types" on page 8-7) and provide a further specification about the type of content that can be contained in a storage location.

When creating a physical item, specify its media type. The available media types depend on the selected object type for the physical item. If you select a media type that is not allowed for the assigned storage location, an error message is displayed and you cannot check in the physical item.

8.5.1 Predefined Media Types

The out-of-the-box Physical Content Management functionality comes with the following predefined media types:

Predefined Media Types	Object Type
Box	Box
Mixed Fax Paper Photo	Document
Folder	Folder
Mixed Microfiche Microfilm	Micro
Mixed CD Disc DVD	Optical
Mixed Audio Data Visual	Tape
Mixed Audio Box CD Data Disc Dvd Fax Folder Microfiche Microfilm Paper Photo Visual	All

8.5.2 Creating or Editing a Media Type

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to create a new media type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Media Types**.

   The Configure Media Types Page is displayed.

2. Click **Add** in the Media Types area.

   The Create or Edit Media Type Page is displayed.

3. Specify the properties of the media type and click **Create**.

   A page is displayed confirming the media type was created successfully.

4. Click **OK**.

The new media type is now added to the list of media types on the Configure Media Types Page and it can be selected on the Create or Edit Physical Item page.

To edit a media type, click **Edit** from the media type's **Action** menu. Modify the properties as needed and click **Submit Update**.

8.5.3 Viewing Media Type Information

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to view information about an existing media type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Media Types**.

   The Configure Media Types Page is displayed.

2. In the list of existing media types, click the Info icon for the type to view.

The Media Type Information Page is displayed. When finished, click **OK** to return to the Configure Media Types Page.

8.5.4 Deleting a Media Type

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to delete an existing media type.

1. Click **Physical** then **Configure** from the Top menu. Click **Types** then **Media Types**.

   The Configure Media Types Page is displayed.

2. Click **Delete Media Type** in the **Action** menu for the item to be deleted. To delete multiple items, select the checkbox for the item and click **Delete** in the Table menu.

   The media type is deleted, and a message to that effect is displayed.

3. Click **OK** to return to the Configure Object Types Page.

8.6 Configuring Default Metadata Values: Offsite and Reservations

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). This content item automatically enters the Reservation Process workflow, if enabled, and the administrator receives a workflow review notification about the request. See "Setting Up Workflows" on page 7-4, for details about creating and enabling the reservation workflow.

After reviewing the reservation request, the administrator can further process the reservation request in accordance with the applicable procedures within the organization.

You can set the default metadata values for the reservation items that are checked into the repository. Default metadata values can be set for items that are allocated for offsite storage. The definition procedure is the same.

Important: Offsite storage options only appear if Offsite Storage functionality is enabled. To check the status, click **Physical** then **Configure** then **Settings** from the Top menu. Verify that the Offsite option is checked.

8.6.1 Setting Default Metadata Values for Reservation Items and Offsite Storage

---

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to set the default metadata values for reservation items checked into the repository. A similar process is used to set metadata values for offsite storage.

1. Click **Physical** then **Configure** from the Top menu. Click **Metadata** then **Reservation Default Metadata**. To configure offsite storage, click **Physical** then **Configure** then **Offsite** then **Offsite Default Metadata**.

   The Default Metadata for Checked-in Reservation or Offsite Entries Page is displayed.

2. Set the metadata values and click **Submit Update**.

The following defaults are set:

- The default content ID is "res" or "offsite." This is a prefix added to the ID to create the full content ID of an item (for example, "res1430068" or "offsite3921"). This setting cannot be modified.
- The default content type is "REQUEST-PCM Request" or "OFFSITEREQUEST - Offsite Request."
- The default title is "Reservation" for reservations and "Offsite Transfer Request" for offsite storage. This is a prefix added to the name to create the full title of an item (for example, "Reservation My Request").
- The default security group is "Reservation" or "Offsite."

Important: You can change the content type and security group, but if you do, you need to modify your reservation process and workflow to match the new settings.

9

Setting Up PCM Storage Space

This chapter explains how to set up and manage a storage environment in Physical Content Management.

This chapter covers the following topics:

Concepts

Tasks

Examples

See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about setting up offsite storage.

9.1 Storage Space Considerations

Storage space is discussed in more detail in the *Oracle Fusion Middleware User's Guide for Universal Records Management*. See that document for background and conceptual information.

The following considerations should be evaluated when considering storage space management:

- At the root (top) level of the storage space hierarchy ("Storage"), only the two highest level location types can be added ("Warehouse" and "Room") by default. If

more location types are needed, modify the following configuration variable in the physicalcontentmanager_environment.cfg:

```
NumberOfStorageTypeRootsToShow=x
```

where *x* is the number of location type levels needed at the highest storage level. For example, if users should be able to add storage locations of location types Warehouse, Room, or Row, change the value from 2 (default) to 3. Restart the Content Server for the change to take effect.

- There is no limit to the number of top-level storage locations that can be created (for example, one for each warehouse).
- At each level in the storage space hierarchy other than top level, only storage locations of a lower location type level can be added. For example, at the Row location type level, storage locations of the types Bay, Shelf, and Position can be added.
- Physical items not assigned to any other storage location are automatically assigned to the "Other" storage location, which is always the last of the top-level storage locations of the storage hierarchy.
- Storage locations can be deleted from the hierarchy only if no items are stored in them. The "Other" storage location cannot be deleted, even if it is empty.
- All storage locations include a percentage which shows how much of the available storage space in the location (and all its children) is currently occupied. For example, 25% means one quarter of the maximum allowed number of stored items is currently assigned to the storage location (and all its children). The percentage of a storage location is updated daily (see next note).
- By default, the available storage space for the entire hierarchy is recalculated daily at midnight. Therefore the displayed storage availability information may not be up to date as the day progresses because it still reflects the situation from the night before. If you are an administrator with the PCM.Admin.Manager right, you can force a recalculation of all available storage space by running the "Process Storage Space Counts" batch service.
- A storage location can be blocked, which prevents any content from being stored in the storage location or any of its child storage locations, even if it was marked to allow storage of content. Only empty storage locations can be blocked. For example, this can be used to create a "dummy" storage location in a situation where a bay cannot be used because there is a support pillar in front of it but matching bay numbering is necessary to retain across multiple rows.
- The `ShowContentForStorageBrowse` configuration variable can be used to hide or reveal content when browsing a storage location. Hiding content can speed response time during browsing. If set to TRUE, content is displayed. If set to FALSE, it is hidden.
- To speed response time during retrieval and browsing, set up storage so no one level has more than 100 items stored there. For example, set up a series of bays and each bay would contain 100 shelves with a maximum of 100 items on the shelf. This will speed up the browsing of objects in storage. It is also recommended that items be stored only at the shelf and position levels, not at the warehouse, room, row, or bay level. This will also speed retrieval and browsing times.

9.2 Browsing the PCM Storage Space

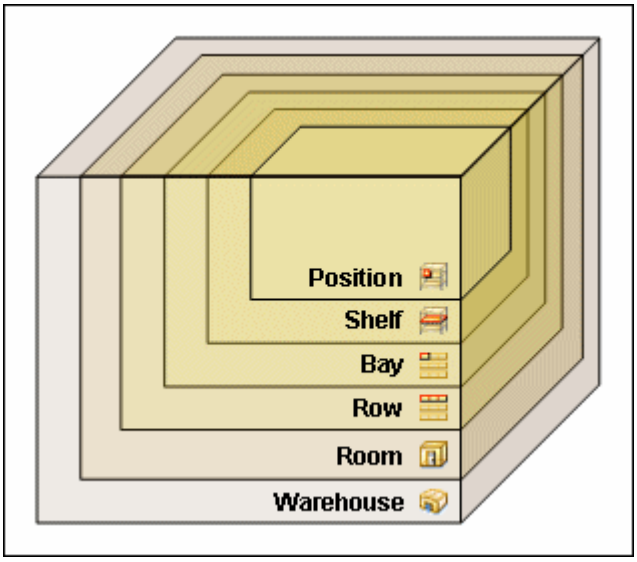
PCM uses defined space environment to keep track of the storage and retention of physical items. When working with a physical item, assign the item to a storage location, so PCM knows where it is stored and track it.

This section describes browsing the defined storage environment in PCM. It covers the following topics:

9.2.1 Storage Space Hierarchy

Storage space in PCM is set up hierarchically. Storage locations contain other, smaller storage locations which contain still smaller storage locations, and so on. The out-of-the-box PCM feature comes with the following storage space hierarchy (from large to small):

Figure 9–1 Default Storage Space Hierarchy

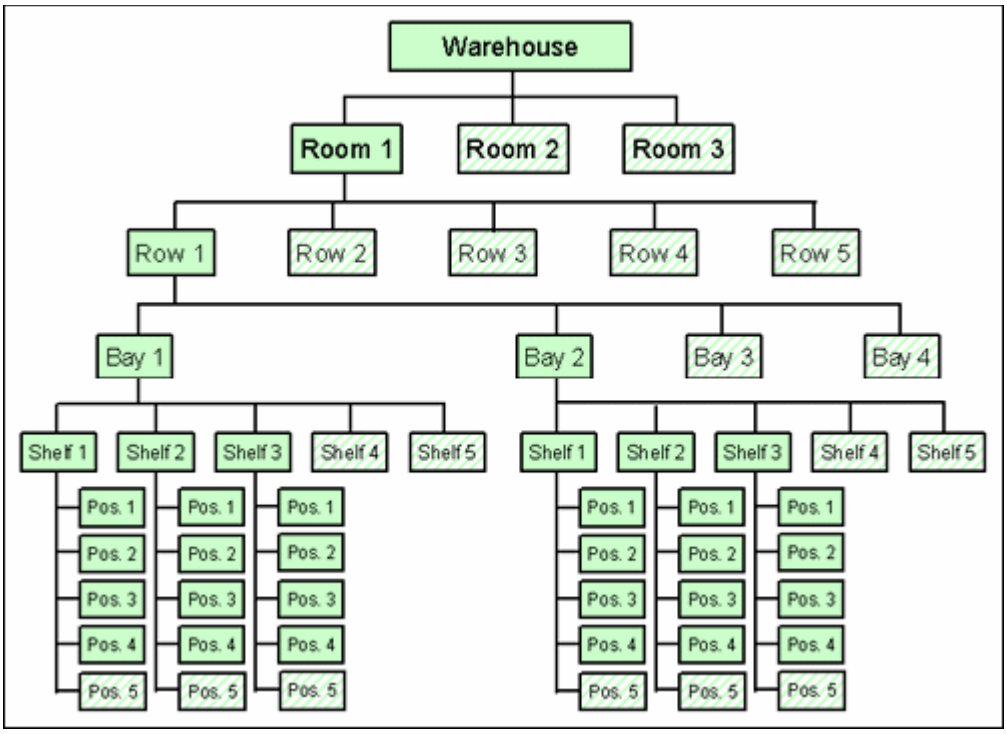


As shown in this figure, a warehouse consists of one or more rooms, a room consists of one or more rows, and so on. The further down in the hierarchy, the more specific (and smaller) the storage locations become.

The storage space environment you are working with may have different hierarchical levels, depending on how the physical content management feature has been set up for your organization.

Storage space can be depicted as in the following figure, which is similar to a genealogy chart. The Warehouse at the top level contains rooms, which in turn contain rows. A row can contain a bay and a bay can contain shelves. Within each shelf distinct positions are noted for items.

Figure 9–2 Example Storage Space Environment



PCM keeps track of the use of space in the defined storage environment, and provides information about the available storage space on the Storage Information Page of a storage location. Items cannot be stored in a location without sufficient space.

Storage locations can be added regardless of the parent location. For example, you can define a row or bay position in a warehouse.

Note: By default, the available storage space is recalculated daily at midnight. Therefore the displayed storage availability information may not be entirely up to date as the day progresses because it still reflects the situation from the night before.

9.2.2 Storage Location Properties

Each storage location in the storage space environment has several properties, including:

- "Location Type" on page 9-5
- "Object Type" on page 9-5
- "Media Type" on page 9-5
- "Storage Status" on page 9-6

Important: The type of content storage allowed applies to a particular level only. For example, in the default hierarchy, shelves have several positions, each of which can hold content items, but no content items can be directly assigned to the shelf level (only to the positions on a shelf). Therefore the location type 'Shelf' cannot store content, whereas the type 'Position' can.

For details about creating and using location, media, and object types, see "Configuring Location Types" on page 8-3, "Configuring Object Types" on page 8-7 and "Configuring Media Types" on page 8-9.

9.2.2.1 Location Type

Each storage location is assigned a location type, which helps specify where it is located in the storage space hierarchy. The available location types are defined by your administrator.

The out-of-the-box PCM feature comes with the following six predefined location types (in hierarchical order), with their standard icons for the default Trays layout:

9.2.2.2 Object Type

The object type of a storage location in the storage space environment specifies what type of items the storage location can hold.

The out-of-the-box feature comes with the following predefined object types:

- All. Note that an "All" object type cannot be assigned to a physical item.
- Box
- Document
- Folder
- Micro
- Optical
- Tape

Your administrator may also have set up a different list of object types to meet the needs of your organization. When creating a new physical item, select its object type on the Create Physical Item page.

9.2.2.3 Media Type

The media type of a storage location in the storage space environment provides a further specification of the type of items the storage location can hold.

The out-of-the-box feature comes with several predefined media types, but your administrator may also have set up a different list of media types to meet the needs of your organization.

The available media types depend on the selected object type of the current storage location (see "Object Type" on page 9-5). The table below explains which predefined media types can be selected for each predefined object type:

Object type	Supports these media types
Box	Box
Document	Mixed Fax Paper Photo
Folder	Folder
Micro	Mixed Microfiche Microfilm

Object type	Supports these media types
Optical	Mixed CD Disc DVD
Tape	Mixed Audio Data Visual
All	Mixed Audio Box CD Data Disc Dvd Fax Folder Microfiche Microfilm Paper Photo Visual

9.2.2.4 Storage Status

If a storage location in the storage space can hold content items, its status determines whether content can be stored in the unit, and if not, why not. The status of a storage location is shown in the status column on the location page and can be any of the following:

- **Available:** Content can be stored in the storage location, and space is available. This is the default. If no status is provided, this one is assumed.
- **Reserved:** No content can be stored in the storage location or any of its child storage locations because it has been reserved. There may be space available in the storage location, but it has been set aside for future storage of physical items (for example, to ensure grouped storage of batches of items as they come in to be stored). If the logged-in user is the one who reserved the space, it will show as available to that person.
- **Occupied:** The storage location has reached its maximum storage capacity, and no further content can be added to it.

A user may have blocked a storage location. This prevents storage of content in a storage location even if space is available. If that is the case, the status column on the location page is empty.

9.3 Managing Storage Spaces

The following tasks are involved in managing storage spaces:

- "Creating a Storage Location" on page 9-7
- "Batch Creating Storage Locations" on page 9-7
- "Editing a Storage Location" on page 9-8
- "Viewing Information about a Storage Location" on page 9-9
- "Deleting a Storage Location" on page 9-9

9.3.1 Creating a Storage Location

Permissions: The PCM.Storage.Create right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to create a new storage location in the storage space hierarchy.

1. Click **Physical** then **Storage**.

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. To create a location at the topmost level of the hierarchy, click **Create** then **Define Storage Location** from the page **Action** menu. You can also choose **Create Storage Location** from the **Action** menu for a storage location in the list to add a new child storage location at that level.

   The Create or Edit Storage Page is displayed.

3. Specify the storage location properties and click **Create** when done.

   The newly created storage location is now included in the storage space hierarchy at its assigned level.

9.3.2 Batch Creating Storage Locations

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to add several storage locations to the storage space hierarchy in a single batch. This is useful in situations where the storage hierarchy (or part of it) consists of a well-defined tree structure with consistent naming and numbering of its constituent objects. This procedure can be used to define this storage location structure in one operation, without having to define each object separately.

You do not add the defined objects to the storage hierarchy directly from this page. Rather, specify the naming and numbering rules to be used to create the storage locations. After clicking **OK**, a file called StorageImport.hda is generated, which can be imported into the existing storage hierarchy.

See "Example: Creating a Batch of Storage Locations" on page 9-12 for an example of this process.

1. Click **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

   The Create Batch Storage Import File Page is displayed.

2. Click the **Browse** button.

   The Select Storage Location Dialog is displayed.

3. Navigate to the level in the storage hierarchy where the new storage location structure should be added and click **OK**.
4. Specify the rules and parameters to be used to create the batch of storage locations.
5. Click **Create** when finished to create the storage locations in accordance with the defined specifications, or click **Reset** to return the screen to its initial values.

   A file called StorageImport.hda is generated, and a dialog opens which enables you to save this file to your hard drive.

   The newly created storage locations are now included in the storage space hierarchy at their assigned level.

   The following information should be considered when considering batch creation of storage locations:

   - When defining a storage space, you must obey the existing location type hierarchy. Start with the highest-level storage location and work your way down the hierarchy. You cannot add a parent location below a child location (for example, a shelf above a row). If you attempt to do this, error messages will be displayed when you import the StorageImport.hda storage definition file.
   - The name and description of each generated storage location is built from the name prefix (if specified) and a sequential number such as "Warehouse_001," "R003," or "WH_NY-012."
   - The default number of digits used in the numeric sequences is 3. To change the number of digits, modify the `AutoStorageNumberWidth` parameter in the storagecreationutility_environment.cfg file. Restart the Content Server after changing the parameter value.
6. Click **OK**.

   The Exploring Page is displayed again.

9.3.3 Editing a Storage Location

> **Permissions:** The PCM.Storage.Edit right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to edit the properties of an existing storage location. Depending on the storage location, you may not be able to edit all location properties.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.
2. Click **Edit** then **Edit Storage Location** from the **Action** menu of the item to edit.

   The Create or Edit Storage Page is displayed.
3. Modify the storage location properties as required and click **Submit Update** when finished.

   A message is displayed stating the storage location was updated successfully, along with a list of the current storage location properties.

9.3.4 Viewing Information about a Storage Location

Permissions: The PCM.Storage.Read right is needed to perform this action. This right is assigned by default to the PCM Administrator and the PCM Requestor role.

Use this procedure to view information about a storage location.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. Click the **Info** icon for the storage location or click **Information** then **Storage Information** from the location's **Action** menu.

   The Storage Information Page is displayed listing the current storage location properties.

3. Click **OK** when done.

   The Exploring Page is displayed again.

This page shows the current properties of the selected storage location, including the total available spaces (calculated from all child storage locations) and the spaces currently used. There are also locator links at the top of the page, which show where the storage location is located in the storage space hierarchy.

By default, the available storage space is recalculated daily at midnight. Therefore, the displayed storage availability information may not be up to date as the day progresses because it reflects the situation from the night before. If you are an administrator with the PCM.Admin.Manager right, you can force a recalculation of the available storage space by running the "Process Storage Space Counts" batch service.

9.3.5 Deleting a Storage Location

Permissions: The PCM.Storage.Delete right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to delete a storage location from the storage space hierarchy. A storage location must be empty before it can be deleted. A location is considered empty if it does not contain any items. If a storage location has all empty child storage locations, the entire branch can be deleted. If you attempt to delete a non-empty storage location, an error message is displayed.

Note: You cannot delete the predefined "Other" storage location, even if it is empty.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. Navigate to the storage location to delete, and click **Delete** then **Delete Storage Location** from the item's **Action** menu.

To delete multiple storage locations from the exploring pages select their boxes and click **Delete** in the Table menu.

If the storage location is empty, it is immediately deleted from the storage space hierarchy (without any further warnings), and the Exploring Page is refreshed. If the storage location is not empty, an error message is displayed and it will not be deleted.

9.3.6 Blocking a Storage Location

Permissions: The PCM.Storage.Block right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Use this procedure to block a storage location. After blocking, no items can be stored in the location and all its child locations, even if space is available.

Only empty storage locations can be blocked. When a location is blocked, its "Allow storage of content" setting is set to "No."

An example of use is to create a "dummy" storage location a storage bay cannot be used (because of physical limitations) but it is necessary to retain sequential numbering across multiple rows.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. Navigate to the storage space level to block and click **Edit** then **Block Storage** from the level's **Action** menu.

   The initial Exploring Page is displayed again and content can no longer be assigned to the storage location. If the status column previously showed "Available," it is now empty. Also, the Storage Information Page of the storage location has the "Allow storage of content" field set to "No."

To cancel the blocked status of a storage location and allow storage of content again, edit the storage location and set its **Allow storage of content** setting to **Yes**. See "Editing a Storage Location" on page 9-8 for details. After unblocking a storage location, its status column on the Exploring pages shows "Available" again. It was empty while the storage location was blocked.

9.3.7 Reserving or Canceling a Reservation for a Storage Location

Permissions: The PCM.Storage.Reserve right is needed to perform this action. This right is assigned by default to the PCM Administrator and PCM Requestor role.

Use this procedure to reserve a storage location for future use.

If you reserve a storage location, all its child locations are also reserved. Only an administrator or the person who reserved a storage location can add items to it.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. Navigate to the storage space level that includes the storage location to reserve.
3. Click **Edit** then click **Reserve Storage** on the location's **Action** menu.
4. Select the requestor reserving the space from the list of users displayed.
5. The initial Exploring Page is displayed again and the storage location now shows "Reserved" in its status column, with the name of the user who made the reservation in parentheses next to the status.

To cancel the reserved status of a storage location, navigate to a reserved location and choose **Edit** then **Cancel Request** on the **Action** menu.

9.3.8 Viewing All Items in a Storage Location

Permissions: The PCM.Storage.View right is needed to perform this action. This right is assigned by default to the PCM Administrator and PCM Requestor role.

Use this procedure to view all items currently contained in a storage location.

1. Click **Physical** then **Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.
2. Navigate to the storage space level that includes the storage location with items to view. Click **Change View** from the Table menu to view a graphical depiction of the storage hierarchy.
3. Click the storage name of a location to view items at that location. Click **Information** on the Action menu for the location to display the following options:
   - **List items that belong here**: This lists all items with the specified storage location as their *permanent* location.
   - **List items that are actually here**: This lists all items with the specified storage location as their *current* location. This list does not include any items normally in the storage location, but currently checked out.

9.3.9 Printing Labels for Storage Locations

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

Use this procedure to create a label for a storage location.

The label file contains the barcodes and other information for the current storage location and all its child storage locations if any exist. Only storage locations that can hold content items are included. Any "intermediate" storage levels are skipped if they cannot hold content.

By default, the label for a storage location contains a barcode uniquely representing the location, the location's name, its description, and its location type.

The format of the label file depends on the Report Label Format setting on the Configure Physical Settings Page.

If the generated label file is in PDF format, Adobe Acrobat Version 6.0 or later is needed to view it.

To create a label for a storage location, complete the following steps:

1. Click **Browse Content** then **Storage** or click **Physical** then **Storage**.

   The Exploring Page for the top level of the storage hierarchy is displayed.

2. Navigate to the storage space level.

3. Depending on the current storage location, click **Create Reports** from the **Action** menu for the location. Select one of the report types listed there.

You can also create a label for a storage location from the **Page** menu on the Storage Information Page. Click **Create Report** then the report type. This menu contains an option to print a label only if the storage location can hold content.

9.4 Example: Creating a Single Storage Location

This example demonstrates how to create a storage location called "Warehouse_003," of location type Warehouse at the top level of the storage hierarchy.

1. Click **Browse Content** then **Browse Storage.**

   The Exploring Page for the top level of the storage hierarchy is displayed.

   You can also access the top-level storage Exploring Page from the Configure Physical Settings Page.

2. Click **Create Storage Item** on the menu bar at the top of the page.

   The Create or Edit Storage Page is displayed.

3. Enter **Warehouse_003** as the storage name and description.

4. Click **Warehouse** as the location type.

5. Click **Create**.

   The newly created storage location is now included in the storage space hierarchy at the top level:

9.5 Example: Creating a Batch of Storage Locations

This example demonstrates how to create the definition file for a storage space structure then import this file to create the defined storage space within Physical Content Management's storage environment. The storage space structure consists of one warehouse at the top level of the storage environment, with several subordinate storage locations. Each of the lowest-level locations (Position) may hold five items, which can be of any object type.

Creating the Batch Storage Definition File

To create the batch storage definition file, complete the following steps:

1. Click **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

   The Create Batch Storage Import File Page is displayed.

2. Click **Browse** to select the highest point of the hierarchy. If not selected, the 'Storage' level is defaulted.

   The Select Storage Location Dialog is displayed. Select a location and click **OK**.

3. Provide these creation rules for Location Type, Name Prefix, Start Number, Number of items, Allow Content, Number Allowed, and Object Type:
   - Room, Room_, 1, 2, unchecked, empty, all
   - Warehouse, Warehouse_, 1, 1, unchecked, empty, all
   - Row, Row_, 1, 2, unchecked, empty, all
   - Bay, Bay_1, 1, 2, unchecked, empty, all
   - Shelf, Shelf_, 1, 2, unchecked, empty, all
   - Position, Position_, 1, 3, checked, 5, all

   If the values provided exceed the limit set for storage (default is 1000) an error message is displayed.
4. Click **Create**.

   A file download dialog is displayed.
5. Click **Save** to store the generated StorageImport.hda file on the local hard drive.

Importing the Batch Storage Definition File

To import the batch storage definition file into Physical Content Management, complete the following steps:

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

   The Import/Export Content and Record Archive Page is displayed.
2. Unselect all items (including those under **Show External Sources**) except for **Include Storage**.
3. Click **Browse** next to the **Archive File** box to select the StorageImport.hda file saved earlier.
4. After selecting the file, click **Import**. The import adds the defined storage space to the existing storage hierarchy at the selected location.

For more details about import and export operations, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

10

Setting Up a Retention Schedule

This section describes how to set up and administer the retention schedule for an organization.

This chapter covers the following topics:

Concepts

Tasks

Examples

10.1 About Retention Schedules

Important: If your retention schedule contains 10,000 or more series, categories, and folders, then your database administrator should build database indexes on the tables to enhance performance. For record folders, add indexes on the columns of the Folders table. For retention categories, add indexes on the columns of the Categories and Dispositions tables. For series, add indexes on the columns of the Series table. For further information about defining an index on a table column, see your database documentation.

A retention schedule is an organized hierarchy of series, categories, and record folders which can cluster content into similar groups, each with its own retention and disposition characteristics. Many retention schedules can be created for the requirements mandated by an organization.

If a record folder does not have its own security settings, the folder inherits security settings from its parent retention category. Each record folder can have its own security settings that further limit access to the items in that folder. Record folders can be further secured by using supplemental markings and custom security fields.

Record folders also inherit disposition rules from their retention category. By default, all record folders within a retention category inherit disposition instructions from the category. A disposition rule defined within a category can be applied to a specific record folder if the folder has a unique disposition instruction.

Record folders for temporary content are destroyed with temporary content as part of final disposition processing. Records administrators create new record folders as necessary to accommodate processing temporary items. Record folders for content subject to review and permanent content are not destroyed, and do not have to be re-created due to final disposition.

Important: The retention schedule is not a contribution mechanism, but rather a disposition mechanism. It defines how and when content should be processed during its lifecycle. It is not intended to check content into the repository.

10.1.1 Retention Schedules and File Plans

In previous versions of Oracle URM the term *file plan* was synonymous with *retention schedule* to designate that functionality used to track and maintain retention objects.

With this release, the product can now be used to track items in conjunction with the MoReq2 specification. The MoReq2 file plan is accessible from the Browse Content tray. To enable MoReq2 file plans, set the `RmaEnableFilePlan` configuration variable to TRUE and restart the Content Server.

A file plan has a strict folder hierarchy consisting of four node types: Class, File, Sub-File and Volume, with only Classes allowed at the top level of the hierarchy. Classes provide a framework for classification and files are used to store like records.

Files and Classes cannot be mixed at a single node in the hierarchy. For example, if a Sub-File is placed in a File folder, that File folder cannot contain any other type of item, including content. The exception is if a folder type contains content items, it can also contain volumes. Classes can contain other Classes, Files, or content. Sub-files can contain content items. Volumes can only contain content. The Oracle URM software

has been configured to allow Create access only to those items which are allowed at the specific point in the hierarchy.

For more details about file plan nodes and the hierarchy, see the *Model Requirements for the Management of Electronic Records*.

Functionality for using the file plan is similar to that for the retention schedule. One major difference is that disposition actions are applied to Classes by linking the class to a category that has a disposition schedule.

As you review the information in this chapter, consider how the information can apply to your file plan as well as any retention schedule in place at your site.

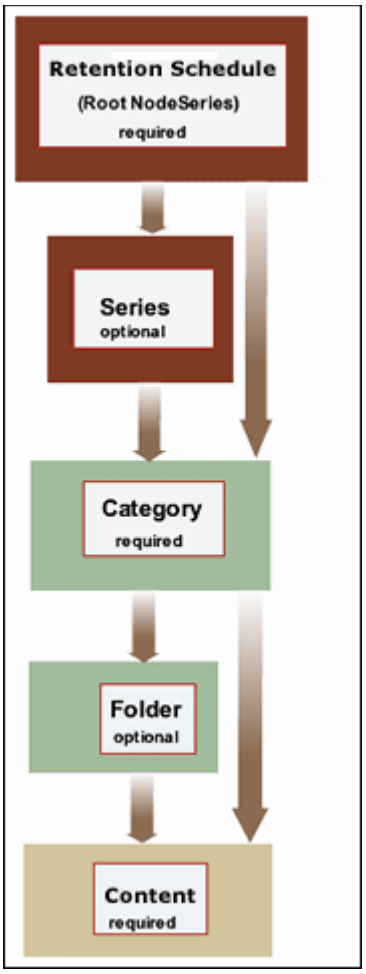
10.1.2 Planning a Retention Schedule

Do not base a category on a dynamic feature such as organization hierarchy because organizations are reorganized on a frequent basis. Use static divisions for category departments, and be more generic with categories. Record folders can be more specific.

10.1.2.1 Retention Schedule Hierarchy

A typical hierarchy of a retention schedule consists of series, categories, and/or record folders. Series are optional top-level nodes that can be nested. A retention category cannot be nested, due to the nature of its disposition schedules. Record folders can be nested. The following figure shows the basic hierarchy of retention schedule objects.

Figure 10–1 Basic Retention Schedule Hierarchy

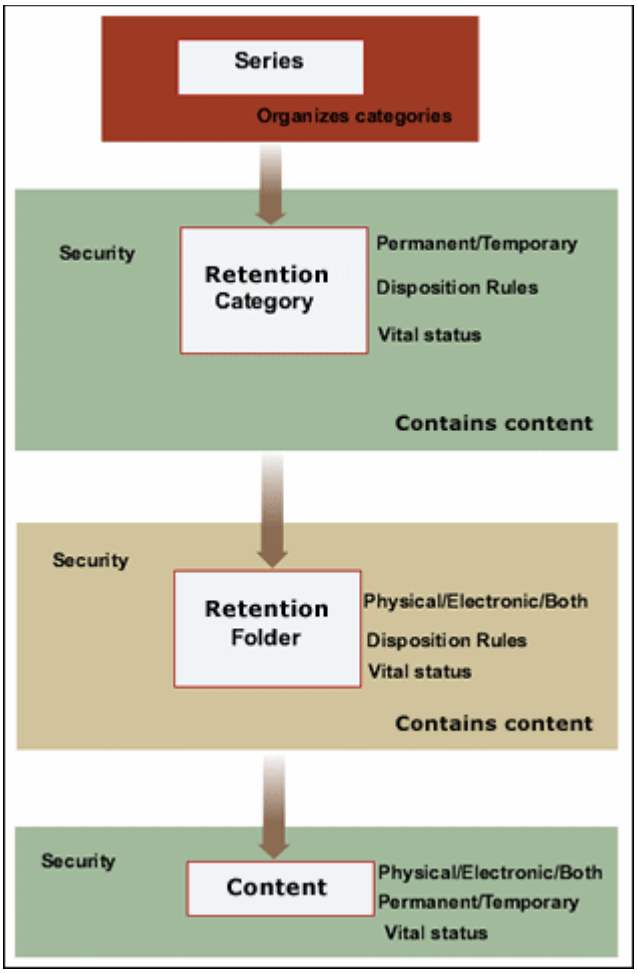


Content is filed directly into a retention category, and optionally can be filed into a record folder under a retention category. The retention schedule is the top-most series root node. The top node is created automatically.

The remaining retention schedule objects (series, folder, or retention category) are created by the Records Administrator. Users or administrators create content for filing within the application. A series is an optional container created by the Records Administrator. A retention category is required, and it contains disposition instructions for processing content. A record folder is optional, and it also organizes content according to some commonality.

The figure below shows the main characteristics of each retention schedule object at a glance. Series do not have security set directly on the series object, whereas retention categories, record folders, and content all have a variety of security options, including access control lists (ACLs), supplemental markings, custom security fields, and (custom) classifications.

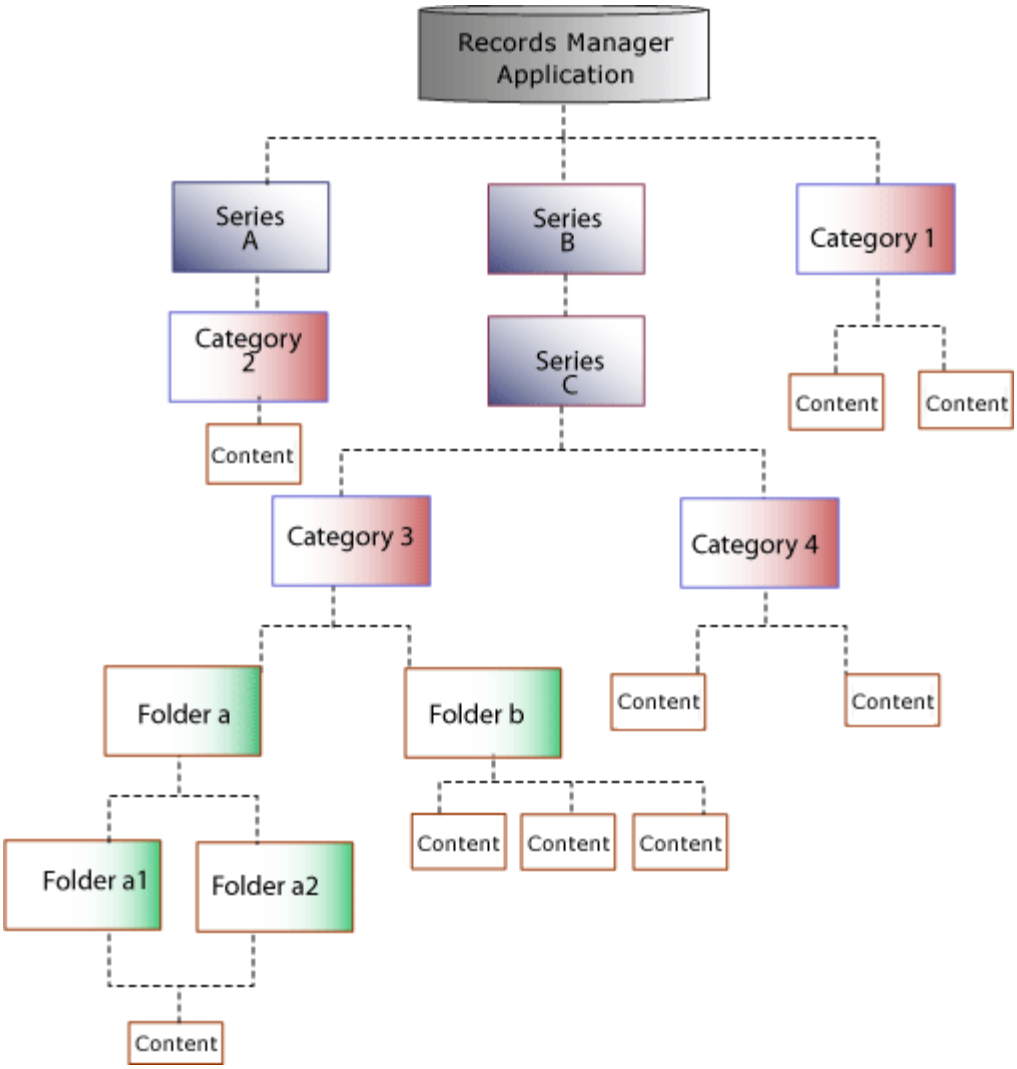
Figure 10–2 Attributes of Retention Schedule Objects



The following figure illustrates a slightly more complex retention schedule hierarchy, with:

- nested series (Series B and C)
- nested folders (Folders a1 and a2 under Folder a)
- content filed directly into a category (Categories 1, 2, and 4) rather than a folder
- categories without a series (Category 1)
- an item filed into multiple folders (Folders a1 and a2).

Figure 10–3 Sample Retention Schedule Hierarchy



While it is possible to file content into multiple locations in the retention schedule, this is not recommended due to the complexity of processing multiple disposition schedules. For best performance results, content should be filed into a single folder or category. When multiple disposition schedules are attached to an item, the item is processed by the disposition with the longest retention period.

10.1.2.2 Attribute Inheritance

Some of the attributes of retention schedule objects are inherited from parent objects. In certain cases, the attributes can be overridden at a lower level.

Some security settings are inherited and overridden as well, which is explained in Chapter 5, "Setting Up Security".

10.1.2.3 Review Status Attributes

Review status, which includes the review period and reviewer, can be set at the retention category level, record folder level and the item level. The lowest level (the item level) takes precedence if all information is of equal duration and is set at the category, folder, and item levels.

In the case of review periods with differing lengths between a parent and child objects, the shortest review period takes precedence for a child folder and is indicated in the relevant content information pages. The longer review period is ignored. However, if the shorter review period is removed or changed, the longer review period reigns again in cycling reviews for content.

Important: Within a parent and child object hierarchy, the review period with the shortest review period takes precedence for a child folder over a longer review period set on the child folder.

For example, a subject-to-review category has a review period of two calendar quarters. A child folder within the subject-to-review category has a review period set as four calendar quarters. Because the category higher in the hierarchy (the 'parent') has a shorter review period, the child folder ignores its own longer review period setting. In essence, the folder has a review period override in effect.

If the review status is not set at the record folder level for a record folder in a subject-to-review category, the folder *always* inherits review status from the category. At the content level, a content can inherit review information from the category, and the content can inherit information from the folder if it does not have its own review settings.

If a content item is filed directly into a subject-to-review retention category, it inherits settings from the category. If a subject-to-review item is filed into a subject-to-review record folder, it inherits settings from the immediate parent folder. Because record folders can be nested, the immediate folder parent determines review attributes for the item.

If a retention category is subject to review, and none of the folders or content items have their own review settings, then the folders and the items all inherit review attributes from the category.

You can create a non-review retention category containing record folders, content, and items subject to review. However, the reverse is not possible: you cannot create a retention category that is subject to review containing non-subject-to-review record folders and items due to inheritance of the subject to review attributes.

10.1.2.4 Permanent Status Attributes

The previous figure showed the permanent status set at the category level only, and how record folders and items inherit the folder status. Permanent items cannot be destroyed by a disposition instruction. Permanent items typically are a small percentage of an organization's information base. Permanent status is determined by the National Archives and Records Administration (NARA) as having sufficient historical value to warrant continued preservation beyond the normal time needed for administrative, legal, or fiscal purposes. Permanent items are sometimes referred to as ""archival" items.

10.1.2.5 Disposition Instructions

Disposition instructions are defined at the retention category level, with some rules being applied uniquely to a child record folder. A record folder inherits disposition rules from the retention category. Content items inherit dispositions from their retention category, and if applicable, a folder with its own uniquely applied disposition rule. For more information, see Chapter 14, "Defining Disposition Instructions".

10.1.2.6 Frozen Folder and Content Status

Freezing a record folder inhibits disposition processing for the folder and its child folders and content.

Record folders and content items inherit the freeze status if it is present on an ancestor. In addition to inheriting the freeze status, freezes can be performed at lower levels within a hierarchy where inheritance is not present. A child record folder or an item within a record folder can be frozen.

Freezing a content item outside of a folder also inhibits disposition processing and prevents the metadata was being updated.

10.1.3 Creating and Navigating Object Levels

To use retention objects, start at Browse Content on the main menu. Depending on a user's rights and role, the user can browse all Retention Schedules or just the ones created by that user.

A user must be at a certain context, or level, within the retention schedule to work with retention schedule objects. Depending on the location within the hierarchy, different menu options appear in the main Actions list when browsing the retention schedule. The table below shows what retention schedule objects can be created at each level.

At this level:	You can create:
Series or root node	▪ Series ▪ Retention category
Retention category	▪ Record folder ▪ Content item
Record folder	▪ Record folder ▪ Content item

10.1.3.1 Retention Schedule Menus

The main root node is considered the retention schedule series node. At the series level, a series or retention category can be created.

Menus are relative to the location in the hierarchy. For example, at the Folder level you can create a folder or content. You cannot create a category.

The following list describes the possible menu options which may appear depending on the location in the hierarchy. These options may appear on an individual item's **Action** menu or on the Page menu. Information in parenthesis indicates the area of the hierarchy where the information appears:

- **Information**
  - Category Information (Category level): displays the Retention Category Information Page.
  - Series Information (Series level): displays the Series Information Page.
  - Folder Information (Folder level): displays the Record Folder Information Page.
  - Metadata History (Category level and Folder level): displays the Metadata History Page.

  - Disposition Information (Category level): displays the Disposition Information Page.
  - Life Cycle (Folder level): displays Life Cycle information. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details.
  - Recent Reviews (Folder level): displays review history information. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details.
  - Retention Schedule Report (all): creates a retention schedule report in the format specified when the system was configured.
- **Edit**
  - Edit Retention Category (Category level): displays the Create or Edit Retention Category Page.
  - Edit Disposition (Category level): displays the Disposition Instructions Page.
  - Edit Review (Category level and Folder level): displays the Edit Review information screen. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details.
  - Edit Series (Series level): displays the Create or Edit Series Page.
  - Move (all): displays the Select Retention Series, Record Folder or Category Dialog.
  - Hide (Series level): displays a prompt to indicate why the object is being hidden.
  - Freeze/Unfreeze (Folder level): Toggles between freeze or unfreeze for a record folder.
- **Copy**: copies the object in question.
- **Delete**: deletes any checked objects. If an object has content (for example, a folder) an error message is displayed and the object is not deleted.
- **Create**
  - Create Record Folder (Category level and Folder level): displays the Create or Edit Record Folder Page.
  - Check In Content (Category level and Folder level): displays the Content Checkin Page.
  - Check in Physical Item: displays the Create Physical Item Page.
  - Create Series (Series level): displays the Create or Edit Series Page.
  - Create Retention Category (Series level): displays the Create or Edit Retention Category Page.
- **Change View**
  - Thumbnail: presents a icon-based 'thumbnail' view.
  - Headline: presents a horizontal, 'headline' view.

In addition, the following options may be available on the individual item **Action** menus on the Folder Page and on the Table menu on the Folder level:

- **Set Dates**
  - Mark reviewed: Marks a folder as reviewed.

  - Mark recursive: Marks all child objects as reviewed.
  - Cancel: Marks the folder as canceled, making it obsolete.
  - Expire: expires all objects in a folder.
  - Obsolete: marks content and the folder as obsolete. This toggles to Undo Obsolete if a folder becomes obsolete due to specific actions.
  - Rescind: rescinds a folder and the items therein.
  - Undo Cutoff (Table menu only): reverses the cutoff status of a folder.
  - Undo Obsolete (Table menu only): marks items and the folder as not obsolete.
- **Add to Favorites**: Used to add the marked object to the Favorites list.

10.2 Using a Series

A series is an optional feature for organizing content. If an organization has a multitude of retention categories, setting up series can assist with managing the view of the retention schedule hierarchies. Series should be a static and non-specific method of organization: for example, "Buildings" not " 7500 Building." This allows the hierarchy to remain static over time. Series can be nested within each other.

Series are also useful for creating work-in-progress retention schedules because series can be hidden from users, which prevents people from filing any data into the hidden series.

10.2.1 Managing a Series

Permissions: The appropriate rights are required to work with series. There are separate rights for reading (viewing), creating, deleting, moving, editing, and hiding/unhiding series. The predefined Records User and Records Officer roles can only read (view) series. The predefined Records Administrator role can perform any of the other series-related tasks.

The following tasks are involved in managing series:

- "Creating or Editing a Series" on page 10-10
- "Viewing Series Information" on page 10-11
- "Hiding and Unhiding a Series" on page 10-11
- "Moving a Series" on page 10-12
- "Deleting a Series" on page 10-12

The retention schedule can be accessed in two ways:

- Click **Browse Content** then **Retention Schedule** from the Main menu.
- Click **Records** then **Retention Schedules** from the Top menu.

10.2.1.1 Creating or Editing a Series

You can create nested series (a series within a series).

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

1. Access the retention schedule and navigate to the location in which to create the series.
2. Click **Create** then click **Create Series** from the Actions menu in an existing series or from the Page menu.

   The Create or Edit Series Page is displayed.
3. Enter an identifier for the series in the **Series Identifier** text box.
4. Enter a name for the series in the **Series Name** text box.
5. Click **Create**. The series is displayed in both the Browse Content area and in the Retention Schedule list.

Use the following procedure to edit the name for the series. Any information except the series identifier can be edited.

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

1. Access the retention schedule. Click **Edit** then **Edit Series** in the **Action** menu for the series to edit.

   The Create or Edit Series Page is displayed.
2. Enter any changes to the value in the Series Name box, and click **Submit Update**. A message is displayed saying the series was updated successfully.
3. Click **OK**.

10.2.1.2 Viewing Series Information

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

1. Access the retention schedule. Click the **Info** icon for the series to view.

   The Series Information Page is displayed. This page shows relevant information about the selected series.
2. Click **OK** when done.

10.2.1.3 Hiding and Unhiding a Series

A hidden series and its children are not visible to anyone without the Series.Hide/Unhide right. This feature provides a staging area for setting up and testing retention schedules. After a retention schedule is ready for production, unhide the series.

Permissions: The Series.Hide/Unhide right is required to perform these actions. This right is assigned by default to the Records Administrator role.

1. Access the retention schedule. Click **Edit** then **Hide Series** from the **Action** menu for the series to hide.
2. You are prompted to enter 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 series icon is now semi-transparent to indicate it is hidden.

Follow the same procedure to unhide the series: access the retention schedule then click **Unhide Series** in the item's **Action** menu. If the action is confirmed, the series icon is no longer semi-transparent to indicate it is not hidden.

10.2.1.4 Moving a Series

All child series, categories, record folders and content items move with the parent series.

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

1. Access the retention schedule. Click **Edit** then **Move Series** from the **Action** menu for the item to move. To move multiple items, click the checkbox for the series and click Move from the Table menu.

   The Select Retention Series, Record Folder or Category Dialog is displayed.
2. Click to expand the tree, and click the series which will contain the item. The location field populates with the new location.
3. Click **OK**. The Exploring Series Page displays the series in its new location.

10.2.1.5 Deleting a Series

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

If a series is populated a message appears when an attempt is made to delete the series, prompting the user to delete the contents as well as the series. Be sure to move any content, record folders, categories, and any nested series from the series to be deleted if any of those objects should be retained.

Tip: To delete multiple items, click the checkbox for the items and click **Delete** from the Table menu.

1. Access the retention schedule. Click **Delete** then **Delete Series** from the **Action** menu for the item to delete.

2. You are prompted to confirm the deletion. Click **OK** to delete the series, or **Cancel** to cancel the delete action. To delete any child objects, click the checkbox for "Include child content items" on the prompt that appears. Click **Yes** when done.
3. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty and click **OK**. Click **Cancel** to abort the entire action.

   If confirmed, the series is deleted from the retention schedule.

10.3 Retention Categories

A retention category is a retention schedule object with associated security settings and disposition instructions defined. Retention categories cannot be nested within other retention categories because they are disposition instructions, not an organization container. They are a method of grouping content with the same disposition requirements.

This section covers the following topics:

- "Managing Retention Categories" on page 10-13
- "Retention Category Example" on page 10-17

If ACLs are on the retention category, the user must also be on the ACL to view or access the retention category.

At the category level, record folders or content items can be created.

The retention schedule can be accessed in two ways:

- Click **Browse Content** then **Retention Schedule** from the Main menu.
- Click **Records** then **Retention Schedules** from the Top menu.

10.3.1 Managing Retention Categories

The following tasks are involved in managing retention categories:

- "Creating or Editing a Retention Category" on page 10-14
- "Viewing Retention Category Information" on page 10-15
- "Viewing Category Metadata History" on page 10-16
- "Moving a Retention Category" on page 10-16
- "Deleting a Retention Category" on page 10-17

> **Permissions:** The appropriate management rights are required to work with retention categories. There are separate rights for reading (viewing), creating, deleting, moving, and editing categories. The predefined Records User and Records Officer roles can only read (view) categories. The predefined Records Administrator role can perform any of the other category-related tasks.

Note that when retention categories are sorted and listed, they are listed on a per-source basis. For example, if three sources are used (Source1, Source2, Source3), all items from Source1 are sorted as a separate group, items from Source2 are sorted as a separate group, and items from Source3 are sorted as a separate group. Then items from each source are displayed in a "round robin" style with the first item of Source1,

the first item from Source2, and the first item from Source3, followed by the second item of each source.

10.3.1.1 Creating or Editing a Retention Category

A retention category can contain record folders or content. You can create retention categories at the root node level, or within a series.

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

1. Click **Browse Content** then **Retention Schedules**. Click **Create** then **Create Retention Category** from the Table menu.

   The Create or Edit Retention Category Page is displayed.

2. (Optional) Accept the default security group or select a group from the **Security Group** list. The **Default Content Server security** box must be enabled on the Configure Retention Settings Page.
3. (Optional) If Accounts are enabled, indicate the associated account for the category in the **Account** box.
4. (Optional) If your organization uses the default security on categories, select an author of the retention category from the **Author** list. The author defaults to the user currently logged in and entering the information.
5. Enter a unique identifier for the category in the **Retention Category Identifier** box.
6. Enter a name for the category in the **Retention Category Name** box.
7. Enter a description of up to 1000 characters in the **Retention Category Description** box.
8. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. Private sector organizations can enter the person or department responsible for the category, or enter "none."
9. To restrict revisions of items in the category, click the **Restrict Revisions** box.
10. To restrict deletions of items in the category, click the **Restrict Deletes** box.
11. To restrict edits of items in the category, click the **Restrict Edits** box.
12. If the retention category is to contain content for review, and all objects should inherit the subject to review status, do the following:
    a. Click the **Subject to Review** box.
    b. To specify a reviewer for the retention category rather than allow the reviewer to revert to the notify recipient system default, select a reviewer from the **Reviewer** list. When selecting a reviewer, make certain that user has the rights required to perform the review. Otherwise an error message is displayed and the user cannot perform the review.
    c. Enter an integer value for the number of review periods in the **Review Period** text box.
    d. Select the defined period from the **Review Period** list.

