

Oracle® WebCenter Content

Setup Guide for Records

11g Release 1 (11.1.1)

E10640-03

November 2011

Oracle WebCenter Content Setup Guide for Records, 11g Release 1 (11.1.1)

E10640-03

Copyright © 2010, 2011 Oracle and/or its affiliates. All rights reserved.

Primary Author: Jean Wilson

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

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xvii
Audience	xvii
Documentation Accessibility	xvii
Related Documents	xvii
Conventions	xviii
1 Introduction	
1.1 About This Guide	1-1
1.2 About This Product	1-1
1.3 What's New	1-2
1.3.1 Conceptual Changes in this Product	1-4
1.3.2 Documentation Changes in this Product	1-4
1.4 Using Help	1-4
1.4.1 Tooltips	1-4
1.4.2 Quick Help	1-5
2 Understanding Retention Management	
2.1 Management of Retained Items	2-1
2.1.1 What To Retain	2-1
2.1.2 Lifecycle for Retained Content	2-2
2.1.3 Types of Retained Content	2-3
2.1.3.1 Internal and External Retained Content	2-3
2.1.3.2 Classified, Unclassified, Declassified Content	2-3
2.1.3.3 Non-Permanent, Transfer or Accession, and Reviewed Content	2-4
2.2 Basic Retention Management Concepts	2-4
2.3 Physical Content Management	2-6
2.4 Interaction with Oracle WebCenter Content	2-6
2.5 Basic Retention Processes	2-7
3 Setting Up the Software	
3.1 Usage Notes	3-2
3.2 Fusion Middleware Security Considerations	3-2
3.2.1 Oracle WebCenter Content Security Considerations	3-2
3.2.2 WNA Redeployment	3-3
3.2.3 Configuration for External LDAP Authentication Provider	3-4

3.2.4	Configuration for SSL	3-4
3.2.5	Configuration for Single Sign-On Use	3-5
3.2.6	Configuring for Web Services Use	3-5
3.3	Software Configuration.....	3-5
3.4	Retention Setup Checklist.....	3-7
3.5	Retention Management Options.....	3-7
3.6	Security Overview	3-9
3.6.1	Security Settings.....	3-9
3.6.2	Classification Security Settings	3-10
3.6.2.1	Supplemental Markings	3-10
3.6.2.2	Security Classifications	3-10
3.6.2.3	Classification Guides.....	3-11
3.6.3	Security Roles and Definitions.....	3-11
3.6.4	Rights for Roles	3-12
3.7	System-Wide Configuration.....	3-12
3.8	Setting Up Physical Content Management	3-13
3.9	Setting Up a Retention Schedule	3-13
3.9.1	Managing a Retention Schedule	3-14
3.9.1.1	Creating a Series	3-14
3.9.1.2	Creating a Retention Category	3-14
3.9.1.3	Creating a Record Folder.....	3-14
3.10	Configuring Content Triggers, Dispositions, and Freezes.....	3-15
3.10.1	Triggers	3-15
3.10.2	Dispositions	3-15
3.10.2.1	Disposition Types	3-16
3.10.2.2	Triggering Events	3-16
3.10.2.3	Retention Periods.....	3-16
3.10.2.4	Disposition Actions	3-16
3.10.2.5	Disposition Rules.....	3-17
3.10.3	Freezes	3-17

4 Interface Overview

4.1	Interface Overview	4-1
4.1.1	Configuring the System	4-1
4.1.2	Configuring Reports.....	4-2
4.1.3	Configuring PCM	4-2
4.2	Individual Page and Actions Menus.....	4-3

5 Security Overview

5.1	Retention Management in an Organization.....	5-1
5.2	Roles.....	5-2
5.3	Tasks and Default Rights for Roles	5-4
5.3.1	Trigger Tasks and Defaults for Predefined RM Roles.....	5-5
5.3.2	Time Period Tasks and Defaults for Predefined Roles.....	5-5
5.3.3	Supplemental Markings Tasks and Defaults for Predefined Roles.....	5-6
5.3.4	Security Classifications Tasks and Defaults for Predefined Roles	5-6
5.3.5	Classification Guides Tasks and Defaults for Predefined Roles.....	5-6

5.3.6	Custom Security Tasks and Defaults for Predefined Roles	5-7
5.3.7	Custom Category or Folder Metadata Tasks and Defaults for Predefined Roles	5-7
5.3.8	Freezes Tasks and Defaults for Predefined Roles	5-7
5.3.9	Series Tasks and Defaults for Predefined Roles	5-7
5.3.10	Retention Category Tasks and Defaults for Predefined Roles	5-8
5.3.11	Folder Tasks and Defaults for Predefined Roles	5-8
5.3.12	Archive Tasks and Defaults for Predefined Roles	5-9
5.3.13	Screening Tasks and Defaults for Predefined Roles	5-9
5.3.14	Audit Trail Tasks and Defaults for Predefined Roles.....	5-9
5.3.15	Disposition Tasks and Defaults for Predefined Roles.....	5-10
5.3.16	Link Tasks and Defaults for Predefined Roles	5-10
5.3.17	Default Report Tasks and Defaults for Predefined Roles	5-10
5.3.18	Content Management Tasks and Defaults for Predefined Roles.....	5-11
5.3.19	Customization Tasks	5-12
5.3.20	Other Common Tasks	5-12
5.4	Common Physical Content Management Tasks and Roles	5-12
5.4.1	Storage Space Tasks and Defaults for Predefined Roles.....	5-13
5.4.2	Reservation Tasks and Defaults for Predefined Roles	5-13
5.4.3	Physical Item Tasks and Defaults for Predefined Roles	5-14
5.4.4	Location, Object, and Media Types Tasks and Defaults for Predefined Roles.....	5-14
5.4.5	Chargeback Tasks and Defaults for Predefined Roles	5-15
5.4.6	Barcode and Label Tasks and Defaults for Predefined Roles	5-15
5.4.7	Additional PCM Administrative Tasks and Defaults for Predefined Roles	5-16
5.5	External Source Management Tasks and Roles	5-16
5.5.1	External Source Tasks and Defaults for Predefined Roles.....	5-16
5.6	Security Groups.....	5-16
5.7	Aliases.....	5-17
5.8	Access Control Lists (ACLs).....	5-17
5.8.1	Setting ACLs During Software Use.....	5-18
5.9	Security Matrix	5-18
5.10	Setting Security Preferences	5-19
5.11	Assigning Rights to User Roles.....	5-20
5.11.1	Setting Rights for Roles.....	5-20
5.12	Default Rights for Roles	5-20
5.12.1	The Series Tab.....	5-21
5.12.2	The Category Tab.....	5-21
5.12.3	Folder Tab	5-21
5.12.4	Record Tab	5-22
5.12.5	Admin Tab	5-22
5.12.6	CBC Tab	5-24
5.12.7	PCM Tab.....	5-24
5.12.8	ECM Tab.....	5-25
5.13	Specifying PCM Barcode Values for Users	5-25

6 Additional Security Settings

6.1	Security Classifications	6-1
6.1.1	About Records Classification.....	6-1

6.1.1.1	Classification Levels	6-2
6.1.1.2	Classified Records Security Hierarchy	6-3
6.1.2	Managing Classified Security	6-3
6.1.2.1	Enabling or Disabling Classified Security.....	6-4
6.1.2.2	Creating or Editing a Custom Security Classification.....	6-4
6.1.2.3	Setting the Order of Security Classifications	6-5
6.1.2.4	Deleting a Security Classification.....	6-6
6.1.2.5	Setting the Declassification Time Frame	6-7
6.1.2.6	Viewing Security Classification References.....	6-7
6.1.2.7	Assigning a Classification to a User.....	6-8
6.1.2.8	Changing a User’s Classification	6-8
6.1.2.9	Removing a User’s Classification	6-9
6.2	Custom Security	6-9
6.2.1	About Custom Security.....	6-9
6.2.2	Managing Custom Security	6-10
6.2.2.1	Enabling or Disabling Custom Security Usage	6-10
6.2.2.2	Creating or Editing a Simple Custom Security Field	6-11
6.2.2.3	Adding or Editing Advanced Security	6-12
6.2.2.4	Viewing Simple Custom Security Field Information	6-13
6.2.2.5	Deleting a Simple Custom Security Field (Simple)	6-13
6.2.3	Simple Custom Security Field Example	6-14
6.2.3.1	Create the Custom Security Field in Configuration Manager	6-14
6.2.3.2	Create the Custom Security Field in User Admin	6-14
6.2.3.3	Create the Custom Security Field.....	6-15
6.2.3.4	Verify the Custom Security Field	6-16
6.3	Classification Guides	6-16
6.3.1	About Classification Guides.....	6-16
6.3.2	Managing Classification Guides.....	6-17
6.3.2.1	Creating or Editing a Classification Guide	6-17
6.3.2.2	Deleting a Classification Guide	6-18
6.3.2.3	Viewing Classification Guide Information	6-18
6.3.2.4	Creating or Editing a Classification Topic	6-18
6.3.2.5	Editing Classification Topic Settings	6-19
6.3.2.6	Deleting a Classification Topic	6-20
6.3.2.7	Viewing Classification Topic Information	6-20
6.4	Supplemental Markings	6-21
6.4.1	Supplemental Markings Details	6-21
6.4.2	Managing Supplemental Markings.....	6-23
6.4.2.1	Enabling or Disabling Supplemental Markings.....	6-23
6.4.2.2	Creating or Editing a Supplemental Marking	6-23
6.4.2.3	Viewing Supplemental Marking Information and References	6-24
6.4.2.4	Deleting a Supplemental Marking	6-25
6.4.2.5	Assign or Remove User Supplemental Markings.....	6-26
6.4.2.6	Using Restricted and Formerly Restricted Supplemental Markings	6-27

7 Configuration Options

7.1	Retention Options	7-1
-----	-------------------------	-----

7.1.1	Setting the Fiscal Calendar	7-3
7.1.2	Setting Performance Monitoring	7-3
7.2	PCM Options	7-4
7.3	Setting Up Workflows.....	7-4
7.3.1	Workflow Prerequisites and Process	7-6
7.3.2	Creating Necessary Workflows	7-6
7.3.2.1	Category Dispositions Workflow	7-7
7.3.2.2	Reservation Processing Workflow	7-7
7.3.2.3	Offsite Storage Workflow	7-9
7.4	Configuration with Desktop Integration Suite	7-10
7.5	Configuration Variables.....	7-10

8 Configuring Physical Content Management

8.1	Physical Content Management	8-1
8.2	Configuring Chargeback Processing.....	8-2
8.3	Configuring Location Types.....	8-3
8.3.1	Predefined Location Types.....	8-3
8.3.2	Location Type Icons.....	8-4
8.3.2.1	Adding Customized Icons.....	8-4
8.3.3	Creating or Editing a Location Type.....	8-4
8.3.4	Viewing Location Type Information.....	8-5
8.3.5	Deleting a Location Type.....	8-6
8.3.6	Reordering Location Types	8-6
8.3.7	Example: Creating a Location Type	8-6
8.4	Configuring Object Types.....	8-7
8.4.1	Predefined Object Types.....	8-7
8.4.2	Creating or Editing an Object Type	8-8
8.4.3	Viewing Object Type Information.....	8-8
8.4.4	Deleting an Object Type.....	8-9
8.4.5	Editing Object Type Relationships	8-9
8.5	Configuring Media Types.....	8-10
8.5.1	Predefined Media Types.....	8-10
8.5.2	Creating or Editing a Media Type.....	8-11
8.5.3	Viewing Media Type Information.....	8-11
8.5.4	Deleting a Media Type	8-12
8.6	Configuring Default Metadata Values: Offsite and Reservations	8-12
8.6.1	Setting Default Metadata Values for Reservation Items and Offsite Storage	8-12