13. (Optional) If your organization uses access control lists (ACLs), then assign group permissions to the category:

    a. To assign group permissions, click **Select** by the **Group Permissions** box. The Select Alias page is displayed.

    b. Select or type the alias, enable the Read, Write, Delete, and Admin permissions as appropriate for the alias, and click **Add to List**. Repeat this step for each alias to set permissions for, and click **OK**. The alias and its permissions display in the Group Permissions text box of the Create Retention Category page.

14. (Optional) If your organization uses access control lists (ACLs), then assign user permissions to the category:

    a. By the **User Permissions** box, click **Select**. The Select User page is displayed.

    b. Select or type the user, enable the Read, Write, Delete, and Admin permissions as appropriate for the user, and click **Add to List**. Repeat this step for each user to set permissions for, and click **OK**. The user and their permissions display in the User Permissions text box of the Create Retention Category page.

15. Click **Create**. The Dispositions Instructions Page is displayed. Create a disposition rule or click **Submit Update** to create a rule later.

    For more detailed instructions about disposition rules and disposition examples, see Chapter 14, "Defining Disposition Instructions".

Use this procedure to edit an existing retention category.

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

1. Access the retention schedule. Click **Edit** then click **Edit Retention Category** from the item's **Action** menu.

   The Create or Edit Retention Category Page is displayed.

2. Enter changes to the available fields.

3. Click **Submit Update**. The successfully updated retention category message is displayed.

4. Click **OK**. The Exploring Series "Retention Schedule" Page is displayed.

10.3.1.2 Viewing Retention Category Information

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

1. Access the retention schedule. Click the Info icon for the item to view.

   The Retention Category Information Page is displayed. This page shows relevant information about the selected retention category.

2. Click **OK** when done.

10.3.1.3 Viewing Category Metadata History

Use this procedure to view the metadata history of a retention category. This displays a list of all changes made to the editable category properties.

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

1. Access the retention schedule. Click **Information** then **Metadata History** from the item's **Action** menu.
2. The Metadata History Page is displayed, showing a list of all changes made to the editable category properties. The following information is provided:
   - The user who made the change
   - The timestamp when the change was made
   - The affected field(s)
   - The old and new field values
3. Click **OK** when done.

10.3.1.4 Copying a Retention Category

Use this procedure to copy a retention category.

1. Access the retention schedule. Find the category to copy and click **Copy** from the item's **Action** menu.
2. The Create or Edit Retention Category Page with some fields already filled in. Edit the remainder of the fields as needed.
3. Click **Submit Update**. The Dispositions Instructions Page is displayed. Create a disposition rule or **Submit Update** to create a rule later.

   For more detailed instructions about disposition rules and disposition examples, see Chapter 14, "Defining Disposition Instructions".

10.3.1.5 Moving a Retention Category

You can move a retention category to another series or to the root node retention schedule level.

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

1. Access the retention schedule. Click **Edit** then **Move** from the item's **Action** menu.
2. The Select Retention Series, Record Folder or Category Dialog is displayed.
3. Click to expand the tree, and click the series to which to move the category. The location field populates with the new location.
4. Click **OK**. The Exploring Series Page and Browse Content area display the retention category in its new location.

10.3.1.6 Deleting a Retention Category

Use this procedure to delete a retention category.

> **Permissions:** The Category.Delete right is required to perform this action. This right is assigned by default to the Records Administrator role. Delete permission (D) for the RecordsGroup security group is also required.

1. Access the retention schedule. Click **Delete** then **Delete Category** from the item's Actions menu.
2. You are prompted to confirm the delete. Click **OK** to delete the category, or **Cancel** to cancel the delete. To delete any child objects, click the checkbox for "Include child content items" on the prompt that appears. Click **Yes** when done.
3. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty, and click **OK**. Click **Cancel** to abort the entire action.

   If confirmed, the retention category is deleted from the retention schedule.

10.3.2 Retention Category Example

This example creates an archive disposition action for the retention category to be reviewed. This example retention category has a three month review period.

1. Click **Browse Content** then **Retention Schedules**.

   The Exploring Series "Retention Schedule" Page is displayed.
2. Click **Create** then **Create Retention Category** from the Table menu.

   The Create or Edit Retention Category Page is displayed.
3. Enter `RCV-101` in the **Retention Category Identifier** box.
4. Enter `Operational for Review` in the **Retention Category Name** box.
5. Enter a description of up to 1000 characters in the **Retention Category Description** box. For this example, type `RCV-101`.
6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `RCV-101`.
7. Click the **Subject to Review** box.
8. Specify a **Reviewer** and a **Review Period**.
9. Click **Create**.

   The Disposition Instructions Page is displayed.

   a. Click **Add**. The Disposition Rule Page is displayed.

   b. Set the **After** (**Triggering Event)** as "Retention Period Cutoff."

   c. Enter `3 Calendar Months` as **Wait For** (the **Retention Period)**.

   d. In the **Do** (**Disposition Action)** list, click **Notify Authors**.

   e. Click **OK**.
10. Click **Submit Update**.
11. Click **OK**.

10.4 Record Folders

Retained items differ from other documents in the repository because they have different metadata are associated with a disposition life cycle. A record folder organizes similar items within a retention category. A retention category can have multiple record folders, and record folders can be nested within other record folders.

Record folders can inherit disposition rules from their parent record folder or category. Separate disposition instructions for individual folders can be set up as well. This is done when the dispositions are created for the category where the folder is stored. It is not done during the creation of the folder.

This section covers the following topics:

10.4.1 About Record Folders

A record folder can inherit security settings from a category, or have its own security settings. Supplemental markings can also be set on a record folder and users to further secure the folder above and beyond all other security mechanisms. In addition to inheriting security settings and disposition rules, folders also inherit content review information from the parent category. If a folder is inheriting review information, it is indicated on the Record Folder Information page.

The review information taking precedence is at the lowest node (the shortest review period prevails), such as in the case of nested folders. Review information can be overridden at the folder level. For example, you can specify a different reviewer or review period cycle. However, you cannot specify a folder within a subject-to-review retention category as a folder that is not subject to review. If you do not want a record folder to be reviewed, you must create the folder in a non-subject-to-review category.

Permissions: The appropriate management rights to work with record folders are required. Separate rights are required for reading (viewing), creating, deleting, opening/closing, editing, moving, and freezing/unfreezing folders. The predefined Records User role can only read (view) record folders. The predefined Records Officer role can read, create, edit, and move folders. The predefined Records Administrator role can perform all folder-related tasks.

It may be necessary at times to create a volume for a folder. When a volume is created, the content in that folder is moved to the newly created *volume folder*. The folder uses a naming convention of *prefix*+timestamp+*suffix*. Both *prefix* and *suffix* can be defined by setting configuration variables. See "RmaFilePlanVolumePrefix and RmaFilePlanVolumeSuffix" on page 7-14 for details. If neither is defined, a prefix of `volume_` is used.

After the volume is created and the content placed inside, the folder is closed and cut off. Subsequent content items can be checked in to the parent folder and additional volumes can be created. The Cutoff and Create Volume disposition action can be used to accomplish this.

Note that volumes are used in retention schedules as well as file plans (used for MoReq tracking).

10.4.2 Managing Record Folders

The following tasks are involved in managing folders:

- "Creating a Record Folder" on page 10-19
- "Creating a Volume Folder" on page 10-20
- "Editing a Record Folder" on page 10-21
- "Changing the Disposition Applied to a Folder" on page 10-21
- "Moving a Record Folder" on page 10-22
- "Deleting a Record Folder" on page 10-22

For details about viewing folder information, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

10.4.2.1 Creating a Record Folder

Use this procedure to create a record folder within a retention category, or as a child folder of another record folder.

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

Prerequisites

- Creating or Editing a Retention Category
- Chapter 12, "Configuring Time Periods" (for cycling items for review).
- Creating or Editing a Supplemental Marking (optional)

This procedure also assumes that security is configured and rights are assigned to users.

1. Open the retention category or folder in which to create a folder.
2. Click **Create** then click **Create Records Folder** from the Page **Action** menu.

   The Create or Edit Record Folder Page is displayed.
3. (Optional) Accept the RecordsGroup as your default security group or select a different group from the Security Group list.
4. (Optional) If your organization uses accounts in its security model, select the account associated to the folder from the Account list. For more information about accounts, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.
5. (Optional) To change the filer (or "author") of the record folder from the default, select the user in the Filer field.
6. Enter a unique identifier.
7. Enter a name for the record folder.
8. (Optional) Enter a description of the folder.
9. (Optional) If the record folder is going to contain subject-to-review items:
   a. Click the **Subject to Review** box.

b. Select a reviewer for notifications to override the system default set in the Configure Retention Settings Page page. The reviewer selected must have the Folder.EditReview right. Without that right, the reviewer cannot mark a record folder as reviewed.

c. Enter the number and select type of period in the Review Period fields. If the category of a record folder is defined as subject to review, and a child record folder does not have its own review information defined, then the record folder inherits the review information from its category or its parent record folder. For further details, see "Attribute Inheritance" on page 10-6.

10. (Optional) To assign supplemental markings to the folder, select one or more markings from the Supplemental Markings list. Even if a user or group has permission to access a record folder, supplemental markings can still restrict record folder access. For more information, see "Supplemental Markings Details" on page 6-2.

11. (Optional, for ACL-enabled implementations) Set up ACL access at the alias level or user level. See "Setting ACLs During Software Use" on page 5-17 for details.

12. Click **Lifecycle Preview** to view the disposition instructions associated with the category and thus the folder.

13. Click **Create**. The record folder is displayed in the exploring retention category or record folder page.

10.4.2.2 Creating a Volume Folder

Use this procedure to create a volume folder within a retention category, or as a child folder of another record folder.

> **Note:** You can only create volumes in a category or folder that contains only content. It cannot contain other retention items.

When a volume is created, all content in the folder is moved to a newly created volume folder. After the volume is created and content is moved, the folder is closed and cut off. Subsequent content items can be checked in to the parent folder, and additional volumes created for them.

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

Prerequisites

- Creating or Editing a Retention Category
- Chapter 12, "Configuring Time Periods" (for cycling items for review).
- Creating or Editing a Supplemental Marking (optional)

This procedure also assumes security is configured and rights are assigned to users.

There are three methods to create a volume folder. This procedure describes two of those methods. See Creating a Volume Through Disposition for details about using dispositions to create volumes.

1. Open the retention category or record folder in which to create a volume folder.

2. Click **Create** then click **Create Volume** or **Schedule Volume Creation** from the Page menu of a folder or a file plan folder (MoReq) containing only content.

   Create Volume creates the volume and inserts content immediately.

   Schedule Volume Creation opens a popup window where the volume creation can be scheduled depending on options selected:

   - The volume will be created when a certain number of items is checked into the folder.
   - The schedule is checked when batch processes are executed and if matched, a volume is created and the content moved then.

10.4.2.2.1 Creating a Volume Through Disposition When creating a disposition that has the **Create Volume** or the **Cutoff and Create Volume** action, slightly different actions occur.

If the Create Volume action is used, a volume is created. The content from the category or folder where the volume was created is then moved into the volume.

If the Cutoff and Create Volume action is used, the volume is created, and the content is moved and the volume is cut off from further processing.

10.4.2.3 Editing a Record Folder

Occasions on which a record folder would be edited include updating:

- specific user access for ACL if alias/group permission is not used
- a reason for freezing a record folder
- activation or expiration dates for internal content
- elaborating on or editing a folder description
- the physical locations and containers for the physical counterpart of electronic items as they progress through their life cycle and are transferred to other locations.

> **Permissions:** To edit a record folder you authored, you must have the Folder.EditIfAuthor right. This right is assigned by default to the Records Officer role. To edit a record folder you did not author, you must have the Folder.Edit right. This right is assigned by default to the Records Administrator role.

1. Navigate to the record folder to edit.
2. Click **Edit** then click **Record Folder** from the Page **Action** menu.

   The Create or Edit Record Folder Page is displayed.
3. Make changes to the available fields.
4. Click **Submit Update**. The successfully updated folder message and the edits are displayed on the Record Folder Information Page. Click **OK**.

10.4.2.4 Changing the Disposition Applied to a Folder

Use this procedure to change the disposition instructions for a particular folder.

1. Navigate to the category that contains the folder to edit.

2. Click **Edit** then **Edit Disposition** in the folder's **Action** menu.

   The Disposition Instructions Page is displayed.

3. Click the **Edit** icon (a pencil) in the row for the disposition to change.

   The Disposition Rule Page is displayed.

4. Change the disposition rules as needed. For more details about dispositions, see Chapter 14, "Defining Disposition Instructions".

5. In the Advanced Options section, select the folder from the pull-down list. Specify to set the new disposition on content only, folders only, or on content and folders.

6. Click **OK** when done.

10.4.2.5 Moving a Record Folder

Use this procedure to move a record folder to a retention category or to another folder.

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

1. Navigate to the record folder to move.

2. Choose **Edit** then choose **Move** from the item **Action** menu.

   The Select Retention Series, Record Folder or Category Dialog is displayed.

3. Click to expand the tree, and drill down in the hierarchy until reaching the category or folder where the record folder will be moved. The location field populates with the new location.

4. Click **OK**. The Exploring Category or Exploring Folder Page and Browse Content area display the record folder in its new location.

10.4.2.6 Deleting a Record Folder

If a record folder has its own disposition rule or rules defined for it, deleting the record folder deletes the disposition rule from the category. To prevent the rule from being deleted, remove the association to the specific record folder. This is discussed in more detail in the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

> **Permissions:** The Folder.Delete right is required to delete a record folder. This right is assigned by default to the Records Administrator role.

1. Open the retention category containing the record folder to delete.

2. Navigate to the record folder to delete.

3. Click **Delete** then click **Delete Record Folder** from the Item **Actions** menu.

4. You are prompted to confirm the deletion. Click **OK** to delete, or **Cancel** to cancel the deletion. To delete any child objects, click the checkbox for "Include child content items" on the prompt that appears. Click **Yes** when done.

5. You are prompted to enter a reason for the action. Enter a reason and click **OK** to confirm or leave the text box empty and click **OK**. Click **Cancel** to abort the entire action.

   If confirmed, the record folder is deleted from the retention schedule.

10.4.3 Folder Examples

The following examples demonstrate folder management tasks:

- "Creating a Record Folder That is Subject to Review" on page 10-23
- "Creating Record Folders Subject to Recurring Audit Triggers" on page 10-23

10.4.3.1 Creating a Record Folder That is Subject to Review

This example record folder has a three month review cycle. Editing a review cycle requires accessing a special edit page. For further information, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

1. Open the retention category or record folder where the record folder will be created.
2. From the **Actions** list, click **Create Record Folder**.

   The Create or Edit Record Folder Page is displayed.
3. Enter `RFV-101` in the **Record Folder Identifier** box.
4. Enter `RFV-101` in the **Record Folder Name** box.
5. Click the **Subject to Review** box.
6. Click a **Reviewer** to receive e-mail notifications when it is time to review the record folder.
7. Enter `3 Months` as the **Review Period**.
8. Click **Create**. The record folder displays in the Exploring Retention Category page. Click the Info icon for the new record folder. The Record Folder Information Page displays "Subject to Review: Yes" and displays the corresponding Review Period. Any inherited review information from a parent record folder or from the retention category is also given.

10.4.3.2 Creating Record Folders Subject to Recurring Audit Triggers

This example demonstrates creating a record folder subject to the recurring audit trigger. For more information about the built-in recurring audit trigger, see "Trigger Overview" on page 11-1. The Audit Periods must already be defined in the Configuration Manager utility. For further information about configuring audit period lists, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

To create an audited record folder, complete the following steps:

1. Open the retention category or record folder where the record folder will be created.
2. From the **Actions** list, click **Create Record Folder**.

   The Create or Edit Record Folder Page is displayed.
3. Enter `RFA-101` in the **Record Folder Identifier** box.
4. Enter `RFA-101` in the **Record Folder Name** box.
5. Click the **Subject to Audit** box, and click an **Audit Period** from the list.

6. Click **Create**. The record folder displays in the Exploring page. Click the Info icon for the new record folder. The Record Folder Information Page displays "Subject to Audit: Yes" and displays the corresponding Audit Period.

11

Setting up Triggers

A trigger starts the processing of a disposition instruction upon the occurrence of a triggering event. Triggers are associated with a disposition rule for a retention category. A triggering event can be a change in content item state, completed processing of a preceding disposition action, retention period cutoff, and custom triggers.

This chapter covers the following topics:

Concepts

Tasks

Examples

11.1 Trigger Overview

Two types of triggers are provided which can be used to initiate disposition processing. System derived triggers are built-in triggers based on defined events. Custom triggers can be created by administrators to define specific events.

To work with triggers, the following rights are required:

- **Admin.RecordManager**: This right enables a user to view information about triggers.

- **Admin.Triggers**: In addition to viewing information about triggers, this right also enables a user to create (add), edit, and delete triggers.

Security groups can be used to block access to triggers. For example, if you do not want users with the Admin.Triggers right to be able to edit and delete triggers, you can use security groups to restrict access to these functions. Only users with access privileges to the security group assigned to a trigger can edit and delete the trigger.

This section covers the following topics:

11.1.1 System-Derived Triggering

System-derived triggering uses the following built-in events or actions:

- Retention period cutoff
- Preceding (disposition) action
- Different content states

11.1.1.1 Retention Period Cutoff

Retention period cutoff causes a cutoff action to occur at the end of the time unit specified in the retention period. After cutoff, the content item is retained for the retention period specified in the disposition rule. For instance, when retention period cutoff is used as a triggering event and a retention period of three calendar years is specified, the cutoff takes place at the end of the current year and the affected content is retained for three years after the end-of-year cutoff.

Retention periods for triggers can only be specified if the `AllowRetentionPeriodWithCutoff` flag is enabled. This is enabled by default.

In previous versions of this product, a negative retention schedule could be supplied for a preceding action. This has now been changed so negative retention periods are available only if the following variables are enabled in the records_management_environments.cfg file:

- `AllowRetentionPeriodWithoutCutoff=1`. When this is enabled, retention periods are allowed with other triggering events in addition to the default ones of Cutoff and Preceding Action.

```
dDispPeriod:allowSignedInteger=1
dDerivedMonthDelay:allowSignedInteger=1
dDerivedDayDelay:allowSignedInteger=1
```

- When these are enabled, a negative retention period can be supplied for any trigger **except for** Cutoff and Preceding Action.

  For example:

```
Triggering Event = Contract Ended
Retention Period = -1 month
Disposition Action = Notify Authors
Triggering Event = Preceding Action
Retention Period = 3 months
Disposition Action = Archive
```

11.1.1.2 Preceding (Disposition) Action

When a preceding action in a disposition instruction sequence completes processing, the next subsequent rule begins. The system tracks when a preceding action completes, and automatically triggers the next step in a disposition sequence.

11.1.1.3 Content or Folder States

System-derived global triggers based on an item or folder state can be affected by an implicit or explicit change in an item or a record folder. An example of an implicit change is when an item has an activation date set in the future. The system is aware of the future activation date and it activates the item at the indicated date. Oracle URM automatically changes the state of the item to active. The Records Administrator does not have to perform any explicit action other than indicating the future activation date. An example of an explicit change in state is when an administrator manually cancels or expires a specific item. When content assumes another trigger-dependent state, the associated disposition rule operates on the item.

11.1.2 Custom Triggers

Custom triggers are defined explicitly by a Records Administrator. Custom triggers are more inclusive and less granular than a system-derived trigger based on content state. A custom trigger can affect all eligible content within a given retention category; whereas a system-derived trigger may only affect one content item within a retention category, because it may be the only item in a given state.

Three types of custom triggers can be defined:

- Global triggers, which happen at a time defined by an administrator
- Custom direct triggers, which use metadata fields as triggering events
- Custom indirect triggers, which occur on a regular schedule based on audit events

The triggers appear in the Triggering Events list of the Disposition Rules screen. For further information, see Chapter 14, "Defining Disposition Instructions".

Access to creating, editing, and viewing information about triggers can be controlled by security settings. If access control list (ACL) security is enabled, access to triggers by group and user permissions can be restricted. If default security is used, then the trigger can be assigned to a security group and the filer be designated.

11.1.3 Global Triggers

Global triggers have an activation date. The activation date can be a past, present, or future date. A user can create a trigger and delay the activation of a trigger for an indefinite amount of time until activation is required. In essence this is a "dormant" trigger, which does not contain an activation date.

A user can create a trigger that activates immediately, activate a trigger on a certain date and time, or delay the activation of a trigger for an indefinite amount of time until activation is required.

11.1.4 Custom Direct Triggers

Use custom direct triggers to create customized trigger functionality in addition to the global triggers built into the product and operating behind the scenes.

Custom direct triggers are system-derived triggers based on a content state, on content, or record folder date fields only. These triggers are not global triggers. They

only affect an item meeting a given state. Unlike regular (global) or event (indirect) triggers, an activation date is not set explicitly for the custom direct trigger and it is not enabled. When created, the custom direct trigger is always active and ready to be used.

Custom direct triggers can be created with a date field, folder date field, or both. There is no logical AND relationship between the content and folder date fields. There is a logical AND relationship between content fields or between folder fields if more than one field is specified. The fields are used to activate the trigger for content and the folder fields are used to activate the trigger for folders.

11.1.5 Indirect Triggers

Unlike a regular (global) trigger, an indirect trigger has a life cycle. Audit Approval is the built-in indirect trigger. This trigger is based on an audit event. It requires the Subject to Audit box to be selected when checking in a content item, and an audit period selected from the Audit list on the check-in page. For more information about checking in content, see the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

The indirect trigger feature saves time in setting up and maintaining triggers that repeat on a regular basis. The Records Administrator must populate the annual triggers list. For information about populating an option list, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

11.2 Managing Triggers

Several tasks are involved in managing triggers:

- "Creating or Editing a Trigger" on page 11-4
- "Viewing Trigger Information" on page 11-6
- "Viewing Trigger References" on page 11-6
- "Deleting a Trigger" on page 11-6
- "Setting Up Indirect Triggers" on page 11-7
- "Deleting an Indirect Trigger Date Entry" on page 11-8
- "Disabling an Indirect Trigger Period" on page 11-8

11.2.1 Creating or Editing a Trigger

Use this procedure to create a new trigger. To assign more granular security settings on triggers than the default roles, be sure that access control list (ACL) security settings are enabled and users are assigned to roles and to an alias for any group permissions.

When creating an indirect trigger, make sure the content field on which the indirect trigger is based has already been created in the Configuration Manager utility. Also make sure the period option list for the indirect trigger periods has been populated.

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

---

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

The Configure Triggers Page is displayed.

2. Select the type of trigger to create (Global, Custom Direct, or Indirect). Click **Add.**

   The Create or Edit Trigger Type Page is displayed.

3. (Optional) If the default security is enabled, select a **Security Group** and **Author** from the lists. Otherwise, the default Security Group is always "RecordsGroup" and the author defaults to the user with the Records Administrator or Records Officer role who created the trigger, even if these fields are not displayed at the time the trigger was created.

4. (Optional) If the organization uses the accounts security model, indicate the **Account** for the trigger.

5. Enter a name up to 100 characters in the **Trigger Name** text box.

6. Enter specific Trigger Information:

   Global Triggers Only: Enter an Activation Date. If not entered it is considered a dormant trigger, which can be activated later.

   Custom Direct Triggers only: Optional, but at least one Content or Folder Date Field should be selected. Select a **Content Date** field or fields for the trigger from the **Content Date Field(s)** list. The field is subject to an ACL character limitation of 100 characters, although the database can be changed to accept more characters into this field.

   Custom Indirect Trigger: Select a content field on which the indirect trigger is based. The list contains all available content fields. Select a folders field on which the indirect trigger is based. The list contains all available fields.

7. (Optional) If ACL-based security is enabled, click **Group** and **User Permissions** for the trigger. This limits who can edit the trigger. See "Setting ACLs During Software Use" on page 5-17 for details.

8. Click **Create**.

   A message is displayed saying the trigger was created successfully.

9. Click **OK**.

   Custom Indirect Triggers: Enter the date periods for the trigger.

Use this procedure to modify the properties of an existing trigger. For example, you may need to change the activation date of a trigger, or change its security access. It is best practice not to use more than two fields at a time for a custom direct trigger, for processing and simplicity.

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

   The Configure Triggers Page is displayed.

2. Select the type of trigger to edit (Global, Custom Direct, or Indirect).

3. Click **Edit** then **Edit Trigger** from the item's **Action** menu for the trigger to edit.

   The Create or Edit Trigger Type Page is displayed.

4. Make the changes to the applicable fields.

5. Click **Submit Update**.

   A message is displayed saying the trigger was updated successfully.

6. Click **OK**.

11.2.2 Viewing Trigger Information

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer role, and the Admin.RecordManager right to the Records Administrator role.

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

   The Configure Triggers Page is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect).
3. Click the trigger name to view.

   The Trigger Information Page is displayed.

4. When done, click **OK**.

11.2.3 Viewing Trigger References

Use this procedure to view references to a trigger (those disposition rules using the trigger in their definitions).

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to view references to a trigger. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer role, and the Admin.RecordManager right to the Records Administrator role.

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

   The Configure Triggers Page is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect).
3. Click the trigger name to view.

   The Trigger Information Page is displayed.

4. From the Page menu, click **References**.

   The Trigger References Page is displayed. This page shows all category dispositions the current trigger is referenced by, with a link to each of the referencing category disposition. If the link is clicked, the Disposition Information Page of the referencing disposition is displayed.

5. When done, click **OK**.

11.2.4 Deleting a Trigger

Use this procedure to delete a trigger. If a trigger is already in use, all references to the trigger must be removed before it can be deleted. Triggers are referenced by triggering events in disposition rules. For more information, see "Creating or Editing a Disposition Rule" on page 14-10.

Permissions: The Admin.Triggers right is required to perform this action. This right is assigned by default to the Records Administrator and Records Officer role. In addition, you must have delete permission (D) for the trigger's security group. The Records Officer roles does not have this permission by default.

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

   The Configure Triggers Page is displayed.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect). Navigate to the trigger to delete.

3. Click **Delete Trigger** on the trigger's **Actions** menu.

   A message is displayed saying the trigger was deleted successfully.

4. Click **OK**.

To delete multiple triggers, click the trigger checkboxes and click **Delete** on the Table menu.

11.2.5 Setting Up Indirect Triggers

Use this procedure to specify the dates required for the Audit Approval periods. The "Audit Approval" indirect trigger is the only built-in indirect trigger available.

Use the same procedure for any other indirect triggers to be created. Select the trigger name and follow the same steps to populate those triggers.

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

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

   The Configure Triggers Page is displayed.

2. Click the Indirect tab. Click **Trigger Dates Info** from the Actions menu for the Audit Approval trigger.

3. Click **Trigger Dates Info** on the Page menu.

   The Indirect Trigger Date Entries Page) is displayed.

4. Click **Add**. The Create or Edit Indirect Trigger Date Entries Page is displayed.

5. Select the trigger period which needs an activation date. If the defaults will not be used, make sure to populate the Trigger Period list in the Configuration Manager utility before performing this action.

6. Enter an activation date for the trigger period. Select the date from the Calendar icon. The time can be edited directly in the Activation Date text box. Be sure to use the time format configured by the system defaults.

7. Click **Create**. The Trigger Date Entry information is added to the Indirect Trigger Date Entries for 'Audit Approval' page:

8. Repeat steps 5 through 7 to define dates for each indirect trigger period.

11.2.6 Deleting an Indirect Trigger Date Entry

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

To delete a date entry (trigger period) for an indirect trigger, complete the following steps:

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

   The Configure Triggers Page is displayed.

2. Click **Delete** from the trigger's **Action** menu.

11.2.7 Disabling an Indirect Trigger Period

Use this procedure to disable, or "disarm," an indirect trigger period at the date entry level. Disabling an indirect trigger period inactivates the trigger, but retains the trigger for archival purposes. The trigger period can be disabled for both built-in and custom indirect triggers.

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

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

   The Configure Triggers Page is displayed.

2. Click **Edit** then **Edit Trigger** from the trigger's Actions menu.

   The Create or Edit Trigger Type Page is displayed.

3. Select the trigger period to disable from the trigger period list, and click **Info**. The Create or Edit Indirect Trigger Date Entries Page is displayed.

4. Clear the **Enabled** box, and click **Submit Update**. The **Enabled** field for the Trigger Period that was edited now displays "No." Click the Configure Retention Schedule Components bread crumb link at the top of the page to return to the Configure Retention Schedule Components page.

11.3 Trigger Examples

This section provides several examples of the following different triggers:

- "Global Triggers" on page 11-9
- "Delayed Global Trigger" on page 11-9
- "Dormant Global Trigger" on page 11-9
- "Activating a Dormant Global Trigger" on page 11-9

- "Custom Direct Trigger" on page 11-9

Permissions: The Admin.Triggers right is required to perform the tasks in these examples. This right is assigned by default to the Records Administrator and Records Officer roles.

11.3.1 Global Triggers

This example creates a global trigger. An active trigger is one that is activated and enabled immediately with no delay in the activation date. In this example, an event trigger with a known activation date is created.

1. Click **Records** then **Configure** then **Triggers** from the Top menu.

   The Configure Triggers Page is displayed.

2. In the Global Triggers area, click **Add**. The Create or Edit Trigger Type Page is displayed.

3. Enter a name up to 30 characters in the **Trigger Name** text box. For this example, type `Case 123 Closed`.

4. Enter an **Activation Date**, either the current date or an earlier date. The activation time is midnight (12:00 AM) by default.

5. Click **Create**. A message is displayed saying the trigger was created successfully. The **Enabled** label indicates "Yes," and the **Activation Date** is displayed.

11.3.1.1 Delayed Global Trigger

Global triggers can be created with a future activation date. The activation of the trigger is delayed until the date and time specified. A user can backdate trigger activation. To do so, use a future activation date when creating the global trigger.

11.3.1.2 Dormant Global Trigger

Triggers can be created with an activation date that is delayed until an activation date is entered. This is a dormant, inactive trigger. A dormant trigger is useful for event triggers when it is known that an event is going to occur, but the exact date is unknown. To avoid system processing overhead, do not enable the trigger. To view an example procedure on activating a trigger at a later date, see "Activating a Dormant Global Trigger" on page 11-9.

To create a dormant global trigger, do not enter an activation date when creating the trigger, but enter it at a later time.

11.3.1.3 Activating a Dormant Global Trigger

A disabled, dormant trigger can be activated without an activation date set for the future. To do so, edit the trigger and enter the activation date.

11.3.2 Custom Direct Trigger

This example creates a custom direct trigger for a custom field based on the termination date of an employee. After the employee termination date is entered on the Content Info Update form, the direct triggers and the item begins its disposition processing. There are three parts to this example:

1. We create the custom field for the Employee Termination Date using the Configuration Manager utility.

2. In Oracle URM, we then create a custom direct trigger keyed off a date field.
3. As part of this example, we will also set up the disposition instruction activated by this custom trigger. The disposition instruction performs the cutoff when the employee termination date is entered, retains the item for 3 years, and then destroys the record. For more information about dispositions, see Chapter 14, "Defining Disposition Instructions".
4. As a last step, we test the trigger to verify it is working correctly.

11.3.2.1 Creating the Record Field

To create the field, complete the following steps:

1. Click **Admin Applets** from the **Administration** menu.

   The Administration Applets are displayed.

2. Click **Configuration Manager**.

   The Configuration Manager utility starts.

3. Click the **Information Fields** tabs, and click **Add**.

   The Add Custom Info Field page is displayed.

4. Enter `EETermDate` in the **Field Name** box, and click **OK**.

   The Edit Page for the field is displayed.

5. In the **Field Caption** box, enter "Employee Termination Date."
6. In the **Field Type** list, click **Date**.
7. Make sure **Required** is not enabled; **User Interface** and **Search Index** are Enabled (typical defaults).
8. Click **OK**.
9. Click **Update Database Design**.

11.3.2.2 Creating the Custom Direct Trigger

Now we have a custom field so we can use it to build an example trigger.

1. Click **Records** then **Configure** then **Triggers** from the Top menu.

   The Configure Triggers Page is displayed.

2. In the Custom Direct Trigger area, click **Add.**

   The Create or Edit Trigger Type Page is displayed.

3. Enter a name in the **Trigger Name** text box. For this example, type "EE Term Date."
4. In the **Brief Description** box, enter "Employee Termination Date."
5. In the **Content Date Field(s)** list, click **EETermDate**. The field is populated with "xEETermDate."
6. Click **Create**.

   A message is displayed saying the custom direct trigger was created successfully.

11.3.2.3 Setting Up the Disposition Instructions

This example creates disposition rules for a category named "Employees." To create the category and disposition instruction, complete the following steps:

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. Click **Create** then click **Create Retention Category** on the Page menu.

   The Create or Edit Retention Category Page is displayed.
3. Enter `EE-RC-1` in the **Retention Category Identifier** box.
4. Enter `Employees` in the **Retention Category Name** box.
5. Enter a description in the **Retention Category Description** box. For this example, type `Employee Retention Category`.
6. (Required for U.S. Government Agencies) Enter the code of the authority for the disposition in the **Disposition Authority** box. For this example, type `EE-RC-1`.
7. Click **Create**. The Disposition Instructions Page is displayed.
8. Create the first rule:
   a. Click **Add**. The Disposition Rule Page is displayed.
   b. In the **Triggering Event** list select the new custom direct trigger called "EE Term Date."
   c. In the **Disposition Action** list, click **Cutoff**.
   d. Click **OK**.
9. Create the second rule:
   a. Click **Add**. The Disposition Rule Page is displayed.
   b. In the **Triggering Event** list, click **Preceding Action**.
   c. In the **Retention Period** fields, enter `3` and click **Calendar Years**.
   d. In the **Disposition Action** list, click **Destroy**.
   e. Click **OK**.
   f. Click **Submit Update**. The successfully updated disposition message is displayed with a summary of the disposition.
10. Click **OK**.

11.3.2.4 Verifying the Custom Direct Trigger

To test the trigger enter an expiration date for a test employee content item in the Info Update Form, accessed from the **Update** option in the Actions list of the content information page. The content item begins disposition processing on the cutoff date. If you check the life cycle for the content item, you can see the dates are already set for the processing.

12

Configuring Time Periods

Periods define a length of time. They are associated with retention periods for dispositions and with review periods for cycling subject-to-review content.

This chapter covers the following topics:

12.1 Using Time Periods

Three types of time periods are used in retention:

- **Custom**: A custom period has a defined start date and time usually not corresponding to a fiscal or calendar year period.
- **Fiscal**: A fiscal period corresponds to a fiscal year.
- **Calendar**: A calendar period corresponds to the calendar year.

Built-in periods cannot be edited or deleted. A user can edit any periods that are created, and created periods can be deleted if the period is not in use.

To work with periods, the following rights are required:

- **Admin.Triggers**: This right enables a user to view information about periods.
- **Admin.RecordManager**: In addition to viewing information about periods, this right also enables a user to create (add), edit, and delete periods.

The following calendar periods are predefined:

- Calendar Quarters (wwRmaCalendarQuarter)
- Calendar Years (wwRmaCalendarYear)
- Months (wwRmaMonth)
- Fiscal Quarters (wwRmaFiscalQuarter)

- Fiscal Halves (wwRmaFiscalHalves)
- Fiscal Years (wwRmaFiscalYear)

Weeks (wwRmaWeekEnd) are defined as a built-in custom period.

12.2 Managing Time Periods

The following tasks are used when managing time periods:

- "Creating or Editing a Custom Time Period" on page 12-2
- "Viewing Period Information" on page 12-3
- "Viewing Period References" on page 12-3
- "Deleting a Custom Period" on page 12-4

12.2.1 Creating or Editing a Custom Time Period

Use this procedure to create a period in addition to the standard calendar periods already defined. For example, you may need a calendar period such as "decade" or "century" for the review cycle or retention period needs of your organization.

> **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 **Periods**.

   The Configure Periods Page is displayed.

2. Click **Add.**

   The Create or Edit Period Page is displayed.

3. Enter a name for the period.
4. Select the type of time period: Calendar, Fiscal, or Custom.
5. Click the calendar icon and select a custom start time or edit the time within the text box.
6. Enter an integer value for the length of the time period and choose a time unit from the Length list.
7. Enter a label to describe the end of the period.
8. Click **Create**.

   A message is displayed saying the period was created successfully, with the period information.

9. Click **OK**.

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

To edit a time period, complete the following steps:

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

   The Configure Periods Page is displayed.

2. Click **Edit Period** from the item's **Action** menu for the period to edit.

   The Create or Edit Period Page is displayed.

3. Edit the appropriate information.

4. Click **Submit Update.**

   A message is displayed saying the period was updated successfully.

5. Click **OK**.

12.2.2 Viewing Period Information

> **Permissions:** Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer roles and the Admin.RecordManager right to the Records Administrator role.

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

   The Configure Periods Page is displayed.

2. Click the period to view from the **Period Name** list.

   The Period Information Page is displayed.

3. When done, click **OK**.

12.2.3 Viewing Period References

Use this procedure to view references to a period (those categories, folders, and disposition rules that use the period in their definitions). Generally, period references are viewed to determine why a custom period cannot be deleted.

> **Permissions:** Either the Admin.Triggers or Admin.RecordManager right is required to perform this action. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer roles. The Admin.RecordManager right to the Records Administrator role.

To view period references, complete the following steps:

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

   The Configure Periods Page is displayed.

2. Click the period to view from the list.

   The Period Information Page is displayed.

3. Click **References** on the Page **Action** menu. The Period Reference Page is displayed. This page shows all folders, categories, and/or category dispositions the current period is referenced by, with a link to each of the referencing items. If a link is clicked, the associated information page for the item is displayed.

4. When done, click **OK**.

12.2.4 Deleting a Custom Period

Built-in periods cannot be deleted. Before deleting a period, make sure the period is not referenced by a retention period within a disposition rule for a category, or by a review period for an item, record folder, or retention category.

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

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

   The Configure Periods Page is displayed.

2. Click **Delete Period** from a period's **Action** menu.

   A message is displayed saying the period was deleted successfully.

3. Click **OK**.

12.2.5 Example: Creating a Custom Period

This example demonstrates creating a custom period with the following characteristics:

- The custom period name is "School Year 2010-2011."
- The custom start time is September 7th, 2010, and the start time is 9:00 am. The system automatically calculates and tracks the end of the period.
- The length of the period is nine months.
- The end of the period label is "End of School Year 2011."

> **Permissions:** The Admin.RecordManager right is required to perform the tasks in this example. This right is assigned by default to the Records Administrator role.

To create a custom school period, complete the following steps:

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

   The Configure Periods Page is displayed.

2. In the Period Name area, click **Add**. The Create or Edit Period Page is displayed.
3. In the **Period Name** box, enter `School Year 2010-2011`.
4. By default, the **Custom** option is already selected in the **Period Type** list. Leave the Custom option selected.
5. Click the calendar icon and select a custom start date: September 7, 2010. The date and default time display in the **Custom Start Time** box. The time defaults to 12 am (midnight) on this page, so to edit the time, you must do so directly in the Custom Start Time text box. Change "`12`" to a "`9`." Make sure you specify the date according to the format used by your system locale.

6. In the **Length** box, enter the length of the custom period in the text box, which is 9 and select the **Months** option from the list.
7. In the **Label for end of period** box, enter `End of School Year 2010-2011`.
8. Click **Create**.

   A message is displayed saying the period was created successfully.
9. Click **OK**.

13

Creating Custom Metadata

If an organization has unique needs for metadata fields for retention categories or record folders, the system software can be customized to include the fields.

This chapter covers the following topics:

Tasks

Examples

13.1 About Custom Metadata

Depending on the field characteristics, the new custom fields are displayed in the Create Category, Create Folder page, or Create Physical Page (if Physical Content Management is enabled). These fields are also displayed on the edit and information pages for those retention schedule objects. See Chapter 10, "Setting Up a Retention Schedule" for details.

The order in which the custom metadata fields appear depends on the order indicated in the custom metadata fields box. The fields can be arranged using the arrows near the custom metadata box.

Custom fields can be added to existing tables already in use in the repository. These fields supplement the fields uses with retention category pages, record folder pages, and physical items pages.

Auxiliary metadata sets can also be created. These are subsets of metadata that can be attached to objects in the repository. This type of metadata is associated with specific properties of an item, such as image size, the character encoding of a document, or other property which must be tracked for specific items. When creating auxiliary metadata, the database table in which the metadata is stored is also created, with a name given to the table and fields added to it. Note that in order to search for auxiliary metadata, Oracle Text Search (full-text searching) must be used.

The process is the same for creating both types of metadata, either complete auxiliary sets or additional fields with the standard metadata sets. The main difference lies in the creation of the table to store the auxliary metadata set.

Note: Using auxiliary metadata sets can slow the search times when using Oracle Text Search because additional tables must be accessed and evaluated.

13.2 Managing Custom Metadata

The following tasks are used when managing custom metadata:

- "Creating or Editing Custom Metadata Fields" on page 13-2
- "Deleting a Custom Metadata Field" on page 13-3

Important: If you plan to use an option list with the custom field, the option list must be created and populated before creating the custom field. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about creating option lists.

13.2.1 Creating or Editing Custom Metadata Fields

The following information is a general navigational procedure for adding metadata fields regardless of type (standard metadata or auxiliary metadata).

Permissions: Users must have the Records Administrator role or the PCM Administrator role in order to perform this action. The user must also have administrative permissions.

1. Click **Records** then **Configure** from the Top menu. Click **Metadata** then **Metadata Sets**.

   The Metadata List Page is displayed.

2. To create a **new auxiliary metadata set**, click **Create Auxiliary Metadata** on the Page menu.

   The Create or Edit Auxiliary Metadata Set Page is displayed. Enter the auxiliary metadata set name, display name, name of the new table being created to house the metadata set, and column prefix. Other fields are optional.

   To **add fields to an existing metadata set**, either auxiliary or standard set (Retention Categories, Record Folders, or Physical), click **Update Fields** from the auxiliary set's individual **Action** menu on the Metadata List Page. The Create or Edit Auxiliary Metadata Set Page is displayed.

3. Add the field information for the new metadata field. Click the **Add** button (a plus sign) to add the field to the field list. Click the **Delete** button (an X) to delete a field from the list. To change the order of fields, highlight a field and move it up or down in the list by clicking the Up or Down arrow.

4. Click **Apply** after adding or editing all the fields.

13.2.2 Viewing Custom Metadata Field Information

Use this procedure to view information about the custom fields added to metadata sets:

1. Click **Records** then **Configure** from the Top menu. Click **Metadata** then **Metadata Sets**.

   The Metadata List Page is displayed.

2. Click **Fields Information** from the **Action** menu of the metadata set to view.

   The Fields for Metadata Page is displayed showing the specific fields created for that metadata set.

13.2.3 Deleting a Custom Metadata Field

> **Permissions:** The Admin.RecordManager right or PCM.Admin.Manager right (when using PCM) is required to perform this action. This right is assigned by default to the Records Administrator and the PCM Administrator roles. The user must also have administrative permissions.

To delete a custom metadata field, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Metadata** then **Metadata Sets**.

   The Metadata List Page is displayed.

2. Click **Update Fields** from the set's individual **Action** menu on the Metadata List Page. The Create or Edit Auxiliary Metadata Set Page is displayed.

3. Select the field name in the Field List and click the Delete button (an X).

4. Click **Apply** after deleting the fields.

13.3 Example: Creating a Custom Category Metadata Field

This example creates a custom retention category metadata field that is an optional text box in which you enter an integer value for a SKU (Stock Keeping Unit).

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

To create a custom retention category metadata field, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Metadata** then **Metadata Sets**.

   The Metadata List Page is displayed.

2. Click **Update Fields** in the **Action** menu for Retention Categories. The Create or Edit Standard Metadata Field Page is displayed.

3. Complete the metadata fields as follows:

   a. Type `DeptSKU` in the **Name** box.

   b. In the **Type** list, click **Integer**.

   c. In the **Caption** box, type `Department SKU`.

   d. Click the **Enabled** box.

e. Click the **Searchable** box.

4. Click the **Add** button (the plus symbol).
5. Click **Apply**. To view the new field, browse content, and click **Create Retention Category** from the Actions menu. The new custom metadata field is displayed.

The field "Department SKU" is added to the Create Retention Category page.

14

Defining Disposition Instructions

Dispositions are the actions taken on content, usually for items no longer required for conducting current business. Disposition actions for content includes the removal of content not needed for legal reasons or for content that has outlasted its usefulness.

Disposition actions can include activities such as transfer to storage facilities or Federal records centers, transfer of permanent content to the National Archives and Records Administration (NARA), the disposal of temporary content, the replacement of content with updated information, and the adjustment of classifications.

Disposition is the last stage of three stages (creation/receipt, use and maintenance, disposition) in content life cycle.

This chapter discusses setting up and administering disposition scheduling. It covers the following topics:

Concepts

Tasks

Examples

14.1 About Dispositions

Dispositions are defined using disposition instructions. A disposition instruction is typically constructed as follows:

1. When a specified triggering event occurs (see "Triggering Events" on page 14-4),
2. Wait a specified period (the retention period, described in "Retention Periods" on page 14-6), if required, and then
3. Perform a specified disposition action (see "Disposition Actions" on page 14-6).

A disposition instruction is created within a retention category. All children record folders and content items normally inherit dispositions from their parent retention category, but a disposition rule can be applied to a specific record folder only.

Access Control Lists (ACLs) can affect what items a user can access when processing dispositions. For example, if a user is not in the ACL for a category, the user will not be able to access a pending disposition even if that user is in the appropriate alias group and has the appropriate rights and permissions. Always verify the ACL in use with a category to ascertain what effect it may have on actions taken on that category.

14.2 Disposition Types

The following types of dispositions are available:

14.2.1 Event Dispositions

An *event disposition* is when items are eligible for disposition when an event takes place. Upon the occurrence of a specified event, or immediately thereafter, an item is eligible for the disposition. The event itself acts as a cutoff or closing occurrence. An event disposition does *not* have a retention period and uses actions like "Delete revision" and "Delete all revisions." Typical examples of an event disposition instruction are "Destroy when obsolete" or, in the case of classified content, "Retain for ten years after declassification." The disposition actions can vary:

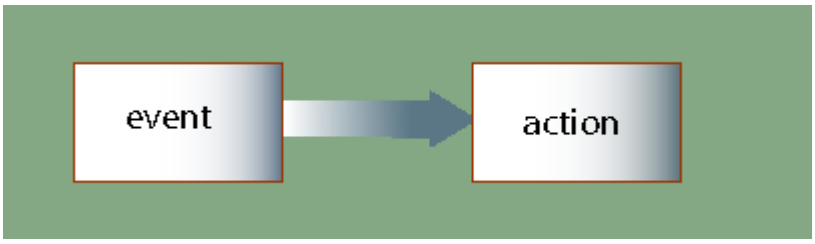
- Content that is tracked for DoD purposes use actions like "destroy" and "retain," and the states of the items are "obsolete" and "declassified," respectively.
- Non-DoD content uses actions like "Delete revision" and "Delete all revisions."

To view an example step-by-step procedure for creating an event disposition, see "Event Disposition" on page 14-14.

If classification is used (an optional security feature for Oracle URM which is also certified to comply with the Chapter 4 requirements of the DoD 5015.2 specification), an event disposition can be set to declassify content on a specific date or downgrade classification on a specific date.

To summarize, event dispositions do not have retention periods and have an implicit, system-derived cutoff.

Figure 14–1 Event Disposition

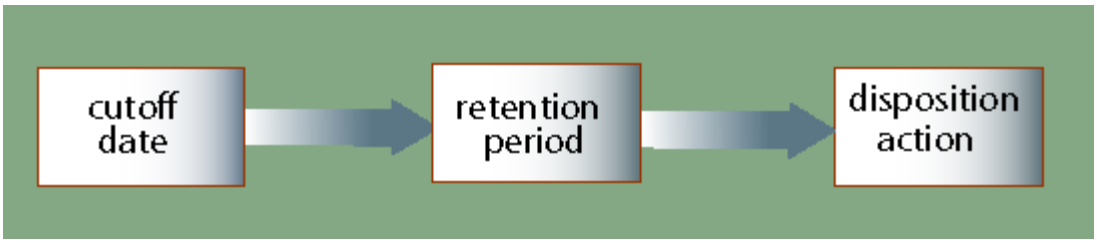


14.2.2 Time Dispositions

A *time disposition* has a fixed retention period and begins with a user-defined file cutoff. The retention period must transpire before the disposition instruction takes action on the content item. Typical examples include "Cutoff at the end of the (fiscal or calendar) year," "retain for three years, then destroy" or, in the case of DoD classified records, "Cut off at declassification, retain for ten years, then destroy." To view an example step-by-step procedure for creating a time disposition, see "Time Disposition" on page 14-15.

To summarize, time dispositions have retention periods and explicitly defined cutoffs.

Figure 14–2 Time Disposition

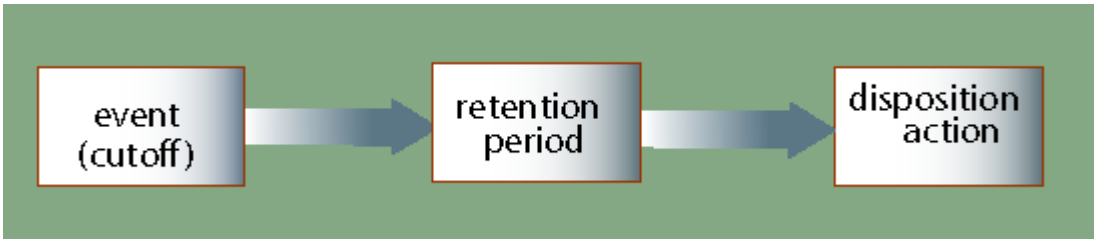


14.2.3 Time-Event Dispositions

A *time-event disposition* is a disposition instruction beginning with a specified triggering event. After the event has transpired, then the folder or content item is cut off and the retention period is applied. A typical example of a time-event disposition instruction is "Destroy five years after a (legal) case is closed." To view an example step-by-step procedure for creating a time-event disposition, see "Time-Event Disposition" on page 14-16.

To summarize, time-event dispositions have explicitly defined events, cutoffs, and retention periods.

Figure 14–3 Time-event Disposition



14.3 Category Rule Review Using Workflows

Make sure to enable functionality allowing the disposition rules for a category to be reviewed through workflow steps before the disposition is available for general use. To use this feature, the following configuration variable must be set:

- Click the checkbox for **Enable Category Dispositions Reviews** on the Configure Retention Settings Page.
- `CategoryDispositionWorkflowContentType`: the default workflow for category dispositions is performed by the retention category content type. Alter this configuration variable to a different content type if needed.
- `UpdateDispositionTableOnWorkflowApproval`: allows the system to update the dispositions table when the workflow is processed and approved. Default: TRUE. If set to false, the table is updated when the content item is released. If a final revision is deleted, the previous revision becomes the current revision and when that revision is released, the dispositions table is updated.

Workflows must be set up to enable the review of disposition rules. See "Setting Up Workflows" on page 7-4 for more details.

Enable the workflow to initiate workflow processing. Once enabled, items proceed into a workflow. If the process is disabled before the items finish the workflow process, the items may become 'stuck' in the workflow and will not complete until the process is enabled again.

After the functionality is enabled, dispositions enter a workflow for approval before use. After creating a disposition, a message is displayed indicating the disposition is in the workflow, awaiting approval.

14.4 Triggering Events

A disposition instruction is activated when a triggering event occurs. This section discusses built-in triggering events. For details about creating custom triggers, see Chapter 11, "Setting up Triggers".

14.4.1 Preceding Actions Triggering Event

- **Retention Period Cutoff**: This event cuts off disposition processing and applies a retention period. It can be used for system-derived triggering events based on time dispositions or time-event dispositions.
- **Period Cutoff with Volume**: This event cuts off disposition processing to a volume and applies a retention period.

14.4.2 Content State Triggering Event

- **Activated**: This event is activated when the associated content or record folders have been activated.
- **Canceled**: This event is activated when the associated content or record folders have been canceled.
- **Delete Approved**: This event is activated when the associated content or record folders have been approved for deletion.
- **Expired**: This event is activated when the associated content or record folders have been expired.

- **Obsolete**: This event is activated when the associated content or record folders have been marked as obsolete.
- **Obsolete and Delete Approved**: This event is activated when the associated content or record folders have been marked as obsolete and have been approved for deletion.
- **Rescinded**: This event is activated when the associated content or record folders have been rescinded (that is, made void because of an enacting authority).
- **Superseded**: This event is activated when the associated content has been superseded that is, supplanted, or displaced, by content that is more recent or improved).

> **Note:** Items must be linked to be superseded.

- **No Longer Latest Revision**: This event is activated when the associated content revisions are no longer the latest revision (that is, a new revision has been checked into the repository). This trigger enables a user to create a rule to initiate automatic disposal of old revisions of content. This is especially useful to keep only the latest revision of content, and automate the disposal of old revisions.
- **Superseded Twice**: This event is activated when the associated superseded content are superseded again. If content item A is superseded by content item B, which is subsequently superseded by content item C, then this trigger is activated for content item A.
- **Last New Record Added**: This event is activated when the associated item is the most recent item added to a record folder. This enables a user to track the activity in a folder, which can be useful to optimize the usage of folders based on their activity level. For example, you may decide to delete (or otherwise process) folders if there has been no activity for a specified period.
- **Scheduled declassify date**: This event is activated when the associated content or record folders are scheduled to be declassified on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.
- **Scheduled downgrade date**: This event is activated when the associated content or record folders are scheduled to be downgraded in their security classification on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.
- **Declassified date**: This event is activated when the associated content or record folders have been declassified on a specific date. This trigger is available only if the ClassifiedEnhancements component is enabled.

14.4.3 Indirect Triggers

- **Audit Approval**: This event is activated when the associated content or record folders have been approved during an audit (using the built-in "Audit Approval" indirect trigger).

14.4.4 Custom Triggers

- **Custom triggers** are also supported. For more information, see "Creating or Editing a Trigger" on page 11-4.

14.5 Retention Periods

The retention period is the amount of time waited after the triggering event before a disposition action is performed. Several built-in period units (including calendar years, fiscal quarters, months, and weeks) are available, but custom periods can be created (see "Creating or Editing a Custom Time Period" on page 12-2).

A retention period can be specified for all triggering events, enabling a user to create disposition rules for content such as "Delete all old revisions three months after the last new revision was checked in."

Examples of retention periods include:

- 5 calendar years
- 2 fiscal quarters
- 6 months
- 4 weeks

14.6 Disposition Actions

A disposition action defines what will happen after Triggering Events occur and Retention Periods, if any, have passed. The following built-in disposition actions are supported. In addition to the built-in disposition actions below, a user can define custom disposition actions (see Appendix C, "Customizing Your System" for details).

Important: Default disposition actions always require approval from an administrator. Custom disposition actions can be configured to perform approvals automatically. Some actions have a separate 'mark complete' step because the system cannot tell if the action is done.

For example, the completion of destruction or moves of physical records cannot be determined by the software, so someone must mark the action complete. The same is true for all transfer, accession, and move actions where the destination is defined using the software and the physical movement of the items is not within control of the software.

14.6.1 Classified Records Actions

- **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 to the next lower security classification in the hierarchy.
- **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 to the next higher security classification in the hierarchy.

These four disposition actions are available only if the ClassifiedEnhancements component is enabled.

14.6.2 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 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 the DoD Config module is enabled, a prompt appears to select either **Delete All Revisions (Destroy Metadata)** or **Delete Revisions (Keep Metadata)** when approving the disposition action. Metadata cannot be retained unless the DoD Config module is enabled.
  - 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 from the repository 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.
- **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.
- **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. This action is not available unless the `RmaEnableFixedClones` configuration variable is set to TRUE.

Note that if deletion rules exist for a category, content is deleted according to the first rule encountered. Therefore, content will be deleted from all folders in the same category and not just from one folder.

14.6.3 Other Actions

- **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 into the repository 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.

- **Accession**: This action indicates it is time to transfer physical and legal custody of materials to an archival institution such as NARA. Choose **Accession (Destroy Metadata)** or **Accession (Keep Metadata)**.
- **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 indicates it is time to supersede a content item by another content item.

In addition to the built-in disposition actions listed above, custom dispositions can be defined to reflect an organization's specific records management needs.

14.6.4 Transfer/Move Actions

- **Archive**: This action indicates it is time to archive content or record folders. Choose **Archive (Destroy Metadata)** or **Archive (Keep Metadata)**.
- **Create Content Server Archive**: This action indicates it is time to create an archive containing the affected content with their metadata.
- **Create Volume**: Creates a volume folder. When the action is encountered, the contents are transferred to the volume folder.
- **Move**: This action indicates it is time to move content and metadata out of the system. Choose to **Move (Destroy Metadata)** or **Move (Keep Metadata)**.
- **Transfer**: This action indicates it is time to transfer content from one location to another, but does not transfer the legal and physical custody (as with accession). Choose to **Transfer (Destroy Metadata)** or **Transfer (Keep Metadata)**.

14.7 Cutoff Guidelines

In most cases, a retention period does not start until a triggering event is set to "cut off." To cut off the records in a file indicates the record will be ended at regular intervals to permit disposal or transfer in complete blocks. For correspondence files, this permits the establishment of new files. Cutoffs involve ending input to old files and starting input to news ones.

The length of the retention period determines when to cut off a content item, category, or folder and at what interval to perform a cutoff. Use the guidelines discussed in this section to help determine when to cut off and apply retention periods.

Retention periods for triggers can only be specified if the `AllowRetentionPeriodWithCutoff` flag is enabled. This is disabled by default.

14.7.1 Time Retention Periods

Content items that have a retention period of less than one year are typically cut off at an interval equal to the retention period. For example, if a retention category has a retention period of one month, cut the folder off at the end of each month. Then, apply the retention period for another month before applying the final disposition, such as destroying the items.

When a content item has a retention period of one or more years, cut off the folder at the end of each fiscal or calendar year. After the end of year cutoff, apply the retention period.

14.7.2 Time-Event Retention Periods

On the date the event or action is completed, perform the cutoff, then apply the retention period.

14.8 Disposition Precedence

Content filed into multiple folders residing in different categories are managed based on the longest time disposition.

When an item has been filed into multiple folders belonging to disparate retention categories, it is subject to multiple disposition processing schedules. In the event of this scenario, the longest retention period prevails. However, the item is processed by disposition instructions belonging in two or more categories. The following scenario describes a disposition processing precedence.

Content is filed into Folder 1 of Category 1 and into Folder 2 of Category 2.

Category 1: Folder 1	Category 2: Folder 2
Expire after 4/1/09	Close after 3/1/09
Archive on 4/10/09	Expire after 4/5/09
Destroy on 4/12/09	Destroy on 4/20/14

The instructions are processed in a staggered order:

1. On 3/1/09, the item will be cutoff with its cutoff date and Folder 2 will be closed.
2. On 4/1/09, the item will be expired and the expiration date will be added to the item (viewable on the content information page).
3. On 4/5/09, the item will not be expired again, so the expiration date is not updated.
4. On 4/10/09, the item and Folder 1 will be archived.
5. On 4/12/09, the pointer to the item is removed from Folder 1 by an update to the content information. The pointer still exists to Folder 2. The items are not actually filed into a folder, but are "pointed" to the folder.

6. On 4/20/14, the item under Folder 2 will finally be destroyed, as the item is not being held by any remaining pointers.

14.9 Managing Dispositions

The following tasks are involved in managing dispositions:

- "Enabling or Disabling User-Friendly Captions" on page 14-10
- "Creating or Editing a Disposition Rule" on page 14-10
- "Viewing Disposition Information" on page 14-13
- "Deleting a Disposition Rule" on page 14-13

14.9.1 Enabling or Disabling User-Friendly Captions

User-friendly captions can be enabled or disabled at any time. This setting also affects the query strings in the Criteria boxes of the Screening pages.

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. Expand the User Interface section if necessary. Click 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 uncheck the box.

14.9.2 Creating or Editing a Disposition Rule

A disposition rule applies to all content and record folders in a category by default. A disposition rule can also be created that applies only to a specific record folder. This is a general navigational procedure; to view example procedures for specific types of dispositions, see the "Disposition Examples" on page 14-14.

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

---

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Action** menu.

   The (initially blank if creating a disposition) Disposition Instructions Page is displayed.

3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.

4. Choose the disposition rule's triggering event from the **Triggering Event (After)** list.

5. If the disposition rule has a retention period, enter an integer value in the **Retention Period (Wait for)** box and select the corresponding period from the **Retention Period** list.

6. Select an action for the rule from the **Disposition Action (Do)** list.

7. (Optional) Click the plus symbol (+) to expand the lower section of the screen. If the disposition instruction applies only to a specific record folder, select the folder from the **Apply to Folder (On folder(s))** list. Otherwise, allow the instruction to apply to all folders within a category.

8. (Optional) If the disposition instruction applies only to other retention objects, select an object from the list.

9. (Optional) If a user other than the category author should review the e-mail notifications triggered by the disposition rule, specify the user in the **Notification Reviewer** field by entering the user name or selecting a user from the list next to the field. If not specified, only the category author is notified of events triggered by the disposition rule. If specified, it depends on the software configuration who will receive e-mail notifications: both the specified user and the category author (= default) or the specified user only.

10. (Optional) When creating a category disposition using Accession, Archive, Move, or Transfer, a field is available to designate how archiving is to be done through the **Location Type** list.

    When an item is archived to an external storage location using File Storage, FTP, or WebDAV, the metadata audit history is included with the item's metadata. Select an alternate metadata path if needed. If the alternate metadata path required authentication, it must match that of the primary archive path. A user can elect to be prompted for this information or use default information provided in the user profile, as discussed below.

    Note that WebDAV will support a PropPatch method that assigns meta values to a file that has been uploaded to a WebDAV server. To enable this functionality, a configuration variable must be set. See "RmaEnableWebdavPropPatchOnExport" on page 7-13 for details.

    By default when the action is performed, a zip file containing the items associated with the disposition is placed in the storage location. Select the box to unpack the zip file at destination.

    Depending on the location type chosen, fill in the following information:

    - File Storage: Enter the storage path where the archive file will be stored.
    - FTP: Specify the path to the FTP server and the directory location for the archive and, if chosen, the meta path. Enter the appropriate user name and password.
    - WebDAV: Specify a valid WebDAV path and, if chosen, the meta path. Enter the appropriate WebDAV user name and password.
    - Other: This selection specifies that the archive will be downloaded manually when the action is performed. If the destination has an associated location or container, enter a description in the appropriate text box.

Items can also be transfered to an external workspace. Set up the external workspace by clicking **My Profile**. Click **Edit** next to the User Workspace caption. An external workspace can be a local file system, a FTP server, a WebDAV server, or a manual download and can be set up in the same way the Location Type is set up here.

Note: You can set defaults for the location type for each user. Click the user name in the top right corner of the screen. The My Profile page is displayed. Click **Edit** in the User Workspace section. You can set default locations, passwords, and other details for the location types there.

---

11. After making selections if necessary reorder the instructions in the list. If Cutoff is present, it must be the first rule. If the Destroy or Accession rule is present, those rules must be last.To reorder an instruction, select it in the list, and click the up or down arrow.
12. Click **Submit Update**. The successfully updated dispositions message is displayed, with the disposition information.
13. Click **OK**.

Use this procedure to edit a disposition rule within the disposition instructions for a retention category.

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

To edit a disposition rule, complete the following steps:

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. Navigate to the appropriate retention category.
3. Click **Edit** then **Edit Disposition** from the item's **Action** menu.

   The Disposition Instructions Page is displayed.
4. In the Disposition Instructions box, select the rule to edit, and click the **Edit** icon (an image of a pencil).
5. The Disposition Rule Page is displayed.
6. Make changes to the rule, and click **OK**. The Disposition Rule page closes.
7. Click **Submit Update**. The successfully updated dispositions message is displayed, with the disposition information.
8. Click **OK**.

14.9.3 Copying a Disposition Rule

Use this procedure to copy rules from other categories to overwrite the ones in a current category.

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

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click **Edit** then **Copy Disposition From** from the item's **Actions** menu.

   A prompt is displayed, asking permission to overwrite the rules with rules from another category. Click **OK** to continue.
4. The Browse for Category Page is displayed. This is similar to the Select Retention Series, Record Folder or Category Dialog. Choose a category in the list from which to copy a disposition rule.

   The Disposition Instructions Page is displayed.
5. If needed, edit the rules in the same manner as described earlier.
6. Click **Submit Update**. The successfully updated dispositions message is displayed, with the disposition information.
7. Click **OK**.

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

14.9.4 Viewing Disposition Information

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

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click the Info icon.

   The Disposition Information Page is displayed.
4. When done, click **OK**.

14.9.5 Deleting a Disposition Rule

Use this procedure to delete a disposition rule from the disposition instructions within a category, or delete the entire set of disposition instructions.

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

1. Click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click **Edit** then **Edit Disposition**.

   The Disposition Instructions Page is displayed.
4. Select the rule to delete and click the Delete icon (a red 'x' in a circle).
5. The rule is deleted from the list. Repeat for each rule to delete.
6. Click **Submit Update**. The successfully updated dispositions message is displayed.
7. Click **OK**. It is advisable to run the Batch Services after deleting a disposition rule in order to recompute disposition actions. Batch services are run automatically or can be initiated by selecting the approrpriate action by clicking **Records** then **Batch Services** from the Top menu.

14.10 Disposition Examples

This section includes the following disposition examples:

- "Event Disposition" on page 14-14
- "Simple Time/Event Disposition" on page 14-15
- "Time Disposition" on page 14-15
- "Time-Event Disposition" on page 14-16
- "Disposition Rules for Specific Folders" on page 14-17
- "Multi-Phased Disposition" on page 14-18

All of the examples in this section use the default (that is, non user-friendly) disposition captions.

14.10.1 Event Disposition

This example creates an event disposition instruction that destroys content after an event. The event is the content becomes obsolete. The disposition action is to destroy the content. This example requires creating one disposition rule.

Disposition instruction: Destroy when obsolete.

1. Navigate to the appropriate retention category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The (initially blank) Disposition Information Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.

4. In the **Triggering Event** list, click the **Obsolete** option.
5. In the **Disposition Action** list, click the **Destroy** option.
6. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
7. Click **Submit Update**. The successfully updated disposition message is displayed.

14.10.2 Simple Time/Event Disposition

This example demonstrates creating a disposition based on an item's revision status.

Disposition Instructions: When a new version of an item is checked in, wait one week and notify the original author.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The Disposition Instructions Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.
4. In the **Triggering Event** list, click the **No Longer Latest Revision** option. The Retention Period field becomes available.
5. In the **Retention Period** fields, enter 1 in the text box and click the **Weeks** period unit from the Retention Period list.
6. In the **Disposition Action** list, click the **Notify Authors** option.
7. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**. The successfully updated dispositions message is displayed.

14.10.3 Time Disposition

This example demonstrates creating a time disposition with a retention period and a final disposition of destroying content. There is a predictable event trigger commencing at the end of a fiscal year.

Disposition Instructions: Cut off at the end of the fiscal year, hold for three fiscal years in the current file area, then destroy.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The Disposition Instructions Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.
4. In the **Triggering Event** list, click the **Retention Period Cutoff** option. The Retention Period field becomes available.
5. In the **Retention Period** fields, enter 3 in the text box and click the **Fiscal Years** period unit from the Retention Period list.

6. In the **Disposition Action** list, click the **Destroy** option.
7. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**. The successfully updated dispositions message is displayed.

Notice this disposition uses a system-derived triggering event. After the item becomes obsolete, it is automatically cut off at the end of the fiscal year then the retention period begins.

14.10.4 Time-Event Disposition

A typical example of a time-event disposition instruction is "Destroy five calendar years after the (legal) case is closed." A time-event disposition is different from a time disposition because the exact time the event might occur cannot be predicted, but when it does, the disposition processing begins. A time-event disposition also uses a built-in or custom trigger. When the event occurs, the activation date for the custom trigger is entered, if applicable.

This example creates an event disposition instruction that destroys items at a specified time after an event. The event is the closing of a pending legal case. The retention time period is five years. The disposition action is to destroy the content.

This example requires creating a custom trigger called "Case closed." Create a custom trigger without an activation date. After the case is closed, you would also need to go in and set the activation date for the custom trigger.

Disposition Instructions: Destroy five calendar years after case closed.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The Disposition Instructions Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.
4. Define the first disposition rule:
   a. In the **Triggering Event** list, click the **Case closed** option under the **Custom Triggers** sublist.
   b. In the **Disposition Action** list, click the **Cutoff** option.
   c. Click **OK**. The rule is displayed in the Disposition Instructions box.
5. Define the second disposition rule:
   a. Click **Add** to add another rule.
   b. In the **Triggering Event** list, click the **Preceding Action** option under the **Preceding Action** sublist.
   c. In the **Retention Period** field, specify 5 calendar years.
   d. In the **Disposition Action** list, click the **Destroy** option.
   e. Click **OK**. The rules are displayed in the Disposition Instructions box. Notice the rule prefaced by a preceding action is indented with an ellipsis.

6. Click **Submit Update**. The successfully updated dispositions message is displayed.

14.10.5 Disposition Rules for Specific Folders

This example demonstrates creating a disposition instruction that applies different rules to the folders within a category.

Disposition Instructions: Close the folder to further filing after a specified event, and then destroy.

- Folder 1: Event trigger is Program ABC canceled.
- Folder 2: Event trigger is Program BBC expired.
- Folder 3: Event trigger is Program CDB rescinded.

This example requires creating three record folders (F1, F2, F3) and a custom event trigger for each folder. Each folder contains correspondence relevant to a particular program.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The Disposition Instructions Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.
4. Define the first disposition rule for record folder 1:
   a. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is "Program ABC Canceled."
   b. In the **Disposition Action** list, click the **Destroy** action.
   c. In the Advanced Options section, select the folder which will have the rule applied. In this example, the record folder is "Folder 1."
   d. Click **OK**. The rule is displayed in the Disposition Instructions box.
5. Define the second rule for record folder 2:
   a. Click **Add** to add another rule.
   b. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is "Program BBC Expired."
   c. In the **Disposition Action** list, click the **Destroy** action.
   d. In the Advanced Options section, select the folder which will have the rule applied. In this example, the record folder is "Folder 2."
   e. Click **OK**. The rule is displayed in the Disposition Instructions box.
6. Define the second rule for record folder 3:
   a. Click **Add** to add another rule.
   b. In the **Triggering Event** list, select the custom trigger you created for the folder. In this example, it is "Program CDB Rescinded."
   c. In the **Disposition Action** list, click the **Destroy** action.

d. In the Advanced Options section, select the folder which will have the rule applied. In this example, the folder is "Folder 3."

e. Click **OK**. The rule is displayed in the Disposition Instructions box.

7. Click **Submit Update**. The successfully updated dispositions message is displayed. Notice there are rules drawn between the multiple instructions.

14.10.6 Multi-Phased Disposition

This example demonstrates defining a disposition instruction that has more phases than is typical in a disposition instruction. This example contains multiple disposition actions: move, transfer, and accession. A "move" disposition action does not transfer the legal responsibility of content, whereas a "transfer" disposition action does transfer both legal responsibility and physical location of content.

Disposition Instructions: Cut off at the end of the calendar year and hold for on year in the current file area, move to off-line storage for on year, transfer to the FRC (Federal Records Center) and retain for ten years, then final accession to NARA.

1. Navigate to the appropriate category.
2. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and click **Edit** then **Edit Disposition** from the Page menu on the Retention Category Information Page.

   The Disposition Instructions Page is displayed.
3. In the Disposition Instructions area, click **Add**.

   The Disposition Rule Page is displayed.
4. Define the first phase of the disposition, which is cut off at the end of the calendar year, retain in the current file area for one year, and then move to offline storage:

   a. In the **Triggering Event** list, click the **Retention Period Cutoff** option. The Retention Period field becomes available.

   b. In the **Retention Period** fields, enter 1 in the text box and click the **Calendar Years** period unit from the Retention Period list.

   c. In the **Disposition Action** list, click the **Move** option to move the content to offline storage.

   d. In the **Destination Location** box, type Offline Storage.

   e. Click **OK**. The rule is displayed in the Disposition Instructions box.
5. Define the next phase of the disposition, which is transfer to the Federal Records Center after a one year retention period of offline storage:

   a. Click **Add** to add another rule.

   b. In the **Triggering Event** list, click the **Preceding Action** option.

   c. In the **Retention Period** fields, enter 1 in the text box and click the **Calendar Years** period unit from the Retention Period list.

   d. In the **Disposition Action** list, click the **Transfer** option to move the content to offline storage.

   e. In the **Destination Location** box, type FRC.

   f. Click **OK**. The rule is displayed in the Disposition Instructions box, indented under the previous rule.

6. Define the final phase of the disposition, which is accession to the National Archives (NARA) after a ten year retention of the content in the FRC:
   a. Click **Add** to add another rule.
   b. In the **Triggering Event** list, click the **Preceding Action** option.
   c. In the **Retention Period** fields, enter 10 in the text box and click the **Calendar Years** period unit from the Retention Period list.
   d. In the **Disposition Action** list, click the **Accession** option.
   e. In the **Destination Location** box, type NARA.
   f. Click **OK**. The rule is displayed in the Disposition Instructions box, indented under the previous rule.
7. Click **Submit Update**. The successfully updated dispositions message is displayed.
8. Click **OK**.

15

Setting Up Freezes

Freezing inhibits disposition processing. This can be used to comply with legal or audit requirements. Different types of freezes can be defined to refine the freeze/hold process needed in an organization.

For information about using Federated Freeze during legal processing, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

> **Important:** Creating custom disposition actions requires in-depth technical knowledge of Oracle UCM. To define custom disposition actions, contact Consulting Services.

This chapter covers the following topics:

Concepts

Tasks

15.1 Freezes

> **Note:** Freezing is also available for content outside Retention Schedules.

Freezing a content item or record folder inhibits disposition processing for the item or the items in the folder. This may be necessary to comply with legal or audit requirements (for example, because of litigation). In addition, metadata for the folder or item is also frozen.

If an item is frozen, all revisions of the item are frozen. The frozen revision is frozen directly and the other revisions inherit the freeze.

For details about using Federated Freezes during the process of legal discovery, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

Recurring freezes can also be scheduled for selected items of content. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about that process.

This section covers the following topics:

15.1.1 Managing Freezes

The following tasks are involved in managing freezes:

15.1.1.1 Creating or Editing a Freeze

Use this procedure to create a freeze users can select if they want to freeze a content item.

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 **Freezes**.

   The Freeze Configuration Page is displayed.

2. Click **Add**.

   The Create or Edit Freeze Page is displayed.

3. Select a **Security Group** from the list. This field is only displayed if default security is enabled on the Configure Retention Settings Page.

4. In the **Filer** field, specify the person who is responsible for creating the freeze. This will normally be the person currently logged in, so the default does not generally need to be changed, but a different user can be chosen from the list if required.

5. Specify a **name** for the freeze.

6. (Optional) Specify a **description** for the freeze.

7. (Optional) Specify group and user permissions to restrict who has access to the freeze. These fields are only displayed if ACL-based security is enabled on the Configure Retention Settings Page. See "Setting ACLs During Software Use" on page 5-17 for details.

8. (Optional) Specify the **end date** of the freeze.

Important: The items are not unfrozen automatically at the specified date. This must be done manually. This field is used for tracking and documentation purposes only.

9. (Optional) Specify a descriptive text with instructions for unfreezing the items.
10. (Optional) Specify if a notification should be sent about the freeze. Notifications are first sent out when the freeze is created.
11. Enter the email address of people to receive the freeze notification and the email address of the person initiating the email.
12. Enter an email message.
13. (Optional) Specify if notification should be periodically re-sent.
14. Select a period to wait before re-sending, and the period value (for example, 1 month).
15. Click **Create**.

    A message is displayed saying the freeze was created successfully, with the freeze information.
16. Click **OK**.

Use the following procedure to edit a freeze:

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

   The Freeze Configuration Page is displayed.
2. Click **Edit** then **Edit Freeze** from a freeze's item **Actions** menu.

   The Create or Edit Freeze Page is displayed.
3. Make modifications as required, and click **Submit Update** when done.

   A message is displayed saying the freeze was updated successfully, with the freeze information.
4. Click **OK**.

15.1.1.2 Viewing Freeze Information

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

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

   The Freeze Configuration Page is displayed.
2. Click a freeze name to view.

   The Freeze Information Page is displayed.
3. When done, click **OK**.

15.1.1.3 Deleting a Freeze

> **Permissions:** The Admin.RecordManager right is required to perform this action. This right is assigned by default to the Records Administrator role. Delete permission (D) for the security group of the freeze is also required.

A freeze cannot be deleted if the freeze is currently applied to any items.

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

   The Freeze Configuration Page is displayed.

2. Click **Delete** from a freeze **Action** menu.

To delete multiple freezes, select the freeze checkbox and click **Delete** on the Table menu on the Freeze Configuration Page.

15.1.1.4 Freezing Items, Folios or Folders

Use this procedure to freeze a folder, content item or folio.

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

1. Search for and find the item to freeze.

   The Search Results Page is displayed.

2. Select the item to freeze by clicking the checkbox next to the item name.

   A dialog is displayed. If changing the freeze that is in use, select a freeze from the list.

3. Click **Edit** then **Freeze Selected** from the Table menu.

   Select a freeze reason from the Freeze Dialog. Freezes added to the user's Favorites list appear. To see all freezes, click the **Show All Freezes** link. Enter a reason for the freeze.

4. Click **OK**.

   A message is displayed saying the item are frozen.

5. Click **OK**. To view frozen items after a freeze is executed from the Search Results Page, click the **Refresh** button or execute a new search.

15.1.1.5 Unfreezing Frozen Items or Folders

Use this procedure to unfreeze all folders or content items currently frozen with a particular freeze.

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

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

The Freeze Configuration Page is displayed.

2. Click **Edit** then **Unfreeze** from a freeze's Item **Actions** menu.

   A dialog is displayed. If changing the freeze that is in use, select a freeze from the list. Freezes added to the user's Favorites list appear. To see all freezes, click the **Show All Freezes** link.

3. In the **Unfreeze Reason** field, specify a reason for the unfreeze action.

4. Click **OK**.

   A message is displayed saying all items with the selected freeze have been successfully unfrozen.

5. Click **OK**.

15.1.1.6 Searching for Frozen Content and Folders

Use this procedure to search for content items or folders currently frozen with a specific freeze.

> **Permissions:** The Admin.RecordManager right and Admin.Screening right is required to perform this task. These rights are assigned by default to the Records Administrator role.

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

   The Freeze Configuration Page is displayed.

2. Click the **Action** menu for a freeze. In the **Information** Page menu, click one of the **Screen...** options:

   - **Screen Frozen Content**: Used to display a list of all content items currently frozen with the selected freeze. The list will not include any frozen content that inherited freeze status from a parent record folder. Either this option or the next option produce essentially the same result.
   - **Screen Derived Content**: Used to display a list of all content items currently frozen with the selected freeze and any items frozen in a folder with this freeze. Therefore, the list includes all frozen items that inherited their freeze status from their parent folders.
   - **Screen Frozen Folders**: Used to display a list of all folders currently frozen with the selected freeze. The list will not include any frozen folders that inherited their freeze status from their parent folders.
   - **Screen All Frozen Folders**: Used to display a list of all folders currently frozen with the selected freeze. The list will also include all frozen folders that inherited their freeze status from their parent folders.

   The Frozen Item Page is displayed, which lists all content or folders meeting the criteria of the selected screening option.

15.1.1.7 Re-sending an E-Mail Notification for a Freeze

If you set up e-mail notification for a freeze, the notification e-mail is first sent out when you initially create the freeze (see "Creating or Editing a Freeze" on page 15-2). You can elect to periodically send out notifications when you set up a freeze.

Use this procedure to send the e-mail notification about the freeze again (for example, because you want to notify the people involved about a change in the freeze implementation).

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

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

   The Freeze Configuration Page is displayed.

2. Click a freeze name.

   The Freeze Information Page is displayed.

3. Make modifications to the e-mail properties (recipients, message text) as required.

4. Click **Submit Update** when done.

   A message is displayed saying the freeze was updated successfully, with the freeze information. The notification e-mail has been sent using default e-mail settings.

5. Click **OK** to return to the "Configure Retention Settings Page" on page A-6 page.

Notifications can also be set by searching for a freeze. On the Freeze Information Page, click **Edit** then **Renotify**.

15.1.2 Example: Creating a Freeze

This example creates a freeze due to litigation with a company that is valid until 2/20/2010.

> **Permissions:** The Admin.RecordManager right is required to perform the tasks in this example. This right is assigned by default to the Records Administrator role.

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

   The Freeze Configuration Page is displayed.

2. In the Freeze area, click **Add**.

   The Create or Edit Freeze Page is displayed.

3. In the Security Group field, make sure `RecordsGroup` is selected.

4. In the **Filer** field, make sure your own user login is displayed.

5. In the **Freeze Name** field, type `Litigation`.

6. In the **Freeze Description** field, type `Litigation With Company XYZ`.

7. In the **End Date** field, specify 2/20/2010 as the end date, by typing or using the calendar icon.

8. In the **Unfreeze Instructions** field, type `Do not unfreeze until the litigation proceedings are completed`.

9. If required, click the **Send Notification** box, and provide the e-mail properties (recipients, from-address, and message text).

10. Click **Create** when you finish.

16

The Oracle UCM Adapter

An *adapter* provides a bridge between Oracle URM (which contains the content management policies) and the adapter server's content vault (which stores additional content). Corporations can then manage records, retention policies, and legal holds across multiple systems from a single location.

An adapter sends information back to the Oracle URM server so it can maintain an up-to-date catalog of the enterprise's important content. By doing so, companies can apply their records and retention policies to more content, more consistently, with less administrative effort and less disruption for users. These same benefits apply to litigation searches and holds. The Oracle UCM Adapter for Oracle Content Server (hereafter abbreviated as the UCM Adapter) obtains these policies from the server and applies them to the content items stored in the vault.

Multiple adapters can be used with Oracle URM to manage an enterprise's content needs. This chapter discusses how to configure and use one specific adapter, the UCM Adapter.

This chapter contains the following topics:

Concepts

Tasks

16.1 UCM Adapter Overview

This section provides an overview of the UCM Adapter and its components. It contains the following topics:

16.1.1 Architecture

The major components involved in a typical UCM Adapter installation include:

- **Oracle URM**: Enables organizations to manage their content and retention policies, disposition processes and litigation or audit holds in a central repository. These policies, dispositions, and holds can then be applied to external repository content through the UCM Adapter.
- **Oracle Content Server**: Stores and manages content in a repository.
- Oracle UCM Adapter for Oracle Content Server: Communicates between Oracle URM and the UCM Adapter server's content vault. The UCM Adapter provides common retention functionality as follows:
  - Identifying the content in the repository that is of interest to Oracle URM.
  - Performing searches and declaring the applicable content items to Oracle URM.
  - Performing disposition actions on the existing content items when their retention periods end.
  - Establishing and removing holds and freezes on the content items, as necessary.

16.1.2 Oracle URM and the UCM Adapter

Oracle URM manages records and retention policies, disposition processes, and litigation holds or freezes in a central repository. Those policies, dispositions, and holds can be applied to content stored in multiple repositories by using adapters. The repositories may be any server or application that holds content whose retention is to be controlled.

The UCM Adapter server's content vault holds content that must be preserved for a retention period, specified in a corporate retention schedule, and then destroyed according to a corporate disposition process. The records are preserved in place because the UCM Adapter ensures that the record remains unalterable during the retention period. Upon request, the UCM Adapter server's content vault can purge the content at the end of the retention period.

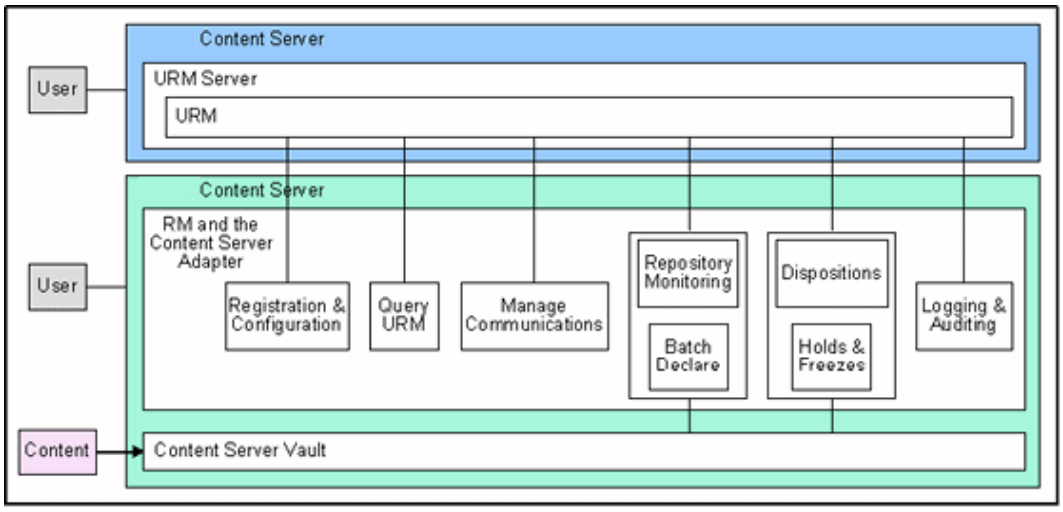
The UCM Adapter server's vault may also hold content that does not need to be retained. When retention of this content is no longer necessary, it can be disposed of according to the disposition processes stored within Oracle URM.

There is an obligation to ensure that any material that is subject to a litigation or audit hold (freeze) is not deleted, either by a user or as part of a disposition process. The UCM Adapter enables Oracle URM to ensure deletions do not happen.

Note: Content items that are non-records and are not subject to a litigation or audit hold are not transferred to Oracle URM. Instead, these documents remain in the UCM Adapter server's content vault and only their metadata is stored in Oracle URM.

The UCM Adapter is the communications intermediary between Oracle URM and the UCM Adapter server's repository. Content is stored in and remains in the UCM Adapter server's content vault while Oracle URM simultaneously enforces corporate retention policies, disposition processes, and legal holds on the stored content.

Figure 16–1 UCM Adapter Retention Functions Overview



The UCM Adapter can be configured to provide the following basic retention functions:

- **Registration**: The UCM Adapter self-registers with Oracle URM, ensuring that Oracle URM knows about the UCM Adapter server's content vault and is thus ready to manage the stored content within the repository.
- **Configuration**: UCM Adapter configuration includes collecting the proper identification and credentials information for Oracle URM security and communications. Configuration information also includes mapping metadata fields and defining searches.
- **Query Oracle URM**: The UCM Adapter queries Oracle URM for certain information. For example, it may need to retrieve retention schedules for specific items of interest. Or the UCM Adapter may need to request Oracle URM metadata for content items and obtain lifecycle information.
- **Manage Communications**: The UCM Adapter monitors batch processes, handles communication errors with Oracle URM, and handles large work requests by grouping them into communication blocks and processing the response in chunks.
- **Repository Monitoring and Batch Declare**: The UCM Adapter monitors its server's content vault by periodically searching the repository and informing Oracle URM of any changes in the repository that may affect disposition processes or audit holds. For example, the UCM Adapter will inform Oracle URM about new content checkins that need to be managed.

- **Perform Oracle URM Tasks**: The UCM Adapter periodically checks Oracle URM for tasks to be performed within the repository. These tasks enable Oracle URM to abide by the corporate retention policies and disposition processes. Typical tasks include:
  - Oracle URM may use the UCM Adapter to perform a search within the UCM Adapter server's content vault and provide a list of items matching the search criteria.
  - When a litigation hold applies to managed content within the UCM Adapter server's content vault, Oracle URM may use the UCM Adapter to retrieve a list of affected items and preserve them to ensure that they are not edited or destroyed.
  - When a litigation hold is removed, the UCM Adapter can be used to stop preserving the affected items and dispose of them according to retention schedule rules and instructions.
- **Logging and Auditing**: The UCM Adapter provides consistent logging for the activities it coordinates. The UCM Adapter contributes event information to the log files that are then uploaded to Oracle URM, consolidated, and stored.

16.2 UCM Adapter Configuration

The initial step in setting up the UCM Adapter is to access the Records menu on the remote server where the UCM Adapter will reside. Select **Records** then **Configure** then **Enabled Features** from the Top menu. Select the Adapter option.

When the UCM Adapter option is chosen on the Enabled Features Page on a remote repository, the necessary component software is enabled. The system must then be restarted in order for the installation to be complete.

Next define an outgoing provider on the UCM Adapter server and register the repository source. The documents in that repository will be managed using Oracle URM retention policies.

After registration of the source a check is automatically made to compare content on the UCM Adapter and the Oracle URM repository. A list is presented of items which do not match those items on the Oracle URM repository. At that time the items on the UCM Adapter repository can be deleted to make sure the two systems are in sync.

Next metadata fields should be mapped. The UCM Adapter repository may contain a wide variety of documents and may have custom fields which do not directly correlate to those on the Oracle URM repository. When UCM Adapter documents are classified into groups, there can be a wide variety of retention categories associated with the content. The metadata fields between the two repositiories must be mapped so the content is categorized correctly.

Note that the UCM Adapter does not synchronize security groups with Oracle URM. If using Oracle I/PM with the UCM Adapter and later plan to synchronize data with Oracle URM, the security groups will not match. Oracle I/PM creates new security groups dynamically, as needed for applications. Therefore, plan to set up the same security groups on Oracle I/PM and the UCM Adapter that will be used on Oracle URM.

In previous versions of this adapter, a Configure Source Disposition Actions screen was used to specify actions for the adapter to complete. That screen is no longer available so those options cannot be limited when using the current system.

For complete details about defining and using providers, see the *Oracle Fusion Middleware System Administrator's Guide for Content Server*.

> **Important:** Revisioning of external items differs from revision of items stored on Content Server. For example, if an item is created on the adapter system and is synchronized to Oracle URM, it appears as a single item. However, if that item is revised on the adapter system then synchronized to Oracle URM, the item now appears in the category as two items, not one item with two revisions. Both items have the same content ID, which is the default behavior for external items.

This section describes the basic tasks needed to configure and use the UCM Adapter:

- "Configuring Sources and Providers" on page 16-5
- "Managing Fields" on page 16-7

16.2.1 Configuring Sources and Providers

Use these procedures to configure the source and provider.

- "Defining a New Outgoing Provider" on page 16-5
- "Editing an Outgoing Provider" on page 16-5
- "Disabling the Adapter's Outgoing Provider" on page 16-6
- "Deleting the Adapter's Outgoing Provider" on page 16-6
- "Registering an External Source" on page 16-6
- "Unregistering and Removing an External Source" on page 16-7
- "Viewing External Source Configuration Settings" on page 16-7
- "Viewing Outgoing Provider Configuration Settings" on page 16-7

16.2.1.1 Defining a New Outgoing Provider

Use this process to define an outgoing provider:

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Source Registration**.

   The Register Source Page is displayed.

2. Click **Add**.

   The Add or Edit New Provider Page is displayed.

3. Enter the required information in the appropriate fields.

4. Click **Add** when done.

16.2.1.2 Editing an Outgoing Provider

Use this process to define an outgoing provider:

> **Note:** The Adapter does not allow you to edit the outgoing provider if it is linked to an external Oracle URM source. You must first undo this link before editing the outgoing provider.

1. Click **Administration** then **Providers** from the Main menu.

   The Provider List Page is displayed.

2. Navigate to the provider to edit and click **Info**.

   The Provider Information Page is displayed.

3. Click **Edit**.

   The Add or Edit New Provider Page is displayed. Edit the information as needed and when done, click **Save**.

16.2.1.3 Disabling the Adapter's Outgoing Provider

To disable an existing outgoing provider on the Adapter server:

1. Click **Administration** then **Providers** from the Main menu.

   The Provider List Page is displayed.

2. Navigate to the provider to disable and click **Info**.

   The Provider Information Page is displayed.

3. Click **Disable**.

   A prompt appears to confirm the choice.

4. Click **OK**.

   The outgoing provider is disabled.

16.2.1.4 Deleting the Adapter's Outgoing Provider

To delete an existing outgoing provider on the Adapter server:

> **Note:** The Adapter does not allow you to delete the outgoing provider if it is linked to an external Oracle URM source. You must first undo this link before deleting the outgoing provider.

1. Click **Administration** then **Providers** from the Main menu.

   The Provider List Page is displayed.

2. Navigate to the provider to delete and click **Info**.

   The Provider Information Page is displayed.

3. Click **Delete**.

   A prompt appears to confirm the choice.

4. Click **OK**.

   The outgoing provider is removed from the Providers table.

16.2.1.5 Registering an External Source

Only one source per adapter can be registered.

Follow this procedure to register an external source.

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Source Registration**.

   The Register Source Page is displayed.

2. Enter the required information in the appropriate fields.
3. Click **Register** when done.

16.2.1.6 Unregistering and Removing an External Source

> **Important:** Unregistering a source clears the data on the external source. You should export and archive the data before unregistering a source.

Follow this procedure to unregister an external source.

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Unregister Source**.
2. A prompt appears to confirm the action. Click **OK** to continue.

Follow this procedure to remove an external source and the database tables associated with the source.

> **Important:** If you remove an external source, you must reconfigure the external source in order to use it again.

1. Click **Records** then **Configure** from the Top menu. Click **Retention** then **Remove External Sources**.

   The Remove External Source page is displayed.
2. This page lists all registered external sources. Highlight the name of a source to remove and click **Remove** or click **Reset** to clear the highlighting. To remove multiple items, hold down the shift key and highlight multiple items.
3. To delete the database tables associated with the source(s), click the checkbox next to **Delete External Source Database Tables**. All database tables associated with the external source will be deleted.

16.2.1.7 Viewing External Source Configuration Settings

To view the external Oracle URM source configuration settings, click **Records** then **UCM Adapter** from the Top menu. Click **Configuration Information**. The Source Configuration Information Page is displayed.

16.2.1.8 Viewing Outgoing Provider Configuration Settings

Follow this procedure to view outgoing provider configuration settings:

1. Click **Administration** then **Providers** from the Main menu.

   The Provider List Page is displayed.
2. Navigate to the provider to delete and click **Info**.

   The Provider Information Page is displayed.

16.2.2 Managing Fields

Make sure to match custom metadata fields that exist on the Adapter's remote source to fields already in use on the local Oracle URM source. If fields do not exist that match those on the Adapter, create a custom metadata field to accomodate the Adapter data.

This section describes the tasks needed to map custom fields:

- "Mapping a Custom Metadata Field" on page 16-8
- "Editing a Mapped Metadata Field" on page 16-8

16.2.2.1 Mapping a Custom Metadata Field

To add a Oracle URM custom metadata field to a remote source:

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Custom Fields**.

   The Map Custom Fields Page is displayed.

2. Click **Add**.

   The Map/Edit Custom Field Dialog is displayed.

3. A list of custom metadata from the remote source is available in a dropdown list. Select a metadata field for use from the list and enter a name and caption for that field to be stored in the Oracle URM database table.

4. Click **OK**.

   The custom metadata field is added to the list of custom metadata fields on the Map Custom Fields Page.

5. To change the field order, use the Up or Down arrow keys to move the position of the field.

16.2.2.2 Editing a Mapped Metadata Field

To edit a previously mapped field:

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Custom Fields**.

   The Map Custom Fields Page is displayed.

2. Select a metadata field from the list, and click **Edit**.

   The Map/Edit Custom Field Dialog is displayed.

3. Alter information as needed and click **Update**.

   The Map Custom Fields Page is displayed.

4. To change the field order, use the Up or Down arrow keys to move the position of the field.

16.3 Synchronizing Data

After configuring the Adapter for use with Oracle URM, determine a synchronization schedule to ensure that content on both systems, the Adapter and the Oracle URM system, are consistently kept in sync. This section describes the tasks involved in establishing synchronization.

The systems can also be synchronized on an as-needed basis by selecting an option from the UCM Adapter menu. Note that these operations synchronize all items involved in the operation. For example, all content involved in freeze events are synchronized. Individual freeze events cannot be selected to be synchronized.

Important: Revisioning of external items differs from revision of items stored on Content Server. For example, if an item is created on the adapter system and is synchronized to Oracle URM, it appears as a single item. However, if that item is revised on the adapter system then synchronized to Oracle URM, the item now appears in the category as two items, not one item with two revisions. Both items have the same content ID, which is the default behavior for external items.

The following options can be synchronized:

- **Retention Schedule**: synchronizes the entire retention schedule between the two systems
- **Content**: choose from the following types of synchronization operations:
  - **Upload**: find and synchronize recently uploaded content
  - **Delete**: find and synchronize newly deleted items
  - **Freeze**: find and synchronize items which have been frozen or unfrozen.
- **Content Dates**: synchronizes any date field which has changed. If both the external source and the local repository have different dates, the earliest date is used regardless of whether it is on the Adapter or the Oracle URM repository.
- **Mark Complete**: synchronizes items that are ready for approval and completion of disposition processing.
- **Upload Archives**: synchronizes uploaded archives.
- **Mark Vital**: synchronizes items marked for vital review.
- **All**: synchronizes all possible operations.

The following sections discuss synchronization:

- "Performing As-Needed Synchronization" on page 16-9
- "Scheduling Synchronization" on page 16-9
- "Viewing Synchronization Logs" on page 16-10

16.3.1 Performing As-Needed Synchronization

Follow this procedure to synchronize content based on specific synchronization operations:

1. Click **Records** then **UCM Adapter** from the Top menu. Click **Synchronize** then click the type of synchronization to perform.
2. The operation is performed.
3. If the operation completes successfully, a message is displayed. Click **OK** to continue.
4. If an error occurs, a message is displayed. Check the synchronization logs to view the details of the operation and which items may have failed synchronization. See "Viewing Synchronization Logs" on page 16-10 for details.

16.3.2 Scheduling Synchronization

Follow this procedure to set up a schedule to perform regular synchronization:

1. To access this page, click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Scheduled Events**.

   The Configure Scheduled Events Page is displayed.

2. Choose the unit of time measurement from the pulldown list and the amount of time to elapse between synchronizations.
3. Choose a time for synchronization which will not affect system performance.
4. Click **Save** when done.

16.3.3 Viewing Synchronization Logs

Follow this procedure to view logs that are automatically generated during any synchronization activity, either on-demand or scheduled.

1. Click **Records** then **UCM Adapter** from the Top menu.
2. Click **Logs** then choose the type of log file to view.

   The Synchronization Log Page is displayed.

3. To view additional details about the logged event, click **View Items** from the operation's **Action** menu.
4. To rerun the operation, click **Rerun Task** from the operation's **Action** menu.

A

User Interface

This section contains information about the interface used with the software.

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

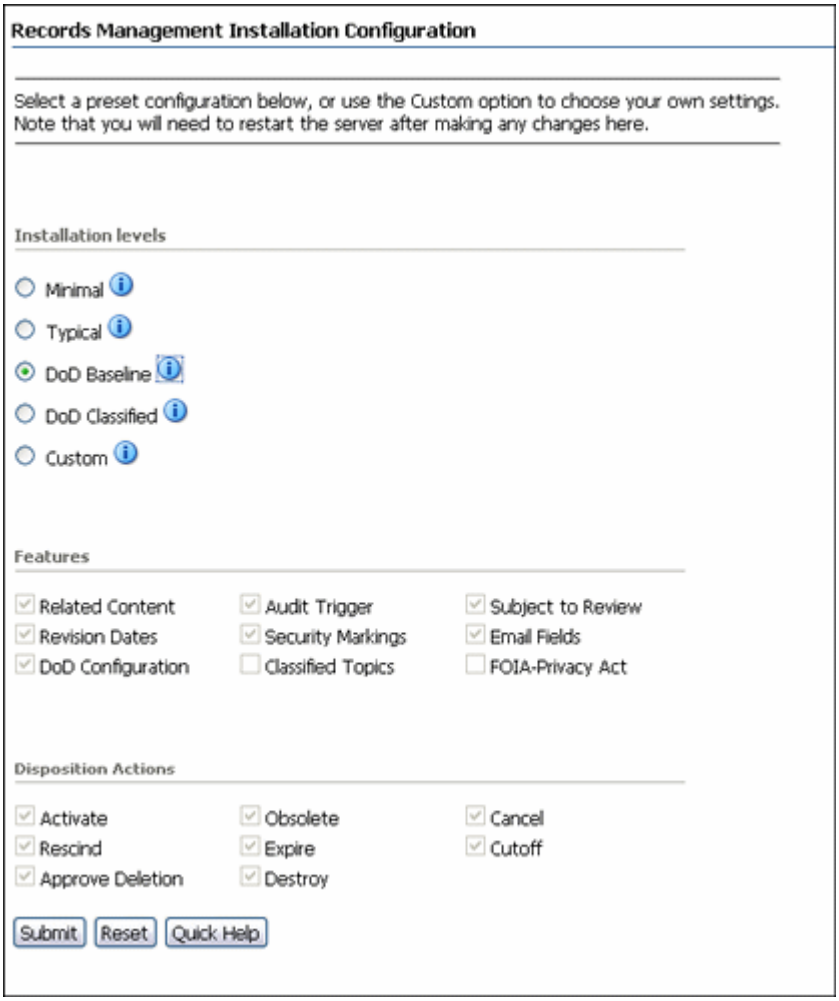
The screens used are divided into the following groupings:

A.1 Initial Features Pages

After installation of the software, two screens are available with information that must be configured before setting up retention policies and procedures:

A.1.1 Enabled Features Page

This page is used to determine which components will be enabled for use.



The page depiction here shows all options displayed.

To access this page, click **Records** then **Configure** from the Top menu. Click **Enabled Features**.

After making selections or if configuration options are changed (for example, switching from Baseline to Classified), restart the Content Server and rebuild the Content Server index. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details.