9 Setting Up PCM Storage Space

9.1	Storage Space Considerations	9-1
9.2	Browsing the PCM Storage Space	9-2
9.2.1	Storage Space Hierarchy	9-2
9.2.2	Storage Location Properties	9-4
9.2.2.1	Location Type.....	9-5
9.2.2.2	Object Type.....	9-5
9.2.2.3	Media Type.....	9-5

9.2.2.4	Storage Status.....	9-6
9.3	Managing Storage Spaces	9-7
9.3.1	Creating a Storage Location	9-7
9.3.2	Batch Creating Storage Locations.....	9-8
9.3.3	Editing a Storage Location.....	9-10
9.3.4	Viewing Information about a Storage Location	9-10
9.3.5	Deleting a Storage Location	9-11
9.3.6	Blocking a Storage Location	9-11
9.3.7	Reserving or Canceling a Reservation for a Storage Location	9-12
9.3.8	Viewing All Items in a Storage Location.....	9-12
9.3.9	Printing Labels for Storage Locations.....	9-13
9.4	Example: Creating a Single Storage Location	9-14
9.5	Example: Creating a Batch of Storage Locations.....	9-14

10 Setting Up a Retention Schedule

10.1	Retention Schedule Overview.....	10-1
10.1.1	Retention Schedules and MoReq2 File Plans.....	10-2
10.1.2	Retention Schedules and Folders Retention Functionality.....	10-3
10.1.3	Planning a Retention Schedule	10-4
10.1.3.1	Retention Schedule Hierarchy	10-4
10.1.3.2	Attribute Inheritance.....	10-7
10.1.3.3	Review Status Attributes	10-7
10.1.3.4	Permanent Status Attributes	10-8
10.1.3.5	Disposition Instructions.....	10-8
10.1.3.6	Frozen Folder and Content Status.....	10-9
10.1.4	Creating and Navigating Object Levels	10-9
10.1.4.1	Retention Schedule Menus.....	10-9
10.2	Using a Series.....	10-11
10.2.1	Managing a Series.....	10-11
10.2.1.1	Creating or Editing a Series.....	10-11
10.2.1.2	Viewing Series Information	10-12
10.2.1.3	Hiding and Unhiding a Series	10-12
10.2.1.4	Moving a Series.....	10-13
10.2.1.5	Deleting a Series.....	10-13
10.3	Retention Categories.....	10-14
10.3.1	Managing Retention Categories	10-14
10.3.1.1	Creating or Editing a Retention Category	10-15
10.3.1.2	Viewing Retention Category Information	10-16
10.3.1.3	Viewing Category Metadata History.....	10-17
10.3.1.4	Copying a Retention Category	10-17
10.3.1.5	Moving a Retention Category.....	10-17
10.3.1.6	Deleting a Retention Category.....	10-18
10.3.2	Retention Category Example	10-18
10.4	Record Folders.....	10-19
10.4.1	About Record Folders	10-19
10.4.2	Managing Record Folders	10-20
10.4.2.1	Creating a Record Folder.....	10-20

10.4.2.2	Creating a Volume Folder	10-21
10.4.2.3	Editing a Record Folder.....	10-22
10.4.2.4	Changing the Disposition Applied to a Folder	10-23
10.4.2.5	Moving a Record Folder	10-23
10.4.2.6	Deleting a Record Folder.....	10-24
10.4.3	Folder Examples.....	10-24
10.4.3.1	Creating a Record Folder That is Subject to Review	10-24
10.4.3.2	Creating Record Folders Subject to Recurring Audit Triggers.....	10-25

11 Setting up Triggers

11.1	Trigger Overview.....	11-1
11.1.1	System-Derived Triggering.....	11-1
11.1.1.1	Retention Period Cutoff.....	11-2
11.1.1.2	Preceding (Disposition) Action	11-2
11.1.1.3	Content or Folder States	11-2
11.1.2	Custom Triggers	11-3
11.1.3	Global Triggers.....	11-3
11.1.4	Custom Direct Triggers.....	11-3
11.1.5	Indirect Triggers.....	11-3
11.2	Managing Triggers.....	11-4
11.2.1	Creating or Editing a Trigger	11-4
11.2.2	Viewing Trigger Information.....	11-6
11.2.3	Viewing Trigger References.....	11-6
11.2.4	Deleting a Trigger	11-7
11.2.5	Setting Up Indirect Triggers.....	11-7
11.2.6	Deleting an Indirect Trigger Date Entry.....	11-8
11.2.7	Disabling an Indirect Trigger Period	11-8
11.3	Trigger Examples	11-8
11.3.1	Global Triggers.....	11-9
11.3.1.1	Delayed Global Trigger	11-9
11.3.1.2	Dormant Global Trigger	11-9
11.3.1.3	Activating a Dormant Global Trigger	11-9
11.3.2	Custom Direct Trigger	11-9
11.3.2.1	Creating the Record Field.....	11-10
11.3.2.2	Creating the Custom Direct Trigger	11-10
11.3.2.3	Setting Up the Disposition Instructions	11-11
11.3.2.4	Verifying the Custom Direct Trigger.....	11-11

12 Configuring Time Periods

12.1	Using Time Periods	12-1
12.2	Managing Time Periods.....	12-1
12.2.1	Creating or Editing a Custom Time Period	12-2
12.2.2	Viewing Period Information	12-3
12.2.3	Viewing Period References	12-3
12.2.4	Deleting a Custom Period	12-4
12.2.5	Example: Creating a Custom Period.....	12-4

13 Creating Custom Metadata

13.1	Managing Custom Metadata.....	13-1
13.1.1	Creating or Editing Custom Metadata Fields.....	13-2
13.1.2	Viewing Custom Metadata Field Information	13-3
13.1.3	Deleting a Custom Metadata Field.....	13-3
13.2	Example: Creating a Custom Category Metadata Field.....	13-3

14 Defining Disposition Instructions

14.1	Disposition Types	14-2
14.1.1	Event Dispositions.....	14-2
14.1.2	Time Dispositions	14-2
14.1.3	Time-Event Dispositions.....	14-3
14.2	Category Rule Review Using Workflows.....	14-3
14.3	Triggering Events.....	14-4
14.3.1	Preceding Actions Triggering Event.....	14-4
14.3.2	Content State Triggering Event	14-4
14.3.3	Indirect Triggers.....	14-5
14.3.4	Custom Triggers	14-5
14.4	Retention Periods	14-5
14.5	Disposition Actions.....	14-6
14.5.1	Classified Records Actions	14-6
14.5.2	Dispose Actions.....	14-6
14.5.3	Other Actions	14-7
14.5.4	Transfer/Move Actions	14-8
14.6	Cutoff Guidelines.....	14-8
14.6.1	Time Retention Periods.....	14-9
14.6.2	Time-Event Retention Periods	14-9
14.7	Disposition Precedence	14-9
14.8	Managing Dispositions	14-9
14.8.1	Enabling or Disabling User-Friendly Captions	14-10
14.8.2	Creating or Editing a Disposition Rule.....	14-10
14.8.3	Copying a Disposition Rule	14-13
14.8.4	Viewing Disposition Information.....	14-13
14.8.5	Deleting a Disposition Rule.....	14-14
14.9	Disposition Examples.....	14-14
14.9.1	Event Disposition.....	14-14
14.9.2	Simple Time/Event Disposition.....	14-15
14.9.3	Time Disposition.....	14-15
14.9.4	Time-Event Disposition	14-16
14.9.5	Disposition Rules for Specific Folders	14-17
14.9.6	Multi-Phased Disposition.....	14-18

15 Setting Up Freezes

15.1	Managing Freezes	15-1
15.1.1	Creating or Editing a Freeze.....	15-1
15.1.2	Viewing Freeze Information	15-3

15.1.3	Deleting a Freeze.....	15-4
15.1.4	Freezing Items, Folios or Folders.....	15-4
15.1.5	Unfreezing Frozen Items or Folders	15-5
15.1.6	Searching for Frozen Content and Folders	15-5
15.1.7	Re-sending an E-Mail Notification for a Freeze	15-6
15.2	Example: Creating a Freeze	15-6

16 The Oracle Content Server Adapter

16.1	Content Server Adapter Overview.....	16-1
16.1.1	Architecture	16-1
16.1.2	Oracle WebCenter Content: Records and the Content Server Adapter.....	16-2
16.2	Adapter Configuration.....	16-4
16.2.1	Configuring Sources and Providers.....	16-5
16.2.1.1	Defining a New Outgoing Provider	16-5
16.2.1.2	Editing an Outgoing Provider	16-6
16.2.1.3	Disabling the Adapter's Outgoing Provider.....	16-6
16.2.1.4	Deleting the Adapter's Outgoing Provider.....	16-6
16.2.1.5	Registering an External Source.....	16-7
16.2.1.6	Unregistering and Removing an External Source	16-7
16.2.1.7	Viewing External Source Configuration Settings	16-8
16.2.1.8	Viewing Outgoing Provider Configuration Settings	16-8
16.2.2	Managing Fields.....	16-8
16.2.2.1	Mapping a Custom Metadata Field	16-8
16.2.2.2	Editing a Mapped Metadata Field	16-9
16.3	Synchronizing Data	16-9
16.3.1	Performing As-Needed Synchronization.....	16-10
16.3.2	Scheduling Synchronization	16-10
16.3.3	Viewing Synchronization Logs.....	16-10

A User Interface

A.1	Initial Features Pages.....	A-1
A.1.1	Enabled Features Page	A-2
A.1.2	Setup Checklist Page	A-3
A.1.2.1	Configuring the Report Library	A-6
A.2	Configure Retention Settings Page.....	A-7
A.3	Configure Physical Settings Page	A-12
A.4	Security Interface	A-14
A.4.1	Assigned Rights Page.....	A-14
A.4.2	Access Control Edit Section.....	A-15
A.4.3	Edit Rights Page.....	A-15
A.4.4	Classification Interface	A-16
A.4.4.1	Configure Security Classification Page	A-16
A.4.4.2	Create or Edit Security Classification Page.....	A-17
A.4.5	Custom Security Interface	A-17
A.4.5.1	Configure Custom Security Page	A-18
A.4.5.2	Create or Edit Simple Custom Security Field Page	A-18