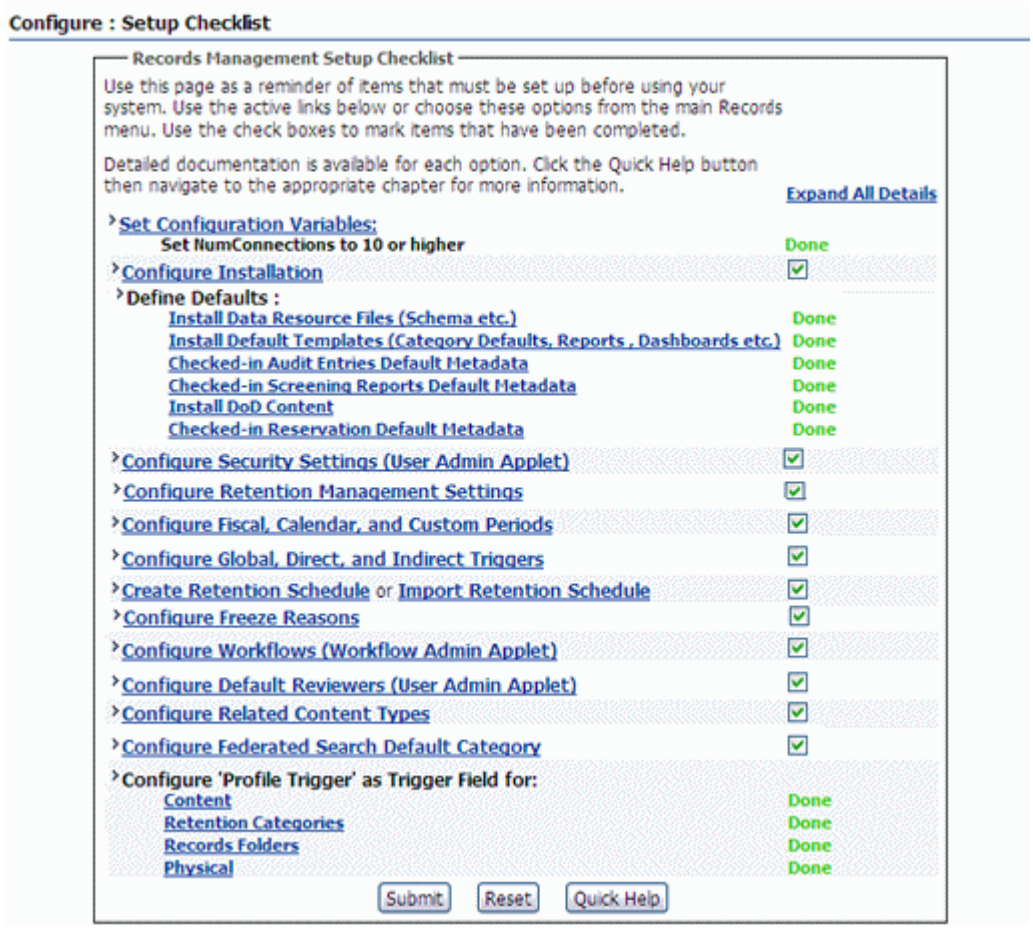
For details about the components enabled for each option, click the **Info** icon.

Element	Description
Installation Level	The type of configuration to be enabled. Options are: ▪ Minimal ▪ Typical ▪ DoD Baseline ▪ DoD Classified ▪ Custom

Element	Description
Features	This section contains a list of features that can be enabled when using the Custom option. Default features are enabled when installation levels are chosen. These features include: ■ Related Content ■ Audit Trigger ■ Subject to Review ■ Revision Dates ■ Security Markings ■ Email Fields ■ DoD Configuration ■ Classified Topics ■ FOIA/Privacy Act
Disposition Actions	This section contains the disposition actions which can be used for content. They include: ■ Activate ■ Rescind ■ Approve Deletion ■ Obsolete ■ Expire ■ Destroy ■ Cancel ■ Cutoff

A.1.2 Setup Checklist Page

This page is used to set global options for aspects of the retention management system.



Important: You must configure all defaults, including any necessary categories, dispositions, and triggers, before checking in content that will use those defaults.

To access this screen, click **Records** then **Configure** then **Setup Checklist** from the Top menu.

If the configuration tasks on this page are not completed, a warning message with a link to this page appears on the home page. Click the link to display this page.

The options on this page vary according to the type of installation chosen. The screen depiction shown here may not be the same as that in use at a site. For example, is an Adapter is installed, an additional entry is available to perform the configuration steps necessary for the Adapter.

After making selections or configuration options are changed (for example, switching from Baseline to Classified), restart the Content Server and rebuild the Content Server index. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about restarting the system and rebuilding the index from the Repository Manager.

Important: If File Store Provider is needed to check in templates for Oracle URM, you must set up the File Store Provider first and then check in the templates. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about using File Store Provider.

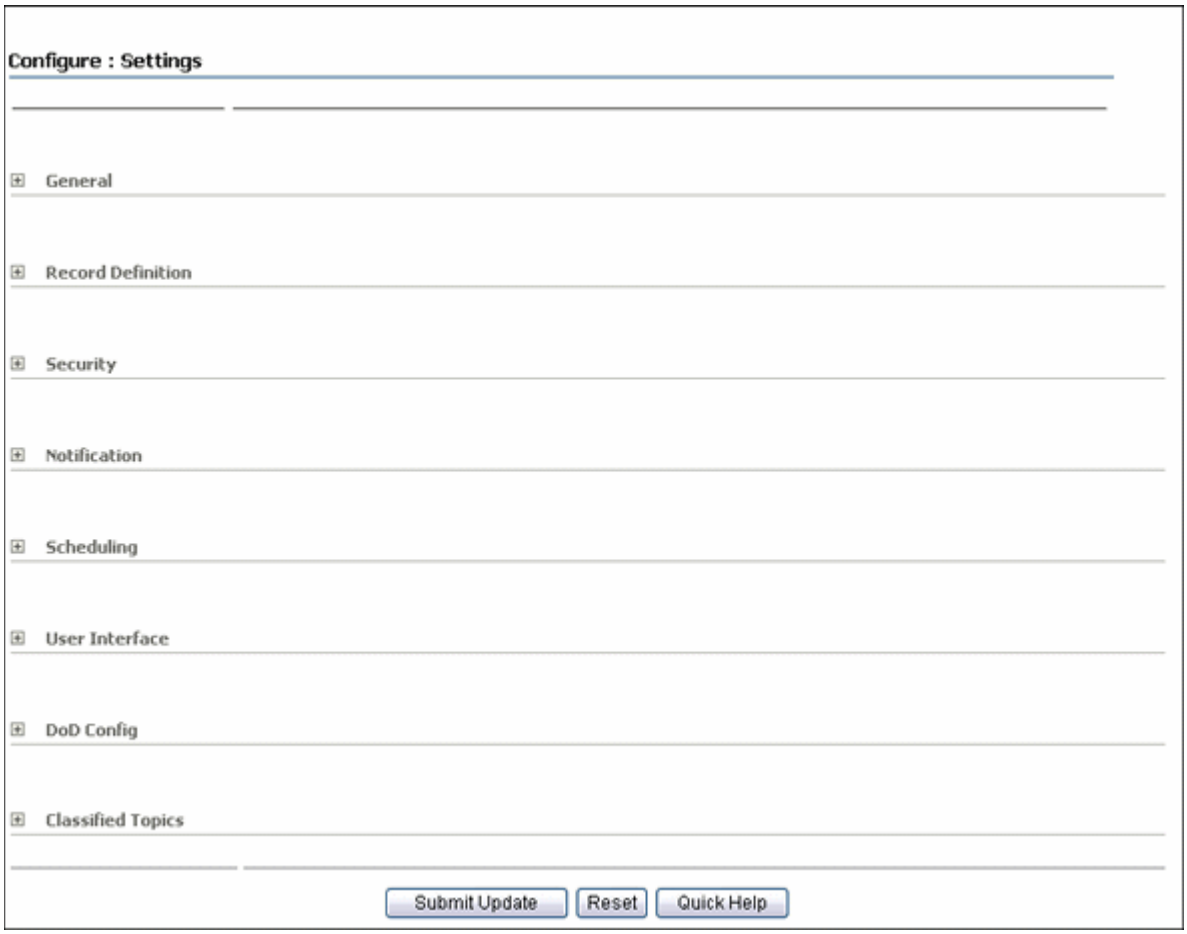
Selecting any option in this list displays a detailed explanation of the option's purpose. Other options may be available, depending on the installation being performed.

Element	Description
Set Configuration Variables	Contains directions on how to set essential configuration variables.
Define Defaults	Used to define the default checkin information for audit trails, template locations, and metadata for content that is automatically checked in on a periodic basis. Also used to configure the metadata used for Audit Entries and for Screening reports. Clicking an option brings up a check in page where the fields to be used as defaults can be edited. This is also used to check in report templates, dashboard panels, and category defaults.
Configure Installation	Used to configure optional components and metadata fields. Select from preset configurations to choose the features that are needed.
Configure Security Settings	Used to define the security settings including roles, rights, and access control list use. This link opens the Admin Applets. Click the User Admin Applet to configure security.
Configure Retention Management Settings	Used to configure many retention management options such as supplemental markings, triggers, and reports. Clicking this option displays the Configure Retention Settings Page.
Configure Fiscal, Calendar, and Custom Periods	Used to set periods used for disposition processing. Selecting this option displays the Configure Periods Page.
Configure Global, Direct, and Indirect Triggers	Used to set up the triggers used for disposition processing. Selecting this option displays the Configure Triggers Page.
Create Retention Schedule or Import Retention Schedule	Used to set up retention schedules. Selecting **Create Retention Schedule** displays the Exploring Retention Schedule Page. Selecting **Import Retention Schedule** displays the Import/Export Screen. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about importing and exporting files.
Configure Freeze Reasons	Used to set up freezes. Selecting this option displays the Freeze Configuration Page.
Configure Workflows	Used to set up workflows to use with offsite storage, reservations, and category disposition processing. These workflows must be set up in order for that functionality to work properly. Click the Workflow Admin Applet to proceed.
Configure Default Reviewers	Used to add users who will be default reviewers. Click the User Admin Applet to proceed.
Configure Related Content Types	Used to set up links. Selecting this option displays the Configure Links Type Page. Links are discussed in the *Oracle Fusion Middleware User's Guide for Universal Records Management*.

Element	Description
Configure Federated Search Default Category	Used to indicate a default category and default folder to use for Federated searches. Selecting this option displays the Admin Server page where the appropriate configuration variables can be entered: ■ FederatedSearchDefaultCategory=*categoryId* ■ FederatedSearchDefaultFolder=*folderId*
Configure Profile Triggers	Used to determine the trigger for profiles used in searching and checking in content and physical items.

A.2 Configure Retention Settings Page

Use this page to set many of the configuration options for the system. When initially opened, the options on this page are unexpanded. To expand an option, click the plus sign next to the section name.



Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role. If **Run Auto Computation of Declassification Date** will be selected, the user must have the highest security classification as well.

To access this page, click **Records** then **Configure** then **Settings** from the Top menu.

The following list describes the sections on this page and the options included in each section. Depending on the configuration, not all options may appear. The following table describes all options in more detail.

- General
  - Start of fiscal calendar
  - Archive Meta Data Format
  - Log Metadata Changes
  - Disable Lifecycle Update
  - Enable Category Dispositions Review
  - Enable Report Exclude Search Options
- Record Definition
  - Always/Never restrict revisions
  - Always/Never restrict deletions
  - Always/Never restrict edits
  - Display Record Icon
- Security
  - ACL-based security
  - Default security on Retention Schedule objects
  - Supplemental Markings
  - User must match all Supplemental Markings
  - Custom Security fields
  - Classified Security
- Notification
  - Do not notify authors
- Scheduling
  - Only allow scheduled screening
- User interface
  - User-friendly disposition
  - Show Export Date
  - Use Page Navigation
  - Paginate Navigation Tree
- DoD Config
  - Enable Custom Script Evaluation
- Classified Topics
  - Maximum years before declassifying
  - Run Auto Computation of Declassification Date

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

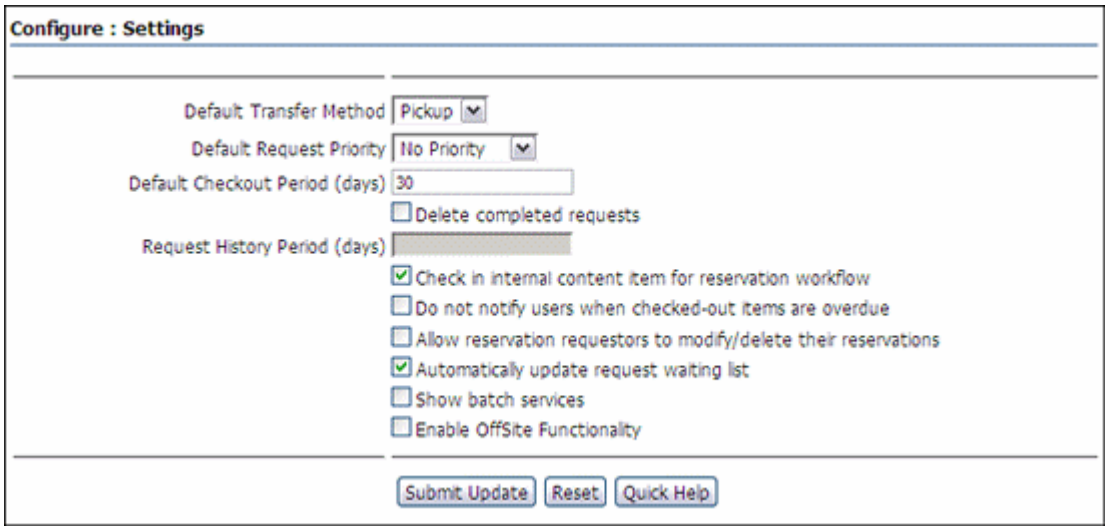
Element	Description
Start of Fiscal Calendar	The date designation for the fiscal year. Type the day of the month and select the month from the list. Required for processing fiscal date periods. **Initial default: April 1**.
Archive Meta Data Format	The storage file format for the metadata of items in a disposition bundle (for example, a zipped archive of items affected by a transfer, archive, or accession disposition action created using the Get Content and Folders command): ■ hda: Proprietary HDA file format, specific to Oracle UCM. ■ xml: (initial default): eXtensible Markup Language (XML) format. ■ csv: Comma-separated values format.
Log Metadata Changes	Enables tracking item-level metadata changes. **Initial default: enabled**.
Enable Category Dispositions Review	Enable the workflow to review category dispositions. The workflow must be set up prior to enabling.
Enable Report Exclude Search Options	Allows the choice to exclude report templates and reports from search results. If this checkbox is checked, options are available for selection on the Configure Reports Settings Page.
Disable Lifecycle Update	Prevents life cycle updates
Always restrict revisions/Never restrict revisions	Allows or prevents revisioning of content.
Always restrict deletions/Never restrict deletions	Allows or prevents deleting of content.
Always restrict edits/Never restrict edits	Allows or prevents editing of content.

Element	Description
Display record icon	Specifies when a record icon should be displayed next to an object name when listing search results. Enabling the icon allows administrators to use a method to easily highlight items with specific qualities, such as: ■ Disable record icon: disable the icon completely ■ Deletes Restricted: display when deletions are restricted ■ Edits Restricted: display when edits are restricted ■ Revisions Restricted: display when revisions are restricted ■ Deletes and Edits Restricted: display when deletions and edits are restricted ■ Deletes and Revisions Restricted: display when deletions and revisions are restricted ■ Edits and Revisions Restricted: display when edits and revisions are restricted ■ Deletes, Edits, and Revisions Restricted: display when deletions, edits, and revisions are restricted.
ACL-based security	Enables security based on access control lists (ACLs). It enables the Group and User Permissions fields on several pages where access control lists can be created to assign security permissions. **Initial default: enabled**.
Default Content Server security on Retention Schedule objects	Enables default security on retention categories, record folders, and triggers. It enables the standard Security Group and Filer fields on several pages where additional security on retention schedule objects and components can be assigned. **Initial default: enabled**. **IMPORTANT**: If your organization requires a change to this feature after your production environment is running, call Technical Support for assistance.
Supplemental Markings	Enables supplemental marking security on content, record folders, and users. This box must be selected to enforce user matching of at least one supplemental marking. **Initial default: enabled.** Supplemental markings security is enabled.
User must match all Supplemental Markings	Forces a user to match *all* supplemental markings to access an item. When not selected, a user must match at least *one* supplemental marking to access an item within a marked record folder. **Initial default: enabled**. A user must match one or more markings to access a record folder or content. The Supplemental Markings box must be enabled for this feature to work.
Custom Security Fields	Only available if the DoD Baseline configuration is used. Enables the custom security field feature. Clear this box if this feature is not needed. **Initial default: not enabled**.
Classified Security	Enables the classified security feature (required for conformance to the Chapter 4 Classified Records section of DoD 5015.2 specification). Displays the Security Classification Field in the Configure menu. After creating classification levels and assigning them, the order on the hierarchy levels. Clear this box if not required. **Initial default: enabled/disabled**, depending if the Classified Enhancements option was selected during configuration.

Element	Description
Do Not Notify Authors	Prevents e-mail notifications from being sent for pending events, reviews, and the Notify Authors disposition action. **Initial default: not enabled**. E-mail notifications are sent.
Only allow scheduled screening	Hides the **Search** button on the screening page to prevent users from starting screenings manually. Useful in cases where the total number of items in the system is so large it is impractical to have users wait for reports. **Initial default: not enabled**. Manual screening is allowed.
User-friendly disposition	Enables user-friendly language for disposition rules. Clear this checkbox for standard DoD 5015 disposition and screening query language. **Initial default: not enabled**. Standard disposition and query language is used.
Show Export Date	Enables users to export items in the retention schedule that changed since a specific date. **Initial default: not enabled**. The date field is not displayed.
Use Page Navigation	Displays more elaborate page navigation controls on screening results lists and disposition record folder lists. **Initial default: enabled**.
Paginate Navigation Tree	Displays the number of pages and page location on screening results lists and disposition record folder lists. **Initial default: enabled**.
Enable Custom Script Evaluation	Allows the creation of custom scripts. This field is only displayed if classified security features are enabled. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about custom scripts. **Initial default: enabled**.
Maximum years before declassifying	The number of years after which content is declassified. **Initial default: 25 years**. This field is only displayed if classified security features are enabled and the user has the Admin.PrivilegedEnvironment rights. This right is assigned by default to the predefined Records Officer and Records Administrator role.
Run Auto Computation of Declassification Date	This field is only displayed if classified security features are enabled and the user has the Admin.PrivilegedEnvironment rights and has the highest security setting (for example, the system default of Top Secret). When checked, records with a *publication date* plus the *Maximum years before declassifying* value that is less than the current date are automatically declassified. NOTE: If this is set to 0 and auto-computation of declassification dates is chosen, any classified items currently in the system are set to declassified. **Initial default: disabled**.

A.3 Configure Physical Settings Page

Use this page to configure many aspects of PCM.



Permissions: You must have the PCM.Admin.Manager right to access this 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.

Element	Description
Default Transfer Method	The default transfer method for reserved physical items: ■ **Copy**: The item is duplicated for the requestor. The copy can be physical (for example, a document run through a copier or a copied DVD) or electronic (for example, a scanned document or an ISO image of a CD). ■ **Fax**: The item is faxed to the recipient. ■ **Mail**: The original item is mailed to the recipient. ■ **Pickup** (initial default): The recipient must pick up the item in person. ■ **E-mail**: The item is e-mailed to the recipient. ■ **Deliver**: The item is delivered to the recipient.
Default Request Priority	The default priority for reservation requests: ■ **No Priority** (initial default): No priority (there is no rush). ■ **ASAP Rush**: Deliver as soon as possible. ■ **This Morning**: Deliver the same morning. ■ **Today**: Deliver the same day. ■ **This Week**: Deliver the same week.
Default Checkout Period (days)	The number of days a reserved physical item can be checked out. Administrators can override this value when processing a reservation. **Default: 30 days**.
Delete completed requests	Specifies if completed reservation requests are automatically deleted from the reservations history after a defined number of days. A reservation request is considered completed no request items are still pending (in process), on a waiting list, or checked out. **Initial default: disabled**.

Element	Description
Request History Period (days)	The maximum number of days a reservation request is stored in a reservations history (useful for logging or tracking). After exceeding this age, the request is deleted from the reservations history. This option is available only if **Delete completed requests** is selected.
Check in internal content item for reservation workflow	Specifies if a new internal content item is checked into the repository when a reservation request is made for a physical item. The internal content item goes through the reservations workflow used for approval and notification purposes. If cleared, users can still make reservations, but no e-mail notifications about them are received. **Initial default: enabled**.
Do not notify users when checked out items are overdue	Specifies if users who check out a reservation item receive an e-mail notification if the item is past its due date.
Allow reservation requestors to modify/delete their reservations	Specifies if users creating a reservation request are allowed to modify or delete their open reservation requests, even if they do not have the PCM.Reservation.Delete and/or PCM.Reservation.Edit rights. When enabled, users creating a reservation request can edit the metadata for their own reservations and request items. They cannot edit the status of a request item, but they can cancel the item. They can also delete their own reservations and request items. **Initial default: disabled**.
Automatically update request waiting list	Specifies if waiting lists for requests are updated automatically. When a reserved item is returned (and marked as such), the waiting list for the item is updated to change the reservation status for the next requestor on the list from "Waiting List" to "In Process." If this box is cleared, the administrator must manually change the status on any of the reservation pages. **Initial default: enabled**.
Show batch services	Specifies if the batch services are available in the External Content menu. These services enable administrators to run scheduled tasks immediately rather than wait for the standard scheduled time (once a day at midnight). **Initial default: disabled**.
Enable offsite functionality	Specifies if external content offsite storage is enabled.

The Batch Services option is only displayed if the corresponding option on the Configure Physical Settings 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 PCM Requestor role) may see a much smaller subset of the administrator menus, depending on their assigned rights.

A.4 Security Interface

The following screens are used to view security settings and to set security for classification.

- "Classification Interface" on page A-16
- "Custom Security Interface" on page A-18
- "Classification Guide Interface" on page A-22

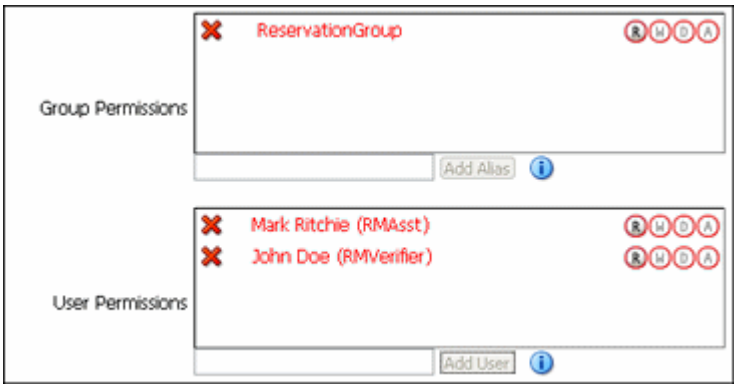
A.4.1 Assigned Rights Page

This page displays the rights assigned to a specific user.

To access this screen, click **Records** then **Rights** from the Top menu. Click any highlighted link to expand the list and show details about the assigned rights.

A.4.2 Access Control Edit Section

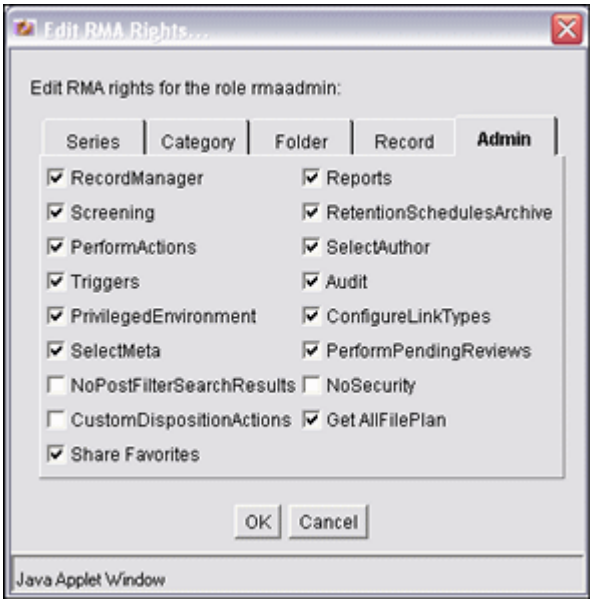
Use this portion of a page to adjust the permissions given to individuals and groups.



This functionality appears on several different screens such as Create or Edit Trigger Type Page and the Create or Edit Freeze Page.

A.4.3 Edit Rights Page

Use this page to assign management rights to roles.



To access this screen, click **Admin Applets** from the **Administration** menu. Click the User Admin icon. Choose **Security** then choose **Permissions by Role** from the menu. Select a role to view the rights. Highlight any role then click **Edit RMA Right** or **Edit ECM Right**.

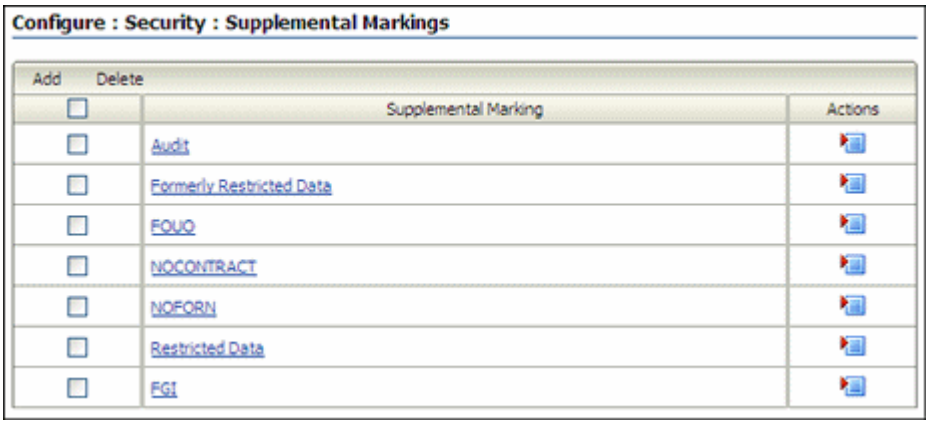
A.4.4 Supplemental Markings Interface

The following screens are used when managing supplemental markings:

- "Configure Supplemental Markings Page" on page A-14
- "Create or Edit Supplemental Marking Page" on page A-15
- "Supplemental Marking Information Page" on page A-15

A.4.4.1 Configure Supplemental Markings Page

This page is used to view, delete, or add supplemental markings. It is available when the **Use Supplemental Markings** box is selected in the Configure Retention Settings Page.

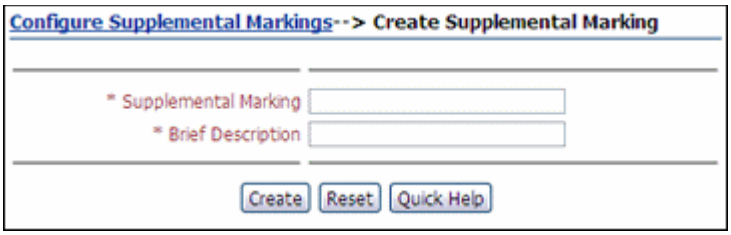


To access the page, click **Records** then **Configure** from the Top menu. Click **Security** then **Supplemental Markings**.

If a marking is deleted the schema must be republished to remove the marking from option lists where the marking may appear. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about republishing schema.

A.4.4.2 Create or Edit Supplemental Marking Page

This page is used to define or edit supplemental markings.



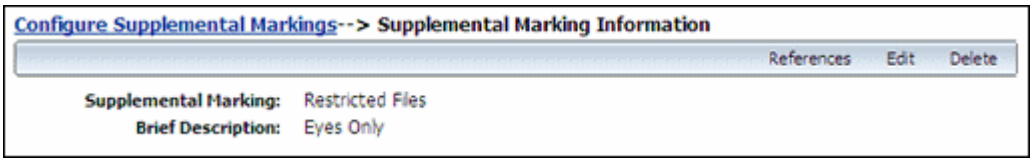
Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role.

To access this page, click **Add** on the Configure Supplemental Markings Page. Use the Edit Page to modify the properties of an existing supplemental marking. To access the Edit Page, choose **Edit Marking** from the item's **Action** menu on the Configure Supplemental Markings Page.

Element	Description
Supplemental Marking	A unique name or acronym for the supplemental marking. Maximum characters: 30. This field is view-only on the edit page. Required.
Brief Description	A brief description of the marking. Maximum characters: 30. Required.
Create button (Create Page only)	Creates the supplemental marking. The supplemental marking does not appear in the Supplemental Marking list until you assign the marking to yourself.

A.4.4.3 Supplemental Marking Information Page

This page is used to view information about a marking.



Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role. With the Admin.Triggers right, you can only view information about supplemental markings. With the Admin.RecordManager right, you can also add, edit, and delete supplemental markings.

To access this page, click the name of a marking on the Configure Supplemental Markings Page.

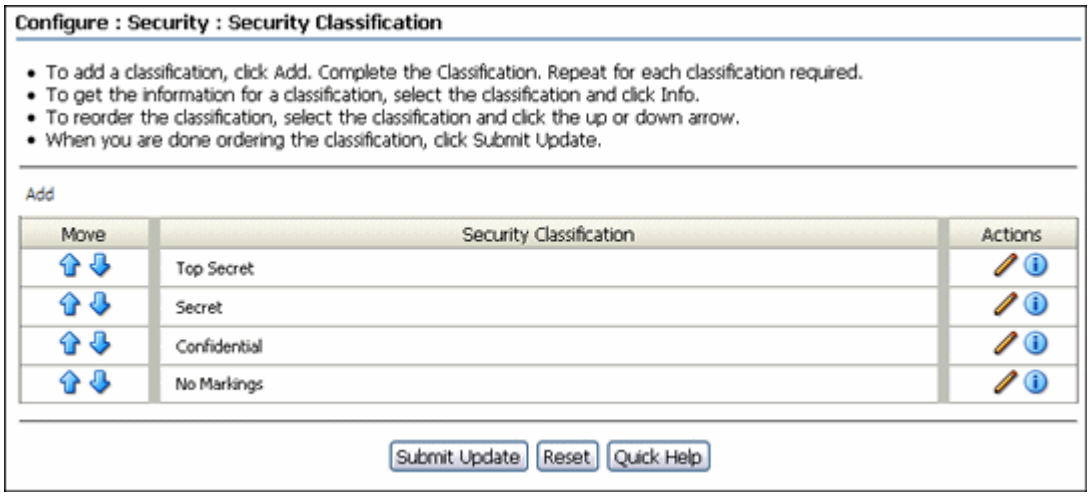
A.4.5 Classification Interface

The following screens are used to manage classifications:

- "Configure Security Classification Page" on page A-16
- "Create or Edit Security Classification Page" on page A-17
- "Security Classification Information Page" on page A-17
- "Security Classification References Page" on page A-18

A.4.5.1 Configure Security Classification Page

Use this page to create security classifications and set the classification hierarchy.



To access this page, click **Records** then **Configure** from the Top menu. Click **Security** then **Security Classification**.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the Records Administrator role.

Element	Description
Up arrow Down arrow	Moves a selected security classification upward or downward one step in the hierarchy with each click.
Add button	Displays the Create or Edit Security Classification Page, where a security classification can be defined.
Info button	Displays the Security Classification Information Page, where information and references for the selected security classification can be viewed. If a user has the appropriate rights, the user can also edit or delete the security classification.

A.4.5.2 Create or Edit Security Classification Page

Use this page to define or change a security classification.

To access the Create page, click **Add** on the Configure Security Classification Page.

After creating a classification, be sure to indicate its order among the other available security classifications, both built-in and custom. The user must have permissions to that level to view it.

Use the Edit page to modify the properties of an existing security classification. To access this page, click the edit icon (a pencil) for a classification on the Configure Security Classification Page.

> **Permissions:** The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the Records Administrator role.

Element	Description
Security Classification	A unique name or acronym for the security classification. Maximum characters: 30. This field is view-only on the edit page. Required.
Brief Description	A brief description of the security classification. Maximum characters: 30. Required.

A.4.5.3 Security Classification Information Page

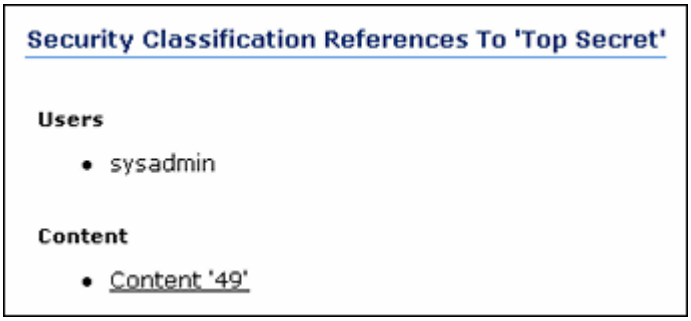
This page displays information about a classification.

To access this page, click the Info icon for a classification on the Configure Security Classification Page.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the Records Administrator role. You must also have the security classification level assigned to you to view or work with it.

A.4.5.4 Security Classification References Page

This page displays references to classifications.



To access this page, click **References** on the Security Classification Information Page.

Permissions: The Admin.RecordManager *and* Admin.SecurityClassifications rights are required to use this page. These rights are assigned by default to the Records Administrator role. You must also have the security classification level assigned to you to view or work with it.

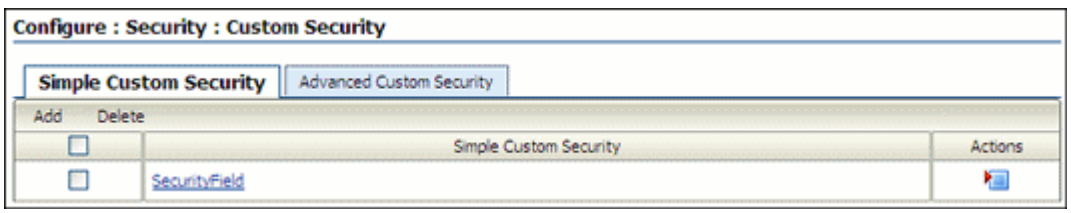
A.4.6 Custom Security Interface

The following screens are used in managing custom security:

- "Configure Custom Security Page" on page A-18
- "Create or Edit Simple Custom Security Field Page" on page A-19
- "Custom Security Field Information Page" on page A-19
- "Advanced Custom Security Dialog" on page A-20
- "Advanced Custom Security Option Page" on page A-20
- "Select Security Dialog" on page A-21

A.4.6.1 Configure Custom Security Page

This page is used to view, delete, or add custom security fields.



To access this page, click **Records** then **Configure** from the Top menu. Click **Security** then **Custom Security**. Two types of security fields can be created:

- *Simple fields*: These types of custom security fields pair a custom content field with a custom user field to create a new field.
- *Advanced security fields*: These custom fields are applied to fields that use option lists. The security can be applied to individual items in the option list.

Custom security is only available when the Custom Security box is selected on the Configure Retention Settings Page.

A.4.6.2 Create or Edit Simple Custom Security Field Page

These screens are used to add or edit simple custom security fields.

Use the Create Page to define a new simple security field. To access this page, click **Add** on the Simple Custom Security tab on the Configure Custom Security Page.

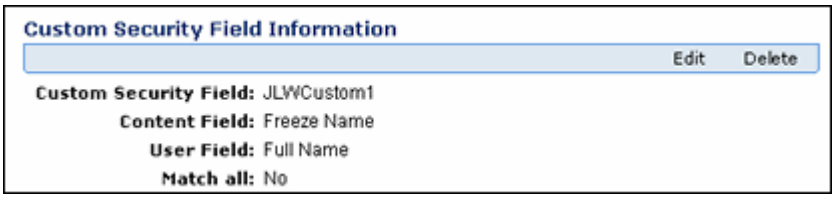
Use the Edit Page to modify the properties of an existing custom security field. To access this page, click **Edit field** from the item's **Action** menu on the Configure Custom Security Page.

> **Permissions:** The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role.

Element	Description
Custom Security Field	A unique name for the field. Maximum characters: 30. This field is view-only on the edit page. Required.
Doc Meta Field list	The content field to match against the user field. The list displays all available content fields, custom or otherwise.
User Field list	The user field to match against the content field. This field must also be set up in the User Admin utility. Required.
"Match all" box	Forces the user to match all content field entries. When cleared, allows access when a user matches at least one content field.

A.4.6.3 Custom Security Field Information Page

Use the Custom Security Field Information page to view information about an existing custom security field.

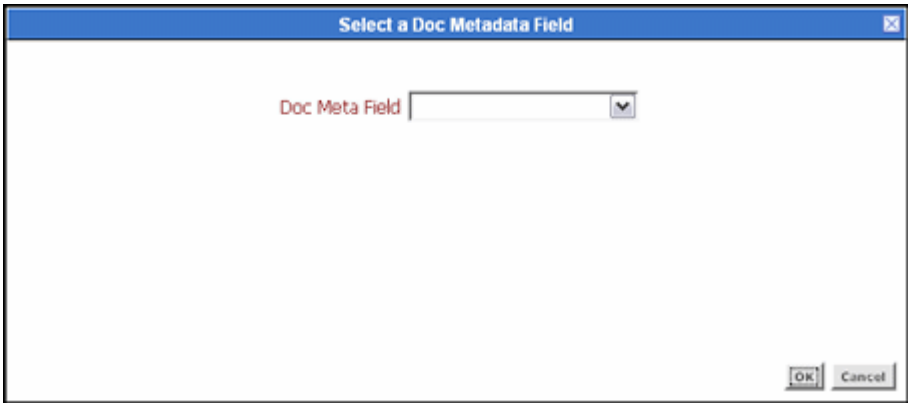


To access this page, click a custom field on the Configure Custom Security Page.

Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles, and the Admin.RecordManager right to the Records Administrator role. With the Admin.Triggers right, you can only view information about custom security fields. With the Admin.RecordManager right, you can also add, edit, and delete custom security fields. You must also have the security classification level assigned to you to be able to view or work with it.

A.4.6.4 Advanced Custom Security Dialog

Use this page to select the metadata field to use for security restrictions.



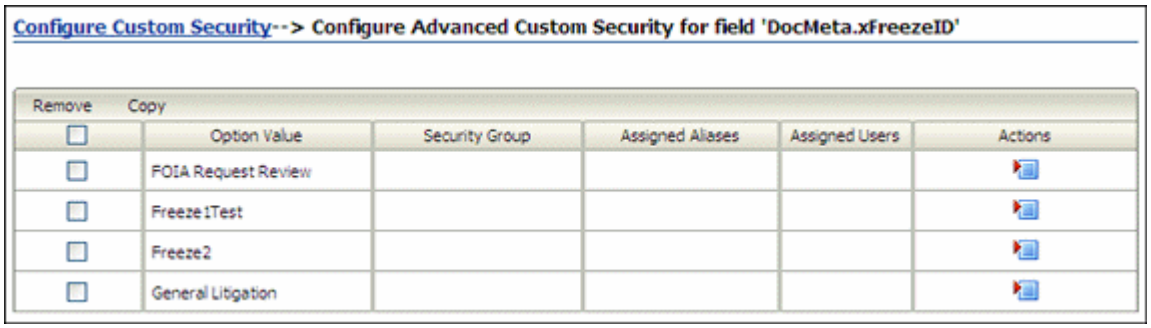
To access this page, click **Add** in the Advanced section of the Configure Custom Security Page.

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

Element	Description
Doc Meta field	Select a field from the list. Only those fields which have option lists are available.

A.4.6.5 Advanced Custom Security Option Page

Use this page to set the security on individual options in the option list associated with the metadata field chosen in the Advanced Custom Security Dialog.



This page is displayed when a metadata field is chosen on the Advanced Custom Security Dialog.

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

Element	Description
Option Value	Select a field from the list. Only those fields which have option lists are shown.
Security Group	The security group which can access this option.
Assigned Aliases	The alias which can access this option.
Assigned Users	The users who can access this option.

A.4.6.6 Select Security Dialog

Use this page to select the users, aliases, and security groups who can access the option.

To access this page, click **Edit Security** from the **Actions** menu of an option on the Advanced Custom Security Option Page.

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

Element	Description
Users	Enter the first two letters of a user name in the dialog box to display a list of user names or type two asterisks (**) to display a list of names. Scroll to the name to use and click **Add**. To adjust the permissions given to that user, click a circled permission next to the name to add or to remove it. To remove the user, click the **X** next to the user name. The name appears with a line through it, indicating it is no longer in use.
Aliases	Enter the first two letters of an alias name in the dialog box or type two asterisks (**) to display a list of aliases. Scroll to the name to use and click **Add**. To adjust the permissions for the alias, click a circled permission next to the name to add or to remove it. To remove the user, click the **X** next to the user name. The name appears with a line through it, indicating it is no longer in use.
Security Group	Select a security group from the list.

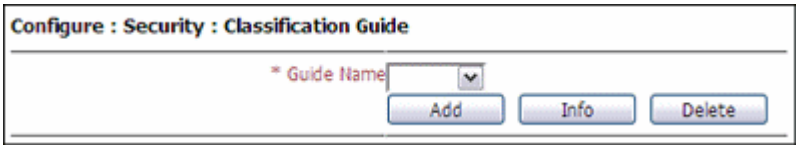
A.4.7 Classification Guide Interface

The following screens are used to configure classification guides:

- "Configure Classification Guide Page" on page A-22
- "Create or Edit Classification Guide Page" on page A-23
- "Classification Guide Information Page" on page A-24
- "Administer Classification Topic Page" on page A-24
- "Create or Edit Classification Topic Page" on page A-25
- "Configure Topic Settings Page" on page A-26
- "Classification Topic Information Page" on page A-26

A.4.7.1 Configure Classification Guide Page

This page is used to start setting up classification guides.



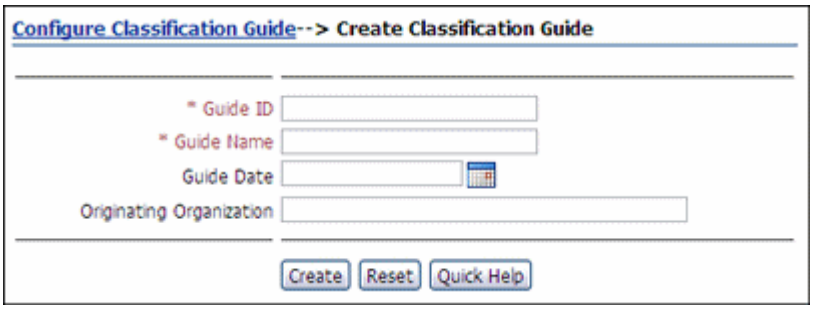
To access this page, click **Records** then **Configure** from the Top menu. Click **Security** then **Classification Guide**.

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

Element	Description
Guide Name	A list containing all defined classification guides. Use the **Info** button to view information about the selected classification guide or edit it, and the **Delete** button to delete it.
Add button	Displays the Create or Edit Classification Guide Page, used to create a new classification guide.
Info button	Displays the information page for the selected classification guide. See Classification Guide Information Page.
Delete button	Deletes the selected classification guide.

A.4.7.2 Create or Edit Classification Guide Page

This page is used to add or edit the classification guide.



To access this page, click **Add** on the Configure Classification Guide Page.

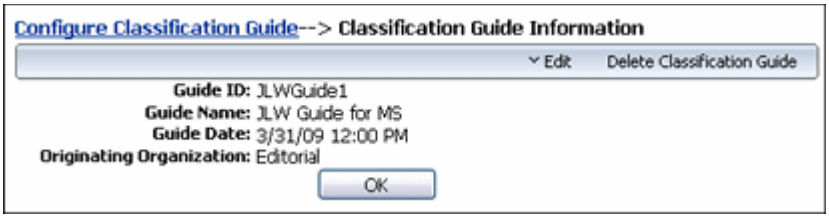
Use the Edit Page to modify the name of an existing classification guide. To access this page, click **Records** then **Configure** then **Security** from the Top menu. Click **Classification Guides**. In the menu list, select the classification guide to edit and click **Info**. From the Top menu menu, choose **Edit**.

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

Element	Description
Guide ID field	An identifier for the classification guide. Maximum characters: 80. This field is view-only on the edit page. Required.
Guide Name field	A name or description for the classification guide. Maximum characters: 100. Required.
Guide Date	The date the guide is activated.
Originating Organization	The organization associated with the guide.

A.4.7.3 Classification Guide Information Page

This page displays information about a classification guide.



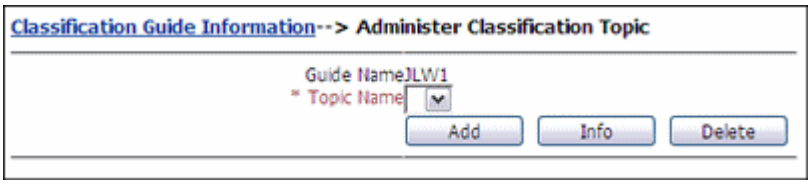
To access this page, click **Records** then **Configure** then **Security** from the Top menu. Click **Classification Guides**. In the menu list, select the classification guide to view and click **Info**.

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

Element	Description
Guide ID field	The identifier of the selected classification guide. This field cannot be edited.
Guide Name field	The name of the selected classification guide. This field cannot be edited.
Guide Date	The date the guide is activated.
Originating Organization	The organization associated with the guide.

A.4.7.4 Administer Classification Topic Page

Use this page to set up and configure classification topics.



To access this page, click **Records** then **Configure** then **Security** from the Top menu. Click **Classification Guides**. In the menu list, select the classification guide to view and click **Info**. From the Page menu, choose **Edit** then **Configure Topics**.

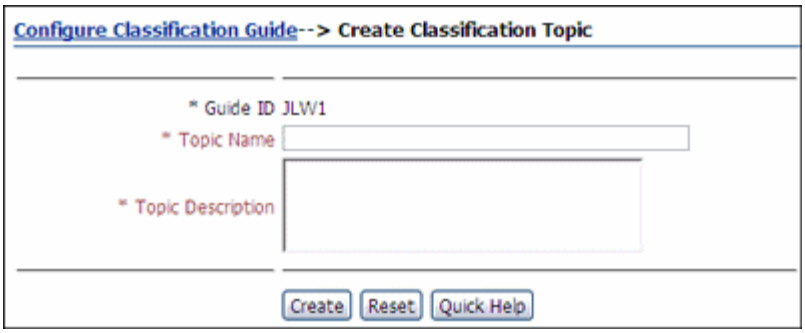
> **Permissions:** The Admin.ClassificationGuide right is required to perform this action. This right is assigned by default to the Records Officer and Records Administrator roles.

Element	Description
Guide Name field	Shows the name of the classification guide the topic is associated with. It cannot be edited.
Topic Name field	Contains all defined topics for the current classification guide.

Element	Description
Add button	Displays the Create or Edit Classification Topic Page, used to create a new classification topic.
Info button	Displays the Classification Topic Information Page.
Delete button	Deletes the selected classification topic.

A.4.7.5 Create or Edit Classification Topic Page

This page is used to add or modify classification topics.



Use the Create Page to define a new classification topic. To access this page, click **Add** on the Administer Classification Topic Page.

Use the Edit Page to modify the properties of an existing classification topic. To access this page, select a topic then click **Info** on the Administer Classification Topic Page. From the Page menu, choose **Edit** then **Configure Topics**. From the **Topic Name** list, select the classification topic to edit and click **Info**. From the Page menu, choose **Edit**.

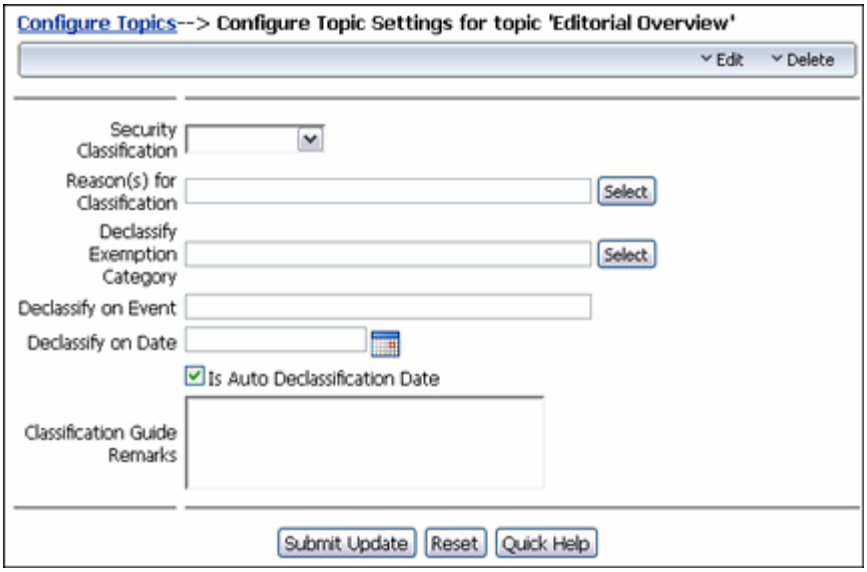
To modify the topic settings (that is, the default metadata field values), choose **Edit Topic Settings** from the Page menu. This displays the Configure Topic Settings Page.

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

Element	Description
Guide ID field	The name of the classification guide with which the topic is associated. It cannot be edited.
Topic Name field	A name for the classification topic. ▪ Required. ▪ Maximum characters: 255. This field is not displayed on the Edit screen.
Topic Description field	A description for the classification topic. ▪ Required. ▪ Maximum characters: 1,000.
Create button (Create Page only)	Creates the new classification topic and displays the Configure Topic Settings Page, where the default metadata field values are specified.

A.4.7.6 Configure Topic Settings Page

Use this page to set or modify the default field values of a classification topic.



To access this page, click **Edit** then **Edit Topic Settings** from the Page menu on the Classification Topic Information Page.

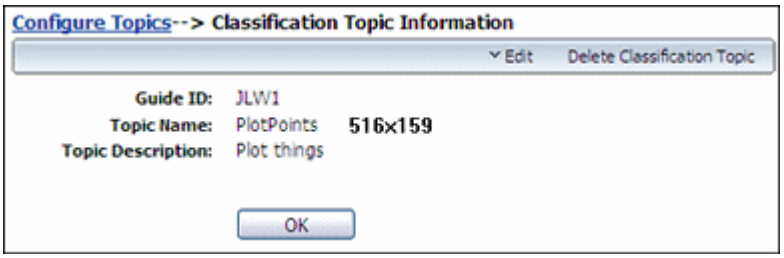
The Reason for Classification, Declassify Exemption Category and Declassify on Event fields contain items defined by the administrator using the Configuration Manager utility.

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

Element	Description
Initial classification	The initial classification assigned to the topic. The list contains all defined classification levels but only displays those the user is entitled to see depending on the user's security level. For example, if your assigned classification level is 'Secret', the list shows 'Secret' and all lower classification levels. Similarly, if no classification level was assigned to you, you see 'No Markings'.
Reason(s) for classification	The default reason(s) for classifications assigned to the topic.
Declassify exemption category	The default declassification exemption category assigned to the topic.
Declassify on event	The default declassification event assigned to the topic.
Declassify on date	The default scheduled declassification date assigned to the topic.
Classification Guide Remarks	Additional remarks about the classification guide to clarify its usage.