A.4.5.3	Advanced Custom Security Option Page	A-19
A.4.5.4	Select Security Dialog.....	A-19
A.4.6	Classification Guide Interface	A-20
A.4.6.1	Configure Classification Guide Page.....	A-21
A.4.6.2	Create or Edit Classification Guide Page.....	A-21
A.4.6.3	Administer Classification Topic Page	A-22
A.4.6.4	Create or Edit Classification Topic Page	A-22
A.4.6.5	Configure Topic Settings Page.....	A-23
A.4.7	Supplemental Markings Interface	A-24
A.4.7.1	Configure Supplemental Markings Page.....	A-25
A.4.7.2	Create or Edit Supplemental Marking Page.....	A-25
A.5	PCM Configuration Interface Screens.....	A-26
A.5.1	Storage Location and Barcode Configuration Pages	A-26
A.5.1.1	Configure Location Types Page	A-26
A.5.1.2	Create or Edit Location Type Page	A-27
A.5.1.3	Default Metadata for Checked-in Reservation or Offsite Entries Page	A-28
A.5.1.4	Create or Edit Storage Page.....	A-30
A.5.1.5	Configuring Custom Barcode Page	A-31
A.5.1.6	Create Custom Barcode Dialog	A-32
A.5.1.7	Create Batch Storage Import File Page.....	A-32
A.5.1.8	Select Storage Location Dialog	A-33
A.5.1.9	Browse Storage Page	A-34
A.5.1.10	Physical Items in Storage Page	A-34
A.5.2	Object Types, Media Types, and Payment Types	A-35
A.5.2.1	Configure Object Types Page.....	A-35
A.5.2.2	Create or Edit Object Type Page.....	A-35
A.5.2.3	Edit Object Type Relationships Page.....	A-36
A.5.2.4	Configure Media Types Page.....	A-37
A.5.2.5	Create or Edit Media Type Page.....	A-37
A.5.2.6	Select Media Type Dialog.....	A-38
A.6	Retention Schedule Interface Screens	A-38
A.6.1	Exploring Retention Schedule Page.....	A-38
A.6.2	Series Interface Pages	A-39
A.6.2.1	Create or Edit Series Page	A-39
A.6.2.2	Series Information Page.....	A-40
A.6.2.3	Select Retention Series, Record Folder or Category Dialog	A-41
A.6.3	Category Interface Screens	A-42
A.6.3.1	Create or Edit Retention Category Page	A-42
A.6.3.2	Retention Category Information Page.....	A-43
A.6.3.3	Metadata History Page	A-44
A.6.4	Record Folders Interface Screens.....	A-44
A.6.4.1	Create or Edit Record Folder Page.....	A-44
A.6.4.2	Record Folder Information Page	A-46
A.7	Triggers Interface	A-47
A.7.1	Configure Triggers Page	A-48
A.7.2	Create or Edit Trigger Type Page.....	A-48
A.7.3	Trigger Information Page	A-49

A.7.4	Indirect Trigger Date Entries Page	A-50
A.7.5	Create or Edit Indirect Trigger Date Entries Page	A-51
A.8	Time Period Interface	A-51
A.8.1	Configure Periods Page	A-52
A.8.2	Create or Edit Period Page	A-52
A.8.3	Period Information Page.....	A-53
A.8.4	Period Reference Page.....	A-53
A.9	Custom Metadata Interface	A-54
A.9.1	Metadata List Page	A-54
A.9.2	Fields for Metadata Page	A-55
A.9.3	Create or Edit Standard Metadata Field Page	A-55
A.9.4	Create or Edit Auxiliary Metadata Set Page	A-56
A.9.5	Metadata Information Page.....	A-58
A.10	Disposition and Freeze Interface	A-58
A.10.1	Disposition Interface	A-58
A.10.1.1	Configure Dispositions Page	A-58
A.10.1.2	Create or Edit Disposition Action Page.....	A-58
A.10.1.3	Disposition Action Info Page	A-59
A.10.1.4	Disposition Actions Configuration Page.....	A-60
A.10.2	Freeze Interface	A-60
A.10.2.1	Freeze Configuration Page	A-60
A.10.2.2	Create or Edit Freeze Page	A-60
A.10.2.3	Freeze Information Page.....	A-62
A.10.2.4	Frozen Item Page	A-62
A.11	Disposition Interface Screens	A-62
A.11.1	Disposition Instructions Page	A-62
A.11.2	Disposition Rule Page	A-63
A.11.3	Disposition Information Page	A-65
A.12	Adapter Interface	A-65
A.12.1	Register Source Page	A-65
A.12.2	Add or Edit New Provider Page	A-66
A.12.3	Provider List Page.....	A-67
A.12.4	Provider Information Page.....	A-68
A.12.5	Source Configuration Information Page	A-68
A.12.6	Map Custom Fields Page.....	A-68
A.12.7	Map/Edit Custom Field Dialog.....	A-69
A.12.8	Configure Scheduled Events Page	A-69
A.12.9	Synchronization Log Page.....	A-70
A.13	Report Interface.....	A-71
A.13.1	Configure Reports Settings Page	A-71
A.13.2	Configure Report Element Page	A-72
A.13.3	Report Checkin Page	A-73
A.13.4	Report Templates Page	A-74
A.13.5	Configure Report Sources Page	A-74
A.13.6	XML Data Dialog	A-75

B Summary of Security Rights and Roles

B.1	Rights and Roles for Oracle WebCenter Content.....	B-1
B.1.1	Triggers	B-1
B.1.2	Periods.....	B-1
B.1.3	Supplemental Markings.....	B-2
B.1.4	Security Classifications	B-2
B.1.5	Custom Security Fields	B-2
B.1.6	Custom Category or Folder Metadata Fields	B-2
B.1.7	Classification Guides.....	B-3
B.1.8	Freezes	B-3
B.1.9	Series	B-3
B.1.10	Categories	B-4
B.1.11	Folders	B-4
B.1.12	Content	B-5
B.1.13	Disposition Rules	B-5
B.1.14	Archiving	B-6
B.1.15	Screening	B-6
B.1.16	Audit Trails.....	B-6
B.1.17	Links	B-7
B.1.18	Reports.....	B-7
B.1.19	Customization	B-7
B.1.20	General Configuration	B-7
B.2	Physical Content Management Rights and Roles	B-7
B.2.1	Physical Item Management	B-7
B.2.2	Storage Space.....	B-8
B.2.3	Location, Media, and Object Types.....	B-8
B.2.4	Reservations.....	B-9
B.2.5	Chargebacks	B-9
B.2.6	Barcodes	B-10
B.2.7	General Configuration	B-10

C Customizing Your System

C.1	Custom Disposition Actions.....	C-1
C.1.1	Managing Custom Dispositions	C-2
C.1.1.1	Creating or Editing a Custom Disposition Action.....	C-2
C.1.1.2	Viewing Custom Disposition Action Information.....	C-4
C.1.1.3	Deleting a Custom Disposition Action.....	C-4
C.1.2	Disabling Custom Disposition Actions	C-5
C.1.3	Creating a Custom Disposition Action Example	C-5
C.1.4	Creating Disposition Rules for Physical Content.....	C-6
C.2	Using Custom Barcodes	C-6
C.2.1	Adding a Custom Barcode Range	C-7
C.2.2	Processing Non-Standard Barcode Data	C-7
C.2.2.1	Header and Footer Information	C-7
C.2.2.2	Data Information	C-8
C.3	Adding a Mobile Bar Code Reader	C-9
C.4	Creating Custom Reports	C-10

C.4.1	Creating Custom Templates.....	C-11
C.4.2	Creating or Editing New Report Sources.....	C-12
C.4.3	Downloading a BI XML Data File	C-13

Glossary

Index

Preface

This guide provides instructions to administer and maintain Oracle WebCenter Content: Records software.

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

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

Access to Oracle Support

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

Related Documents

The following documentation is available:

- *Installation Guide* for the product: This document provides information about installing the software.
- *Oracle WebCenter Content Setup Guide for Records*: This document provides information about setting up the software.
- *Oracle WebCenter Content Administrator's Guide for Records*: This document provides information about administering and managing the software.
- *Oracle WebCenter Content User's Guide for Records*: 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.
<i>italic</i>	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.
<i>IntradocDir</i> /ucm/urm /config	The default location for configuration files mentioned in this documentation. <i>IntradocDir</i> is used to refer to the root directory for the actual configuration and data files specific to an instance deployed on the Oracle WebCenter Content domain on an Oracle WebLogic Server.

Introduction

This section covers the following topics:

- [Section 1.1, "About This Guide"](#)
- [Section 1.3, "What's New"](#)
- [Section 1.4, "Using Help"](#)

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 WebCenter Content Administrator's Guide for Records* or the *Oracle WebCenter Content User's Guide for Records*. 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 WebCenter Content and its use. References to appropriate 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 are used interchangeably.

1.2 About This Product

Oracle WebCenter Content: Records 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.

The following options are available after installing the software:

- **Minimal:** Installs a small amount of the Records system 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 E-mail.
- **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.

This documentation describes features available in the majority of configuration scenarios. The features available at your site will vary depending on the options chosen during configuration.

1.3 What's New

The 10g version (and older 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 the 11g 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 that 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 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 shown there as are the assigned roles.
- A dashboard is now available that can be used to quickly organize product features for easy access and use. This is discussed in detail in the *Oracle WebCenter Content User's Guide for Records*.
- 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 that 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 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 WebCenter Content Services Reference Guide*. 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 to track batches processes, items, and other processes.
- 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.
- Oracle WebCenter Content: Records, in conjunction with Oracle WebCenter Content, has been verified by a third party to be compliant with the technical elements of FDA 21 CFR Part 11, specifically the electronic signature portion of that specification.
- New functionality called Folders Retention is available to provide retention capability for draft items in folders.

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 that 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 that can be performed by either a user or a privileged user (administrator or user with other administrative privileges) is now documented in the *Oracle WebCenter Content User's Guide for Records*.

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

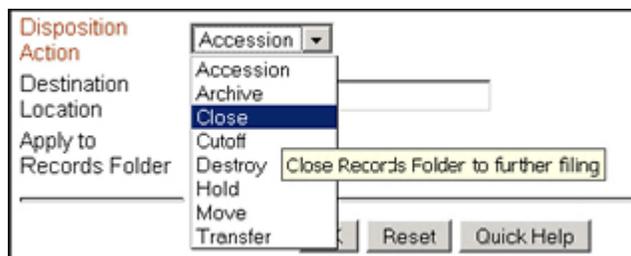
If the mouse cursor is held over a field label in a web browser, context-sensitive information about the field label opens. A question mark is displayed then the tooltip appears.

Figure 1–1 Field Label Tooltip



When using Netscape or Firefox as a web browser, tooltips 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 **Quick Help** where available on pages and screens to view context-sensitive help for that page or screen.

Understanding Retention Management

This section covers the following topics:

- [Section 2.1, "Management of Retained Items"](#)
- [Section 2.2, "Basic Retention Management Concepts"](#)
- [Section 2.3, "Physical Content Management"](#)
- [Section 2.4, "Interaction with Oracle WebCenter Content"](#)
- [Section 2.5, "Basic Retention Processes"](#)

2.1 Management of Retained Items

Oracle WebCenter Content: Records 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.

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

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

This section covers the following topics:

- [Section 2.1.1, "What To Retain"](#)
- [Section 2.1.2, "Lifecycle for Retained Content"](#)
- [Section 2.1.3, "Types of Retained Content"](#)

2.1.1 What To 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 revised, retained and can be managed on a disposition schedule. An organization may choose to manage content to eliminate outdated and misleading information and track documents related to legal proceedings.

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

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.

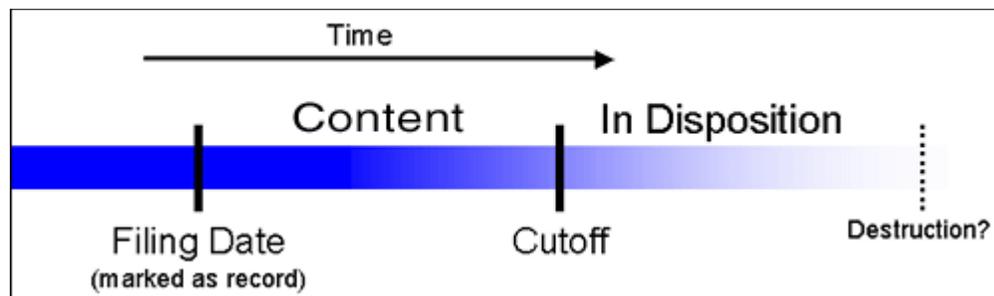
There may be business-related needs for effective and efficient retention management:

- To organize items that are created in a variety of forms (email, CDs, DVDs) and which are stored in a variety of locations (employee computers, central file storage, and so on).
- To provide a uniform infrastructure for retrieving and sharing the content across the organization.:
- 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).
- To ensure that content items are retained over the period they are useful to the business.

Oracle WebCenter Content: Records manages all content, regardless of source, in a single, consistent, manageable infrastructure.

2.1.2 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 checkin date. However, it is possible for an active content item already checked in to be tracked.

The information may need to be 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 **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.

Items are disposed of by authorized people according to the requirements of the organization. Disposition actions can include destruction, storage, transfer, or an item can be 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 Types of Retained Content

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

- [Section 2.1.3.1, "Internal and External Retained Content"](#)
- [Section 2.1.3.2, "Classified, Unclassified, Declassified Content"](#)
- [Section 2.1.3.3, "Non-Permanent, Transfer or Accession, and Reviewed Content"](#)

2.1.3.1 Internal and External Retained Content

An *internal* retained content item is an electronic item stored within Oracle WebCenter Content and managed by the product.

External content can also be managed. An *external* retained content item is a source file not stored in Oracle WebCenter Content. It can be in a variety of formats, both physical or electronic. 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.

2.1.3.2 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 checkin 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.

2.1.3.3 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 WebCenter Content: Records is used to manage content, regardless of source or format, in a single, consistent, manageable infrastructure. Managed items are assigned retention schedules and disposition rules that allow users to schedule life cycles for content to eliminate outdated or superseded information, manage storage resources, or comply with legal audit holds.

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

Disposition schedules of content in the repository can also be managed, enabling the scheduling of life cycles 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 that 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 checkin 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 that 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).
- **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 WebCenter Content: Records enables organizations to manage the retention and disposition of content, PCM 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 WebCenter Content

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.
7. A batch process is run to process an approval.

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. A notification e-mail is sent to reviewers 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.

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.

This chapter covers the following topics:

- [Section 3.1, "Usage Notes"](#)
- [Section 3.2, "Fusion Middleware Security Considerations"](#)
- [Section 3.3, "Software Configuration"](#)
- [Section 3.4, "Retention Setup Checklist"](#)
- [Section 3.5, "Retention Management Options"](#)
- [Section 3.6, "Security Overview"](#)
- [Section 3.7, "System-Wide Configuration"](#)
- [Section 3.8, "Setting Up Physical Content Management"](#)
- [Section 3.9, "Setting Up a Retention Schedule"](#)
- [Section 3.10, "Configuring Content Triggers, Dispositions, and Freezes"](#)

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, "Security Overview"](#).

3.1 Usage Notes

Before setting up the system, review [Chapter 2, "Understanding Retention Management."](#) It 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. 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.

When using Records with a Safari browser, menus can appear behind the icons for the Admin Applets. Therefore, if you select **Administration** then **Admin Applets** then select **Records** or **Physical**, the options on the Records or Physical menu appear behind the icons for the Admin Applets. This is a known problem and Oracle is working to solve this issue.

When using the IBM WebSphere Application Server (WAS) in a browser using tabs, the login/logout process performs differently than in browsers not using tabs. Authentication is not set at the "tab level" but rather at the "browser level." For example, consider this scenario:

- Oracle WebCenter Content and Oracle WebCenter Content: Records are installed in the same cell on WAS.
- A user logs in to Oracle WebCenter Content then opens a new tab and enters the Records system URL in the browser.
- That user is automatically logged in to the Records system with the same permissions as when that user logged in to Oracle WebCenter Content. There is no need to re-authenticate.
- If the user logs out of the Oracle WebCenter Content system, the user is also automatically logged out of the browser tab session for the Records system. This is reflected on the next action or when the tab is refreshed.

3.2 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.

3.2.1 Oracle WebCenter Content Security Considerations

Oracle WebCenter Content 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 WebCenter Content'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 the Records system.

Oracle WebCenter Content and workflow services use Java Platform Security (JPS) and the User and Role API. Oracle Internet Directory stores user and group information. When Oracle WebCenter Content 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 administrator and other users must be defined in Oracle Internet Directory.

Oracle WebCenter Content 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 WebCenter Content to retrieve the roles of the Oracle WebLogic Server defined administrative users will fail.

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

3.2.2 WNA Redeployment

For Windows Native Authentication through Kerberos to work, you must redeploy Oracle WebCenter Content: Records.

First create then save an .xml file for the Oracle WebCenter Content: Records 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
source-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 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**.

3.2.3 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	<i>Installation Guide for Oracle Enterprise Content Management Suite: Section 4.4, Reassociating the Identity Store with an External LDAP Authentication Provider</i>

3.2.4 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	<i>Oracle Fusion Middleware Administration Guide: Chapter 6, SSL Configuration in Oracle Fusion Middleware</i>
Configuring SSL with Oracle WebLogic Server	<i>Oracle Fusion Middleware Security Oracle WebLogic Server Guide: Chapter 12, Configuring SSL</i>

3.2.5 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	<i>Oracle Fusion Middleware Security Guide: Chapter 10, Configuring Single Sign-On in Oracle Fusion Middleware</i>
Using Windows Native Authentication for Single Sign-on	<i>Oracle WebLogic Server Admin Console Help: Configure Authentication and Identify Assertion Providers</i>

3.2.6 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	<i>Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Appendix A: Using Oracle Web Service Security Policies</i>
Use MTOM with Web Services	<i>Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Section 2.2: Example of Adding Security to MTOM Web Service</i>

3.3 Software Configuration

Software configuration should be done before configuring any other aspects of the software. By choosing specific options, specific components are enabled and ready for use. To view details about the components that are installed and the disposition actions enabled with each option, click the *i* button next to the option.

The following options are available for installation:

- Folders Retention:** Enables functionality to apply retention rules for deletions of items stored together in a retention query folder. This functionality is described in detail in the *Oracle WebCenter Content Application Administrator's Guide for Content Server*. See [Chapter 10, "Setting Up a Retention Schedule"](#) for a summary of this feature.

- **Minimal:** Enables the minimal amount of functionality and excludes some 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.
- **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 if the FOIA/PA functionality is installed, fast index rebuilds may not be possible. Deselect the **Fast Index Rebuild** option when using FOIA/PA. If you install FOIA/PA after the system has been in use, you should rebuild the index.

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.

Note that if DoD functionality is enabled by using either DoD option (or a customized option that enables DoD features), then some features will automatically be enabled as well. For example, when creating custom search templates, the Security Classification status of a content item will always be displayed whether or not the classification was chosen for inclusion in the template. It is a requirement of the DoD specification that the classification level always be displayed in a search result.

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

If a component is disabled, the data used with that component is not deleted. If the component is enabled again, the old data can still be used.

3.4 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, 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 WebCenter Content 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 *Category or Folders* metadata field.
- Configure the installation: Before using the system, complete the installation steps outlined in [Section 3.3, "Software Configuration."](#)
- Configure the security settings: Determine the appropriate roles, rights, and user permissions to perform certain tasks. For details, see [Chapter 5, "Security Overview."](#)

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**.

3.5 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 WebCenter Content Administrator's Guide for Records* 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 3.6.2, "Classification Security Settings"](#) and for details, see [Chapter 6, "Additional Security Settings."](#)
- Configure system settings. For an overview, see [Section 3.7, "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 13.1, "Managing Custom Metadata."](#)
- Set up the retention schedule. For an overview, see [Section 3.9, "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 3.10, "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, "Managing Freezes."](#)
- Establish relationships between content. See the *Oracle WebCenter Content User's Guide for Records* for details about establishing links between content items.

Additional tasks discussed in the *Oracle WebCenter Content Administrator's Guide for Records* 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 WebCenter Content Administrator's Guide for Records* 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 WebCenter Content User's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

3.6 Security Overview

Multiple layers of security are available to control access to content. System security combined with security permissions and privileges for users allow you to customize the security easily. The intersection of all security mechanisms in place are used to determine user privileges with the strictest setting prevailing. See [Chapter 5, "Security Overview"](#) for complete details.

This section discusses the following topics:

- [Section 3.6.1, "Security Settings"](#)
- [Section 3.6.2, "Classification Security Settings"](#)
- [Section 3.6.3, "Security Roles and Definitions"](#)
- [Section 3.6.4, "Rights for Roles"](#)

3.6.1 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 WebCenter Content. PCM security is set using the Records system security measures.

Important: After your production environment is underway, we recommend you do not change the security settings for ACLs or the default Oracle WebCenter Content 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 6.4.1, "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 6.1.1, "About Records Classification."](#)

When done, click **Submit Update**.

3.6.2 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 3.6.2.1, "Supplemental Markings"](#)
- [Section 3.6.2.2, "Security Classifications"](#)
- [Section 3.6.2.3, "Classification Guides"](#)

3.6.2.1 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.

3.6.2.2 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 6.1.2.2, "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 6.1.2.3, "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.

3.6.2.3 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 6.3.2.4, "Creating or Editing a Classification Topic."](#)

3.6.3 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.
 - **rlocalrecordsofficer**, 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 \(ACLs\)."](#)

3.6.4 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."](#)

3.7 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 that 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 6.4, "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.

3.8 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 3.6, "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 WebCenter Content Administrator's Guide for Records* for details about setting up barcodes and labels for processing reservations and invoices.

3.9 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 3.9.1.1, "Creating a Series"](#)
- [Section 3.9.1.2, "Creating a Retention Category"](#)

- [Section 3.9.1.3, "Creating a Record Folder"](#)

3.9.1 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."](#)

3.9.1.1 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."](#)

3.9.1.2 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.

3.9.1.3 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. Access Control Lists (ACLs) can also be applied to a 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 WebCenter Content Administrator's Guide for Records* for other record folder task information.

Record folders cannot be created at the root level.