A.4.7.7 Classification Topic Information Page

This page is used to view classification topic information.



To access this page, select a topic then click **Info** on the Administer Classification Topic Page.

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

A.5 PCM Configuration Interface Screens

The following screens are used to configure PCM.

- "Object Types, Media Types, and Payment Types" on page A-27
- "Storage Location and Barcode Configuration Pages" on page A-32

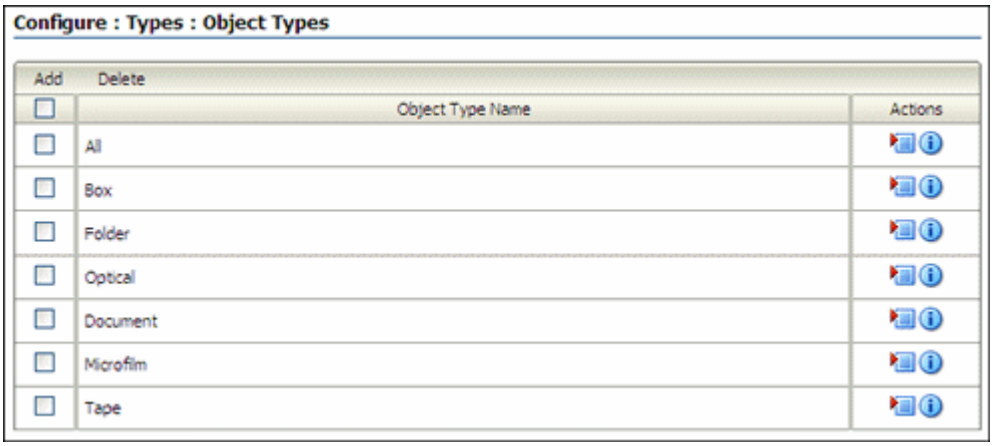
A.5.1 Object Types, Media Types, and Payment Types

The following screens are used to configure object, media, and payment types:

- "Configure Object Types Page" on page A-27
- "Create or Edit Object Type Page" on page A-28
- "Edit Object Type Relationships Page" on page A-29
- "Object Type Information Page" on page A-29
- "Configure Media Types Page" on page A-30
- "Select Media Type Dialog" on page A-31
- "Create or Edit Media Type Page" on page A-31
- "Media Type Information Page" on page A-32

A.5.1.1 Configure Object Types Page

Use this page to manage defined object types.



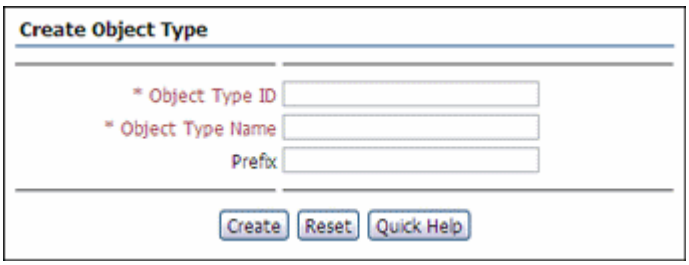
Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

To access this page, click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**.

Element	Description
Object Types list	Lists all currently defined object types including the predefined object types and custom object types.
Add button	Displays the Create or Edit Object Type Page where a new object type can be defined.
Info button	Displays the Object Type Information Page for a selected object type where the properities of the object type can be viewed or edited or deleted.

A.5.1.2 Create or Edit Object Type Page

Use this page to add or edit an object type.



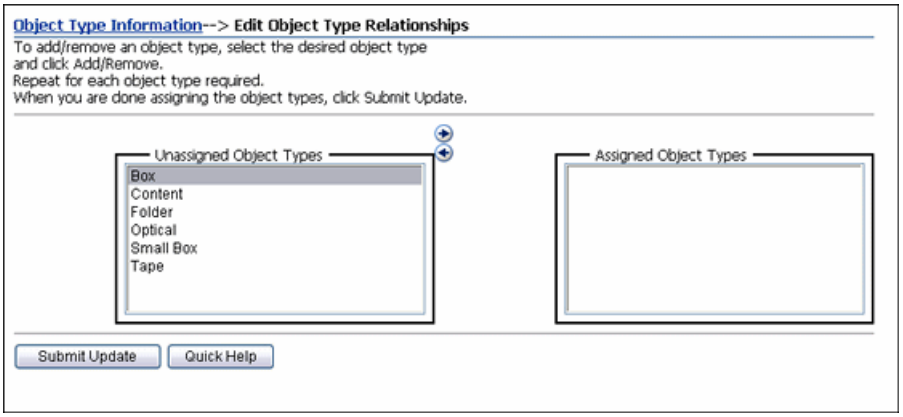
To access this page, click **Add** on the Configure Object Types Page. To edit a type, click **Edit Object Type** from the Actions menu for the item.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Object Type ID	A unique identifier for the object type. Maximum number of characters: 30. This field is view-only on the Edit Object Type page. Required.
Object Type Name	A name for the object type. Displayed in the object type list on the Create Physical Item page. Maximum number of characters: 30. Required.
Prefix	A prefix to be used to designate this object type.

A.5.1.3 Edit Object Type Relationships Page

Use this page to edit the relationships between the current object type and other object types. This action defines what object types can be contained within the current object type.



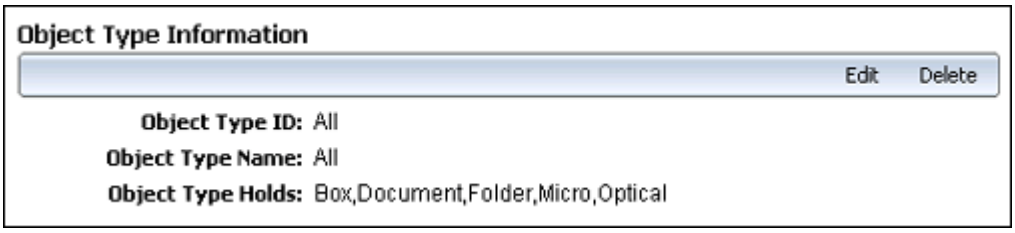
To access this page, click **Physical** then **Configure** from the Top menu. Click **Types** then **Object Types**. Select an object type from the list and click **Edit Object Type Relationships** from the object's **Action** menu.

> **Permissions:** The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Assigned Object Types list	A list of object types that can be contained within the current object type, used to control what type(s) of physical items can be created within another physical item.
Unassigned Object Types list	All object types that cannot be contained in the current object type.
Add arrow	Moves an object type from the Unassigned Object Types box to the Assigned object Types box (and make it available for the current object type).
Remove arrow	Moves an object type from the Assigned Object Types box to the Unassigned object Types box (and no longer make it available for the current object type).

A.5.1.4 Object Type Information Page

Use this page to view the properties of an existing object type.



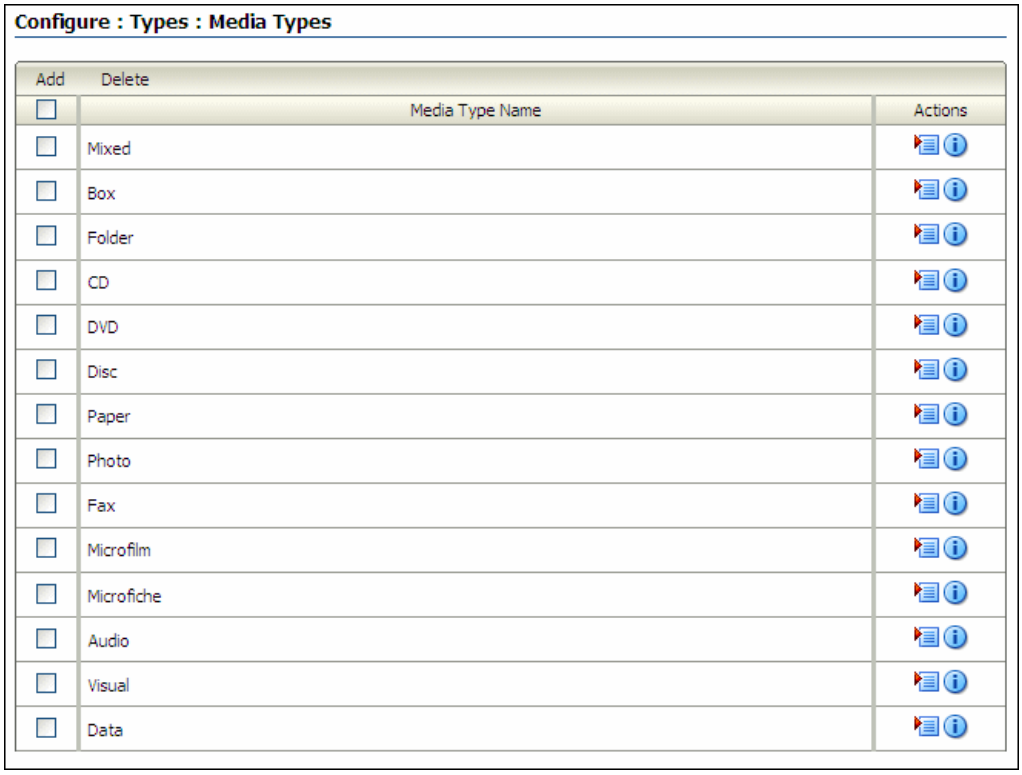
To access this page, click the **Info** icon of an object on the Configure Object Types Page.

This page shows the ID and name of the selected object type. In addition, it lists the object types that can be contained within the current object type. Modify this list on the Edit Object Type Relationships Page.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

A.5.1.5 Configure Media Types Page

Use this page to manage defined media types.



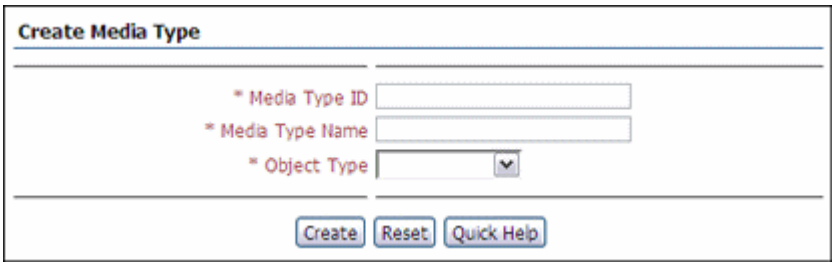
To access this page, click **Physical** then **Configure** from the Top menu. Click **Types** then **Media Types**.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Media Types list	Lists all currently defined media types. It includes the predefined media types and any custom media types.
Add button	Displays the Create or Edit Media Type Page, used to define a new media type.
Info button	Displays the Media Type Information Page for a selected item used to view or edit the properties of the media type or delete the media type.

A.5.1.6 Create or Edit Media Type Page

This page is used to create or edit a media type.



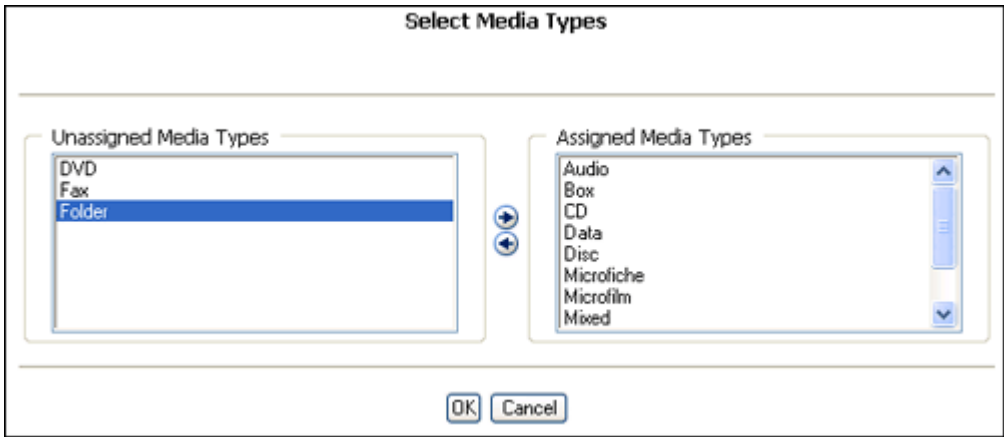
To access this page, click **Add** on the Configure Media Types Page.

> **Permissions:** The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Media Type ID	A unique identifier for the media type. Maximum number of characters: 30. This field is view-only on the Edit Media Type page. Required.
Media Type Name	A name for the media type to be displayed in the media type list on the Create Physical Item page. Maximum number of characters: 30. Required.
Object Type	The object type with which the media type is associated. The media type is available only if the object type is selected for the physical item. Only one object type can be associated with the media type.

A.5.1.7 Select Media Type Dialog

This page is used to choose the media type for a selected charge type.



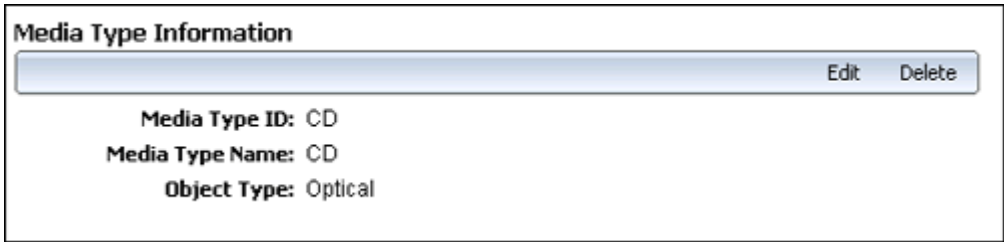
This dialog is displayed when you click **Browse** next to the Media Type field on the Create or Edit Charge Type Page.

A media type is the material on which the data is being stored. Media types are contained within object types. Object types can be defined to hold any media type, or multiple types of media, including all possible types of media.

Use the arrow keys to move items from the Unassigned to the Assigned Media Type lists.

A.5.1.8 Media Type Information Page

Use this page to view the properties of an existing media type.



To access this page, click the Info icon of a media type on the Configure Media Types Page.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

This page shows the ID and name of the selected media type. In addition, it lists the object type associated with the current media type. Modify this on the Create or Edit Media Type Page.

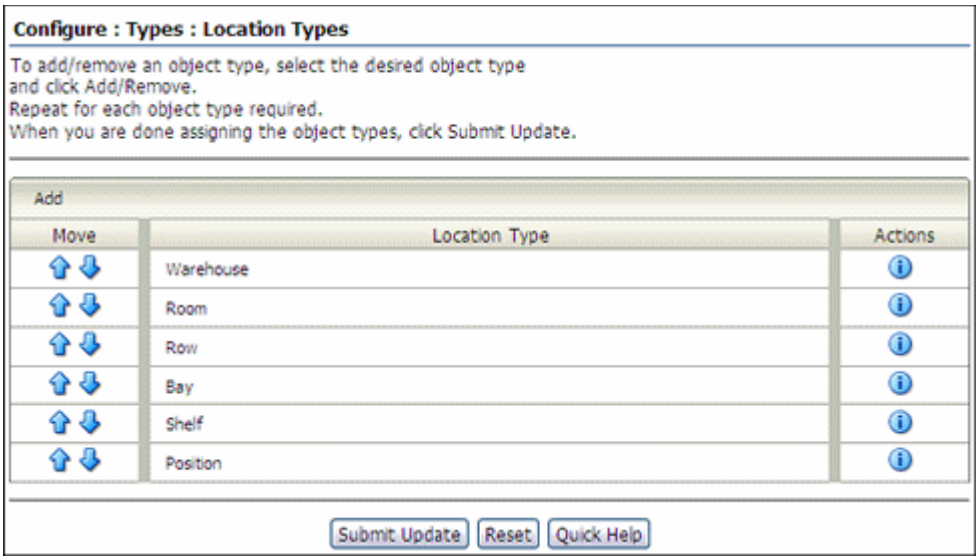
A.5.2 Storage Location and Barcode Configuration Pages

The following screens are used when configuring locations and barcodes:

- "Configure Location Types Page" on page A-33
- "Create or Edit Location Type Page" on page A-34
- "Location Type Information Page" on page A-35

A.5.2.1 Configure Location Types Page

Use this page to add, edit, delete, or reorder location types.



To access this page, click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

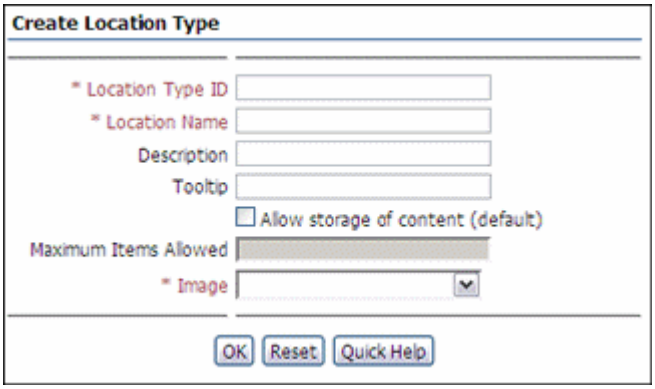
> **Permissions:** The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Element	Description
Location types list	Lists all defined location types in their assigned hierarchical order. The higher in the list, the higher the item is in the storage hierarchy. A location type contains all location types below it in the list. The location type at the bottom of the list is the most specific (and smallest) storage location. This may be the only storage location actually holding physical content. All higher-level units are then used for space management purposes.
Up Arrow Down Arrow	Moves the associated item up or down one level in the storage hierarchy.

Element	Description
Add button	Displays the Create or Edit Location Type Page, used to define a new location type.
Info button	Displays the Location Type Information Page for a selected item where a user can view or edit the properties of the location type or delete the location type.

A.5.2.2 Create or Edit Location Type Page

Use the Create Page to define a new location type to be used in the definition of the storage environment. Use the Edit Page to modify an existing location type.



To access this page, click **Physical** then **Configure** from the Top menu. Click **Types** then **Location Types**.

To edit a type, click **Edit Type** from the **Action** menu of the type.

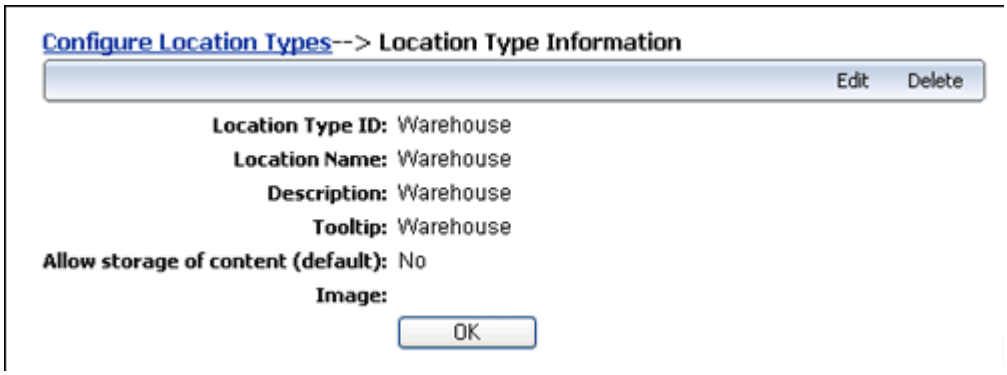
Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

Element	Description
Location Type ID	A unique ID for the location type displayed in the location type hierarchy. Maximum number of characters: 30. This field is view-only on the Edit Location Type page. Required.
Location Name	The name of the location type. Maximum number of characters: 30. Required.
Description	A description for the location type. Maximum number of characters: 30.
Tooltip	Tooltip text for the location type. This text appears if the mouse cursor is held over the option in the location type selection list on the Create or Edit Storage Page (only in Netscape, Mozilla, and Firefox web browsers). Maximum number of characters: 30.

Element	Description
Allow storage of content (default)	Specifies if the location type can hold content items by default. This can be overridden when defining storage locations. Overriding the default setting may be useful to accommodate abnormal storage locations, or to create a "dummy" storage location enables a user to maintain consistent numbering across parallel objects. This setting applies to this specific location type level only, not to any location types lower in the hierarchy. Therefore, the box for a location can be disabled if its child location types will contain content. For example, in the default hierarchy shelves have several positions, each of which can hold content items. But no content items can be directly assigned to the shelf level (only to the positions on a shelf). Therefore, the 'Shelf' location type does not allow storage of content, whereas the 'Position' location type does.
Maximum Items Allowed	This field is available only if **Allow storage of content (default)** is selected. It specifies the default maximum number of content items a location type can hold. This can be overridden when defining storage locations in the storage space hierarchy. This number applies to storage of content on this specific location type level only, not to any location types lower in the storage space hierarchy.
Image	Specifies the icon to use for the location type in the Browse Storage tree in the Trays layout.

A.5.2.3 Location Type Information Page

This page shows the current properties of the selected location type. Only the fields containing information are displayed. For example, if no tooltip text has been specified for the location type, this field is not shown on the page.

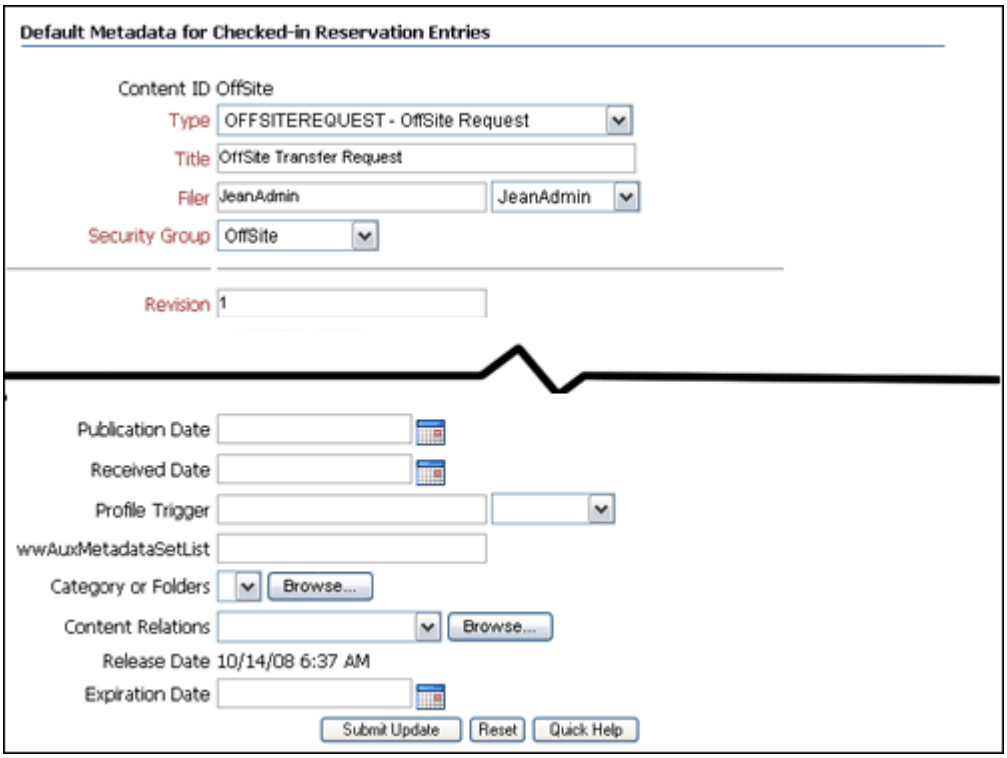


To access this page, click the Info icon of a location type on the Configure Location Types Page.

Permissions: The PCM.Admin.Manager right and the PCM.Admin.LocationTypes right are needed to perform this action. These rights are assigned by default to the PCM Administrator role.

A.5.2.4 Default Metadata for Checked-in Reservation or Offsite Entries Page

This page is used to set the default metadata values for reservation items checked into the repository. A similar page is used to set default metadata for offsite storage items.



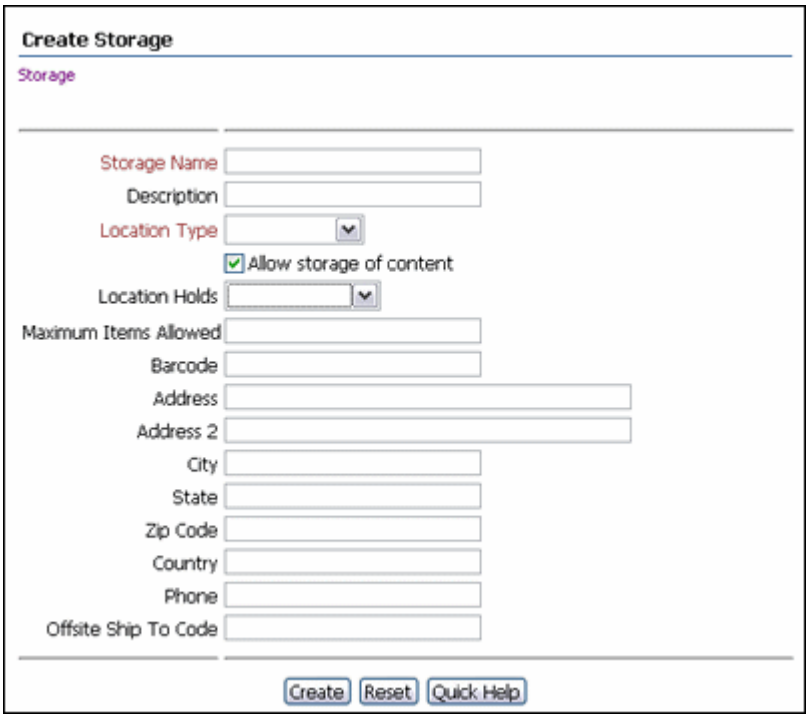
To access this page, click **Physical** then **Configure** from the Top menu. Click **Offsite Storage** then **Offsite Default Metadata** to access the Offsite Storage page or **Configure** then **Metadata** then **Reservation Default Metadata** to access the reservation page

This page is similar to the a check-in page. Fill in the fields to use for defaults when using reservations.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

A.5.2.5 Create or Edit Storage Page

Use this page to create or edit storage locations where physical items can be assigned.



To access this page, click **Physical** then **Storage** from the Top menu. Select a location for the new storage item and click **Create** then **Define Storage Location** from the Action menu of a location or from the Table menu.

Depending on the location in the hierarchy, a user can create a new storage location or create a physical item in another location.

To edit a location, select an item from the list and click **Edit** then **Edit Storage Location** from the Page menu.

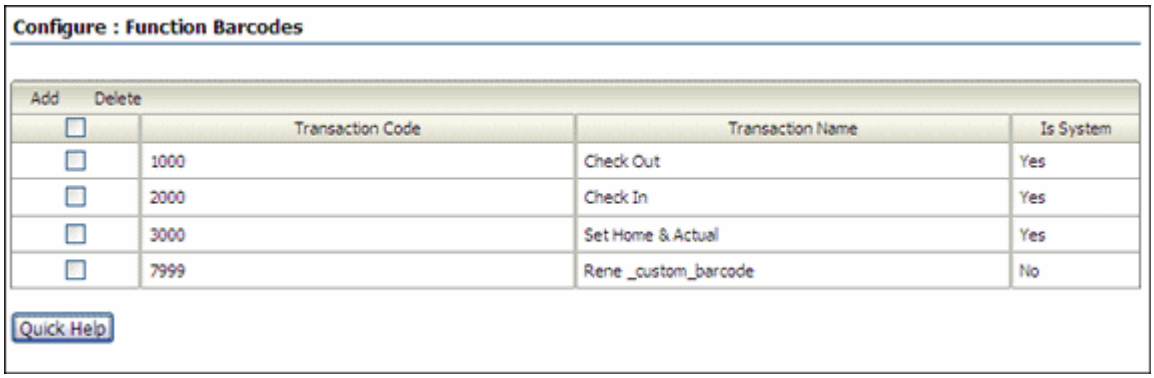
Permissions: The PCM.Storage.Create right and the PCM.Storage.Edit right are needed to perform these actions. These rights are assigned by default to the PCM Administrator role.

Element	Description
Storage Name	A unique name for the storage location. Maximum number of characters: 30. Required.
Description	A brief description for the storage location. Maximum number of characters: 30.
Location Type	The location type of the storage location. This field is view-only on the Edit Storage page. The available location types are defined on the Configure Location Types Page. The available location types depend on where the cursor is located in the storage hierarchy. Required.

Element	Description
Allow storage of content	Specifies if the storage location can hold content items. The default is the configured default setting for the selected location type, but it can be overridden if required. This setting applies to this specific storage location, not to any child storage locations. It controls if items can be stored in it. This box does not have to be enabled if any of the location's child locations will hold content. For example, you may have a storage location of type "Shelf" with several positions, each of which can hold content items. If you do not want any items to be directly assigned at the shelf level but only to the positions on a shelf (stored at a position, not on a shelf), then you set the shelf storage location to not allow storage of content, and the position storage location to allow storage. If you click this box, all fields (except Requestor) below it become available.
Status available for locations that can hold items	Available for locations that can hold items. Used to specify the current status of the storage location. The default status is 'Available'.
Requestor	Available only if the storage location allows storage of content and the storage status is set to "Reserved." Used to specify the user who reserved the storage location, either by entering the user manually or by selecting a name from the list of available users.
Location Holds	Available only for storage locations that can hold items. Used to specify what type of physical items are stored in the storage location. Choose from all defined object types. An object type does not need to be specified here. The storage location can then hold any type of content. If an object type is selected and someone attempts to store an inappropriate object type, an error message is displayed and the physical item is not checked in.
Maximum Items Allowed	Available only for storage locations that can hold items. Used to specify the maximum number of items the location can hold. This number is used to track space availability. If not specified, 1 (one) is assumed, which means only a single item can be assigned to the storage location.
Barcode	Available only for storage locations that can hold items. Used to specify a barcode for the location. If not specified, a random 19-digit number is automatically assigned. Maximum number of characters: 30
Address Information	Addressing information for offsite storage.
Offsite Ship To Code	Available only for offsite storage. Used to specify the Ship To code for offsite storage.

A.5.2.6 Configuring Custom Barcode Page

This page is used to set a barcode numbering system.



To access this page, click **Physical** then **Configure** then **Function Barcodes** from the Top menu.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Transaction Code	The barcode used for the type of activity or transaction.
Transaction Name	The type of transaction or activity associated with the barcode.
Is System	An indicator of the type of barcode. System barcodes are default barcodes provided with the software.

A.5.2.7 Create Custom Barcode Dialog

This dialog is used to create a new custom barcode.

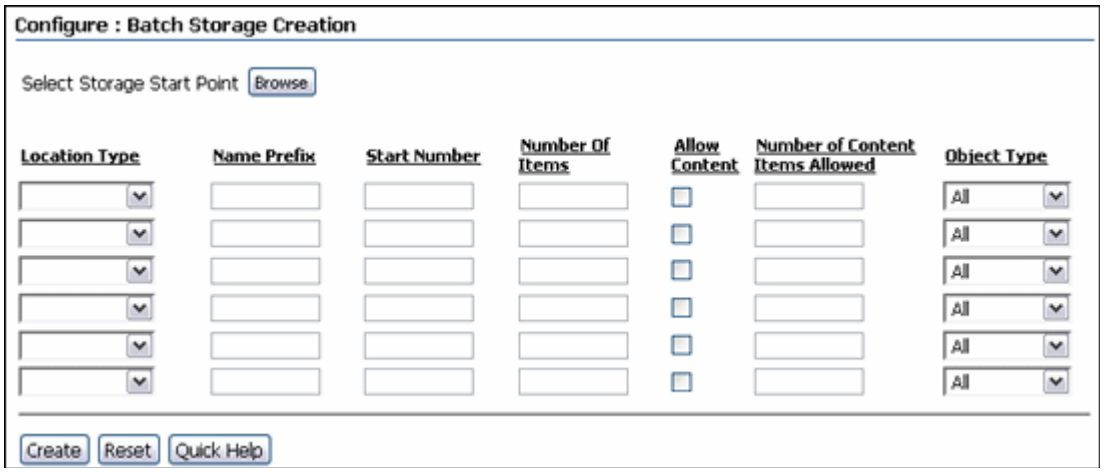
This dialog is displayed after clicking **Add** on the Configuring Custom Barcode Page.

Permissions: The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Transaction Code	Enter the code to be associated with the new transaction type. Values must be between 7000 and 9999. Required.
Transaction Name	Enter the activity or event associated with the barcode. Required.

A.5.2.8 Create Batch Storage Import File Page

This page is used to define a new storage hierarchy by specifying several creation rules.



To access this page, click **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

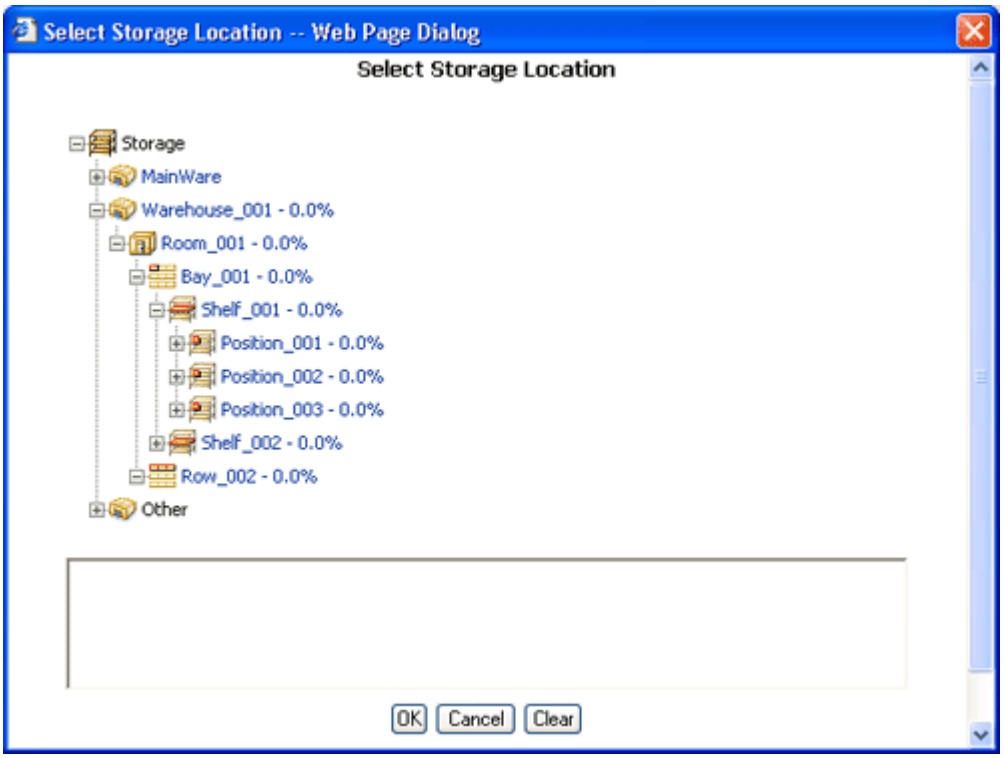
> **Permissions:** The PCM.Admin.Manager right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

Element	Description
Browse button	Opens the Select Storage Location Dialog where the location in the existing storage space is specified that will hold the new storage hierarchy defined on this page.
Location Type	Accesses a list of the location type of each level in the storage hierarchy. A parent location cannot be added below a child location (for example, a shelf above a row). If you attempt to do this, error messages are displayed when you import the *StorageImport.hda* storage definition file.
Name Prefix	Specifies a prefix for the storage location name. The prefix is included in the name and description of the storage location. If not specified, the name and description of the storage location contains only numbers (for example, "003").
Start Number	Specifies the starting number for the number sequence. The sequential number is included in the name and description of the storage location. If not specified, 1 (one) is assumed.

Element	Description
Number Of Items	Specifies how many instances of the storage location to include in the storage space. The default number of digits used in the numeric sequences is 3, resulting in names such as "Warehouse_001." The AutoStorageNumberWidth parameter in the storagecreationutility_environment.cfg file can be modified to change this. Restart the Content Server after changing the parameter value.
Allow Content	Allows items to be stored directly in the storage location. This applies to this storage location, not to any child locations. It is not necessary to enable this if any of child locations will hold content. For example, a "Shelf" storage location may have several positions, each of which can hold content items. To allow assigning of items only to the positions and not the shelf, do not check this box and set the position location to allow storage.
Number of Content Items Allowed	Available if **Allow Content** is checked. Used to specify the maximum number of items the storage location can hold. Used to track space in the storage location. If not specified, 1 (one) is assumed (only one item can be assigned to the storage location.)
Object Type	Available if **Allow Content** is checked. Used to select the type of physical content items the storage location can hold from all defined object types. If not specified, the storage location can hold any type of physical content. If an object type is selected and someone attempts to store an inappropriate object type, an error message is displayed and the physical item is not checked in.
Create	Creates a *StorageImport.hda* file, which can be imported into the existing storage hierarchy.

A.5.2.9 Select Storage Location Dialog

Use this dialog to select the location in the current storage environment to hold the new storage hierarchy defined on the Create Batch Storage Import File Page.

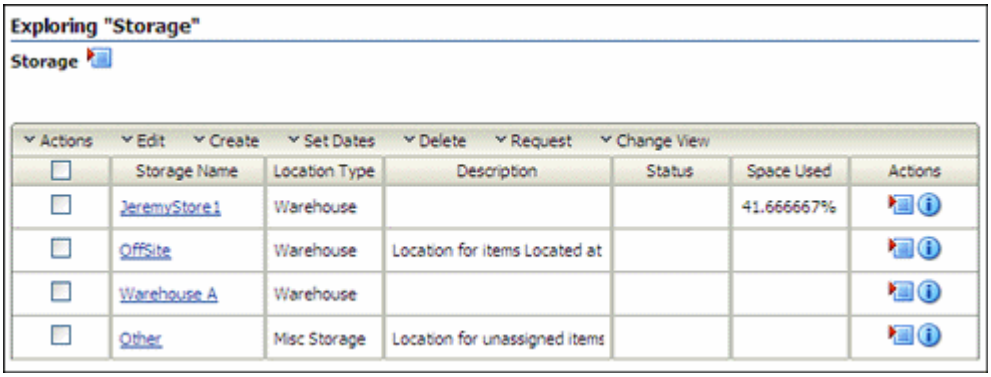


To access this dialog, click the **Browse** button on the Create Batch Storage Import File Page.

The main box at the top shows the defined storage space environment. After selecting a location in the hierarchy, the box at the bottom shows the full navigation path to the selected location.

A.5.2.10 Browse Storage Page

Use this page to view all defined storage locations.



To access this page, click **Physical** then **Storage** from the Top menu.

A.5.2.11 Storage Information Page

Use the Storage Information Page to view information about an existing storage location.

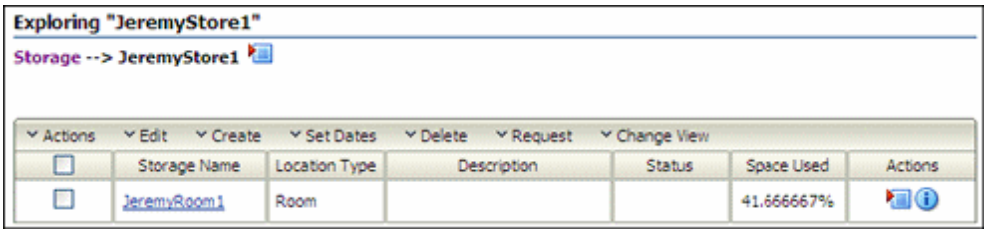
To access this page, click the **Info** icon for a storage location on theBrowse Storage Page.

> **Permissions:** The PCM.Storage.Read right is needed to perform this action. This right is assigned by default to the PCM Administrator role.

The Page menu is identical to the one on the Edit Storage page.

A.5.2.12 Physical Items in Storage Page

This page lists physical items contained in a storage location (and its child locations.)



To access this page, click **Physical** then **Storage** from the Top menu. Click the name of a storage location on the Browse Storage Page.

A.6 Retention Schedule Interface Screens

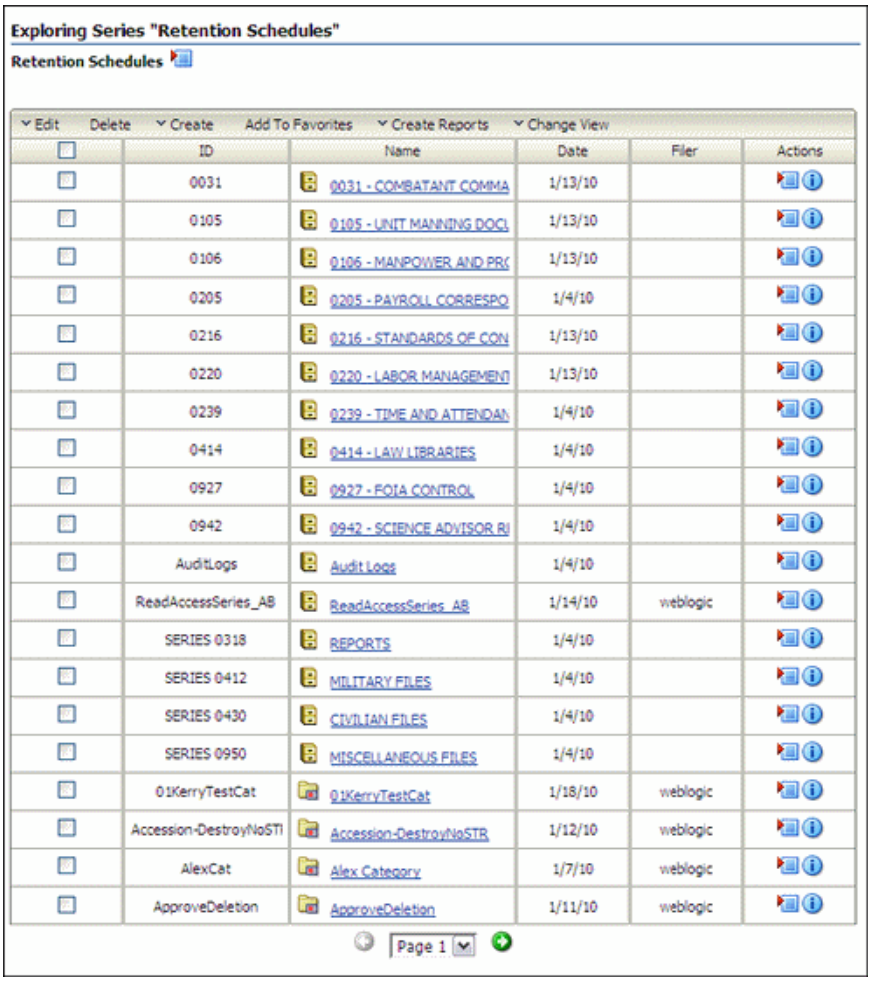
The following screens are used to manage Retention Schedules:

- "Series Interface Pages" on page A-44
- "Category Interface Screens" on page A-47
- "Record Folders Interface Screens" on page A-50

See the *Oracle Fusion Middleware User's Guide for Universal Records Management* for details about icons depicting retention schedule objects.

A.6.1 Exploring Retention Schedule Page

This page displays all currently defined retention series or categories.



To access this screen, click **Browse Content** then **Retention Schedules** from the Main menu.

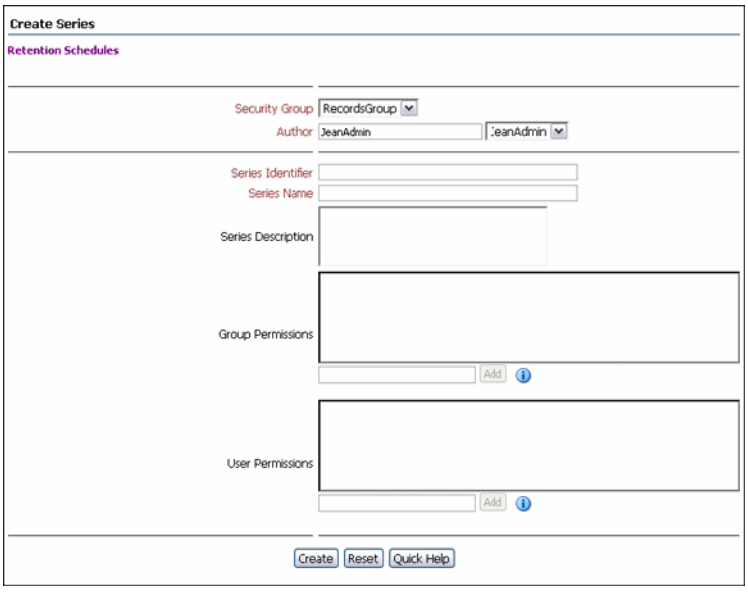
A.6.2 Series Interface Pages

The following screens are used to manage series:

- "Create or Edit Series Page" on page A-44
- "Series Information Page" on page A-45
- "Select Retention Series, Record Folder or Category Dialog" on page A-46

A.6.2.1 Create or Edit Series Page

This page is used to add or modify a series.



Use the Create Page to create a new series. To access this page, click **Create** then **Create Series** from the Table menu on the Exploring Retention Schedule Page.

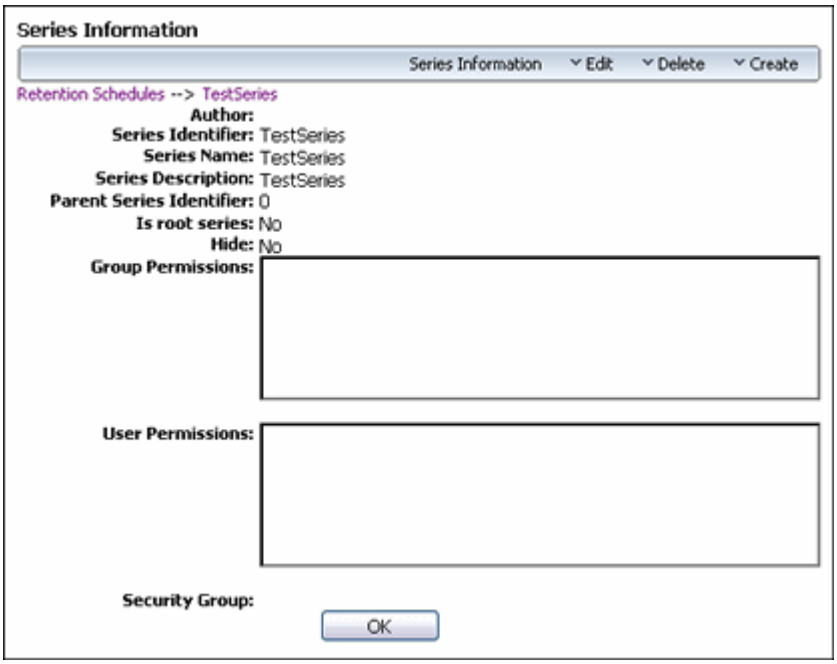
Use the Edit Series Page to edit the name of an existing series. To access this page, click **Edit** then **Edit Series** from the item's **Action** menu on the Exploring Retention Schedule Page.

> **Permissions:** The Series.Create right is required to use these pages. This right is assigned by default to the Records Administrator role.

Element	Description
Security Group	Select the security group associated with this series. Required.
Author	Enter the name of the creator of the series or select a name from the list. Required.
Series Identifier	A unique identifier for the series. This field is view-only on the edit page. Maximum characters: 100
Series Name	A name for the series. Maximum characters: 100. Required.
Series Description	A description for the series. Maximum characters: 1,000
Group and User Permissions	Select specific groups and users who can access the series. To select a group or user, type two asterisks (**) in the entry line. A list of groups and users is displayed. Select an item from the list and click **Add**. The name is inserted into the Group Permission or User Permission box. To further refine permissions, click on a displayed permission to add or remove it from the listed user or group. To remove a group or user, click the X next to the name. The name appears with a line through it, indicating it is no longer in use.

A.6.2.2 Series Information Page

This page is used to view information about a series. Anyone with the Series.Read right (assigned to all predefined roles) can view this page.

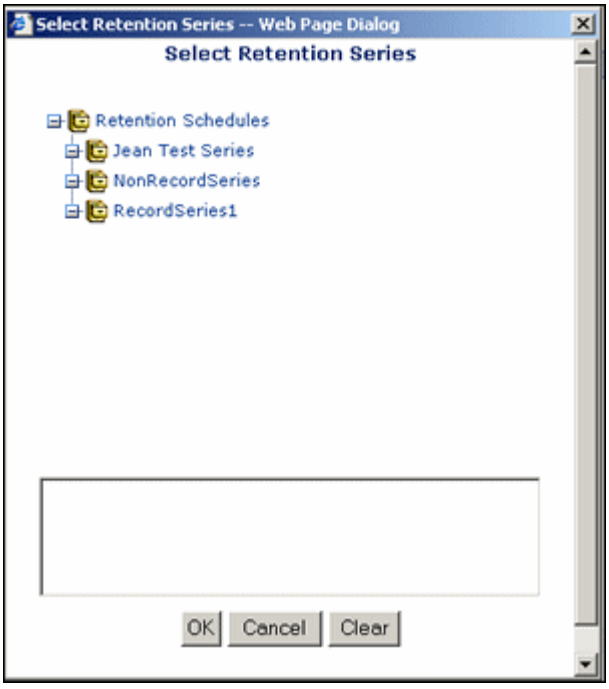


To access this page, click the **Info** icon for the series on the Exploring Retention Schedule Page.

Depending on a user's assigned rights, the user may also see the **Actions Page** menu.

A.6.2.3 Select Retention Series, Record Folder or Category Dialog

This dialog is displayed to select a series, folder or category for moving. Series can be nested within a retention schedule.



- To open the retention schedule, click the plus (+) sign or the icons to open it. Continue to click and expand the tree until reaching the desired location.

- Selectable content is indicated in red text.
- The locator links for the selected location appears in the box.
- When done, click **OK**.

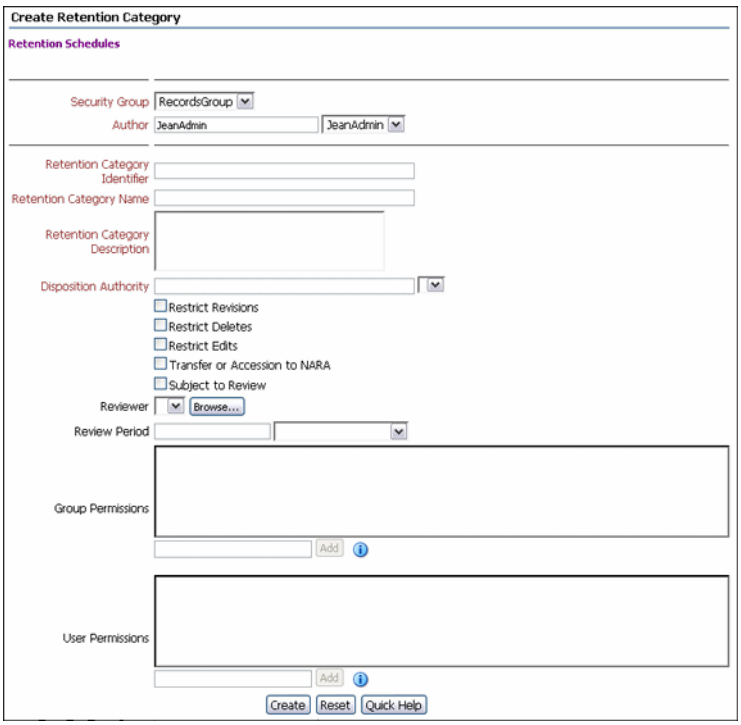
A.6.3 Category Interface Screens

The following screens are used to manage categories:

- "Select Retention Series, Record Folder or Category Dialog" on page A-46
- "Create or Edit Retention Category Page" on page A-47
- "Retention Category Information Page" on page A-49
- "Metadata History Page" on page A-50
- "Retention Category Information Page" on page A-49

A.6.3.1 Create or Edit Retention Category Page

Use the Create Retention Category Page to create a new retention category. Use the Edit Page to modify the category.