3.10 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 3.10.1, "Triggers"](#)
- [Section 3.10.2, "Dispositions"](#)
- [Section 3.10.3, "Freezes"](#)

3.10.1 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."](#)

3.10.2 Dispositions

Dispositions are predefined actions taken on content, usually for items no longer needed for current business. For details, see [Chapter 14, "Defining Disposition Instructions."](#)

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

```
When a triggering event occurs,
wait a specified retention 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.

3.10.2.1 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.

3.10.2.2 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 14.3, "Triggering Events."](#)

3.10.2.3 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."](#)

3.10.2.4 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.

3.10.2.5 Disposition Rules

After configuring the types of dispositions, rules are created that are 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 14.9, "Disposition Examples."](#)

3.10.3 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."](#)

Interface Overview

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

- [Section 4.1, "Interface Overview"](#)
- [Section 4.2, "Individual Page and Actions Menus"](#)

For an explanation of terminology used in this documentation, see the glossary at the end of this book.

Also see the *Oracle WebCenter Content User's Guide for Records* 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** options in the Top menu to access most aspects of Oracle WebCenter Content: Records. The exact 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 menu options any user sees depend on the rights assigned to the user. For details about rights assigned to different roles, see [Section 5.11, "Assigning Rights to User Roles."](#)

You can frequently perform actions from several different locations. For example, you can create a series within a series by choosing **Create Series** from the Page menu on the Series Information Page. Or you can choose **Create Series** from the **Actions** 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 WebCenter Content User's Guide for Records* for information about viewing rights and roles.
- **Favorites:** Accesses the Favorites interface, showing items added to a Favorites list. See the *Oracle WebCenter Content User's Guide for Records* for details about using Favorites.

- **Dashboards:** Used to configure a dashboard that is a shortcut to frequently used screens. See the *Oracle WebCenter Content User's Guide for Records* for information about configuring dashboards.
- **Approvals:** Accesses items awaiting review, approval or completion.
- **Scheduled:** Accesses scheduled actions, reports, and freezes.
- **Reports:** Accesses 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 (only visible if specific rights are enabled.)
- **Sources:** Used to access 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 modify the default report templates used and the default formats used for reports. 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, choose **Records** then **Configure** from the Top menu. Choose **Reports** then **Settings**. See the *Oracle WebCenter Content Administrator's Guide for Records* for details about reports and their configuration.

4.1.3 Configuring PCM

Use the **Physical** options in the Top menu to access most aspects of Physical Content Management. The 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:** Opens a list of all current reservations. See the *Oracle WebCenter Content User's Guide for Records* for details about reservations.
- **Storage:** Opens the Exploring Storage page where storage locations can be defined and edited.
- **Invoices:** Shows current invoices and also allows the addition of new invoices.
- **Requests:** Shows pending requests, checked-out requests, and overdue requests for physical items.
- **Process Barcode File:** Opens 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 Actions Menus

When using this product, individual **Actions** menus are available for items on a page and in many cases for individual items. The options on the **Actions** 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:** Opens a menu allowing access to information pages for folders, life cycle of the item, recent reviews, metadata history, and retention schedule reports.
- **Edit:** Provides options to edit folders or reviews, and options to alter an item's status by moving, closing, freezing, or unfreezing an item.
- **Set Dates:** Provides options to mark items for review, cancel, rescind, or expire 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 **Actions** menu for a retention category, Create suboptions include Series and Retention Category.

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

In addition, several pages have a page-level **Actions** menu that 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.

Security Overview

Multiple layers of security are available, including roles, rights, security groups, and Access Control Lists. As with the standard Oracle WebCenter Content 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 WebCenter Content System Administrator's Guide for Content Server*. For details about user roles, accounts, and permission considerations, see [Section 3.2, "Fusion Middleware Security Considerations."](#)

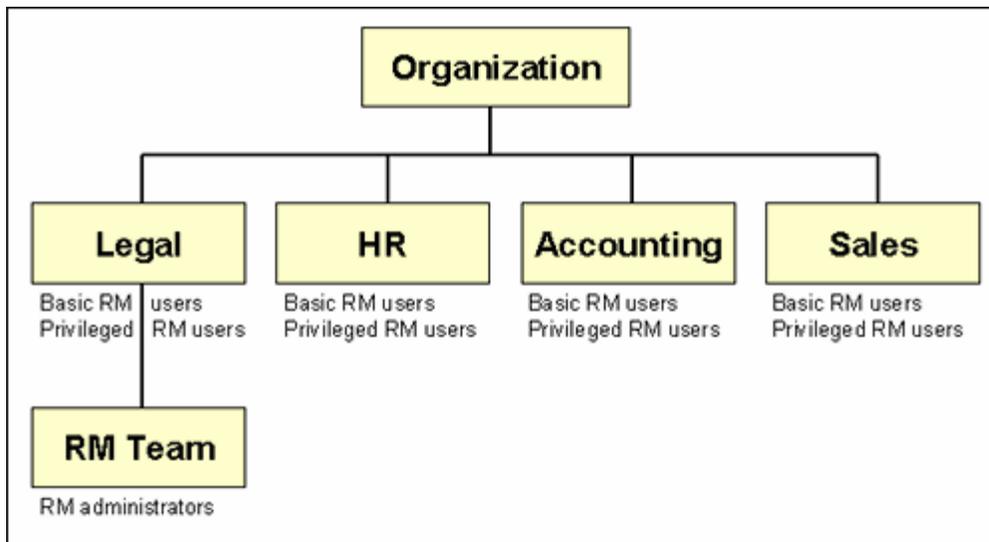
This section provides an overview of the available security. It covers the following topics:

- [Section 5.1, "Retention Management in an Organization"](#)
- [Section 5.2, "Roles"](#)
- [Section 5.3, "Tasks and Default Rights for Roles"](#)
- [Section 5.4, "Common Physical Content Management Tasks and Roles"](#)
- [Section 5.5, "External Source Management Tasks and Roles"](#)
- [Section 5.6, "Security Groups"](#)
- [Section 5.7, "Aliases"](#)
- [Section 5.8, "Access Control Lists \(ACLs\)"](#)
- [Section 5.9, "Security Matrix"](#)
- [Section 5.10, "Setting Security Preferences"](#)
- [Section 5.11, "Assigning Rights to User Roles"](#)
- [Section 5.12, "Default Rights for Roles"](#)
- [Section 5.13, "Specifying PCM Barcode Values for Users"](#)

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 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`, `rlocalrecordsofficer`, 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. 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 roles, as described below. For details about predefined security groups, see [Section 5.6, "Security Groups."](#)

- **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.

- **rlocalrecordsofficer** (denoted by Records Officer in this documentation): This role is generally assigned to users who have all the permissions assigned to basic users (the 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.

- **rmasdiscovery**: This role is generally assigned to users who must perform duties associated with Federated searches. Users with this role have read permission (R) to the Records Group security group.

rcreatedisposition: This role is generally assigned to those users who will create custom dispositions and custom reports. Users with this role have read permission to the Records Group security group as well as the Customization right.

- **radmin** (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.

- **chargebackadmin**: This role is assigned to users who manage invoicing and other chargeback functions. Users with this role are granted external ECM rights as well as other rights appropriate to chargeback management.

Note that Physical Content Management is treated as an external source, just as an adapter is treated. Therefore, if Physical Content Management is enabled, 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.

Most 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 WebCenter Content. 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. For details, see [Section 5.11, "Assigning Rights to User Roles."](#)

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, choose **Records** then **Rights** from the Top menu. The [Assigned Rights Page](#) opens. 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 WebCenter Content System Administrator's Guide for Content Server*.

5.3 Tasks and Default Rights for Roles

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.

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. For more details, see [Chapter 6, "Additional Security Settings"](#) and [Section 5.8, "Access Control Lists \(ACLs\)."](#)

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

The information is presented in tabular form in [Appendix B, "Summary of Security Rights and Roles."](#)

- [Section 5.3.1, "Trigger Tasks and Defaults for Predefined RM Roles"](#)

- Section 5.3.2, "Time Period Tasks and Defaults for Predefined Roles"
- Section 5.3.3, "Supplemental Markings Tasks and Defaults for Predefined Roles"
- Section 5.3.4, "Security Classifications Tasks and Defaults for Predefined Roles"
- Section 5.3.5, "Classification Guides Tasks and Defaults for Predefined Roles"
- Section 5.3.6, "Custom Security Tasks and Defaults for Predefined Roles"
- Section 5.3.7, "Custom Category or Folder Metadata Tasks and Defaults for Predefined Roles"
- Section 5.3.8, "Freezes Tasks and Defaults for Predefined Roles"
- Section 5.3.9, "Series Tasks and Defaults for Predefined Roles"
- Section 5.3.10, "Retention Category Tasks and Defaults for Predefined Roles"
- Section 5.3.11, "Folder Tasks and Defaults for Predefined Roles"
- Section 5.3.12, "Archive Tasks and Defaults for Predefined Roles"
- Section 5.3.13, "Screening Tasks and Defaults for Predefined Roles"
- Section 5.3.14, "Audit Trail Tasks and Defaults for Predefined Roles"
- Section 5.3.15, "Disposition Tasks and Defaults for Predefined Roles"
- Section 5.3.16, "Link Tasks and Defaults for Predefined Roles"
- Section 5.3.17, "Default Report Tasks and Defaults for Predefined Roles"
- Section 5.3.18, "Content Management Tasks and Defaults for Predefined Roles"
- Section 5.3.19, "Customization Tasks"
- Section 5.3.20, "Other Common Tasks"

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 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 [Section 6.3, "Classification Guides."](#)

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 [Section 10.2, "Using a Series."](#)

- 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 [Section 10.3, "Retention Categories."](#)

- 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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content User's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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

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.

- [Section 5.4.1, "Storage Space Tasks and Defaults for Predefined Roles"](#)
- [Section 5.4.2, "Reservation Tasks and Defaults for Predefined Roles"](#)
- [Section 5.4.3, "Physical Item Tasks and Defaults for Predefined Roles"](#)
- [Section 5.4.4, "Location, Object, and Media Types Tasks and Defaults for Predefined Roles"](#)
- [Section 5.4.5, "Chargeback Tasks and Defaults for Predefined Roles"](#)
- [Section 5.4.6, "Barcode and Label Tasks and Defaults for Predefined Roles"](#)

- [Section 5.4.7, "Additional PCM Administrative Tasks and Defaults for Predefined Roles"](#)

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content: Records 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 [Section 5.3, "Tasks and Default Rights for Roles."](#)

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
- RmaReviewersGroup

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 WebCenter Content and the Records system is configured to one of the DoD settings (which re-enables ACLs), the Oracle WebCenter Content ACLs are overridden. And if the **Typical** or **Minimal** Record 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.

ACLs 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 as well as other security features, such as custom security fields and supplemental markings. When possible, use the default Oracle WebCenter Content security features and consider disabling ACLs for faster search retrieval performance.

Note that ACLs in the Records system behave differently than those in Oracle WebCenter Content in the following ways:

- Oracle WebCenter Content administrative users or users with the RWDA rights assigned to them have no automatic rights in the Records system. All users must have rights defined for them when using ACLs in the Records system.
- Oracle WebCenter Content: Records ACLs are hierarchical. If ACLs are enabled only in the Records system (and not in Oracle WebCenter Content), then ACLs are defined only on categories and folders, not directly on content. ACL rights are propagated down to content based on all rights assigned to the parent category or folder.

The `UseEntitySecurity` configuration variable is used to enable Oracle WebCenter Content ACL functionality. Set that variable to true to enable that feature.

The `SpecialAuthGroups` configuration variable is used to determine what security groups can be used with ACLs. For example, `SpecialAuthGroups=Private, RecordsGroup` enables those security groups to be used with ACLs. By default, `RecordsGroup` is set as the `SpecialAuthGroup` value when Oracle WebCenter Content: Records is enabled.

5.8.1 Setting ACLs During Software Use