To access this page, click **Create** then **Create Retention Category** from the Table menu on the Exploring Retention Schedule Page.

Use the Edit Retention Category Page to edit an existing retention category. To access this page, click **Edit** then **Edit Category** from the item's **Actions** menu on the Exploring Retention Schedule Page.

The information in the following table is applicable in many cases for both folders and for retention categories.

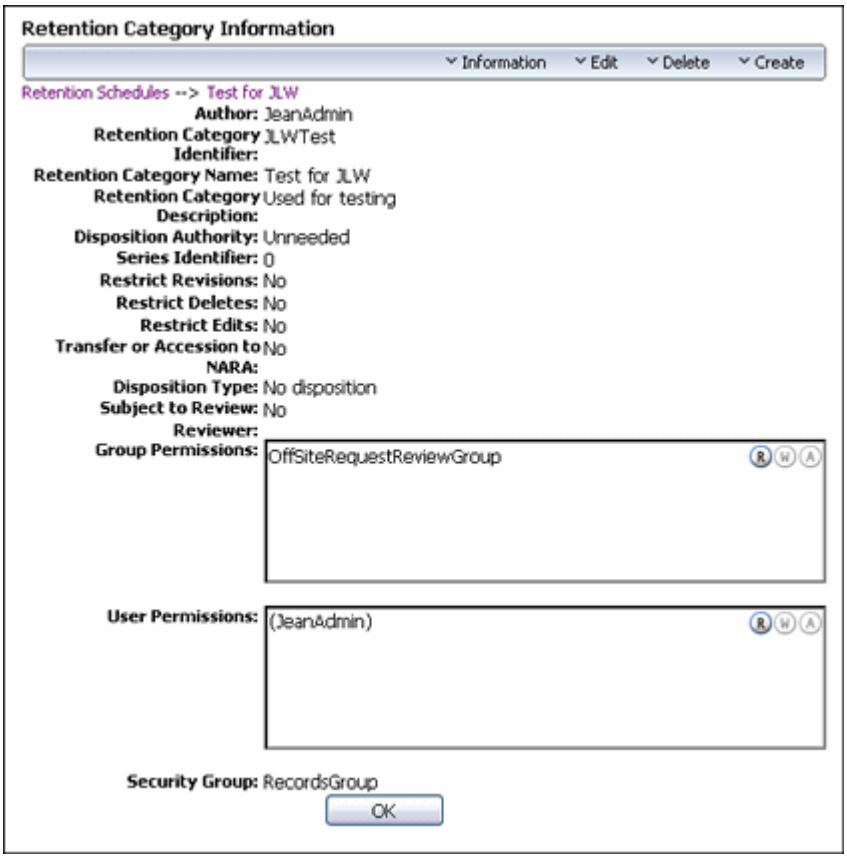
Permissions: The Category.Create right is required to use the Create Retention Category page. This right is assigned by default to the Records Administrator role. The Category.Edit right is required to use the Edit Retention Category page. This right is assigned by default to the Records Administrator role.

Element	Description
Security Group	The security group allowed access to the folder/category. When working with folders, set the security group permissions at the folder level to prevent the folder inheriting security settings from its parent category. **Default: RecordsGroup.** This field is only displayed if default security is enabled. Required.
Account	An account allowed access to the folder/category. This field is only displayed if accounts are enabled.
Filer	The person who initially created the folder/retention category. Select the filer from the options list. This field is only displayed if default security is enabled. Required.
Identifier	A unique identifier for the folder/retention category. Maximum characters: 100. This field is view-only on the edit page. Required.
Name	A name for the folder/retention category. Maximum characters: 100. Required.
Description	A description of the folder/retention category. Maximum characters: 1,000. Required.
Disposition Authority	The code of the disposition authority. When using this software for DoD tracking, the disposition authority code represents the legal authority who empowers a United States government agency to dispose of temporary items, or to transfer permanent items to the National Archives and Records Administration (NARA). The disposition authority for permanent items must be obtained from NARA. For certain temporary items, the authority must be obtained from the General Accounting Office (GAO). ■ Required for government sector. Private sector organizations can indicate a person or department responsible for the item, or enter "none." ■ Maximum characters: 100.
Restrict and permanence boxes	Indicates if a retention category will allow revisions, deletions, or edits or if it will contain permanent items. **Default: not selected**
Transfer or Accession to NARA	Indicates if this category will be used to transfer data to the National Archives.
Subject to Review box (Create Page only)	Indicates if a retention category contains items subject to review. All child record folders and items inherit the review status. **Default: not selected**. After this box is selected, the Reviewer and Review Period fields become available.

Element	Description
Reviewer (Create Page only)	The person responsible for reviewing content. The user receives an e-mail when a review period for the category indicates a review cycle as determined by the review period for the category. If a reviewer is not specified at the retention category level, the **Notify recipient** reviewer receives notifications for review. The system default reviewer is specified on the Configure Retention Settings Page. Reviewers for folders must have the Folder.EditReview.right. Otherwise the person cannot mark the folder as reviewed.
Review Period text box and list (Create Page only)	An integer indicating the number of periods to cycle the content. Select a corresponding period to go with the integer value from the Review Period list. Review periods for folders are required if the Subject to Review checkbox is selected.
Group and User Permissions	Select specific groups and users who can access the category. To select a group or user, type the first two letters of the name ot display a list of name or type two asterisks (**) in the entry line. A list of groups and users is displayed. Select an item from the list and click **Add**. The name is inserted into the Group Permission or User Permission box. To further refine permissions, click on a displayed permission to add or remove it from the listed user or group. To remove a group or user, click the X next to the name. The name appears with a line through it, indicating it is no longer in use.

A.6.3.2 Retention Category Information Page

Use this page to view information about a retention category. Anyone with the Category.Read right (assigned to all predefined roles) can view this page.

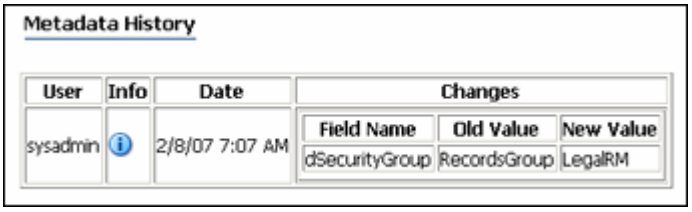


To access this page, click **Information** then **Category Information** from an item's Action menu on the Exploring Retention Schedule Page.

The information displayed depends on the configuration of the system and if optional fields were populated.

A.6.3.3 Metadata History Page

Use this page to view the metadata history for a retention category (a list of all changes made to the editable category properties).



To access this page, click **Information** then **Metadata History** from the item's **Action** menu on the Exploring Retention Schedule Page.

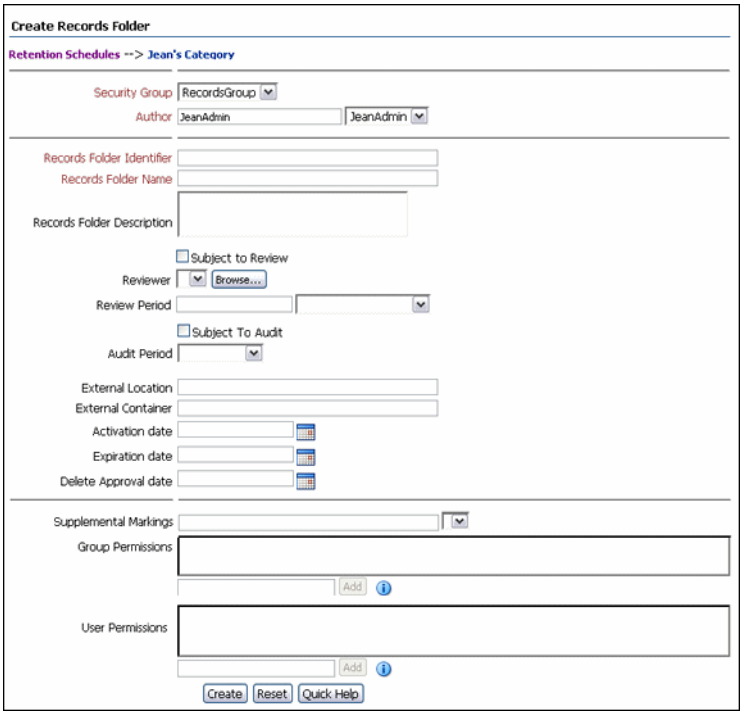
A.6.4 Record Folders Interface Screens

The following screens are used to manage record folders:

- "Create or Edit Record Folder Page" on page A-51
- "Record Folder Information Page" on page A-52

A.6.4.1 Create or Edit Record Folder Page

Use the Create Record Folder Page to create a new record folder and the Edit Record Folder Page to modify the folder.



To access this page, navigate to the retention category or record folder location level where the folder will be created. Choose **Create** then **Create Record Folder** from the Table menu.

Use the Edit Record Folder Page to modify the properties of an existing record folder. To access this page, navigate to the retention category or record folder containing the record folder to edit. Click **Edit** then **Edit Record Folder** from the item's **Action** menu.

The following fields are described in "Create or Edit Retention Category Page" on page A-47.

- Security group
- Account
- Filer
- Identifier
- Name
- Description
- Reviewer
- Review period
- Group permissions
- Select (Group) button
- User Permissions
- Select (User) button

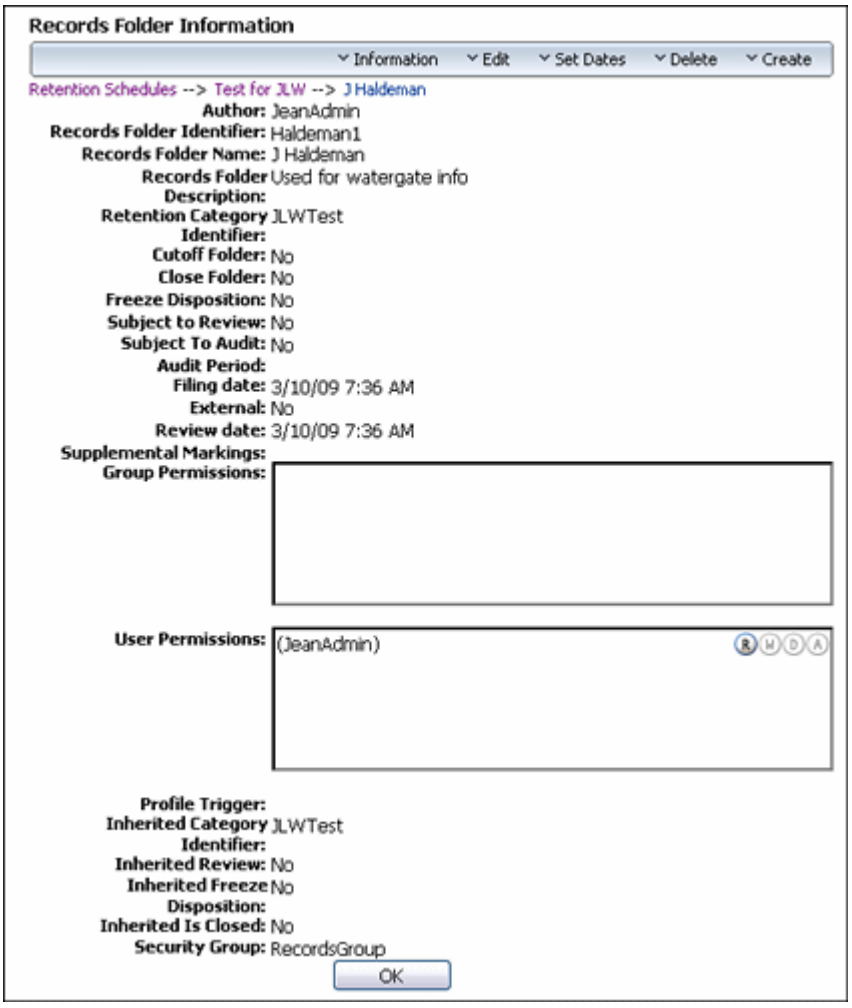
The information in the following table is applicable to folders only.

Permissions: The Folder.Create right is required to use the Create Record Folder page. This right is assigned by default to the Records Administrator role. The Folder.Edit right is required to use the Edit Record Folder page. This right is assigned by default to the Records Administrator role.

Element	Description
Freeze Reason	Available if a freeze reason was entered when the record folder was frozen. Not applicable when creating a new record folder. The freeze reason can be updated from this location if editing a record folder. Recommended. Maximum characters: 100.
Subject to Review box (Create Page only)	Enables the record folder as subject to review. For the folder to inherit review information from a parent folder or category, clear the box and enter a number and select the period from the list. **Default: not selected** (not subject to review). If a parent record folder or category has a review period of shorter duration than the review period for the child folder, the child folder assumes the shorter period.
Subject to Audit box	Indicates the record folder is subject to an audit. The Audit Period list becomes available. Clear the box if the record folder is not subject to an audit.
Audit Period list	Enabled if the folder is subject to audit. Select an audit period from the list. The records administrator configures the audit periods.
Activation Date	Date corresponding to a date in a content item but external to Oracle URM. For example, if an item has to do with a legal contract, the activation date represents the contract start date. The date format depends on user locale and preferences set in system properties. This field can also be used to treat a record folder and its content as a single piece of content from a disposition standpoint.
Expiration Date	A deactivation date corresponding to a content item but external to Oracle URM. For example, if an item has to do with a legal contract, the expiration date represents the date the contract expires. This date differs from the expiration date for documents in the repository because the content can still be accessed in Oracle URM after deactivation. Content expired in Oracle UCM cannot be accessed after expiration.
Delete Approval date	The date the delete action was approved for the record folder. After this date, the record folder can be deleted.
Supplemental Markings	Defined supplemental markings to secure the record folder.

A.6.4.2 Record Folder Information Page

Use the Record Folder Information Page to view information about a record folder.



To access this page, click **Information** then **Record Folder Information** from the item's **Actions** menu on the Exploring Retention Schedule Page.

Permissions: The Folder.Read right is required to use this page. All predefined roles this right.

The information displayed depends on the configuration for the software and if optional fields were populated.

A.7 Triggers Interface

Similar pages are used to create Global Triggers, Custom Direct Triggers and Indirect Triggers. This section uses the Custom Direct Trigger interface pages as an example of these interface screens. In the field descriptions an indication is given to where the field is used for specific trigger types.

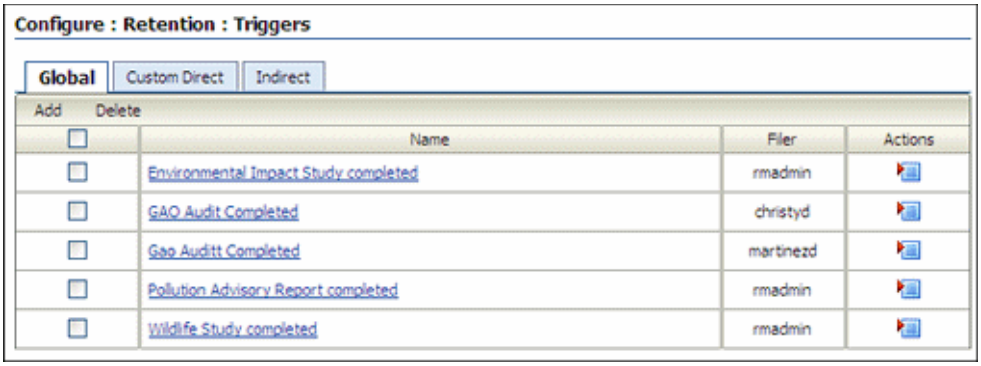
The following screens are used to manage triggers:

- "Create or Edit Trigger Type Page" on page A-54
- "Trigger Information Page" on page A-56
- "Indirect Trigger Date Entries Page" on page A-57

- "Create or Edit Indirect Trigger Date Entries Page" on page A-57

A.7.1 Configure Triggers Page

This page is used to select a type of trigger or a trigger for use.

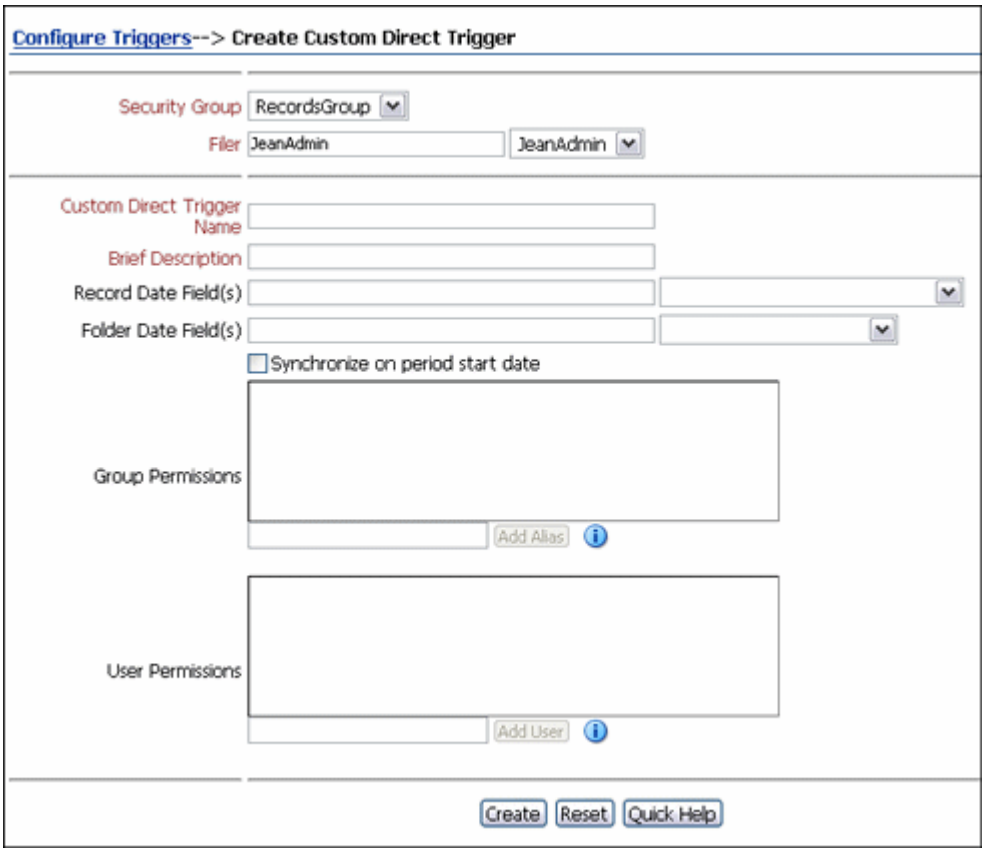


To access this page, click **Records** then **Configure** from the Top menu. Click **Retention** then **Triggers**.

This page lists the name of the trigger, the person who created it and an Action menu for each trigger.

A.7.2 Create or Edit Trigger Type Page

Use the Create Trigger Type Page to define a new trigger and the Edit Page to modify an existing trigger.



To access this page, select a trigger type and click **Add** from the Configure Triggers Page.

Use the Edit Trigger Type Page to modify the properties of an existing trigger. To access this page, select a trigger type and click **Edit** then **Edit Trigger** from a trigger's item **Action** menu.

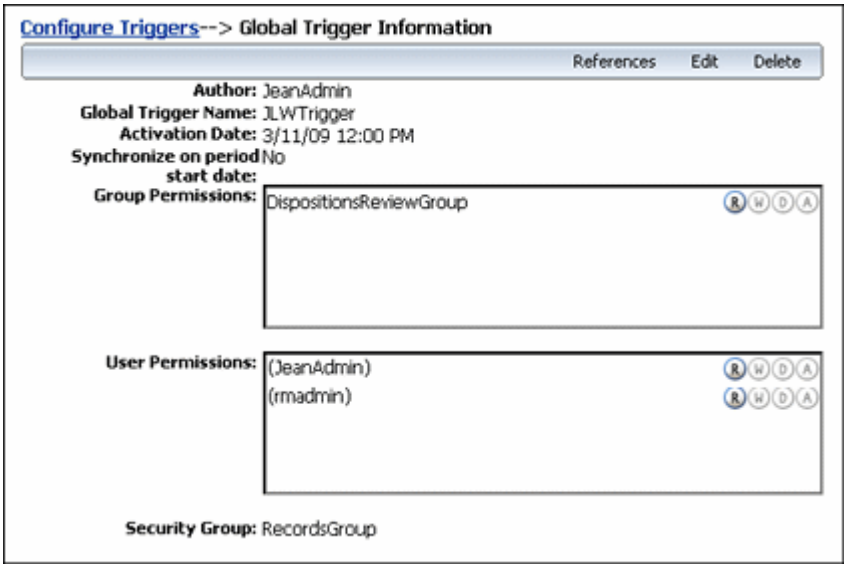
When a date is selected from the list, the Content Date metadata fields are automatically prefixed with an 'x', and the Folder Date metadata fields are prefixed with a 'd'.

Element	Description
Security Group	The security group allowed access to the trigger. Required. This field is only displayed if default security is enabled on the Configure Retention Settings Page. **Default: RecordsGroup**
Account	An account allowed access to the trigger. This field is only displayed if accounts are enabled.
Filer/Author	The author of the trigger. Select the author from the options list if you are not the author. **Default: Current user**. This field is only displayed if default security is enabled. Required.
Trigger Name	A name for the trigger that appears in the Disposition Rule Page. If this is an indirect trigger, the name appears in the Recurring Custom Triggers section. Maximum characters: 100. This field is view-only on the edit page. Required.
Brief Description (Custom direct triggers only)	A brief description of the trigger. Maximum characters: 100. Required.
Content Date Field(s) (Custom direct triggers only)	One or more date-related content fields. Maximum characters: 100. The New Revision Date option in the list is available only if the Enable New Revision Date Trigger Field option was selected during configuration. With this date field selected, whenever a new revision of a content item is checked in, all revisions of the content item, including the latest one, are stamped with the date of the new revision. With this functionality retention rules such as "Delete if not updated in *x* number of years" can be created.
Folder Date Field(s) (Custom direct triggers only)	One or more record folder date fields. All folder date fields are available, including any custom date fields. Maximum characters: 100.
Enabled box (Global triggers only)	Activates or disarms the trigger. To disable the trigger, clear the box. **Default: Enabled**. The trigger is active according to the set activation date.
Activation Date (Global triggers only)	The date when a trigger is activated. If no date is entered, an enabled trigger is delayed indefinitely (it is a dormant trigger). An activation date can be entered at a later time.
Synchronize on Period Start Date	When checked, indicates that the start date should be used to synchronize the trigger. This is similar to a cutoff disposition action. For example: if a disposition is "After activate wait 1 month then delete", if a record is activated on 1/15/10, then the system will synchronize to 1/31/10 and add 1 month before deleting.

Element	Description
Group and User Permissions	Select specific groups and users who can access the trigger. To select a group or user, type two asterisks (**) in the entry line. A list of groups and users is displayed. Select an item from the list and click **Add**. The name is inserted into the Group Permission or User Permission box. To further refine permissions, click on a displayed permission to add or remove it from the listed user or group. To remove a group or user, click the X next to the name. The name appears with a line through it, indicating it is no longer in use.

A.7.3 Trigger Information Page

This page is used to view information about existing triggers.



Similar pages are used to view information about Global Triggers, Custom Direct Triggers and Indirect Triggers. This section uses the Custom Direct Trigger interface pages as an example of these interface screens. In the field descriptions an indication is given as to where the field is used for specific trigger types.

> **Permissions:** Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the Records Administrator and Records Officer roles and the Admin.RecordManager right to the Records Administrator role.

To access a Trigger information page, click the **Info** icon for the trigger on the Configure Triggers Page. Depending on the type of trigger viewed, different information will appear.

If you have the Admin.Triggers right, the page includes a menu which provides the following options:

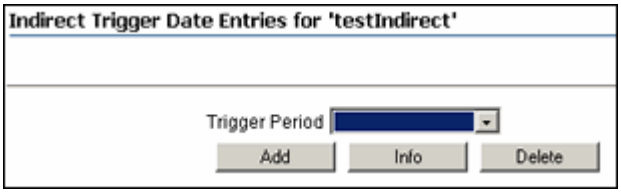
- **Indirect Trigger Date Information** (Indirect Trigger Information Page Only): Used to set recurring dates and periods for the indirect trigger.
- **Edit**: Used to edit the current indirect trigger.
- **Delete**: Used to delete the current indirect.

- **References**: Enables the user to see trigger references.

> **Note:** You cannot edit or delete the built-in Audit Approval indirect trigger.

A.7.4 Indirect Trigger Date Entries Page

Use the Indirect Trigger Date Entries Page to create, view information about, edit, and delete date entries for indirect triggers.



To access the page, click **Trigger Dates Info** in the Actions menu of an indirect trigger on the Configure Triggers Page.

> **Permissions:** The Admin.Triggers right is required to work with indirect trigger date entries. This right is assigned by default to the Records Administrator and Records Officer roles.

Element	Description
Trigger Period	The name of the trigger period.
Enabled	Specifies if the trigger date entry is enabled.
Trigger Period option list	A list of Trigger Periods from which a user can add, find information for, or delete.
Add button	Opens the Create or Edit Indirect Trigger Date Entries Page used to define the periods.

Note the following considerations:

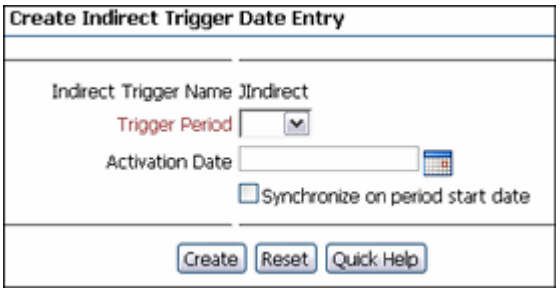
- Click **Add** to define an indirect trigger date entry.

  The Create or Edit Indirect Trigger Date Entries Page is displayed.

- If trigger date entries are already defined, select one from the **Trigger Period** list, and click **Info** to view the date information.

A.7.5 Create or Edit Indirect Trigger Date Entries Page

Use the Create Page to define the trigger period, enable or disable the trigger, and set an activation date for an indirect trigger.



To access this page, click **Records** then **Configure** from the Top menu. Click **Retention** then **Triggers**. In the Indirect Trigger area, click **Add**.

Use the Edit Page to modify the properties of an existing indirect trigger date entry. To assess this page, click **Edit** from a trigger's item **Action** menu on the Configure Triggers Page.

> **Permissions:** The Admin.Triggers right is required to use this page. This right is assigned by default to the Records Administrator and the Records Officer roles.

Element	Description
Indirect Trigger Name	The name of the indirect trigger for which date are being set. This field is view-only on both the create and the edit pages.
Trigger Period	The name of the indirect trigger period for which dates are being set. This field is view-only on the edit page.
Activation Date	Activation date for the indirect trigger.

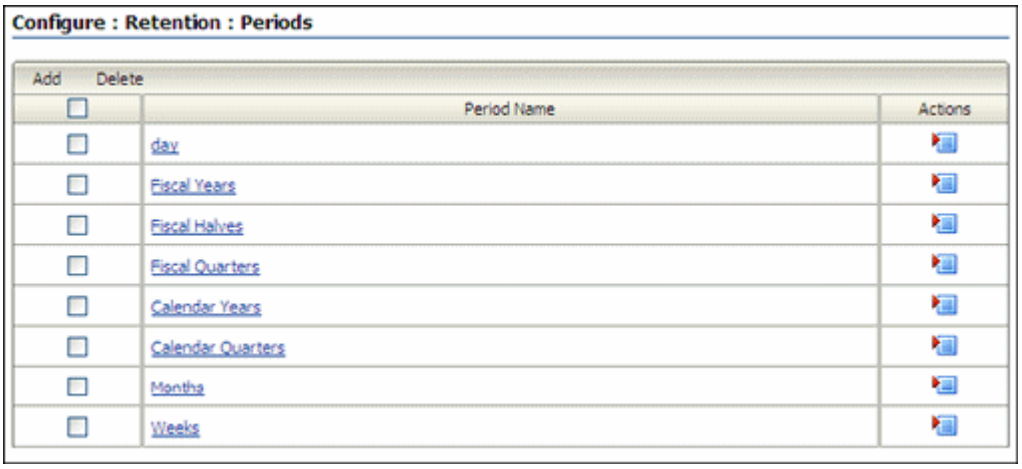
A.8 Time Period Interface

The following screens are used when managing time periods:

- "Configure Periods Page" on page A-58
- "Create or Edit Period Page" on page A-59
- "Period Information Page" on page A-60

A.8.1 Configure Periods Page

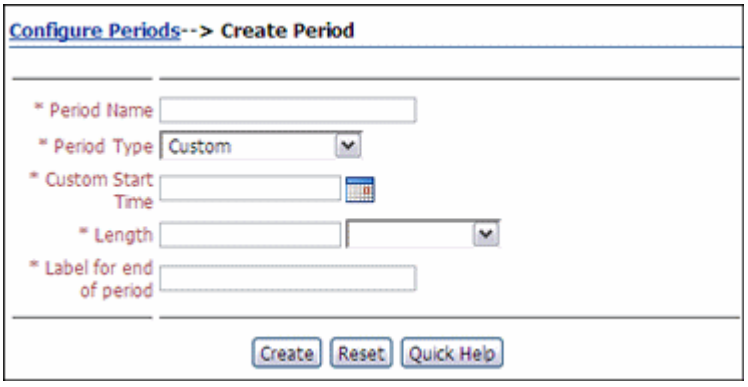
This page is used to select a period for editing or to add a new period.



To access this page, click **Records** then **Configure** from the Top menu. Click **Retention** then **Periods**.

A.8.2 Create or Edit Period Page

Use the Create Period page to define a new period and the Edit Period page to modify the properties of a time period.



To access this page, click **Add** from the Configure Periods Page.

Use the Edit Period page to modify the properties of an existing period. To access this page, click **Edit Period** from the item's **Action** menu on the Configure Periods Page.

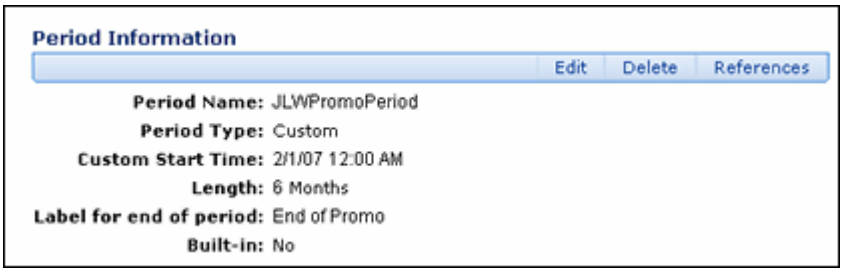
> **Permissions:** The Admin.RecordManager right is required to use this screen. This right is assigned by default to the Records Administrator role.

Element	Description
Period Name	The name appears in the Period options lists, such as the review period lists or retention period lists. Maximum characters: 30. This field is view-only on the edit page. Required.

Element	Description
Period Type	Required. The type of period: ■ **Fiscal**: A period based on the fiscal year as defined by the organization. The start date of the fiscal year is set in the Configure Retention Settings Page. ■ **Calendar**: A period based on the calendar year. ■ **Custom (default)**: A period based on organizational factors. The custom option is useful for creating lengthy periods such as decades or centuries, or unusual periods such as "school year session" or "software development cycle."
Custom Start Time	The start date and time for a custom period. The selected Period Type must be "Custom" to enable this field. Click the calendar icon to choose a date. The date and time appear in the format according to user locale and system properties. The date and time can be edited within the text box.
Length box	Integer value for the length of the period. Required.
Length list	Required. The period length. **Default: Blank**. Available options are: ■ Years ■ Months ■ Weeks ■ Days
Label for end of period	Label for the end of the period. The label appears in the Triggering Event ("After") fields in dispositions. Maximum characters: 30. Required.

A.8.3 Period Information Page

Use this page to view information about a period.



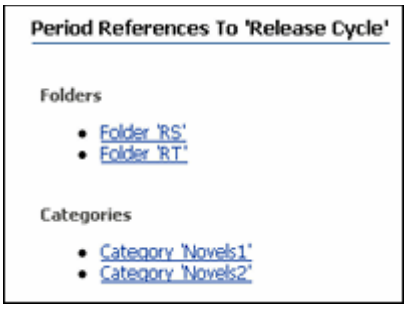
Permissions: Either the Admin.Triggers or Admin.RecordManager right is required to use this page. The Admin.Triggers right is assigned by default to the Records Officer and Records Administrator roles and the Admin.RecordManager right to the Records Administrator role. With the Admin.Triggers right, you can only view information about periods. With the Admin.RecordManager right, you can also add, edit, and delete periods.

To access this page, click a period name on the Configure Periods Page.

The Built-in label indicates if a period was a predefined, out-of-the box period. A period created by an administrator always displays "No" for the Built-in label. If a period is a built-in period, the **Edit** option is not displayed on the page because a user cannot edit a predefined period. The Actions list is not available to any users other than those with the Admin.RecordManager right.

A.8.4 Period Reference Page

This page is used to view those objects which reference a particular period.



To access this page, click **Reference** on the Period Information Page.

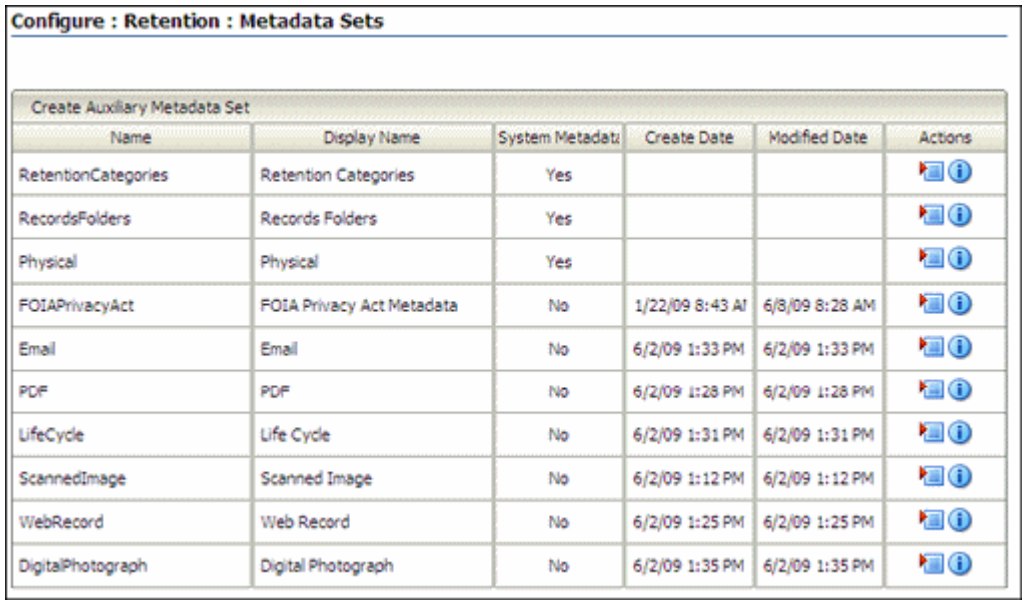
A.9 Custom Metadata Interface

The following screens are used to set up custom metadata:

- "Metadata List Page" on page A-61
- "Fields for Metadata Page" on page A-62
- "Create or Edit Auxiliary Metadata Set Page" on page A-64
- "Metadata Information Page" on page A-67

A.9.1 Metadata List Page

This page displays the tables used to store metadata.



Name	Display Name	System Metadata	Create Date	Modified Date	Actions
RetentionCategories	Retention Categories	Yes			
RecordsFolders	Records Folders	Yes			
Physical	Physical	Yes			
FOIAPrivacyAct	FOIA Privacy Act Metadata	No	1/22/09 8:43 AM	6/8/09 8:28 AM	
Email	Email	No	6/2/09 1:33 PM	6/2/09 1:33 PM	
PDF	PDF	No	6/2/09 1:28 PM	6/2/09 1:28 PM	
LifeCycle	Life Cycle	No	6/2/09 1:31 PM	6/2/09 1:31 PM	
ScannedImage	Scanned Image	No	6/2/09 1:12 PM	6/2/09 1:12 PM	
WebRecord	Web Record	No	6/2/09 1:25 PM	6/2/09 1:25 PM	
DigitalPhotograph	Digital Photograph	No	6/2/09 1:35 PM	6/2/09 1:35 PM	

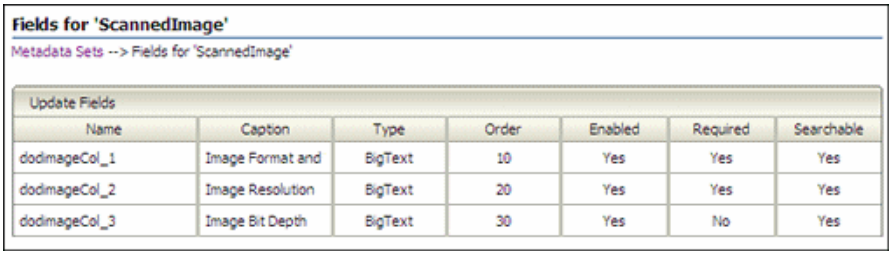
To access this page click **Records** then **Configure** from the Top menu. Click **Metadata** then **Metadata Sets**.

Click **Create Auxiliary Metadata Set** to create a new set. To add fields to an existing metadata set, click **Update Fields** from the **Action** menu for the set.

Element	Description
Name	The name of existing metadata sets to which a user can add fields. If an auxiliary metadata set has not been created, this page is empty.
Table Name	The table in which a user can create new fields. If creating auxiliary metadata fields, this lists the tables previously created.
Individual Actions Menu	When creating standard metadata sets, this menu contains two options: ▪ **Update Fields**: used to update the fields in the metadata set. ▪ **Fields Information**: used to display the Fields for Metadata Page, listing information about the metadata fields. If creating an auxiliary metadata set, a third option is available for existing sets: ▪ **Delete set**: used to delete the previously created auxiliary metadata set. It is not possible to delete a set which has a value of Yes in the System Metadata column.

A.9.2 Fields for Metadata Page

This page displays any previously created metadata fields and is used to add new fields.

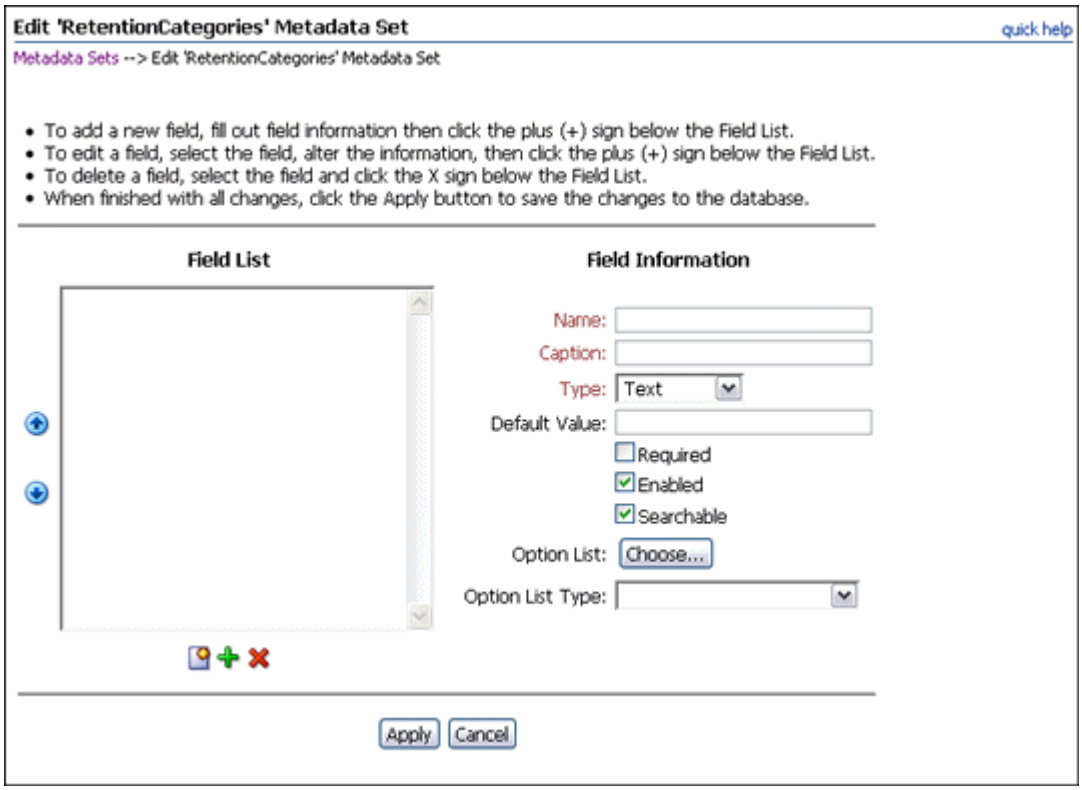


To access this page click **Field Information** in the **Action** menu of a set on the Metadata List Page.

See "Create or Edit Auxiliary Metadata Set Page" on page A-64 for details about the information on this screen.

A.9.3 Create or Edit Standard Metadata Field Page

Use this page to create or edit a custom metadata field for a retention category, folder or physical content.



To access this page, click **Update Fields** in the **Action** menu of a set on the Metadata List Page.

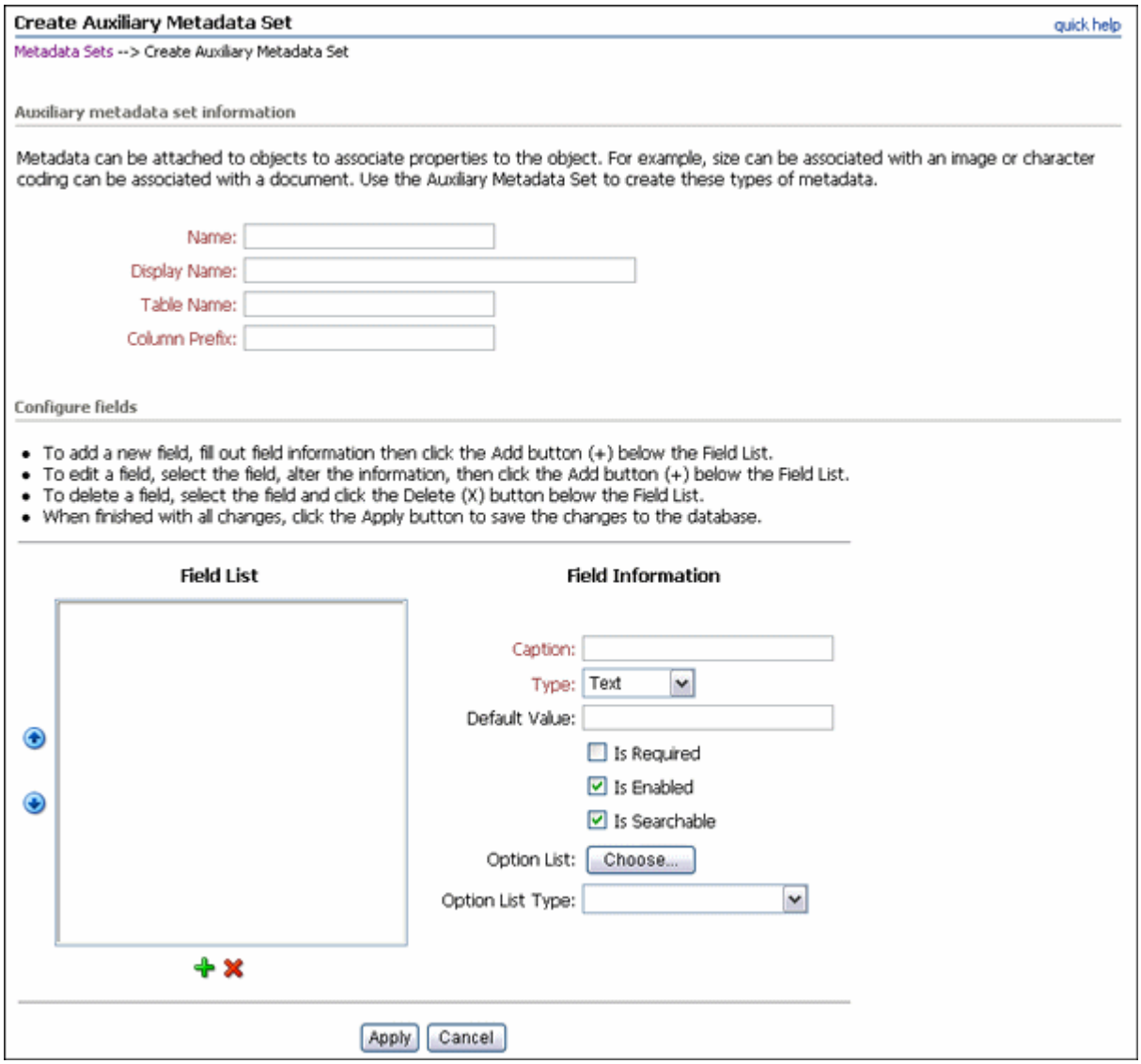
> **Permissions:** The Admin.RecordManager right or PCM.Admin.Manager right is required to perform this action. This right is assigned by default to the Records Administrator and PCM Administrator roles. The user must also have administrative privileges.

Element	Description
Name	A unique name for the field in the database. Maximum characters: 30. Required. Restricted characters: spaces, tabs, line feeds, carriage returns, semi-colon (;) caret (^), question mark (?), colon (:), at-sign (@), ampersand (&), plus sign (+), double-quote ("), pound or hash sign (#), percent sign (%), less than sign (<), asterisk (*), tilde (~), pipe (|), or dash (-).
Caption	A caption for the field displayed on the user interface. Maximum characters: 30. Required.

Element	Description
Type	The data type for the field. ■ **Text** (default): Text field, 30 characters maximum. ■ **Long Text**: Text field, 100 characters maximum. ■ **Integer**: An integer value ranging from -2^{31} to 2^{31} (-2 billion to +2 billion). Decimal values and commas not permitted. ■ **Memo**: Text field, 1000 characters maximum. ■ **Date**: A date field according to the date format specified in system settings. Selecting this type puts the Calendar component icon next to the date field.
Default Value	Default value for an Option List, Text, or Long Text field. Maximum characters: 30.
Required	Specifies if the custom metadata field is required or optional. Select the box to make the field required.
Enabled	Specifies if the field is enabled on Oracle UCM pages. Select the box to enable the field.
Searchable	Specifies if the field is indexed in the database and searchable by end users. Select the box to make it searchable.
Option List Key	Specifies the field used for the option list. Use the Choose button to select a key from the displayed list. An option list must be created and populated before it can be used.
Option List Type	The type of option list, selected from the menu.
Field List	Displays the captions for fields already created. To create a new field, enter the field information and click the Add button (plus symbol). To delete a field, highlight the field and click the Delete button (an X).
Ordering Buttons	Arrows used to change the field order. To change the order, highlight the field and select either the Up or Down arrow.

A.9.4 Create or Edit Auxiliary Metadata Set Page

Use this page to create or edit auxiliary metadata sets or fields in a previously created set.



To access this page, click **Create Auxiliary Metadata Set** from the Metadata List Page. To add fields to a current set, click **Update Fields** from the **Action** menu of the metadata set on the Metadata List Page.

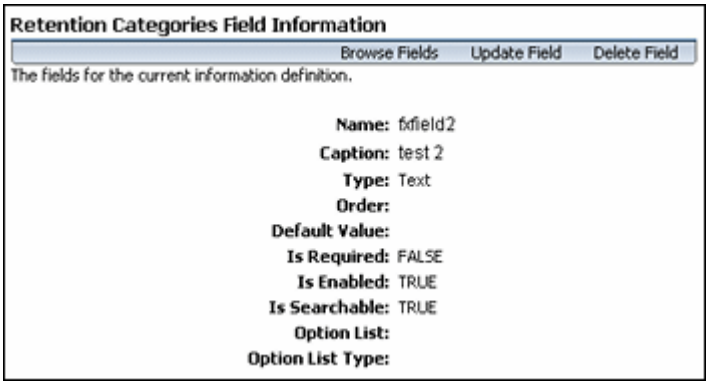
Permissions: The Admin.RecordManager right or PCM.Admin.Manager right is required to perform this action. This right is assigned by default to the Records Administrator and PCM Administrator roles. The user must also have administrative privileges.

Table Information Section	Description
Name	A unique name for the metadata set. Maximum characters: 30. Required. Restricted characters: spaces, tabs, line feeds, carriage returns, semi-colon (;) caret (^), question mark (?), colon (:), at-sign (@), ampersand (&), plus sign (+), double-quote ("), pound or hash sign (#), percent sign (%), less than sign (<), asterisk (*), tilde (~), pipe (|), or dash (-).
Description	A caption for the metadata set. Maximum characters: 30. Required.
Table Name	The name of the table in the database. Required.

Field Information Section	Description
Name	A unique name for the field in the database. Maximum characters: 30. Required. Restricted characters: spaces, tabs, line feeds, carriage returns, semi-colon (;) caret (^), question mark (?), colon (:), at-sign (@), ampersand (&), plus sign (+), double-quote ("), pound or hash sign (#), percent sign (%), less than sign (<), asterisk (*), tilde (~), pipe (|), or dash (-).
Caption	A caption for the field displayed on the user interface. Maximum characters: 30. Required.
Type	The data type for the field. ■ **Text** (default): Text field, 30 characters maximum. ■ **Long Text**: Text field, 100 characters maximum. ■ **Integer**: An integer value ranging from -2^{31} to 2^{31} (-2 billion to +2 billion). Decimal values and commas not permitted. ■ **Memo**: Text field, 1000 characters maximum. ■ **Date**: A date field according to the date format specified in system settings. Selecting this type puts the Calendar component icon next to the date field.
Default Value	Default value for an Option List, Text, or Long Text field. Maximum characters: 30.
Required	Specifies if the custom metadata field is required or optional. Select the box to make the field required.
Enabled	Specifies if the field is enabled on Oracle UCM pages. Select the box to enable the field.
Searchable	Specifies if the field is indexed in the database and searchable by end users. Select the box to make it searchable.
Option List Key	Specifies the field used for the option list. Use the Choose button to select a key from the displayed list. An option list must be created and populated before it can be used.
Option List Type	The type of option list, selected from the menu.
Field List	Displays the captions for fields already created. To create a new field, enter the field information and click the Add button (plus symbol). To delete a field, highlight the field and click the Delete button (an X).
Ordering Buttons	Arrows used to change the field order. To change the order, highlight the field and select either the Up or Down arrow.

A.9.5 Metadata Information Page

This page displays information about previously created fields.



To access this page, click a field name on the Fields for Metadata Page. Use this page to browse all created fields, to update the field, or to delete the field.

A.10 Disposition and Freeze Interface

The following screens are used when managing dispositions and freezes:

- "Disposition Interface" on page A-67
- "Freeze Interface" on page A-70

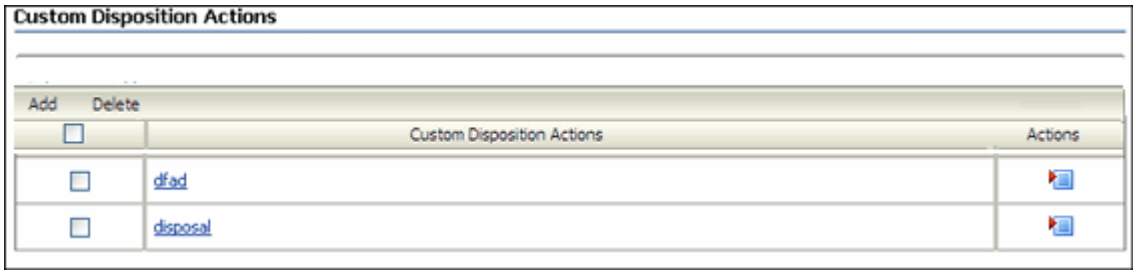
A.10.1 Disposition Interface

The following screens are used when managing dispositions:

- "Configure Dispositions Page" on page A-67
- "Create or Edit Disposition Action Page" on page A-67
- "Disposition Action Info Page" on page A-69

A.10.1.1 Configure Dispositions Page

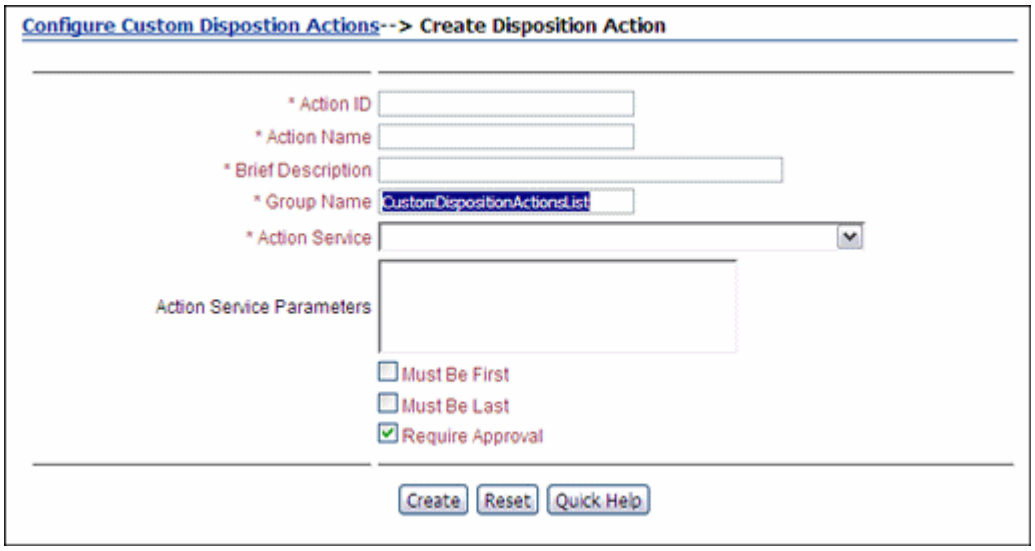
This page is used to access any previously configured dispositions and to add new dispositions.



To access this page, click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

A.10.1.2 Create or Edit Disposition Action Page

Use the Create Page to define a new custom disposition action and the Edit Page to modify an action.



To access this page, click **Add** from the Configure Dispositions Page**.**

Use the Edit Page to modify the properties of an existing custom disposition action. To access this page, click **Edit Action** from the disposition's Item **Actions** menu on the Configure Dispositions Page.

Permissions: The Admin.CustomDispositionActions right is required to use this page. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

Element	Description
Action ID field	A unique name for the custom disposition action. Maximum characters: 30. This field is view-only on the edit page. Required.
Action Name field	A name for the custom disposition action. The name is shown in the list of available disposition actions. Required. Maximum characters: 30.
Brief Description field	A description of the custom disposition action. Maximum characters: 100. Required.
Group Name field	The heading name where the custom disposition action is grouped in the list of available disposition actions on the Disposition Rule Page. Required. The default value for this field is wwOptGroupLabelCustomDispositionActionsList in the ww_strings.htm file, which is set to "Custom Actions" by default. To use a different group name than "Custom Actions," modify the string value in the resource file and restart the Content Server. Do not change the suggested default value in the Group Name field.
Action Service field	The service to be used for the custom disposition action. Contact Consulting Services for assistance with setting up custom disposition actions.
Action Service Parameters field	The parameter(s) to be used for the selected action service.

Element	Description
Must Be First box	Specifies that the custom disposition action can only be used as the first action in a disposition instruction.
Must Be Last box	Specifies that the custom disposition action can only be used as the last action in a disposition instruction.
Require Approval box	If checked, approval is required for the disposition action to be performed. **Default: selected**. Approval is required for the disposition action to be performed.

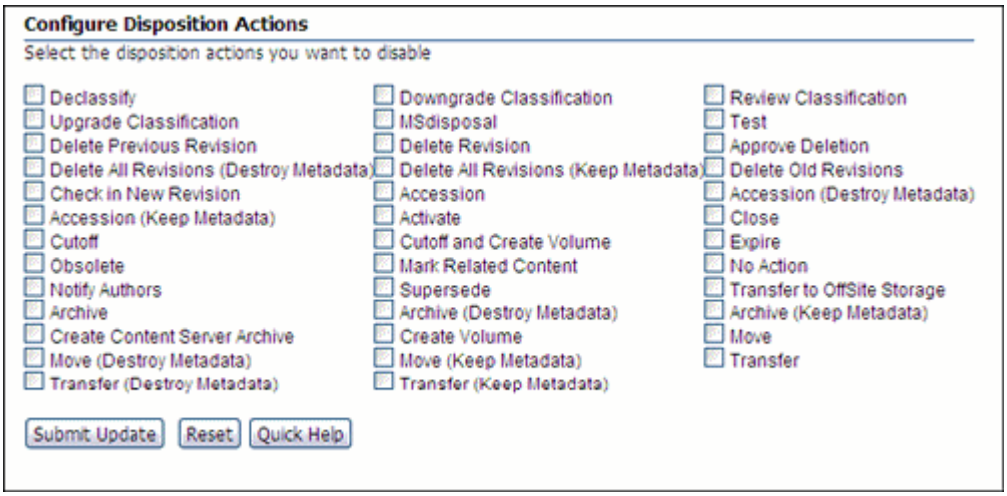
A.10.1.3 Disposition Action Info Page

The Disposition Action Info Page displays the current characteristics of the selected custom disposition action.

To access this page, click a disposition name on the Configure Dispositions Page.

A.10.1.4 Disposition Actions Configuration Page

Use this page to set what dispositions actions are disabled and unavailable for use.



This page lists all dispositions, including custom dispositions. The page depiction here may vary from because available dispositions are dependent on the type of configuration performed (Chapter 2, Chapter 2 and 4, and so on).

To access this page, click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Disable**. This page displays the actions which can be disabled.

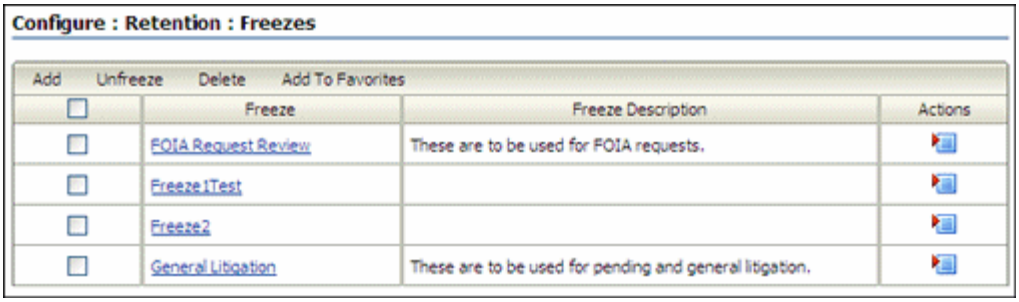
A.10.2 Freeze Interface

The following screens are used when managing freezes;

- "Freeze Configuration Page" on page A-70
- "Create or Edit Freeze Page" on page A-70
- "Freeze Information Page" on page A-73
- "Frozen Item Page" on page A-74

A.10.2.1 Freeze Configuration Page

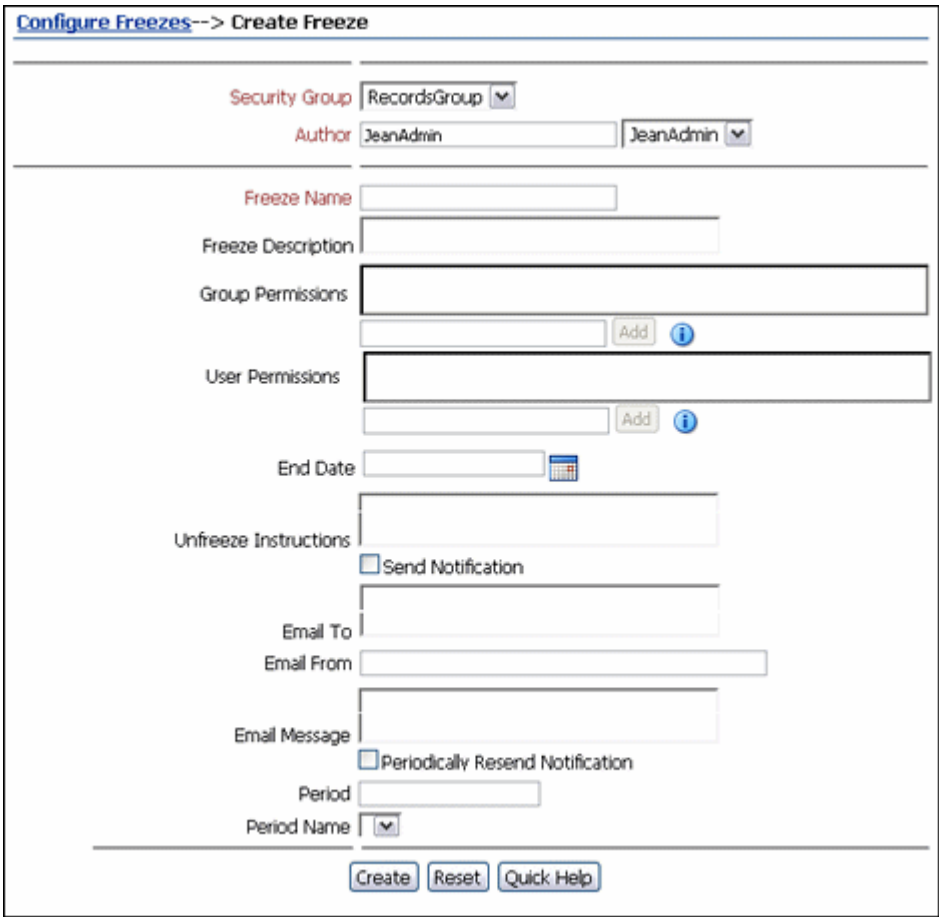
This page is used to add new freezes or to access previously created freezes for editing or deletion.



To access this page, click **Records** then **Configure** from the Top menu. Click **Retention** then **Freezes**.

A.10.2.2 Create or Edit Freeze Page

Use the Create Page to define a new freeze and the Edit Page to modify a freeze.



To access this page, click **Add** on the Freeze Configuration Page.

Use the Edit Page to modify the properties of an existing freeze. To access this page, click **Edit** then **Edit Freeze** on a freeze's Item Actions menu on the Freeze Configuration Page.

> **Permissions:** The Admin.RecordManager right is required to use this page.

Element	Description
Security Group list	The security group allowed access to the freeze. **Default: RecordsGroup**. This field is only displayed if default security is enabled. Required.
Author	The person who created the freeze. Select a person from the list if you are not the person responsible for creating the freeze. **Default: Current user.** This field is only displayed if default security is enabled. Required.
Freeze Name	The name shown in the list of available freezes. It will also appear in the subject line of an e-mail notification about the freeze. Maximum characters: 30. This field is view-only on the edit page. Required.
Freeze Description	A description for the freeze. Maximum characters: 1,000. Required.

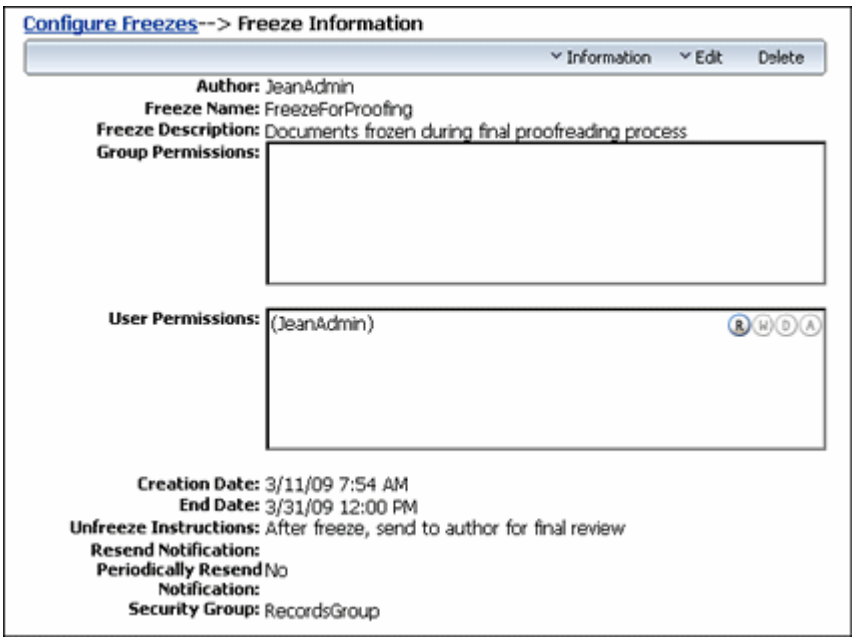
Element	Description
Creation Date (Edit Page only)	The date and time the freeze was created. This field is view-only and is displayed for tracking and documentation purposes.
Group and User Permissions	Select specific groups and users who can access the freeze. To select a group or user, type two asterisks (**) in the entry line. A list of groups and users is displayed. Select an item from the list and click **Add**. The name is inserted into the Group Permission or User Permission box. To further refine permissions, click on a displayed permission to add or remove it from the listed user or group. To remove a group or user, click the X next to the name. The name appears with a line through it, indicating it is no longer in use.
End Date	Specifies the date when the freeze ends and when the items should be unfrozen again. Click the calendar icon to choose a date. The content items are not unfrozen automatically at the specified date. This field is displayed for tracking and documentation purposes only.
Unfreeze Instructions	Specifies a descriptive text with instructions for unfreezing items (for example, "Do not unfreeze until..."). This field is displayed for tracking and documentation purposes only. Maximum characters: 1,000.
Unfreeze Reason (Edit Page only)	Specifies a reason for unfreezing all items frozen with a particular freeze.
Send Notification and Periodically Resend Notification Check	Sends e-mail to one or more persons when the freeze is created or edited. For example, you could create a freeze for a lawsuit and notify all people working on the lawsuit they need to check in any items pertaining to the lawsuit using the associated freeze. The e-mail is (re)sent when you click the Create button (on the Create Freeze page) or the Submit Update button (on the Edit Freeze page). The subject line of the e-mail is the freeze name. When an e-mail is sent, a freeze audit information log is checked into the repository. This log contains information about the freeze (freeze name, description, and creation date) and information about the e-mail notification sent (sender, recipient, message, and send date). E-mail cannot be sent if default metadata for checked-in audit logs has not been defined.
E-mail To	The e-mail address(es) where the notification should be (re)sent (in the form *user@domain.com*). Use commas to separate multiple e-mail addresses. Spaces are ignored. Do not press Enter to put e-mail addresses on separate lines. If you do, all e-mail addresses after the first line break will not receive the notification. Required if Send Notification box is selected. Maximum characters: 3,000.
E-mail From	The e-mail address of the person who sent the notification. Only one e-mail address can be specified. If left blank, the sender of the e-mail notification is the e-mail address of the user who created the freeze or resent the notification (as specified in the user profile). Maximum characters: 100.
E-mail Message	The body text of the e-mail notification (the actual message), for example, "A new freeze called 'Legal Case 19403' has been created. Please make sure you apply this freeze to all documents pertaining to this case." Required (if Send Notification box is selected). Maximum characters: 3,000.

Element	Description
E-mail Sent Date (Edit Page only)	The date and time the e-mail notification about the freeze was last sent.

Security Group list, Filer, Group Permissions, the Select button (Group Permissions), User Permissions, Select button (User Permissions) are only displayed if specific security settings are enabled on the Configure Retention Settings Page.

A.10.2.3 Freeze Information Page

The Freeze Information Page displays the characteristics of the selected freeze.



To access this page, click a freeze name on the Freeze Configuration Page.

This page shows the current properties of the selected freeze.

- **Edit**: Used to edit the current freeze, unfreeze the freeze, or alter the notification.
- **Delete**: Used to delete the current freeze.

> **Important:** You cannot delete a freeze if that freeze is currently applied to any content items. If you try, an error message is displayed.

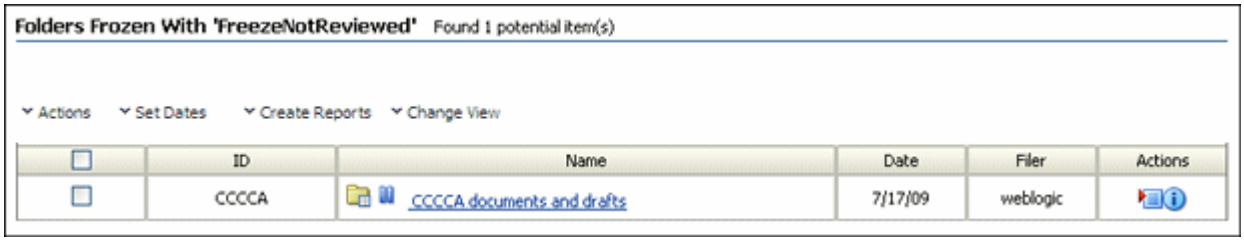
- **Information**: Used to perform the following searches:
  - **Screen Frozen Content**: Used to display a list (see Frozen Item Page) of content items frozen with the current freeze. The list does not include any frozen content that inherited its freeze status from the parent record folder.
  - **Screen All Frozen Content**: Used to display a list (see Frozen Item Page) of all content items frozen with the current freeze. The list also includes all frozen items that inherited their freeze status from their parent folders.
  - **Screen Frozen Folders**: Used to display a list (see Frozen Item Page) of folders frozen with the current freeze. The list does not include any frozen folders that inherited their freeze status from their parent folders.

– **Screen All Frozen Folders**: Used to display a list (see Frozen Item Page) of all folders frozen with the current freeze. The list includes all frozen folders that inherited their freeze status from their parent folders.

Permissions: The Screen... options are available only if you have the Admin.Screening right.

A.10.2.4 Frozen Item Page

This page displays a list of the content items or folders frozen with the current freeze.



To access this page, click **Information** then the screening type from a freeze on the Freeze Configuration Page.

Permissions: The Admin.RecordManager right and Admin.Screening right is required to use this page.

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

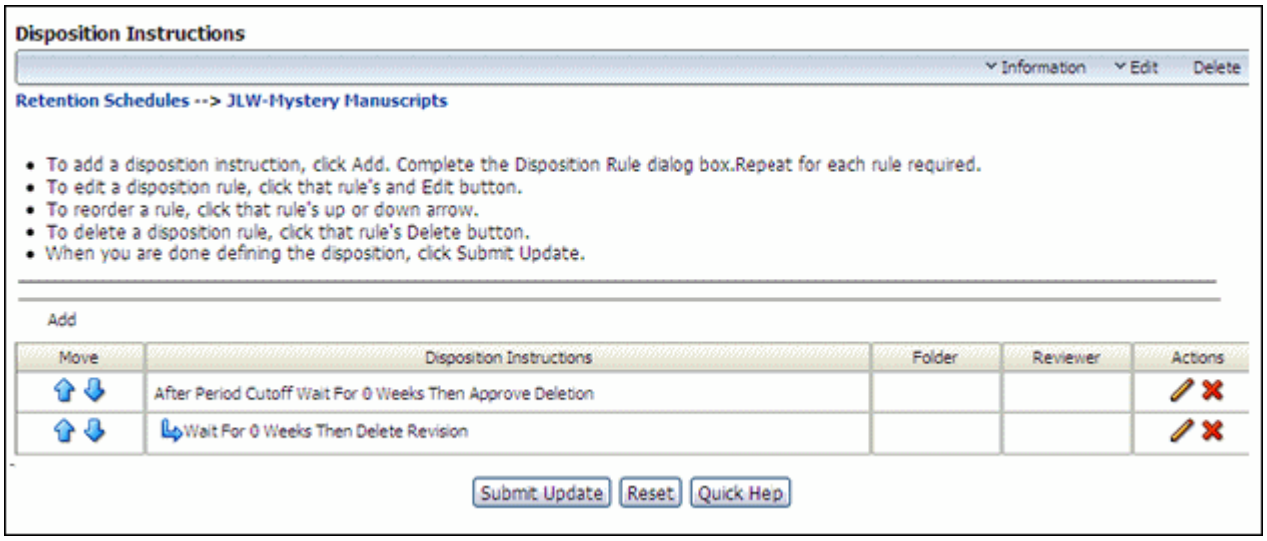
A.11 Disposition Interface Screens

The following screens are used to manage dispositions:

- "Disposition Instructions Page" on page A-74
- "Disposition Rule Page" on page A-75
- "Disposition Information Page" on page A-77

A.11.1 Disposition Instructions Page

Use the Disposition Instructions Page to add, edit, and delete disposition instructions for a retention category.



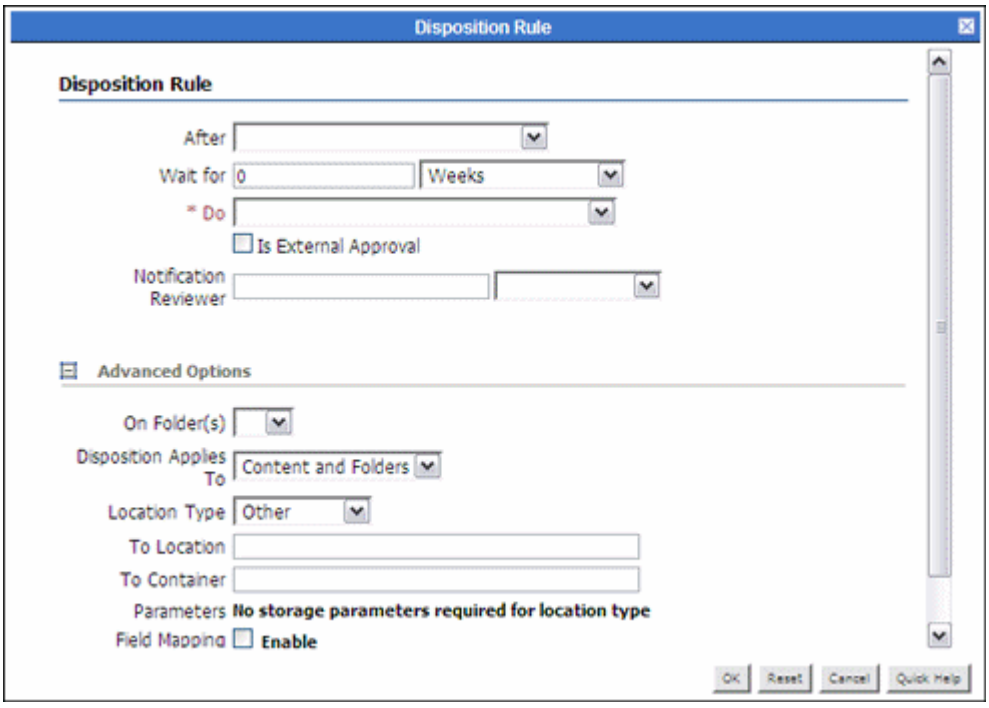
To access this page, browse through content at the series level for the retention category. In the row for the retention category, click **Edit** then **Edit Disposition** from the item's **Action** menu.

This page is also displayed when a retention category is initially created. At the top of the page, there are bulleted instructions to assist the user with its basic use.

Element	Description
Disposition instructions box	Displays any defined disposition instructions for the retention category.
Up or Down button	Up arrow or Down arrow. Moves a selected disposition rule upward or downward one row with each click.
Add button	Opens the Disposition Rule Page, where a new disposition rule can be defined.
Edit icon	Pencil icon (Edit). Opens the Disposition Rule Page for the disposition rule selected within the Disposition Instructions box.
Delete icon	Red "X" (Delete). Deletes the disposition rule selected within the Disposition Instructions box.
Submit Update button	Submits the updates.
Reset button	Resets the page to the initial default settings. If on an editing page, reset returns the original settings.

A.11.2 Disposition Rule Page

Use the Disposition Rule page to define or edit disposition rules for a retention category.



To access this screen, click the Edit icon (a pencil) for the disposition to edit or click **Add** to create a disposition on the Disposition Instructions Page.

Depending on the captions settings in the Configure Retention Settings Page page, there are two views of this screen: user-friendly captions for ease in reading disposition instructions and standard captions for those organizations accustomed to disposition language.

Element	Description
Triggering Event (user-friendly label = *After*)	Triggering events to associate with a disposition rule. Required.
Retention Period text box and list (user-friendly label = *Wait for*)	The number of periods and period unit. This is how long to retain scheduled items. The list displays all defined periods. Required. Required or optional depending on the disposition instruction scenario. For retention categories, a user can specify a retention period only for the Retention Period Cutoff and Preceding Action triggering events. For content item categories, a user can specify a retention period for all triggering events. With this functionality, a user can create disposition rules for content such as "Delete all old revisions three months after the last new revision was checked in."
Is External Approval	This option only appears if an external approval process has been set up on the system (for example, if a record on an external system is to be managed by the local system without being physically present). **IMPORTANT**: If **Is External Approval** is checked, the notification reviewer list should display a list of the registered processes. If that list does not include external process, restart the Content Server to populate the dropdown list to include the external process.

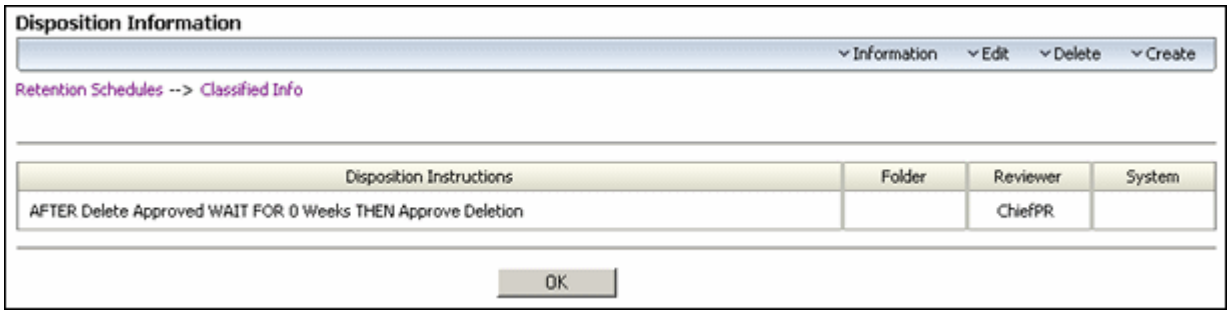
Element	Description
Disposition Action (user-friendly label = *Do*)	The disposition action defined for the rule. The system does not perform the action but sends an e-mail notification to the person responsible for carrying out the action. Required.
Notification Reviewer	Specifies who is notified of the event. If no one is specified, the category author is notified. If an additional reviewer is specified, both the category author and the additional reviewer are notified. See the note regarding the **Is External Approval** box for external process notification reviewers.
Apply to Record Folder list (user-friendly label = On Folder(s))	Applies a disposition rule to a specific record folder within a retention category. Any existing record folders within the retention category are displayed in the list. **Default: All**. The disposition rule is applied to all record folders within a retention category.
Disposition Applies To	Applies a disposition rule to a specific retention object within a retention category. Any existing objects are displayed in the list. **Default: All**. The disposition rule is applied to all retention objects within a retention category.
Location Type	If the disposition action is an option like archive, move, or transfer, choose a location from the **Location Type** list. Depending on the location type chosen, fill in the following information: ■ File Storage: Enter the storage path where the archive file will be stored. ■ FTP: Specify the path to the FTP server and the directory location for the archive and, if chosen, the meta path. Enter the FTP user name and password. ■ WebDAV: Specify a valid WebDAV path and, if chosen, the meta path. Enter the FTP user name and password. ■ Other: This selection specifies that the archive will be downloaded manually when the action is performed. If the destination has an associated location or container, enter a description in the appropriate text box.
Destination Container (user-friendly label = To Container)	A physical container for an external record folder, such as a barcode or some other means of identification. Maximum characters: 30.
Field mapping	Used to map fields when exporting data to another system which may have metadata fields with different names. Field mapping can be used when creating the meta file for export. If a field is mapped, then the mapped name will be used in the file instead.

Tip: If you want the specified notification reviewer to be the only user who receives e-mail notifications for the events triggered by the disposition rule (and not the category author as well), make sure the records_management_environment.cfg configuration file contains the following line: `RmaNotifyDispReviewerAndCatAuthor=false`. Restart the Content Server for this setting to take effect.

A.11.3 Disposition Information Page

Use this page to view information about disposition instructions for a retention category. The Records Administrator can configure the disposition rules to display

standard or user-friendly captions by toggling the captions setting on the Configure Retention Settings Page page.



To view this page, click **Browse Content** then **Retention Schedules**. The Exploring Series "Retention Schedule" Page is displayed. Navigate to the appropriate retention category.

Click **Information** then **Disposition Information** from the item's **Actions** menu or click **Information** then **Disposition Information** from the Page menu on the Retention Category Information Page.

Permissions: Anyone with the Category.Read rights can view information disposition information for a retention category. All predefined roles have this role by default. To edit or delete disposition rules, the Category.Edit or Category.Delete rights are required.

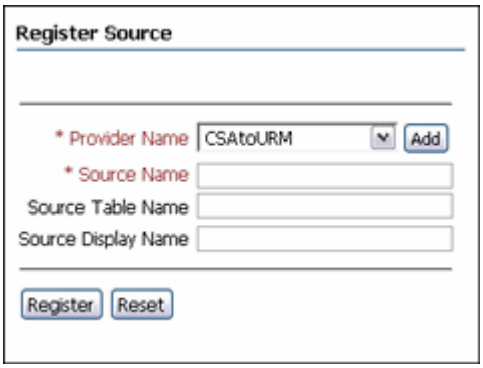
A.12 Adapter Interface

The following screens are used when configuring and using the UCM Adapter.

- "Register Source Page" on page A-78
- "Add or Edit New Provider Page" on page A-79
- "Provider List Page" on page A-80
- "Provider Information Page" on page A-81
- "Source Configuration Information Page" on page A-82
- "Map Custom Fields Page" on page A-82
- "Map/Edit Custom Field Dialog" on page A-83
- "Configure Scheduled Events Page" on page A-84
- "Synchronization Log Page" on page A-85

A.12.1 Register Source Page

This page is used to register the external Adapter source.



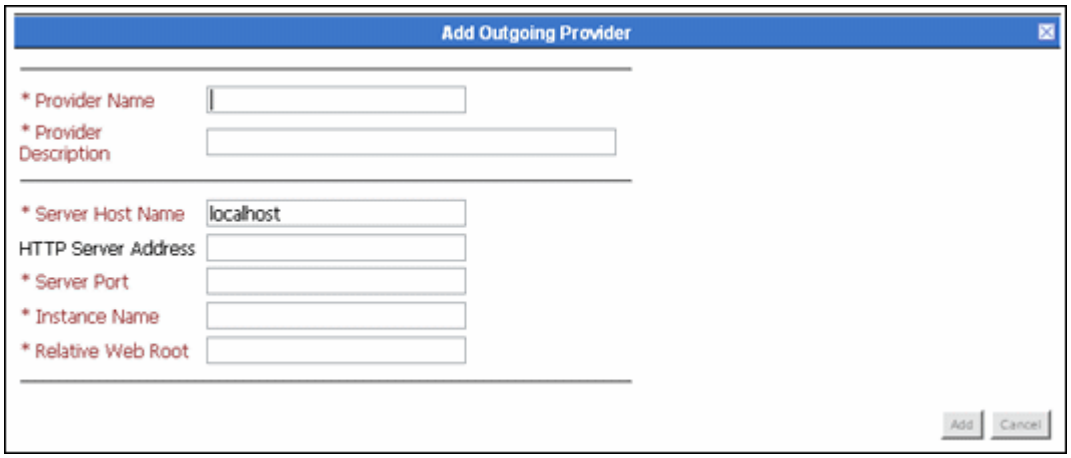
To access this page, click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Source Registration**.

> **Note:** You can only register one source per Adapter instance. If you need to change the configuration settings of the registered source, you must delete (unregister) the current source and register a new source.

Element	Description
Provider Name field	The name of the outgoing provider that was configured for communication between the Adapter server and the Oracle URM server.
Source Name field	The name of the Oracle URM source to be created on the Oracle URM server.
Source Display Name field	The descriptive name used to identify the Oracle Oracle URM Adapter source. It is displayed on the Search page on the Oracle UCM server.
Source Table Name field	The prefix of the database tables that are created for the Oracle URM source.
Register button	Registers the Oracle URM Adapter with Oracle URM. Registration ensures that Oracle URM is aware of the Adapter and is ready to manage the stored content in the Adapter server's repository.
Reset button	Clears any populated fields on the screen and resets the screen fields to their initial default settings.

A.12.2 Add or Edit New Provider Page

Use this page to define the outgoing provider that enables the Adapter server to connect to the Oracle URM server.



To access this page, click **Add** on the Register Source Page.

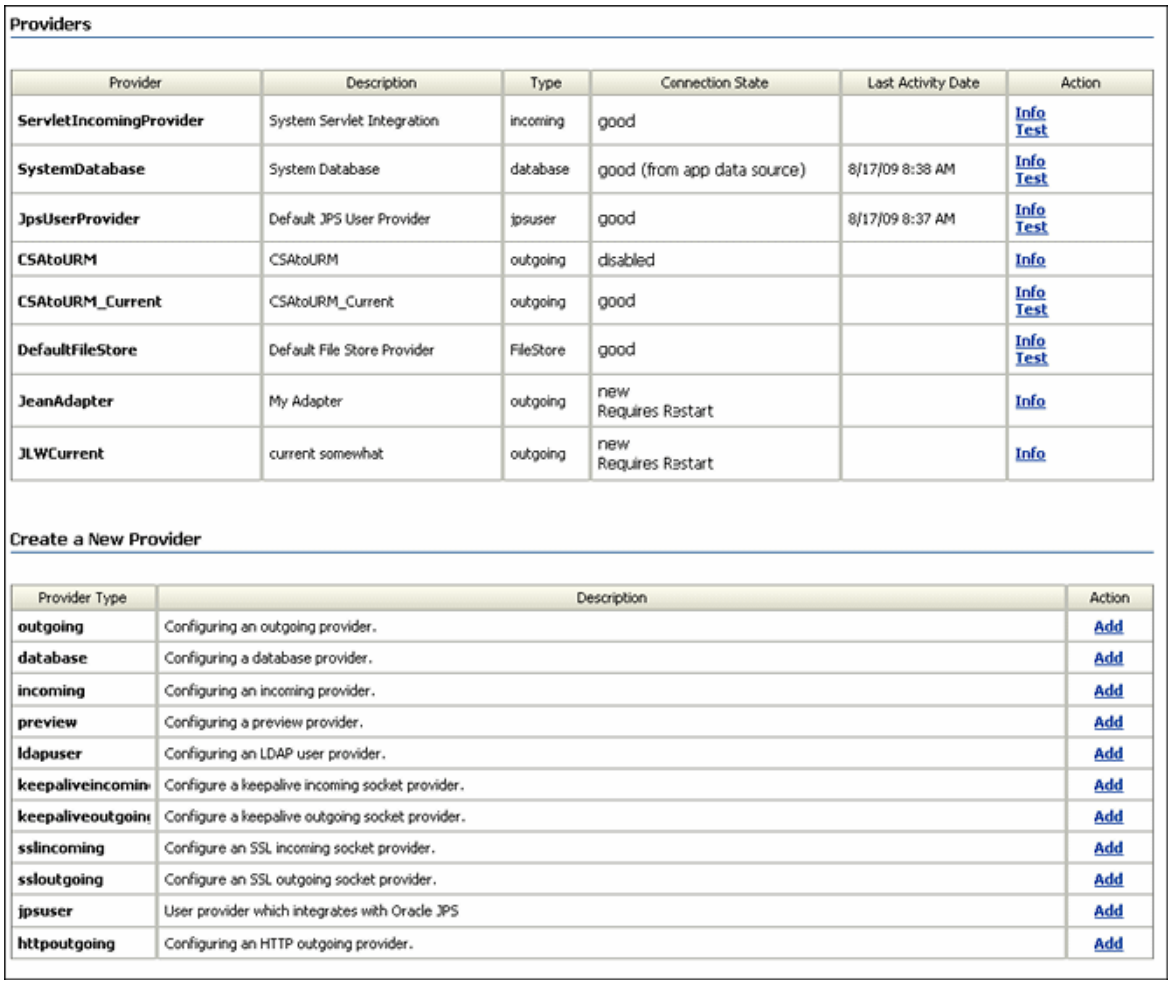
This page is an abbreviated version of the full Outgoing Providers page. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about using that page.

> **Important:** The `IntradocServerPort` configuration variable must be set to 4444 (or any other arbitrary number) on Oracle URM in the config.cfg file. This can be done during installation of Oracle URM, but it may be overlooked.

Element	Description
Provider Name field	The name of the outgoing provider for the Adapter server. Do not use special characters or hyphens in the outgoing provider's name.
Provider Description	A description of the provider.
Server Host Name field	The server host name of the instance on the Oracle URM server.
HTTP Server Address	The URL of the instance on the Oracle URM server.
Server Port field	The port on which the provider communicates with the instance on the Oracle URM server.
Instance Name field	The instance name on the Oracle URM server.
Relative Web Root field	The relative web root of the instance on the Oracle URM server
Add button	Saves the configuration settings and adds the outgoing provider to the Oracle UCM's Providers table.
Reset button	Clears any populated fields on the screen and resets the screen fields to their initial default settings.

A.12.3 Provider List Page

This screen shows the providers that have been configured for the system.



Providers

Provider	Description	Type	Connection State	Last Activity Date	Action
ServletIncomingProvider	System Servlet Integration	incoming	good		Info Test
SystemDatabase	System Database	database	good (from app data source)	8/17/09 8:38 AM	Info Test
JpsUserProvider	Default JPS User Provider	jpsuser	good	8/17/09 8:37 AM	Info Test
CSAtoURM	CSAtoURM	outgoing	disabled		Info
CSAtoURM_Current	CSAtoURM_Current	outgoing	good		Info Test
DefaultFileStore	Default File Store Provider	FileStore	good		Info Test
JeanAdapter	My Adapter	outgoing	new Requires Restart		Info
JLWCurrent	current somewhat	outgoing	new Requires Restart		Info

Create a New Provider

Provider Type	Description	Action
outgoing	Configuring an outgoing provider.	Add
database	Configuring a database provider.	Add
incoming	Configuring an incoming provider.	Add
preview	Configuring a preview provider.	Add
ldapuser	Configuring an LDAP user provider.	Add
keepaliveincomin	Configure a keepalive incoming socket provider.	Add
keepaliveoutgoin	Configure a keepalive outgoing socket provider.	Add
sslincoming	Configure an SSL incoming socket provider.	Add
ssloutgoing	Configure an SSL outgoing socket provider.	Add
jpsuser	User provider which integrates with Oracle JPS	Add
httpoutgoing	Configuring an HTTP outgoing provider.	Add

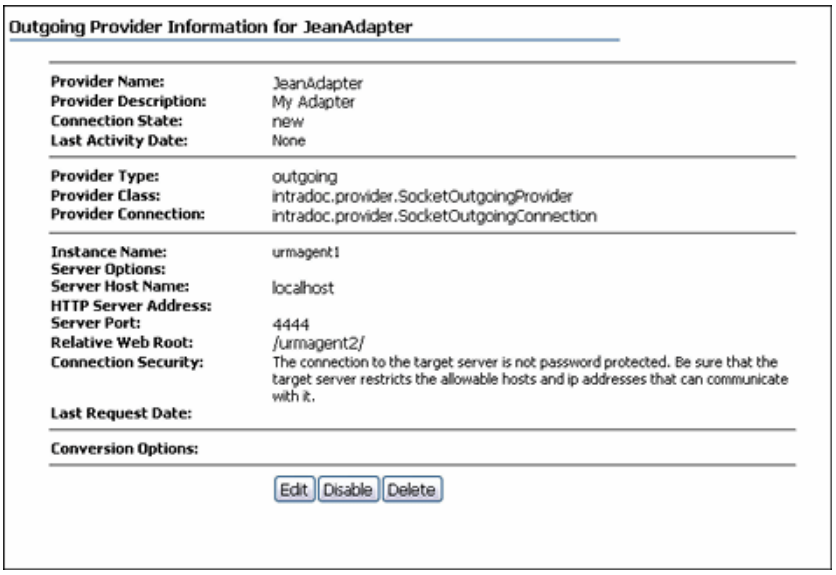
To access this page, click **Administration** then **Providers** from the Main menu.

The top half of this page displays the currently configured providers. The bottom half can be used to add a new provider. See the *Oracle Fusion Middleware System Administrator's Guide for Content Server* for details about using this page.

Element	Description
Provider Name	The name of the outgoing provider for the Adapter server. Do not use special characters or hyphens in the outgoing provider's name.
Provider Description	A description of the provider.
Type	The designated type of provider.
Connection State	The status of the connection.
Last Activity Date	The date of the last activity with that provider.
Action	Links to display the information page for the provider or to test the connection.

A.12.4 Provider Information Page

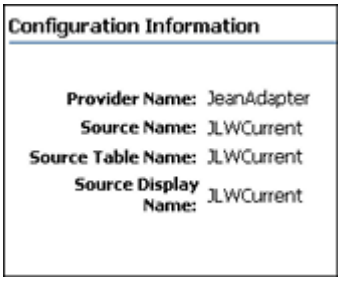
This page lists information about an outgoing provider.



To access this page, click **Administration** then **Providers** from the Main menu. Click the **Info** link next to an outgoing provider.

A.12.5 Source Configuration Information Page

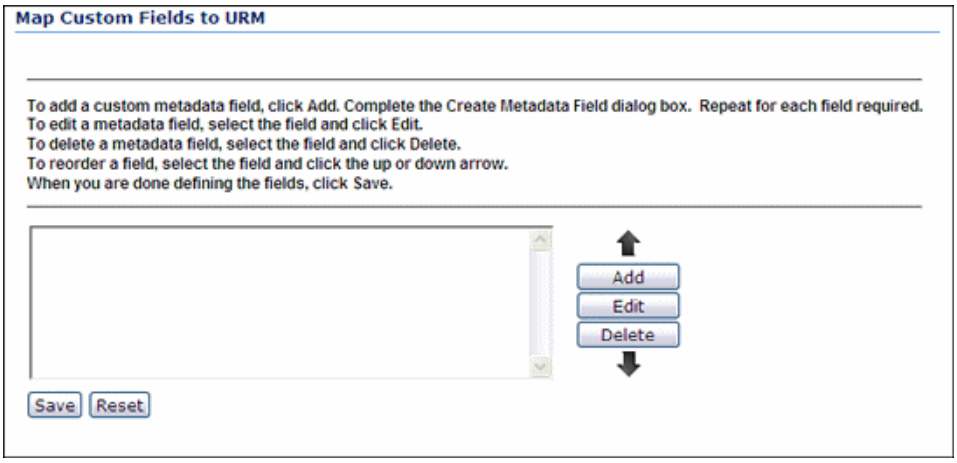
This page displays information about a registered source.



To access this page, click **Records** then **UCM Adapter** from the Top menu. Click **Configuration Information**.

A.12.6 Map Custom Fields Page

This page is used to create and define custom metadata fields for the Oracle URM source.

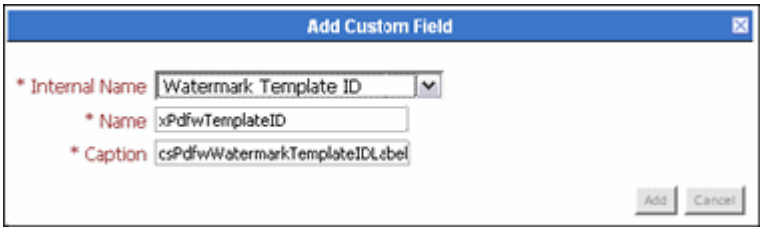


This page is displayed when a souce is first registered. It can also be accessed by clicking **Records** then **UCM Adapter**. Click **Configure** then **Custom Fields**.

Element	Description
Custom metadata fields pane	Lists the available custom metadata fields that can be edited or deleted, as necessary.
Add button	Displays the Map/Edit Custom Field Dialog which is used to create new custom metadata fields.
Edit button	Displays the Map/Edit Custom Field Dialog for an existing custom metadata field and enables a user to modify the settings.
Up/down arrows	Used to adjust the specific placement order of the selected custom metadata field. The position of each custom field in the list is relevant to its priority on the Item Information page.
Save button	Saves the configured settings.
Reset button	Clears any populated fields on the screen and resets the screen fields to their initial default settings.

A.12.7 Map/Edit Custom Field Dialog

This dialog is used to add a custom metadata field for use with the UCM Adapter.

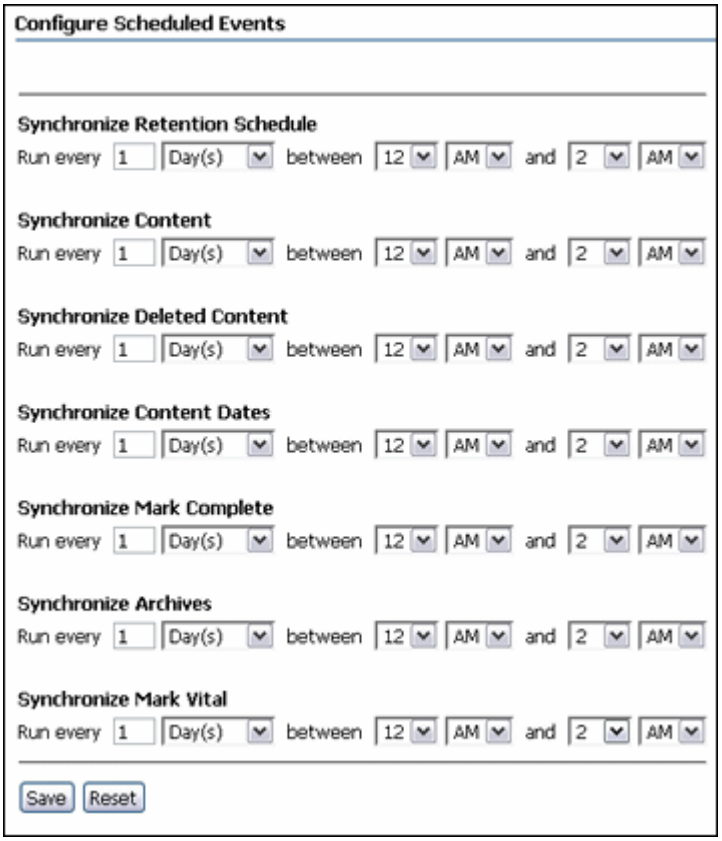


This dialog is displayed when a user clicks **Add** or **Edit** on the Map Custom Fields Page.

Elements	Description
Internal Name list	Lists the Adapter's available custom metadata fields that can be mapped to Oracle URM custom metadata fields. A user can either select a metadata field in the list or enter a different name. If entering a new name, the Adapter automatically creates a corresponding custom metadata field for the name.
Name field	Enter the name of the custom metadata field to be created.
Caption field	The descriptive name of the Oracle URM custom metadata field that is displayed on the Item Information page in Oracle URM.
Add button	Saves the settings and adds the new Oracle URM custom metadata field to the list on the Map Custom Fields Page.
Cancel button	Clears any populated fields on the screen and resets the screen fields to their initial default settings.

A.12.8 Configure Scheduled Events Page

This page is used to schedule synchronization activities for the Adapter.



To access this page, click **Records** then **UCM Adapter** from the Top menu. Click **Configure** then **Scheduled Events**.

Elements	Description
Synchronization choices	Each section of this screen displays items which can be synchronized.

Elements	Description
Synchronization schedule	Select the time period for the synchronization from the menu list.
Synchronization time	Select the time of day for the synchronization.

A.12.9 Synchronization Log Page

This page displays information about synchrnoization activities.

To access this page, click **Records** then **UCM Adapter** from the Top menu. Click **Logs** then the log type. The example displayed here is a log for an Archive operation.

Important: Revisioning of external items differs from revision of items stored on Content Server. For example, if an item is created on the adapter system and is synchronized to Oracle URM, it appears as a single item. However, if that item is revised on the adapter system then synchronized to Oracle URM, the item now appears in the category as two items, not one item with two revisions. Both items have the same content ID, which is the default behavior for external items.

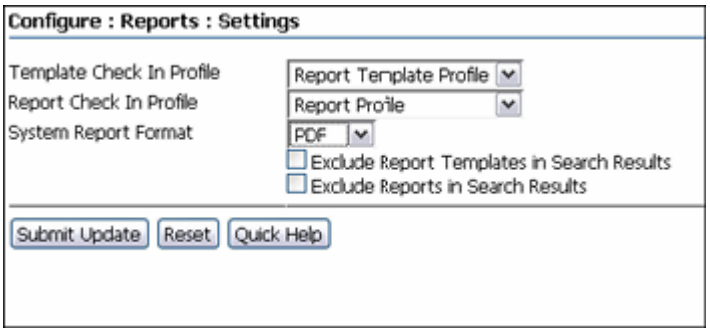
A.13 Report Interface

The following screens are used to create and edit custom reports. This functionality is not available by default. It must be enabled by adding the Rma.Admin.Customization right to a user's rights.

- "Configure Reports Settings Page" on page A-85
- "Configure Report Element Page" on page A-86
- "Report Checkin Page" on page A-88
- "Configure Report Sources Page" on page A-89

A.13.1 Configure Reports Settings Page

Use this page to set up reports for retention items, chargebacks, and other functionality. The settings on this page affect report formatting for internal, record, and physical reports. Note that users can set a report format preference on the user profile page. That preference takes precedence over the format specified here.



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**. Note that this is used to create Records reports as well as Physical Item reports. In previous versions of this software, Physical reports were accessed on a separate menu.