ACLs for individual users and groups and aliases can be adjusted while setting up elements of the Records system. 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 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; ACLs	R	R	RWD

Objects and Retention Schedule Components	Subject to Additional Security of Type	Records User (rma)	Records Officer (recordsofficer)	Records Administrator (rmaadmin)
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 WebCenter Content. 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Settings**.

The [Configure Retention Settings Page](#) opens. 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, select **ACL-based security**. This is enabled by default when DoD Baseline or DoD Classified is enabled.
3. (Recommended): To activate the default security inherent in Universal Content Management for extra security on categories, folders, and triggers, select **Default Content Server security on Categories, Folders, and Triggers**.
4. (Required for DOD 5015.2 compliance): To use supplemental markings, select **Supplemental Marking**.
5. (Optional based on the security model): To make users match all supplemental markings on a record folder, select **User must match all Supplemental Markings**. 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), deselect the box. For more information, see [Section 6.4.1, "Supplemental Markings Details."](#)
6. (Optional): To create custom security fields at the content field level to further restrict users, select **Custom Security Fields**.
7. (Optional): To use classified security, select **Classified Security**. For more information, see [Chapter 6, "Additional Security Settings."](#)

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 [Section 5.3, "Tasks and Default Rights for Roles"](#) and [Section 5.4, "Common Physical Content Management Tasks and Roles."](#)

5.11.1 Setting Rights for Roles

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

1. Choose **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](#) opens.
5. Set the rights by selecting checkboxes 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 is enabled automatically.

Rights appear in the following locations:

- [Section 5.12.1, "The Series Tab"](#)
- [Section 5.12.2, "The Category Tab"](#)
- [Section 5.12.3, "Folder Tab"](#)
- [Section 5.12.4, "Record Tab"](#)
- [Section 5.12.5, "Admin Tab"](#)
- [Section 5.12.6, "CBC Tab"](#)
- [Section 5.12.7, "PCM Tab"](#)
- [Section 5.12.8, "ECM Tab"](#)

5.12.1 The Series Tab

For more information, see [Section 10.2, "Using a Series."](#)

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 [Section 10.3, "Retention Categories."](#)

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 WebCenter Content Administrator's Guide for Records*.

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 WebCenter Content User's Guide for Records* for details.
- **Create:** Allows a user to create content or check it in to the retention schedule. For details, see the *Oracle WebCenter Content User's Guide for Records*.
- **Unlink:** Allows a user to unlink content. See the *Oracle WebCenter Content User's Guide for Records* 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 option is only available if the Classified Security option is enabled.
- **Upgrade/Downgrade:** Allows a user to upgrade and downgrade the security classification of content. This option 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 WebCenter Content Administrator's Guide for Records* for more details.
- **PrivilegedEnvironment:** Allows a user to set the de-classification time frame. For details, see [Section 6.1.2.5, "Setting the Declassification Time Frame."](#) This right is assigned by default to the Records Officer and Records Administrator roles. This option 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. For details, 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 WebCenter Content Administrator's Guide for Records* 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. They may also 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.

- **Customization:** Allows users to define custom disposition actions or to delete any disposition action. Also allows users to define custom reports. 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. This option is only available if the Classified Security option is 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 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 PCM 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 opens.
5. In the **Barcode** field, specify a unique value for the user. This value is 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 is 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.

Additional Security Settings

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

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.

- [Section 6.1, "Security Classifications"](#)
- [Section 6.2, "Custom Security"](#)
- [Section 6.3, "Classification Guides"](#)
- [Section 6.4, "Supplemental Markings"](#)

6.1 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.

This section discusses the following topics:

- [Section 6.1.1, "About Records Classification"](#)
- [Section 6.1.2, "Managing Classified Security"](#)

6.1.1 About Records Classification

Oracle WebCenter Content: Records 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 can be enabled if needed. For details, see [Section 6.1.2.1, "Enabling or Disabling Classified Security."](#)

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. For details, see [Section 6.1.2.2, "Creating or Editing a Custom Security Classification."](#)

Content is either classified, unclassified, or declassified:

- **Classified** content has an initial classification and a current classification. 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.

6.1.1.1 Classification Levels

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

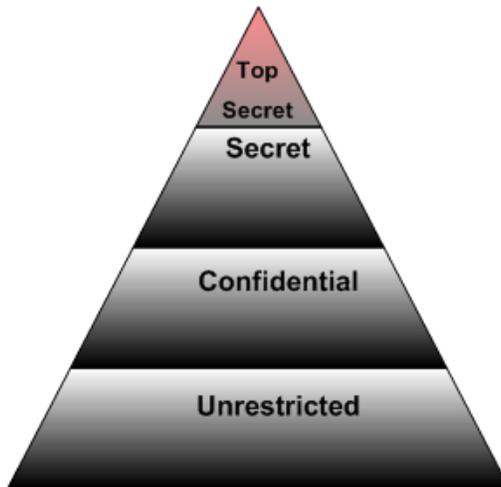
1. Top Secret
2. Secret
3. Confidential
4. No markings (unclassified)

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 content that is critical to the operation of your company and should never be deleted, while Confidential may apply to content that 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. For details, see [Section 6.1.2.2, "Creating or Editing a Custom Security Classification."](#)

The following descriptions are applicable for those companies that are using the Oracle WebCenter Content: Records product for DoD compliance.

Figure 6–1 Classified Hierarchy



6.1.1.1.1 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>

6.1.1.1.2 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."

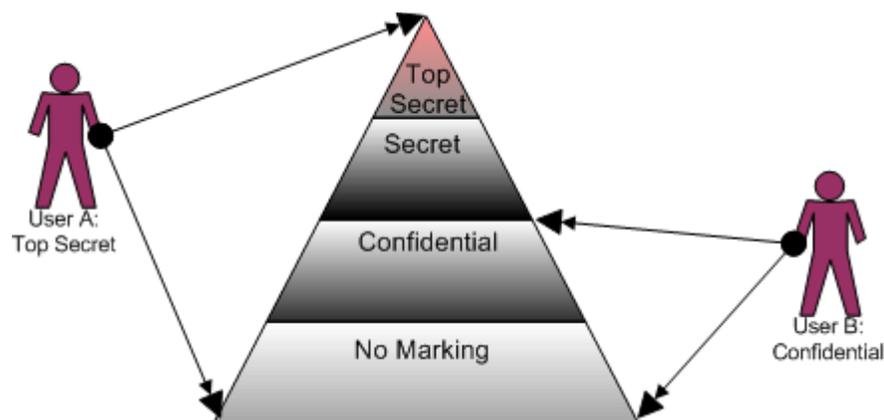
6.1.1.1.3 Confidential According to EO 12958, the Secret classification level is "applied to information, the unauthorized disclosure of which could be expected to cause **damage** to the national security that the original classification authority is able to identify or describe."

6.1.1.2 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 6–2 Hierarchical User Access



6.1.2 Managing Classified Security

When using classified security, you must first set the classifications to be used. Then set the timeframe for classifying and declassifying, then lastly assign classification ability to different users. The following tasks are discussed in regard to managing classifications:

- [Section 6.1.2.1, "Enabling or Disabling Classified Security"](#)
- [Section 6.1.2.2, "Creating or Editing a Custom Security Classification"](#)
- [Section 6.1.2.3, "Setting the Order of Security Classifications"](#)
- [Section 6.1.2.4, "Deleting a Security Classification"](#)
- [Section 6.1.2.5, "Setting the Declassification Time Frame"](#)
- [Section 6.1.2.7, "Assigning a Classification to a User"](#)

- [Section 6.1.2.8, "Changing a User's Classification"](#)
- [Section 6.1.2.9, "Removing a User's Classification"](#)

6.1.2.1 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. It is not recommended that classified security be disabled after it has been in use.

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 [Section 6.1.2.3, "Setting the Order of Security Classifications."](#)

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 **Settings** from the Top menu.
The [Configure Retention Settings Page](#) opens. If necessary, expand the Security section.
2. Select **Classified Security**.
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. Choose **Records** then **Configure** then **Settings** from the Top menu.
The [Configure Retention Settings Page](#) opens.
2. Deselect **Classified Security**.
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.

6.1.2.2 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 [Section 6.1.2.3, "Setting the Order of Security Classifications."](#)

Security classifications can be created only if the classified security feature has been enabled. For details, see [Section 6.1.2.1, "Enabling or Disabling Classified Security."](#)

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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Security Classification**.

The [Configure Security Classification Page](#) opens.

2. Click **Add**.

The [Create or Edit Security Classification Page](#) opens.

3. Enter a name for classification with a maximum length of 30 characters.
4. Enter a description if needed. Maximum length is 30 characters.
5. Click **Create**. A message indicates creating the classification was successful.
6. Click **OK**. The [Configure Security Classification Page](#) opens 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 [Section 6.1.2.3, "Setting the Order of Security Classifications."](#)

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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Security Classification**.

The [Configure Security Classification Page](#) opens.

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

The [Create or Edit Security Classification Page](#) opens.

3. Make any changes to the description and click **Submit Update**. A message is displayed stating the security classification was updated successfully.
4. Click **OK**.

6.1.2.3 Setting the Order of Security Classifications

Prerequisites

- Create any custom security classifications that are required. For details, see [Section 6.1.2.2, "Creating or Editing a Custom Security Classification."](#)
- Assign yourself the highest classification level so you can view and reorder all levels. For details, see [Section 6.1.2.8, "Changing a User's Classification."](#)

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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Security Classification**.

The [Configure Security Classification Page](#) opens.

2. Use the Up or Down arrow to move a selected security classification 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 designated as unclassified.

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

6.1.2.4 Deleting a Security Classification

A classification cannot be deleted until any references to the classification in content are removed. Security classification assignments must also be manually removed from users. 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 WebCenter Content Administrator's Guide for Records*.

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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Security Classification**.

The [Configure Security Classification Page](#) opens.

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**.

6.1.2.5 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. Choose **Records** then **Configure** then **Settings** from the Top menu.
The [Configure Retention Settings Page](#) opens. If necessary, expand the Security section.
2. Expand the Classified Topics area of the page. 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.
If 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**.

6.1.2.6 Viewing Security Classification References

Use this procedure to view references to a security classification (those disposition rules that 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Security Classification**.
The [Configure Security Classification Page](#) opens.
2. Select the security classification to view, and click **Info**.
The Security Classification Information page opens.
3. Choose **Reference** from the Page menu.
The Security Classification Information Page opens.
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 opens.

6.1.2.7 Assigning a Classification to a User

You can assign security classifications only if the classified security feature has been enabled.

Permissions: Administrator privileges in Oracle WebCenter Content 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. Choose **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 opens.
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 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).

6.1.2.8 Changing a User's Classification

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

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

1. Choose **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 opens.
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**.

6.1.2.9 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 WebCenter Content are required to perform this action. Your own assigned classification level must also be at least the level being accessed.