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.

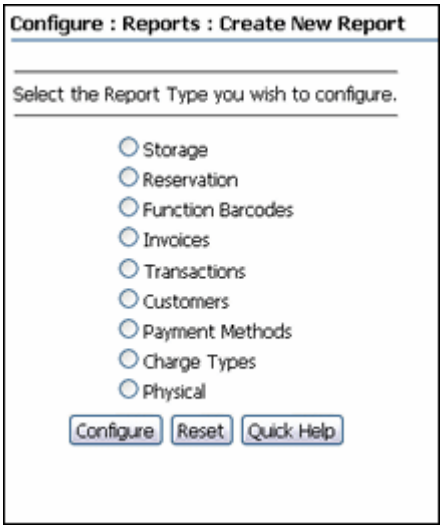
A.13.2 Configure Report Element Page

This screen is used to configure different aspects of reports, including templates, report data, and so on. The image shown here is that used to choose a type of report to configure.

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

To access this page, click **Records** then **Configure** from the Top menu. Click **Reports** then one of the report options, discussed in the following text.

The screen used for physical content is similar, used to create reports for storage, reservations, invoices, transactions, and so on.



To access this page, click **Physical** then **Configure** then **Reports** from the Top menu. Then choose a report option:

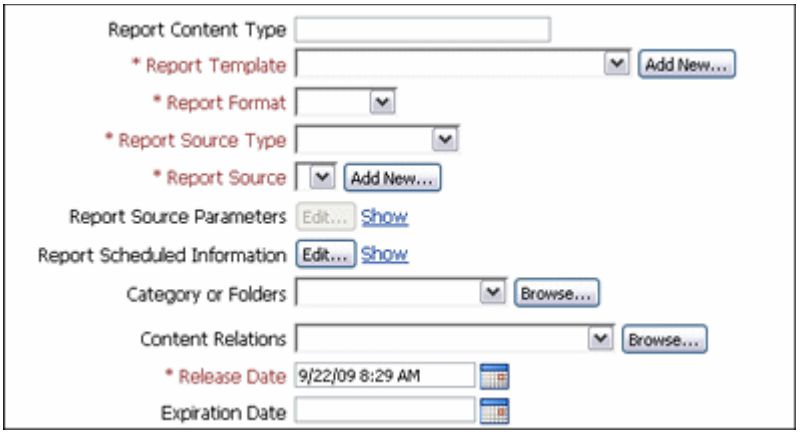
- **Create New Report**: used to start the process of creating a new report. This option displays a Report Checkin Page, used to save the report name and save other detailed report information.
- **Report Sources**: displays the Configure Report Sources Page, used to choose the criteria to gather data for the report.

- **Templates**: displays a search results page listing templates that can be used for reports.
- **Download BI XML Data**: opens a dialog box where a user can choose to open the XML data used for the reports or save the data.

After choosing a report option, the Configure Report Element Page is displayed. Choose the type of report to create.

A.13.3 Report Checkin Page

This page is used to check in a new report and add pertinent information about that report. The screen here shows a portion of the checkin page that pertains to reports.

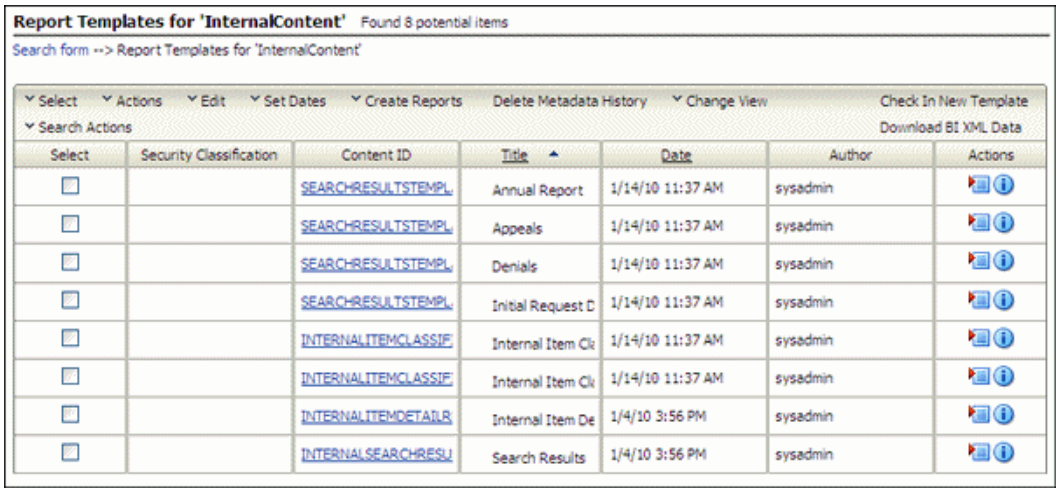


To access this page, click **Records** then **Configure** from the Top menu. Click **Reports** then **Create New Report**. Choose the type of report to create then click **Configure**.

Element	Description
Report Template	Choose a template from the dropdown list or click **Add New** to create a new template.
Report Format	Choose a format for the report from the dropdown list. Note that when creating a report for barcodes, the user must choose PDF as the report type.
Report Source Type	Choose the type of source to use to gather the data for the report. Options include: ■ Service: use Content Server services to build data for the report. ■ Query: use Content Server queries to gather data. ■ Dynamic Query: use a dynamic query to gather data. If Services or Query are chosen, the correct service or query must be used to work with the template. A dynamic query will gather the appropriate data for use.
Report Source	Choose a source for the data or click **Add New** to create a new source using the Configure Report Sources Page.

A.13.4 Report Templates Page

This page shows templates that can be used for the report or which can be copied and edited for a new template.



This page shows all current templates. To access this page, click **Records** then **Configure** from the Top menu. Click **Reports** then **Templates**. Choose a template type then click **Configure**.

Element	Description
Select	A checkbox used to select a template file for use.
Security Classification	Classification associated with a template.
Content ID	The content ID of the template file.
Title	The template title.
Date	The date the template file was created or modified.
Author	The author of the file.
Actions	Actions which can be taken using the specified template file. These include checking in a similar file, checking out this file, retrieving the native file for use, or viewing the metadata history of the file.

The Table menu on this page can be used to perform actions for all template files or only selected files. The options shown depend on the configuration of the system nand the permissions of the user accessing the page.

- **Select**: allows the selection of all items or the deselection of items.
- **Actions**: used to add items to a Content Basket or to a folio.
- **Edit**: used to freeze or unfreeze selected items.
- **Set Dates**: used to mark dates associated with items such as review dates, rescind dates, and other action dates.
- **Create Reports**: used to create a report using a specified template.
- **Delete Metadata History**: used to clear the metadata history changes.
- **Change view**: used to change the way search results are displayed.
- **Search actions**: used to save the search under a search name.

A.13.5 Configure Report Sources Page

This page is used to choose queries and service calls to gather data for the report.

Important: Creating custom report sources requires in-depth technical knowledge of services and queries. Contact Consulting Services for further assistance if needed.

To access this page, click **Add New** on the Report Checkin Page or click **Records** then **Configure** from the Top menu. Click **Reports** then **Report Sources**. A user can also access this page by clicking **Physical** then **Configure** then **Reports** then **Report Sources** from the Top menu.

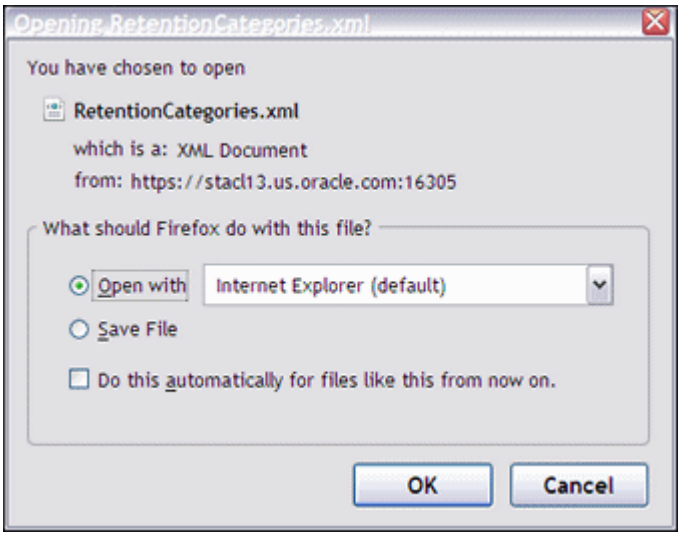
To use this screen, highlight a query or a service on the left side of the screen. Click the right arrow to move the query or service to the right column for use.

To remove a query or service from use, highlight the name and click the left arrow to move the item to the left column.

Click **Update** when done.

A.13.6 XML Data Dialog

The XML Data Dialog opens when the user elects to download an XML data file.



This file appears after clicking **Configure** on the Configure Report Element Page after choosing to download XML data.

To view the file, click **Open With** and choose a browser type from the pulldown menu. To save the file, click **Save File**. A window opens with a prompt to save the file. Choose a filename and file location for the data and click **OK**.

To use one method (save or open) as the default, click the checkbox next to the **Do this automatically...** prompt.

B

Summary of Security Rights and Roles

This chapter provides tables that show the default rights assigned to default roles for different functions in the product. The information here is the same as that described in "Security Classifications Tasks and Defaults for Predefined Roles" on page 5-5. It is merely presented in a different manner.

This chapter describes the following topics:

B.1 Rights and Roles for Oracle URM

This section describes the default rights and roles for tasks encountered while using Oracle URM.

The default roles are **rma** (User), **rmalocalrecordsofficer** (Officer), and **rmaadmin** (Admin).

B.1.1 Triggers

The following table describes the default rights assigned to the default roles for tasks involving triggers.

Task	Required RM Right	User	Officer	Admin
View information about triggers	Admin.Triggers or Admin.RecordManager		X	X
Create a trigger	Admin.Triggers		X	X
Edit a trigger	Admin.Triggers		X	X
Delete a trigger	Admin.Triggers and Delete permission for the trigger's security group. The Delete permission is not granted by default.		X	X

B.1.2 Periods

The following table describes the default rights assigned to the default roles for tasks involving periods.

Task	Required RM Right	User	Officer	Admin
View information about periods	Admin.Triggers or Admin.RecordManager		X	X
Create a period	Admin.RecordManager			X

Task	Required RM Right	User	Officer	Admin
Edit a custom period	Admin.RecordManager			X
Delete a custom period	Admin.RecordManager			X

B.1.3 Supplemental Markings

The following table describes the default rights assigned to the default roles for tasks involving supplemental markings.

Task	Required RM Right	User	Officer	Admin
View information about supplemental markings	Admin.Triggers or Admin.RecordManager		X	X
Enable/disable supplemental markings	Admin.RecordManager			X
Create/edit a supplemental markings	Admin.RecordManager			X
Delete a supplemental marking	Admin.RecordManager			X

B.1.4 Security Classifications

The following table describes the default rights assigned to the default roles for tasks involving security classifications.

Task	Required RM Right	User	Officer	Admin
View information about classifications	Admin.RecordManager **and** Admin.SecurityClassifications			X
Enable/disable classifications	Admin.RecordManager **and** Admin.SecurityClassifications			X
Create/edit a classification	Admin.RecordManager **and** Admin.SecurityClassifications			X
Delete a classification	Admin.RecordManager **and** Admin.SecurityClassifications			X
Reorder security classifications	Admin.RecordManager **and** Admin.SecurityClassifications			X

B.1.5 Custom Security Fields

The following table describes the default rights assigned to the default roles for tasks involving security classifications.

Task	Required RM Right	User	Officer	Admin
View information about a custom security field	Admin.Triggers or Admin.RecordManager		X	X
Enable/disable custom security fields	Admin.RecordManager			X
Create/edit a custom security field	Admin.RecordManager			X
Delete a custom security field	Admin.RecordManager			X

B.1.6 Custom Category or Folder Metadata Fields

The following table describes the default rights assigned to the default roles for tasks involving custom metadata fields.

Task	Required RM Right	User	Officer	Admin
Create/edit a custom metadata field	Admin.RecordManager			X
Delete a custom metadata field	Admin.RecordManager			X

B.1.7 Classification Guides

The following table describes the default rights assigned to the default roles for tasks involving classification guides.

Task	Required RM Right	User	Officer	Admin
View information about classification guides	Admin.ClassificationGuide		X	X
Create/edit a classification guide	Admin.ClassificationGuide		X	X
Delete a classification guide	Admin.ClassificationGuide		X	X
View information about classification topics	Admin.ClassificationGuide		X	X
Create/edit a classification topic	Admin.ClassificationGuide		X	X
Delete a classification topic	Admin.ClassificationGuide		X	X

B.1.8 Freezes

The following table describes the default rights assigned to the default roles for tasks involving freezes.

Task	Required RM Right	User	Officer	Admin
View information about freezes	Admin.RecordManager			X
Create/edit a freeze	Admin.RecordManager			X
Delete a freeze	Admin.RecordManager and Delete permission for the freeze's security group. The Delete permission is not granted by default.			X
Send email notification about a freeze	Admin.RecordManager			X

B.1.9 Series

The following table describes the default rights assigned to the default roles for tasks involving series.

Task	Required RM Right	User	Officer	Admin
Browse and view information about freezes	Series.Read	X	X	X
Create/edit a series	Series.Create, Series.Edit			X
Delete a series	Series.Delete			X
Hide/unhide a series	Series.Hide, Series.Unhide			X
Move a series	Series.Move			X

B.1.10 Categories

The following table describes the default rights assigned to the default roles for tasks involving retention categories.

Task	Required RM Right	User	Officer	Admin
Browse and view information about retention categories, including disposition instructions	Category.Read	X	X	X
Create/edit a retention category	Category.Create, Category.Edit			X
Edit the review information for a retention category	Category.Edit.Review			X
Delete a category	Category.Delete			X
Apply disposition instructions to specific records in a category	Category.Edit			X
Move a category	Category.Move			X

B.1.11 Folders

The following table describes the default rights assigned to the default roles for tasks involving folders.

Task	Required RM Right	User	Officer	Admin
Browse and view information about folders	Folder.Read	X	X	X
View the life cycle of a folder, the review history of a folder and the metadata history of a folder	Folder.Read	X	X	X
Create a folder	Folder.Create		X	X
Edit a folder if author of the folder	Folder.EditIfAuthor		X	
Edit a folder if not author of the folder	Folder.Edit			X
Edit the review information for a folder	Folder.Edit.Review		X	X
Delete a folder	Folder.Delete			X
Move a folder	Folder.Edit			X
Close/unclose a folder	Folder.Open/Folder.Close		X	X
Freeze/unfreeze a folder	Folder.Freeze/Folder.Unfreeze			X
Cancel or expire a folder	Folder.Edit		X	X
Rescind or make a folder obsolete	Folder.Edit		X	X
Undo a folder's obsolescence status	Folder.Edit		X	X
Undo a folder's cutoff status	Folder.UndoCutoff			X
Review a folder	Admin.PerformPendingReviews		X	X
Mark a folder as reviewed	Folder.Edit		X	X
Set dates (activation, expiration, delete, and approval) for a folder	Folder.Edit		X	X
Assign or remove supplemental markings on a folder	Folder.Edit		X	X

Task	Required RM Right	User	Officer	Admin
Apply a disposition rule to one or many folders	Category.Edit			X

B.1.12 Content

The following table describes the default rights assigned to the default roles for tasks involving content.

Task	Required RM Right	User	Officer	Admin
Create or check in an item	Record.Create	X	X	X
Search for an item	Record.Read	X	X	X
Link items	Record.CreateLink	X	X	X
Unlink items	Record.Unlink		X	X
Download a content item for viewing	Record.Read	X	X	X
View information about content	Record.Read	X	X	X
View the life cycle of an item, the review history of an item, the classification history of an item or the metadata history of an item	Record.Read	X	X	X
Edit the review information for an item	Record.EditReview		X	X
Review the classification of an item	Record.Edit		X	X
Delete the metadata history of an item	Record.DeleteHistoryFile		X	X
Delete an item	Record.Delete			X
Freeze/unfreeze a folder	Record.Freeze/Record.Unfreeze			X
Cancel or expire an item	Record.Edit		X	X
Rescind or make an item obsolete	Record.Edit		X	X
Undo an item's obsolescence status	Record.Edit		X	X
Move an item to another category or folder.	Record.Edit		X	X
Edit record metadata before cutoff. Note: non-record metadata can be edited after cutoff as well as before.	Record.UndoCutoff			X
Upgrade or downgrade an item's classification status	Record.Upgrade/Record.Downgrade		X	X
Review an item	Admin.PerformPendingReviews		X	X
Remove supplemental markings	Record.Edit		X	X
Undo the cutoff status of an item	Record.UndoCutoff			X
Undo the record status of an item	Record.UndoRecord			X

B.1.13 Disposition Rules

The following table describes the default rights assigned to the default roles for tasks involving disposition rules.

Task	Required RM Right	User	Officer	Admin
View disposition information	Category.Read	X	X	X
Enable/disable user-friendly captions	Admin.RecordManager			X
Create a rule	Category.Create			X
Edit a rule	Category.Edit			X
Delete a rule	Category.Delete			X
Define a custom disposition rule	Admin.CustomDispositionActions			
Disabling a disposition rule	Admin.CustomDispositionActions			

B.1.14 Archiving

The following table describes the default rights assigned to the default roles for tasks involving archiving.

Task	Required RM Right	User	Officer	Admin
Import an archive	Admin.RetentionSchedulesArchive and other rights for specific items in the import			X
Export an archive	Admin.RetentionSchedulesArchive and other rights for specific items in the export			X

B.1.15 Screening

The following table describes the default rights assigned to the default roles for tasks involving screening.

Task	Required RM Right	User	Officer	Admin
Enable/disable user-friendly captions	Admin.RecordManager			X
Screen a category, folder, or content	Admin.Screening			X

B.1.16 Audit Trails

The following table describes the default rights assigned to the default roles for tasks involving audit trails.

Task	Required RM Right	User	Officer	Admin
Configure the audit trail	Admin.Audit			X
Choose metadata fields to audit	Admin.SelectMeta			X
Generate and view an audit trail	Admin.Audit			X
Search an audit trail or an archived audit trail	Admin.Audit			X
Set default metadata for audit trail check-in	Admin.Audit			X
Check in and archive audit trail	Admin.Audit, Admin.RecordManager			X

B.1.17 Links

The following table describes the default rights assigned to the default roles for tasks involving the configuration of links. Rights involved in using links are noted in "Content" on page B-5.

Task	Required RM Right	User	Officer	Admin
Add a custom link type	Admin.ConfigureLinkTypes			X
Edit a custom link type	Admin.ConfigureLinkTypes			X
Delete a custom link type	Admin.ConfigureLinkTypes			X

B.1.18 Reports

The following table describes the default rights assigned to the default roles for tasks involving the configuration of reports.

Task	Required RM Right	User	Officer	Admin
Create a user, role, group, or user-group report	Admin.Reports			X

B.1.19 Customization

The Rma.Admin.Customization right is required to create custom dispositions, custom reports, or custom barcode actions. This right is not assigned by default to any role.

A detailed knowledge of services and their uses is required in order to customize your system.

B.1.20 General Configuration

The following table describes the default rights assigned to the default roles for tasks involving general product configuration.

Task	Required RM Right	User	Officer	Admin
Set the fiscal calendar	Admin.RecordManager			X
Perform disposition actions (process events)	Admin.RecordManager			X
Specify default review recipients	Admin.RecordManager			X

B.2 Physical Content Management Rights and Roles

This section describes the rights and roles for tasks encountered while using Physical Content Management.

The default roles provided with PCM are **pcmrequestor** (Requestor) and **pcmadmin** (PCM Admin).

B.2.1 Physical Item Management

The following table describes the default rights assigned to the default roles for tasks involving physical items.

Note that the ability to freeze or screen physical items are not enabled by default for any role. The menu options to perform these tasks are not visible until those rights are assigned to a role.

Task	Required RM Right	Requestor	Admin
View information about physical items	PCM.Physical.Read and PCM.Storage.Read	X	X
Create (check in) a physical item	PCM.Physical.Create and PCM.Storage.Read	X	X
Edit a physical item	PCM.Physical.Edit and PCM.Storage.Read	X	X
Move a physical item	PCM.Physical.Edit, PCM.Physical.Move and PCM.Storage.Read		X
Delete a physical item	PCM.Physical.Delete and PCM.Storage.Read		X
Search physical items	PCM.Physical.Read and PCM.Storage.Read	X	X
Print labels for physical items	PCM.Admin.PrintLabel		X
Freeze or unfreeze physical items	Record.Freeze/Record.Unfreeze		
To manually override freeze errors	Admin.PerformActions		
To screen for physical items	Admin.Screening		

B.2.2 Storage Space

The following table describes the default rights assigned to the default roles for tasks involving storage locations.

Note that the ability to import a storage hierarchy is not enabled by default for any role. The menu option to perform this task is not visible until that right is assigned to a role.

Task	Required RM Right	Requestor	Admin
View information about locations	PCM.Storage.Read	X	X
Create a location	PCM.Storage.Create		X
Edit a location	PCM.Storage.Edit		X
Delete a location	PCM.Storage.Delete		X
Reserve a location	PCM.Storage.Reserve	X	X
Block a location	PCM.Storage.Block		X
Print labels for a location	PCM.AdminPrintLabel		X
Import batch-created storage hierarchy	Admin.RetentionScheduleArchive		

B.2.3 Location, Media, and Object Types

The following table describes the default rights assigned to the default roles for tasks involving the creation of location, media, and object types.

Task	Required RM Right	Requestor	Admin
Set up location types	PCM.Admin.Manager and PCM.Admin.LocationTypes		X
Set up object types	PCM.Admin.Manager		X

Task	Required RM Right	Requestor	Admin
Set up media types	PCM.Admin.Manager		X
Set up custom metadata fields	PCM.Admin.Manager		X

B.2.4 Reservations

The following table describes the default rights assigned to the default roles for tasks involving reservations.

Task	Required RM Right	Requestor	Admin
View reservation information	PCM.Reservation.Read	X	X
Create a reservation request	PCM.Reservation.Create	X	X
Edit a reservation request	PCM.Reservation.Edit		X
Delete a reservation request	PCM.Reservation.Delete		X
Process a reservation request	PCM.Reservation.Process		X
Run a reservation request report	PCM.Admin.Manager		X
Configure default metadata for reservations	PCM.Admin.Manager		X

B.2.5 Chargebacks

The following table describes the default rights assigned to the default roles for tasks involving chargebacks.

Task	Required RM Right	Requestor	Admin
Set up chargeback types, payment types, and customers	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
View information about chargebacks (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Read		X
Create chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Read		X
Edit chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Edit		X
Delete chargeback items (transactions, invoices, and so on)	PCM.Admin.Manager, CBC.ChargeBacks.Admin and CBC.ChargeBacks.Delete		X
Screen for charges	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
Browse invoices	PCM.Admin.Manager and CBC.ChargeBacks.Admin		X
Print invoices	PCM.Admin.Manager and CBC.ChargeBacks.PrintInvoice		X
Adjust invoices	PCM.Admin.Manager and CBC.ChargeBacks.Adjust		X

B.2.6 Barcodes

The following table describes the default rights assigned to the default roles for tasks involving barcodes and barcode labels.

Task	Required RM Right	Requestor	Admin
Process barcode files	PCM.Barcode.Process		X
Print labels for users, storage locations, and physical locations	PCM.Admin.PrintLabel		X

B.2.7 General Configuration

The following table describes the default rights assigned to the default roles for tasks involving general configuration options.

Task	Required RM Right	Requestor	Admin
Configure the PCM environment	PCM.Admin.Manager		X
Run batch services	PCM.Admin.Manager		X

C

Customizing Your System

In addition to the configuration available with the software you can create your own customized barcodes, custom disposition actions and custom reports.

> **Important:** Creating custom disposition actions, custom barcodes or custom reports requires in-depth technical knowledge of Content Sever. Contact Consulting Services for more information before proceeding.

This chapter covers the following topics:

C.1 Custom Disposition Actions

> **Important:** If custom dispositions were previously created using an older version of Oracle URM, those dispositions should be re-examined and updated to use the newest services and actions. The Action Service parameters have changed from previous versions of this software and any changes to existing custom dispositons are not mapped automatically.

Disposition actions are used in disposition instructions, which define the sequence of actions to be performed on content during its life cycle. A large number of built-in disposition actions are included, including Cutoff, Destroy, Transfer, Move, Declassify.

Your environment may require disposition actions other than the predefined options. You can set up disposition actions to reflect your organization's specific needs.

Custom disposition actions are based on Oracle UCM services, which can be called with specific parameters to define the behavior of the disposition actions. For example, you could create a disposition action to automatically retain the last three revisions of content items using the DELETE_ALL_BUT_LAST_N_REVISIONS_SERVICE service with the 'NumberOfRevisions=3' parameter.

Important: Custom disposition features are available only to users with the Rma.Admin.Customization right. By default, this right is not assigned to any of the predefined roles. You must assign it to a role before this functionality is exposed.

This section covers the following topics:

- "Managing Custom Dispositions" on page C-2
- "Disabling Custom Disposition Actions" on page C-5
- "Deleting a Custom Disposition Action" on page C-4

C.1.1 Managing Custom Dispositions

The following tasks are used when managing dispositions:

- "Creating or Editing a Custom Disposition Action" on page C-2
- "Viewing Custom Disposition Action Information" on page C-4
- "Deleting a Custom Disposition Action" on page C-4

C.1.1.1 Creating or Editing a Custom Disposition Action

Use this procedure to create a custom disposition action. For example, you may need a disposition action that retains the last three revisions of a content item.

Important: Creating custom disposition actions requires in-depth technical knowledge of Oracle UCM. Contact Consulting Services to define custom disposition actions.

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

   The Configure Dispositions Page is displayed.

2. Click **Add** in the Custom Disposition Action area.

   The Create or Edit Disposition Action Page is displayed.

3. Enter a unique ID for the custom disposition action in the **Action ID** text box.
4. Enter a name for the custom disposition action in the **Action Name** text box.
5. Enter a description for the custom disposition action in the **Brief Description** text box.
6. Enter a group name for the custom disposition action in the **Group Name** text box.
7. Select the service to be used for the custom disposition action from the **Action Service** list.
8. (Optional) Specify one or more parameters for the selected action service.

9. (Optional) Select or clear any of the boxes as required. Selections include **Must Be First**, **Must Be Last**, **Require Approval**.
10. Click **Create**.

    A message is displayed saying the disposition action was created successfully, with the action information.
11. Click **OK**.

The following Action Service Parameters are required for the specific ActionService:

Disposition/Event	Service Paramters
Superseded	isScrub=1
Delete All Revisions (Destroy Metadata)	NumberOfRevisions=0, isDestroy=1, dRevRank=0
Delete Revision	NumberOfRevisions=0, isDestroy=1
Mark Transfer Completed	NumberOfRevisions=0, isDestroy=1, dRevRank=0
Mark Move Completed	NumberOfRevisions=0, isDestroy=1, dRevRank=0
Mark Accession Completed	NumberOfRevisions=0, isDestroy=1, dRevRank=0
Delete Previous Revision	NumberOfRevisions=1
Delete Old Revision	NumberOfRevisions=1
Mark Archive Completed	NumberOfRevisions=0, isDestroy=1, dRevRank=0
Archive Leave Metadata	isScrub=1
Mark Accession Completed (leave metadata)	isScrub=1
Mark Move Completed (leave metadata)	isScrub=1
Mark Transfer Complete (leave metadata)	isScrub=1
Mark Delete Revision Completed	NumberOfRevisions=0, isDestroy=1
Delete Complete	NumberOfRevisions=0, isDestroy=1
Mark Transfer Completed (prompt to keep or delete metadata)	NumberOfRevisions=0, isDestroy=1
Mark Move Complete (prompt to keep or delete metadata)	NumberOfRevisions=0, isDestroy=1
Mark Accession Complete (prompt to keep or delete metadata)	NumberOfRevisions=0, isDestroy=1
Mark Archive Complete (prompt to keep or delete metadata)	NumberOfRevisions=0, isDestroy=1
Mark Related Content	IsMarkAllRelations=1

To edit a custom disposition action, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

The Configure Dispositions Page is displayed.

2. Click **Edit Action** from a disposition **Action** menu.

   The Create or Edit Disposition Action Page is displayed.

3. Make modifications as required, and click **Submit Update** when you finish.

   A message is displayed saying the disposition action was created successfully, with the action information.

4. Click **OK**.

C.1.1.2 Viewing Custom Disposition Action Information

Use this procedure to view the information about a custom disposition action.

> **Permissions:** The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

To view the information about a custom disposition action, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

   The Configure Dispositions Page is displayed.

2. Click the disposition name to view.

   The Disposition Action Info Page is displayed.

3. When you finish viewing the information, click **OK**.

C.1.1.3 Deleting a Custom Disposition Action

> **Permissions:** The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

You can only delete custom disposition actions if they are no longer being used in the disposition instructions for any category. If you attempt to delete a disposition action still in use, an error message is displayed.

To delete a custom disposition action, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

   The Configure Dispositions Page is displayed.

2. Click **Delete Action** from a disposition's Item Actions menu. You can also click the checkbox by the action name and click **Delete** from the Table menu.

   A message is displayed saying the disposition action was deleted successfully.

3. Click **OK**.

To delete multiple dispositions, click the checkbox for the dispositions to delete on the Configure Dispositions Page and click **Delete** from the Table menu.

C.1.2 Disabling Custom Disposition Actions

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

Important: Some dispositions are required for processing of instructions to occur. Disabling a disposition could interfere with the processing of disposition instructions. Always verify ahead of time that it is acceptable to disable a disposition.

To disable a custom disposition action, complete the following steps:

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Disable**.

   The Disposition Actions Configuration Page is displayed.

2. Select the checkbox next to the actions which should be disabled and made unavailable for use.

3. Click **Submit Update** when done.

C.1.3 Creating a Custom Disposition Action Example

This example creates a custom disposition action that automatically retains the last three revisions of a content item.

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

1. Click **Records** then **Configure** from the Top menu. Click **Disposition Actions** then **Custom**.

   The Configure Dispositions Page is displayed.

2. In the Custom Disposition Action area, click **Add**.

   The Create or Edit Disposition Action Page is displayed.

3. Complete the metadata fields as follows:

   a. In the **Action ID** field, type `RetainLast3Rev`.

   b. In the **Action Name** field, type `Retain Last 3 Revisions`.

   c. In the **Brief Description** field, type `Only keep the last 3 revisions of a content item`.

   d. In the **Group Name** field, type `Custom`.

e. From the **Action Service** list, click DELETE_ALL_BUT_LAST_N_REVISIONS_SERVICE.

f. In the **Action Service Parameters** field, type `NumberOfRevisions=3`.

g. Click the **Require Approval** and **Allow Scheduling** boxes.

4. Click **Create**.

The newly created disposition action can now be selected from the list of available disposition actions when creating disposition rules.

C.1.4 Creating Disposition Rules for Physical Content

Physical items can be assigned retention schedules, which define their life cycle. When creating a physical item you can assign a retention schedule to it. 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 you may also define disposition rules specifically for physical items.

C.2 Using Custom Barcodes

The PCM software is shipped with a default set of barcodes ranges and barcode transaction types (check in, check out and set locations). You can add your own set of barcode numbers to coincide with the system in place at your site and use them to provide additional custom functionality. After adding the numbers, a customized service must be created to use the new functionality. Consulting Services should be used to design this service.

You can also customize the system to process barcode files that are in a format other than the standard format used by PCM. This is done by altering a processing file to accomodate the format in use at your site. A detailed knowledge of Idoc script is required to customize the processing file used to upload barcode data.

Note that PCM barcodes are prefixed with a value when printing that should be stripped before processing. User barcodes are prefixed with "U", storage barcodes with "S", and object barcodes with "O".

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed.

C.2.1 Adding a Custom Barcode Range

Use this procedure to add custom barcode ranges.

1. Click **Physical** then **Configure** then **Function Barcodes** from the Top menu.

   The Configuring Custom Barcode Page is displayed.

2. Click **Add**.

   The Create Custom Barcode Dialog is displayed.

3. Enter the barcode and the activity or event associated with the barcode (for example, Inventory or Storage Disposal). Custom codes must be a number between 7000 and 9999. Click **OK** when done.
4. The Configuring Custom Barcode Page is displayed showing the new barcode in the listing.

After defining the barcode range, contact Consulting Services to define a service called by the custom barcodes. The type of service used will vary depending on the type of functionality defined.

C.2.2 Processing Non-Standard Barcode Data

Important: A detailed knowledg of Idoc Script is required to customize the file that processes barcode data. Contact Consulting Services for more assistance if needed.

Barcode processing in PCM uses code written with Idoc script in a *processing file* to evaluate each line in a *data file*. The processing file can be modified to customize how the system parses and processes the barcode data files.

The processing file is stored in the barcode\resources directory and is named barcode_process_resource.htm.

The following is an example of a standard barcode data file:

```
H YYYYMMYYHHMMSS 00 0000000000       - Header
20050721125151 00 1000                - Transaction code
20050721125201 00 URMUSER             - Location
20050721125204 00 OB1                 - Object to be processed
20050721125204 00 OB2                 - Object to be processed
T 000                                 - Footer
```

C.2.2.1 Header and Footer Information

The header line in the standard data file begins with the value "H" and is ignored by the processing file. This can be customized if a header line is different or if one is absent. To modify this, change the `barcodeHeaderStartsWith` variable in the barcode environment file.

The standard footer line in the data file begins with "T 000". When the processing file encounters this notation, processing stops and the processed data is uploaded. The `barcodeFooterStartsWith` variable can be changed to indicate a different footer type.

C.2.2.2 Data Information

Each line in the file that is not a Header or a Footer is parsed as data. Each valid transaction must have a Transaction Code, a Location, and Items to assign to the location.

C.2.2.2.1 Transaction Codes Three default transaction codes are available:

- 1000: check in
- 2000: check out

- 3000: set permanent and actual locations; this can also be used as a check-in transaction.

As noted in Adding a Custom Barcode Range you can also create custom Transacton Codes. If custom codes are used, the location must be set to a user, storage item or object (for example, a box, folder, or tape).

The Transaction Date (dTransDate) and the Transaction Type (dTransType, which is the code designation of 1000, 2000, 3000, or custom number) must be set in the processing file. The following values should be cleared in the processing file:

- Location Type (dLocationType)
- Location (dLocation)
- Object Type (dExtObjectType)
- Barcode (dBarcode)
- Barcode Date (dBarcodeDate). Dates must bein the format MM/dd/yyyy HH:MM:SS.

The following variables should be set to FALSE:

- Barcode Transaction Location (barcodeTransLocation)
- Barcode Item (barcodeItemSet)

C.2.2.2.2 Location The dLocationType and dLocation values must be set in order to set the location. In addition, the `barcodeTransLocation` variable must be set to TRUE. This indicates that a location has been set for the current transaction.

If the location is a user, dLocationType must be set to `wwUser`. If the location is a storage location, dLocationType must be set to `wwStorage`. If the location is an object, dLocationType can be left blank and the processing code will determine the object type of the object during processing.

Multiple items can be assigned to the same location with one transaction. If the value for barcodeTransLocation is set to TRUE, it is assumed that the item being processed is an object being assigned to the current location set earlier. Make sure the barcodeItemSet value is set to TRUE after each item is parsed so it is processed.

C.2.2.2.3 Ojbect To set the item, set dBarcode and dBarcode Date values. Also set barcodeItemSet to TRUE. This indicates that an item is ready to be processed.

C.3 Adding a Mobile Bar Code Reader

This section describes the steps needed to install bar code scanner software on a mobile device which can be enabled for that functionality. Consult the device documentation for complete details about installing and enabling software on the device.

The following files are needed for installation. Note that Windows Mobile version 5.0 is currently the only supported version:

- BarcodeUtilityMobile.cab: installed with the PCM software and usually found at *IntradocDir*\ucm\urm\config\MobileEdition. This must be installed on the mobile device.
- The following files to be installed on the computer:
  - Microsoft ActiveSync, version 4.1 or later

- The .NET Compact Framework 2.0 sp2 Redistributable file. This should already be installed .
- The Symbol Managed Class Libraries. Download the file from the following location:

  http://support.symbol.com/support/search.do?cmd=displayKC&docType=kc&externalId=11683&sliceId=&dialogID=163824222&stateId=1%200%20163812949

  Install the file. After installation, the file will be stored on the local disk in C:\Program Files\Symbol Mobility Developer Kit for .NET\v1.7\SDK\Smart Devices\wce500\armv4i.

Depending on the type of device and the software downloaded, usage instructions may vary. The following are general instructions for use. See the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management* for details about using default scanner wands and for background information about bar codes.

1. Start the application on the mobile device.
2. A login screen is displayed. After logging in, a Direct Scan window is displayed on the device.
3. Scan items and click the **Process** icon.
4. A Results screen is displayed, showing the effects of scanning.

The following menu options are available from the main menu on the Direct Scan window:

- Real-time processing: used to process and immediately upload data
- Save transaction code: used to temporarily save a transaction
- Options: used to set different defaults (for example, upload time out or the application locale)

On the Results screen, two different views are available: **List**, to display a text list of all transations and **Detail**, a table list of all transactions.

C.4 Creating Custom Reports

Permissions: The Rma.Admin.Customization right is required to perform this task. This right is not assigned by default to any of the predefined roles, which means you must assign it to a role before this functionality is exposed. To create custom reports with a report source type of Query, a user must also have the Rma.Admin.NoSecurity right.

Customized reports can be created to tailor data presentation for your site. Data is gathered for the report, a report template is chosen, the data is populated, and the report is generated. The data is gathered in XML format then formatted for use using a template. This process allows you to keep the data separate from the presentation of the data.

Several default reports and templates are provided when you install Oracle URM. You can create new reports by using the current reports as a base then editing them, or you can create entirely new reports.

When creating custom reports, content on Oracle URM Adapter systems is not included in the report even if the content is managed by Oracle URM. To generate reports concerning Adapter content, run the reports on the Oracle URM Adapter system.

This section describes how to create customized reports using Oracle UCM services and queries. To create reports about users and content using the default reports provided with the software, see the *Oracle Fusion Middleware Administrator's Guide for Universal Records Management*.

In order to create new templates, the Oracle BI Publisher functionality must be purchased and installed. This documentation describes how to use the default templates provided with the system. For details about creating new templates or editing the default templates, see the BI Publisher documentation.

After you have created a new template, you can add it to the list of available templates for others to use. You can check in the templates used to create reports and you can check in the reports themselves (that is, a report with data included). These are separate checkins, thus keeping data separate from the report format.

A similar interface is used to create the different elements of a report (report type, template, report sources).

Click **Browse Content** then **Custom Physical Reports** or **Custom Record Reports** to access reports that have been created.

Note that user permissions are needed to access the data for a report as well as permissions to the report itself. Therefore, if two different people run a report, they might see different results depending on their rights.

Follow this procedure to create a custom report using default templates and sources.

1. Click **Records** then **Configure** then **Reports** to create a report for content items. Click **Physical** then **Configure** then **Reports** to create reports for physical items.

   Click **Create New Report**.

   The Configure Report Element Page is displayed.

2. Choose the type of report you wish to create. Click **Configure**.

   A Report Checkin Page is displayed.

3. Enter content information for the report as required at your site. Also enter the following report-specific information for the report:

   - **Report Template**: Choose a template from the dropdown list or click **Add New** to create a new template. See "Creating Custom Templates" on page C-11 for details about creating a new template.
   - **Report Format**: Choose a format from the dropdown list. If creating a barcode report, use PDF as your format type. Choices include:
     - System
     - User
     - HTML
     - PDF
     - RTF
     - XLS

- **Report Source Type**: Choose the type of source to use to gather the data for the report. Options include:
  - Service: use Oracle UCM services to build the report data.
  - Query: use Oracle UCM queries to gather data.
  - Dynamic Query: use a dynamic query to gather data. If Services or Query are chosen, the correct service or query must be used to work with the template. A dynamic query will gather the appropriate data for use.
- **Report Source**: Choose a previously configured report source for the data or click **Add New** to create a new source using the Configure Report Sources Page. See "Creating or Editing New Report Sources" on page C-11 for details.

C.4.1 Creating Custom Templates

Follow this procedure to edit or create a new custom template. Note that templates are files that can be checked in and checked out of the system. They are treated as content items.

For details about creating a new template without using an existing template as a guide, see the BI Publisher documentation.

1. Click **Records** then **Configure** then **Reports** to create a template for content items. Click **Physical** then **Configure** then **Reports** to create reports for physical items.

   Click **Templates**.

   The Configure Report Element Page is displayed.

2. Choose the type of template you wish to create. Click **Configure**.

   A Report Templates Page is displayed.

3. The following options are available:
   - To create a new template based on an existing template, click **Get Native File** from the **Action** menu of the template to be used. You can then save the file, edit the file as needed, and check it in as a new template.
   - To check out and edit an existing template, click **Check Out** from the **Action** menu of the template to be used. Save the file, edit it, then check it back in to the system.
   - If you have a template and would like to check it in using similar metadata as another template, click **Check In Similar** from the **Action** menu of the template with metadata to be copied.

Additional options on this page can be used to freeze or unfreeze template files, add files to a folio or Content Basket for later use, set dates for processing files, or create reports from a template.

C.4.2 Creating or Editing New Report Sources

Important: Creating custom report sources requires in-depth technical knowledge of services and queries. Contact Consulting Services for further assistance if needed.

Follow this procedure to edit report sources.

1. Click **Records** then **Configure** then **Reports** to edit sources for a report for content items. Click **Physical** then **Configure** then **Reports** to edit sources for reports for physical items.

   Click **Report Sources**.

   The Configure Report Element Page is displayed.

2. Choose the report whose sources will be altered. Click **Configure**.

   The Configure Report Sources Page is displayed.

3. To use this screen, highlight a query or a service on the left side of the screen. Click the right arrow to move the query or service to the right column for use.

   To remove a query or service from use, highlight the name and click the left arrow to move the item to the left column.

4. Click **Update** when done. The report sources for that particular type of report are altered and will be used the next time the report is run.

Follow this procedure to create a new report source:

1. Use the previously described procedure to create a new report.
2. Click **Add New** in the Report Source section of the Report Checkin Page.
3. A dialog opens. Follow the previously described procedure to add queries and services for the new source.
4. Click **OK** when done. The report source is added and is available for use with the new report.

C.4.3 Downloading a BI XML Data File

You can use the provided XML data files in conjunction with BI Publisher to customize report templates Using the XML data file, you can import data into a Word document and then edit the template to create a specialized report.

Follow this procedure to select a XML data file.

1. Click **Records** or **Physical** then **Configure** from the Top menu. Click **Reports** then **Download BI XML Data**.

   The Configure Report Element Page is displayed.

2. Choose the type of XML data file to download. Click **Download**.

   The XML Data Dialog is displayed.

3. You can open the data file to examine the contents in a browser window or you can save the file for later use.
4. Click **OK** when done.

Glossary

accession

The transfer of legal and physical custody of permanent content to the National Archives.

audit trail

An electronic means of tracking interactions with content items in a system so that any access to the content item within the system can be documented as it occurs or afterward. An audit trail may be used to identify unauthorized actions in relation to the items (for example, modification, deletion, or addition).

category

A description of a particular set of content items within a retention schedule. Each category has retention and disposition data associated with it, applied to all content items within the category.

classified record

An item that requires protection against unauthorized disclosure (for example, because it contains information sensitive to the national security of the United States). See also: unclassified content, declassified record.

classification guide

A mechanism that defines default values for several classification-related metadata fields on the content check-in page for content. This enables convenient implementation of multiple classification schemes.

classification markings

Identifications or markings that leave no doubt about the classified status of the information, the level of protection required, and the duration of the classification.

create

To file a new electronic content item and its associated metadata.

current item

Active content item. A content item necessary to conduct current business, and therefore is generally maintained in an office space.

See also: noncurrent content item, semi-current record, permanent item.

custom disposition action

A disposition action defined by Records Administrators, as opposed to a disposition action that is built into the product.

See also: disposition action.

custom period

A period defined by Records Administrators, as opposed to a period that is built into the product.

See also: period.

custom security fields

Optional layer of security in addition to supplemental markings. As with supplemental markings, users must match the metadata field value to be allowed access to content. However, custom security fields allow you to configure *any* custom field (except date fields) that should be matched by a user rather than a designated supplemental marking. Also, custom security fields are enforced only at the content level whereas supplemental markings can be set at the content or record folder level.

custom supplemental markings

See: custom security fields.

custom trigger

A trigger defined by Records Administrators, as opposed to a trigger that is built into the product.

See also: trigger.

cutoff

The moment that the status of a content item changes and the content item goes into disposition. A content item may be cut off after a specific period, at a specific event, or after an event. Content items need to be cut off before they can be processed further in accordance with their disposition rules, for example, destroyed, transferred to an external storage facility, and so on

cycle

The periodic replacement of obsolete copies of content that is subject to review with copies of current content that is subject to review. This may occur daily, weekly, quarterly, annually, or at other designated intervals as specified by regulations or by the records administrator.

declassified record

Content that was formerly classified, but whose classified status has been lifted.

See also: classified record, unclassified content.

declassification

The authorized change in the status of information from classified to unclassified.

See also: downgrade, regrade, upgrade.

disposition

All actions to be taken when a retention period of a content item has ended and it has reached a designated disposition date.

disposition action

An individual operation to be performed when a retention period of a content item has ended and it has reached a designated disposition date.

disposition authority

Legal authority that empowers a United States Government agency to dispose of temporary items, or to transfer permanent items to the National Archives. The disposition authority for permanent content must be obtained from NARA. For certain temporary content, the authority must also be obtained from the General Accounting Office (GAO).

disposition instruction

A set of individual actions that are to be performed when a retention period of a content item has ended and it has reached a designated disposition date.

downgrade

Determination by a declassification authority that information classified at a specified level shall be classified and safeguarded at a lower classification level.

See also: declassification, regrade, upgrade.

electronic record

An item stored in a form that a computer can process. Electronic items are also referred to as machine-readable content items.

event disposition

A disposition instruction in which an item is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention period is applied.

See also: time disposition, time-event disposition.

external item

A content item, physical or electronic, whose source file is not specifically stored in Oracle URM. Oracle URM can be used to track and search metadata associated with the external file, including disposition schedules, and can even manage an electronic rendition of an external file. An electronic rendition can be checked in as a primary file of an external content item, or be filed as a separate file, and then linked to the external file metadata.

See also: internal item.

file plan

See: retention schedule.

folder

A collection of similar items in the retention schedule. This allows the items to be organized into groups. Record folders can be nested within other record folders.

FRC

Federal Records Center. A facility operated by NARA for low-cost storage and servicing of Federal records that are pending disposal or transfer to the National Archives.

freeze

To pause disposition processing of a content item or record folder due to special circumstances, such as a lawsuit, court order, or investigation. Freezing content items temporarily extends an approved retention period.

inactive record

See noncurrent content item.

internal item

An electronic item stored within Oracle URM.

See also: external item.

link

A defined relationship between content items. This may be useful when content items are related and need to be processed together.

media type

The material or environment on which the information of a content item is inscribed (for example, microform, electronic, paper).

metadata

Data describing stored data; that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic content items.

move

To transfer content and metadata out of the records management system.

See also: accession, transfer.

NARA

National Archives and Records Administration. Records repository for permanent records continually preserved by the Federal Government. The Archivist of the United States determines the historical or other value of content and deems the item as permanent.

See also: FRC.

noncurrent content item

Items no longer required to conduct business and therefore ready for final disposition.

See also: current item, semi-current record, permanent item.

original classification

An initial determination that information requires protection against unauthorized disclosure (for example, in the interest of national security).

originating organization

Official name or code identifying the office responsible for the creation of a document.

period

The segment of time that must pass before a review or disposition action can be performed. Several built-in periods (for example, "one year") are available, but you also can create custom periods to meet your unique business needs.

permanent item

Content appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are normally needed for administrative, legal, or fiscal purposes. Content that is not authorized for destroying is retained permanently.

privileged user

An individual who is given special permission to perform functions beyond those of typical users.

publication date

The date and time that the author or originator completed the development of, or signed the document. For electronic documents, this date and time should be established by the author or from the time attribute assigned to the document by the application used to create the document. This is not necessarily the date or time that the document was filed in the system.

record

Any content item whose disposition and location must be tracked and maintained according to an organization's requirements. Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics. In this documentation, this term is synonymous with 'content'.

record folder

See: folder.

retention schedule

The collective set of the series, categories, folders, or content item contained in a hierarchical structure.

See also: category.

records management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creating, maintenance (use, storage, retrieval), and disposal, regardless of media.

records manager

An individual who is responsible for records management administration.

regrade

A determination by a classification or declassification authority that information classified and safeguarded at a specified level requires a different level of classification and safeguarding.

See also: declassification, downgrade, upgrade.

rendition

Replication of a content item that provides the same content but differs from the reference because of storage format or storage medium (for example, an HTML version generated from an original Word document).

rescind

To made void by an enacting authority.

retention period

Length of time that a content item must be kept in its repository before the item can enter its final disposition instruction, such as destroy or archive.

screening

The process of aggregating and reviewing content items for management, review, and disposition purposes.

semi-current record

Content so seldom required that it should be moved to a holding area or to a records center.

See also: current item, noncurrent content item, permanent item.

series

A collection of retention categories in the retention schedule. You cannot file content items directly into a series; you must file the items into a category or retention folder.

subject to review

Essential agency or private-sector business content items required to meet operational responsibilities in the event of a national security emergency or other emergency or disaster. Items subject to review also protect the legal and financial rights of the Government, businesses in the private sector, and individuals affected by the actions of Government and business. These content items are subject to periodic review and update. Also referred to as "essential content."

supersede

To supplant, or displace, an item by another item that is more recent or improved (superior).

supplemental markings

Document markings not related to classification markings per se, but which elaborate or clarify document handling. Supplemental markings can be set at the content or record folder level, and can be used to restrict user access to content or folders.

See also: custom supplemental markings.

temporary item

Content approved by NARA for disposal, immediately or after a retention period. Also referred to as "disposable item."

time disposition

A disposition instruction specifying when a content item is cut off, after which a fixed retention period is applied before disposition.

See also: event disposition, time-event disposition.

time-event disposition

A disposition instruction specifying that a content item is disposed of a fixed period after a predictable or specified event. After the specified event has occurred, then the retention period is applied.

See also: event disposition, time disposition.

transfer

The process of moving content from one location to another; particularly, from an office space in which it is used to storage facilities for temporary or permanent preservation. The legal and physical custody of transferred content is not affected (as opposed to accession).

See also: accession, move.

trigger

An event that must take place before a disposition instruction is processed. They are associated with disposition rules for retention categories. Examples of triggering events include changes in state, completed processing of a preceding disposition action, and retention period cutoff.

unclassified content

Content that is not and has never been classified.

See also: classified record, declassified record.

upgrade

Determination by a declassification authority that information classified at a specified level shall be classified and safeguarded at a higher classification level.

See also: declassification, downgrade, regrade.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X