1. Choose **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 opens.
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**.

6.2 Custom Security

Custom security is optional and are another layer of security in addition to supplemental markings.

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:

- [Section 6.2.1, "About Custom Security"](#)
- [Section 6.2.2, "Managing Custom Security"](#)
- [Section 6.2.3, "Simple Custom Security Field Example"](#)

6.2.1 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. 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.

6.2.2 Managing Custom Security

The following tasks are often performed when managing custom security:

- [Section 6.2.2.1, "Enabling or Disabling Custom Security Usage"](#)
- [Section 6.2.2.2, "Creating or Editing a Simple Custom Security Field"](#)
- [Section 6.2.2.3, "Adding or Editing Advanced Security"](#)
- [Section 6.2.2.4, "Viewing Simple Custom Security Field Information"](#)
- [Section 6.2.2.5, "Deleting a Simple Custom Security Field \(Simple\)"](#)

6.2.2.1 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. Choose **Records** then **Configure** then **Settings** from the Top menu.

The [Configure Retention Settings Page](#) opens. Expand the Security section if needed.

2. Select **Custom Security**.

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

To disable the feature, deselect **Custom Security**.

6.2.2.2 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. For a step-by-step sample of setting up a simple custom security field, see [Section 6.2.3, "Simple Custom Security Field Example."](#)

You can create custom security fields only if the custom security field feature has been enabled.

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

1. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.
The [Configure Custom Security Page](#) opens.
2. In the Custom Security Field area, click **Add**.
The [Create or Edit Simple Custom Security Field Page](#) opens.
3. Enter a name for the field.
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) Select **Match all** to force the user entries to match **all** content field entries. Leave this box unselected to allow only one content field to match the user field.
7. Click **Create**. A message is displayed, indicating success.
8. Click **OK**.

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

1. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.
The [Configure Custom Security Page](#) opens.
2. Choose **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 (if needed) **Match all**.
4. Click **Submit Update**. A message indicates the update was successful.
5. Click **OK**.

6.2.2.3 Adding or Editing Advanced Security

Use this procedure to add advanced security to an existing field. The field used must be one that has an option list associated with it. The option list must be created before this feature can be used.

You can add custom security only if the custom security feature is enabled.

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

1. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.
The [Configure Custom Security Page](#) opens. If necessary, click the **Advanced Custom Security** tab to open that page.
2. Click **Add**.
The [Select Security Dialog](#) opens.
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](#) opens showing the option items associated with the field that was chosen.
5. Choose the **Actions** menu for the option item that needs security. Click **Edit Security**.
The [Select Security Dialog](#) opens.
6. Select users or aliases who will have access to content items with that individual option list value. For details about choosing users or aliases, see [Section 5.8.1, "Setting ACLs During Software Use."](#)
7. If needed, select a security group from the list.
8. The [Advanced Custom Security Option Page](#) opens, showing the selections just made.

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

1. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.
The [Configure Custom Security Page](#) opens.
2. In the Advanced Custom Security area, choose **Edit Security** from the **Actions** menu of the option item. To remove security for the option item, choose **Remove Security** from the **Actions** menu of the option item.

When editing, a dialog opens so you can select a field for use. Only fields with option lists are available for selection.

3. Click **OK**.

The [Advanced Custom Security Option Page](#) opens showing the option items associated with the field that was chosen.

4. Choose **Edit Security** from the **Actions** menu for the option item that needs security.

The [Select Security Dialog](#) opens.

5. Select users or aliases who will have access to content items with that individual option list value. For details about choosing users or aliases, see [Section 5.8.1, "Setting ACLs During Software Use."](#)

6. If needed, select a security group from the list.

7. The [Advanced Custom Security Option Page](#) opens, showing the selections just made. The security is now in place.

6.2.2.4 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.

The [Configure Custom Security Page](#) opens.

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

The Information Page opens.

3. Click **OK** when done.

6.2.2.5 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**.

The [Configure Custom Security Page](#) opens.

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

3. A message is displayed, indicating the deletion was successful.

4. Click **OK**.

6.2.3 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 WebCenter Content assigns the u prefix. Assign the field options to the user.
3. Rebuild the search index, and restart Content Server. Complete instructions are in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.
4. [Create the Custom Security Field](#) using the exact field names defined in the Oracle WebCenter Content 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](#).

6.2.3.1 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. Choose **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 opens.
5. Type `ProjectName`, and click **OK**. The Add Custom Info Field page opens. Specify the field attributes:
 - a. For **Field Caption**, 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, select **Long Text**.
 - c. Select **Enable Options List**. The **Configure** button is enabled. Click this button.
 - d. The Configure Option List page opens. In the **Options List Type**, select the **Edit and Multiselect List** option.
 - e. Click **Edit** next to **Use Option List**. The Option List page opens.
 - 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**.

6.2.3.2 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. Choose **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 opens.
5. Type `ProjectName` and click **OK**. The Add Metadata Field page opens. Specify the field attributes:
 - a. For **Field Caption**, 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, select **Long Text**.
 - c. Select **Enable Options List**. The Options List Settings tab is enabled.
 - d. In the **Options List Type**, click the **Edit and Multiselect List** option.
 - e. Choose **Edit**. The Option List page opens.
 - 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 user named `User1` then select that name and click **Edit**. The Edit User page for the user opens.
 - a. In the Project Name list, click the down arrow, and select 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 Content Server.

6.2.3.3 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](#) opens.
3. In **Custom Security Field**, type `Project Name`.
4. From the **Content Field** list, select **ProjectName**.
5. From the **User Field** list, select **ProjectName**.
6. Select **Match all** 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**.

6.2.3.4 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.

6.3 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:

- [Section 6.3.1, "About Classification Guides"](#)
- [Section 6.3.2, "Managing Classification Guides"](#)

6.3.1 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.

6.3.2 Managing Classification Guides

The following tasks are performed when managing classification guides:

- [Section 6.3.2.1, "Creating or Editing a Classification Guide"](#)
- [Section 6.3.2.2, "Deleting a Classification Guide"](#)
- [Section 6.3.2.3, "Viewing Classification Guide Information"](#)
- [Section 6.3.2.4, "Creating or Editing a Classification Topic"](#)
- [Section 6.3.2.5, "Editing Classification Topic Settings"](#)
- [Section 6.3.2.6, "Deleting a Classification Topic"](#)

6.3.2.1 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

2. Click **Add**.

The [Create or Edit Classification Guide Page](#) opens.

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

An information page opens 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.

4. Click **OK** to return to the [Configure Classification Guide Page](#).

Use this procedure to edit a classification guide:

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

The [Configure Classification Guide Page](#) opens.

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

The Classification Guide Information Page opens.

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

The [Create or Edit Classification Guide Page](#) opens.

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

A information page opens 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.

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

6.3.2.2 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

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](#).

6.3.2.3 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

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

The [Configure Classification Guide Page](#) opens.

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.

3. Click **OK** to return to the [Configure Classification Guide Page](#).

6.3.2.4 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

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

The [Configure Classification Guide Page](#) opens.

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

The [Administer Classification Topic Page](#) opens.

4. Click **Add**.
5. The [Create or Edit Classification Topic Page](#) opens.
6. Provide a name and description for the classification topic, and click **Create** when done.
7. The [Configure Topic Settings Page](#) opens.
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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

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

The Classification Guide Information Page opens.

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

The [Administer Classification Topic Page](#) opens.

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

The Classification Topic Information Page opens.

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

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

A confirmation page opens.

7. Click **OK** to return to the [Administer Classification Topic Page](#).

6.3.2.5 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.

The [Configure Classification Guide Page](#) opens.

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

The Classification Guide Information Page opens.

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

The [Administer Classification Topic Page](#) opens.

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

The Classification Topic Information Page opens.

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 opens.
7. Click **OK** to return to the [Administer Classification Topic Page](#).

6.3.2.6 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.
The [Configure Classification Guide Page](#) opens.
2. In the list select the classification guide whose topic to delete, and click **Info**.
The Classification Guide Information Page opens.
3. From the Page menu, choose **Configure Topics**.
The [Administer Classification Topic Page](#) opens.
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](#).

6.3.2.7 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Classification Guide**.
The [Configure Classification Guide Page](#) opens.
2. In the list, select the classification guide whose topic information is to be viewed, and click **Info**.
The Classification Guide Information Page opens.
3. From the Page menu, choose **Edit** then choose **Configure Topics**.
The [Administer Classification Topic Page](#) opens.
4. From the **Topic Name** list, select the classification topic to view, and click **Info**.
The Classification Topic Information Page opens.
5. Click **OK** to return to the [Administer Classification Topic Page](#).

6.4 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:

- [Section 6.4.1, "Supplemental Markings Details"](#)
- [Section 6.4.2, "Managing Supplemental Markings"](#)

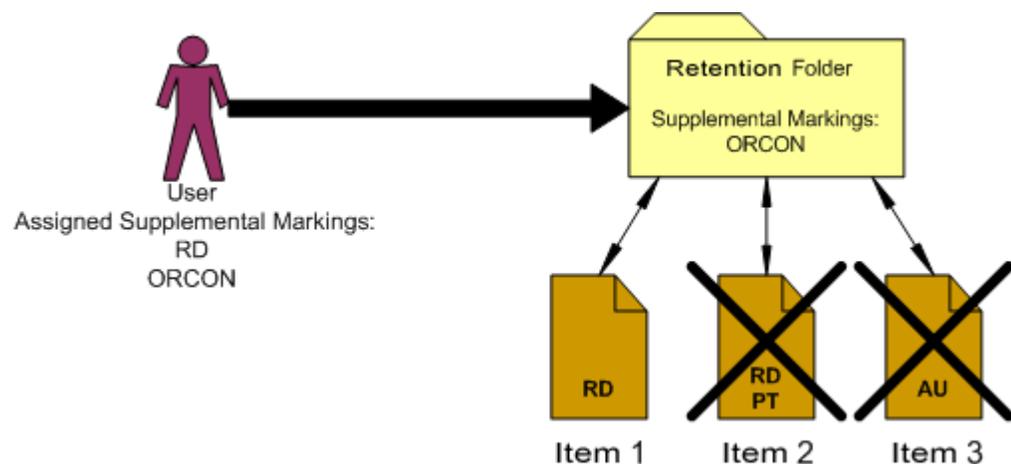
6.4.1 Supplemental Markings Details

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, deselect *Supplemental Markings* 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 6–3 User Must Match All Supplemental Markings

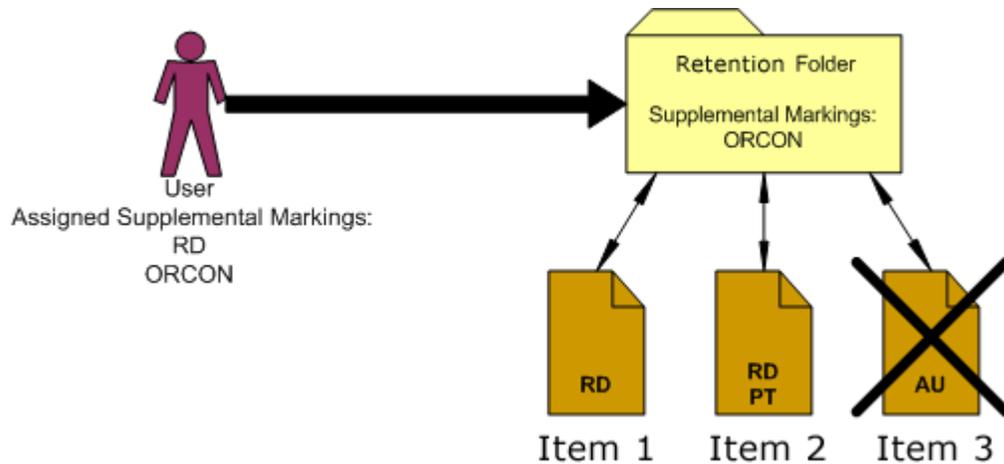


For example, in the diagram above, the user is assigned the supplemental markings RD and ORCON. The folder is marked with ORCON, therefore the user can access the folder.

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 6–4 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, either access granted or access denied to users. In contrast, the classified security does have a hierarchy to its classification levels. For further information, see [Section 6.1.1.2, "Classified Records Security Hierarchy."](#)

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 WebCenter Content administrative permissions are required to perform this action.

6.4.2 Managing Supplemental Markings

The following procedures are followed when managing supplemental markings:

- [Section 6.4.2.1, "Enabling or Disabling Supplemental Markings"](#)
- [Section 6.4.2.2, "Creating or Editing a Supplemental Marking"](#)
- [Section 6.4.2.3, "Viewing Supplemental Marking Information and References"](#)
- [Section 6.4.2.4, "Deleting a Supplemental Marking"](#)
- [Section 6.4.2.5, "Assign or Remove User Supplemental Markings"](#)
- [Section 6.4.2.6, "Using Restricted and Formerly Restricted Supplemental Markings"](#)

6.4.2.1 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. Choose **Records** then **Configure** then **Settings** from the Top menu.
The [Configure Retention Settings Page](#) opens. Expand the Security section if needed.
2. Select **Supplemental Markings**.
3. (Optional) To force a user to match **all** supplemental markings assigned to an item or record folder before granting access, select **User must match all Supplemental Markings**. To allow access if the user has at least one of the markings, leave the checkbox unselected.
4. Click **Submit**. A confirmation message is displayed.

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

6.4.2.2 Creating or Editing a Supplemental Marking

You can create supplemental markings only if they are enabled. For details, see [Section 6.4.2.1, "Enabling or Disabling Supplemental Markings."](#)

After creating a supplemental marking, it is available to apply 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Supplemental Markings**.
The [Configure Supplemental Markings Page](#) opens.
2. Click **Add**.
The [Create or Edit Supplemental Marking Page](#) opens.
3. Enter a name using a maximum of 30 characters.
4. Enter a description of the marking with a maximum of 30 characters.
5. Click **Create**.
6. The Supplemental Marking Information Page opens 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Supplemental Markings**.
The [Configure Supplemental Markings Page](#) opens.
2. You can edit the marking in one of two ways:
 - Choose **Edit Marking** from the item's **Actions** menu. The [Create or Edit Supplemental Marking Page](#) opens.
 - Choose the name of the marking to edit. The Supplemental Marking Information Page opens. Choose **Edit** from the Page menu. The [Create or Edit Supplemental Marking Page](#) opens.
3. Make the changes and click **Submit Update**. The Supplemental Marking Information Page opens 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.

6.4.2.3 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Supplemental Markings**.

The [Configure Supplemental Markings Page](#) opens.

2. Click the name of the marking with information to view.
3. The Supplemental Marking Information Page opens. Use the page to edit or delete the marking, or view references to the marking by choosing the appropriate option on the Page menu.
4. Click **OK** when done.

6.4.2.4 Deleting a Supplemental Marking

You can delete supplemental markings regardless of whether markings are enabled. A supplemental marking cannot be deleted until all 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 WebCenter Content Administrator's Guide for Records* 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. Choose **Records** then **Configure** from the Top menu. Choose **Security** then **Supplemental Markings**.

The [Configure Supplemental Markings Page](#) opens.

2. Choose **Delete** from the item's **Actions** menu. To delete multiple markings, select the checkbox next to the marking name and choose **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 WebCenter Content Administrator's Guide for Records*.

6.4.2.5 Assign or Remove User Supplemental Markings

Permissions: Administrator privileges in Oracle WebCenter Content 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. Choose **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 opens.
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. Multiple markings can be assigned to a user.
5. Click **OK**. Repeat the process for each user who needs markings.
6. Restart Content Server.

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

1. Choose **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 opens.
4. In the **Supplemental Markings** field, delete a marking by editing the text in the **Supplemental Markings** field.

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 Content Server. For more information about restarting, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.4.2.6 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 [Section 6.4.2.1, "Enabling or Disabling Supplemental Markings"](#)).
2. Click *Restricted Data* or *Formerly Restricted Data* as the supplemental marking.
3. Restart Content Server.

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:

- [Section 7.1, "Retention Options"](#)
- [Section 7.2, "PCM Options"](#)
- [Section 7.3, "Setting Up Workflows"](#)
- [Section 7.4, "Configuration with Desktop Integration Suite"](#)
- [Section 7.5, "Configuration Variables"](#)

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.

- [Section 7.1.1, "Setting the Fiscal Calendar"](#)
- [Section 7.1.2, "Setting Performance Monitoring"](#)

Most of these options can be set by selecting the checkbox next to the option. For details about each option, see [Section A.2, "Configure Retention Settings Page."](#) Other options that require further configuration are discussed later in this section.

General configuration choices are available by choosing **Records** then **Configure** from the Top menu. Choose **Settings** to open the [Configure Retention Settings Page](#).

General options:

- **Start of fiscal calendar:** Sets the start date for the calendar used for fiscal accounting. For details, see [Section 7.1.1, "Setting the Fiscal Calendar."](#)
- **Archive Metadata 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 shown. Options include when editing, deleting, or revising 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 on Retention Schedule objects based on Access Control Lists.
- **Default Oracle WebCenter Content 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:** Computes 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. Choose **Records** then **Configure** then **Settings** from the Top menu.
The [Configure Retention Settings Page](#) opens.
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. To enable this, choose **Records** then **Audit** from the Top menu. Choose **Configure** then **Performance Monitoring**.

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 WebCenter Content Administrator's Guide for Records*.

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, choose **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 WebCenter Content Administrator's Guide for Records* 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.

Note that if you enable the disposition workflow feature on the Configure Retention Settings page but do not set up the workflow, you must set the `UpdateDispositionsTableOnWorkflowApproval` configuration variable to `false` in the `config.cfg` file.

- **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 that 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 are 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 WebCenter Content Application Administrator's Guide for Content Server*. This section describes only the information needed to establish the three workflows necessary for Oracle WebCenter Content: Records.

- [Section 7.3.1, "Workflow Prerequisites and Process"](#)
- [Section 7.3.2, "Creating Necessary Workflows"](#)

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 WebCenter Content 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 Necessary 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 WebCenter Content: Records functionality:

- [Section 7.3.2.1, "Category Dispositions Workflow"](#)
- [Section 7.3.2.2, "Reservation Processing Workflow"](#)
- [Section 7.3.2.3, "Offsite Storage Workflow"](#)

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. Choose **Administration** then **Admin Applets** from the Main menu.
The Administration Applets Page opens.
2. Click **Workflow Admin**.
The Workflow Admin dialog opens.
3. Click the **Criteria** tab. Click **Add**.
The New Criteria Workflow dialog opens.
4. Enter the following information:
 - Workflow name: `CategoryDispositionsProcess`.
 - Description: `Category Disposition Processing`.
 - Security Group: Select **RecordsGroup** from the list.
 - Original Author Edit Rule: Select **Edit Revision**.
 - Has Criteria Definition: Select this checkbox.
 - Field: Select *Type* from the list.
 - Operator: This should say *Matches*.
 - Value: Select **RetentionCategory** from the list.
 Click **OK** when done. The Workflow Admin dialog opens.
5. In the Criteria portion of the dialog, in the Steps section, click **Add**.
The Add New Step dialog opens.
6. Enter the following information:
 - Step name: `CategoryDispositionsReview`.
 - Description: `Review Category Dispositions`.
 - Users can review and edit (replace) the current revision: Select this checkbox.
 - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will review dispositions and click **OK**.
 - Click the **Exit Condition** tab. In the Required Approvers portion, select the checkbox for **All Reviewers**.
7. Click **OK**. The Workflow Admin dialog opens.
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. Choose **Administration** then **Admin Applets** from the Main menu.
The Administration Applets Page opens.
2. Click **Workflow Admin**.
The Workflow Admin dialog opens.
3. Click the **Criteria** tab. Click **Add**.
The New Criteria Workflow dialog opens.
4. Enter the following information:
 - Workflow name: `ReservationProcess`.
 - Description: `Processes reservations`.
 - Security Group: select **Reservation**.
 - Original Author Edit Rule: Select **Edit Revision**.
 - Has Criteria Definition: Select this checkbox.
 - Field: Select **Type**.
 - Operator: This should say **Matches**.
 - Value: Select **Request**.Click **OK** when done. The Workflow Admin dialog opens.
5. In the Criteria portion of the dialog, in the Steps section, click **Add**.
The Add New Step dialog opens.
6. Enter the following information for the first step:
 - Step name: `RequestReview`
 - Description: `Review Request`
 - Users can review and edit (replace) the current revision: selected.
 - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will review reservation requests and click **OK**.
 - Click the **Exit Condition** tab. In the Required Approvers portion, select **At Least This Many Reviewers** and enter 1 for the value.
 - Click **OK**. The Workflow Admin dialog opens.
7. In the Criteria portion of the dialog, in the Steps section, click **Add**.
The Add New Step dialog opens.
8. Enter the following information for the second step:
 - Step name: `RequestComplete`
 - Description: `Complete the request`
 - Users can review the current revision: selected.
 - Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will complete the reservation requests and click **OK**.
 - Click the **Exit Condition** tab. In the Required Approvers portion, select **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 select **Custom Script Evaluation**. Enter the following code

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

Click **OK**.

- Click **Edit** in the Update section. Click the **Custom** tab then select **Custom Script Evaluation**. 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 opens.
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. Choose **Administration** then **Admin Applets** from the Main menu.

The Administration Applets Page opens.

2. Click **Workflow Admin**.

The Workflow Admin dialog opens.

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

The New Criteria Workflow dialog opens.

4. Enter the following information:

- Workflow name: `OffsiteProcess`.
- Description: `Processes Offsite Requests`.
- Security Group: select **Offsite**.
- Original Author Edit Rule: select **Edit Revision**.
- Has Criteria Definition: selected.
- Field: select **Type**.
- Operator: this should say `Matches`.
- Value: select **Offsiterequest**.

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

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

The Add New Step dialog opens.

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**: selected.

- Click the **Users** tab then click **Add Alias**. Select the alias list for the users who will review reservation requests and click **OK**.
 - Click the **Exit Condition** tab. In the Required Approvers portion, select **At Least This Many Reviewers** and enter 1 for the value.
7. Click **OK**. The Workflow Admin dialog opens.
 8. Click **Enable** to start the workflow.

7.4 Configuration with Desktop Integration Suite

When using Oracle DIS with the Records system 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, that means an item cannot be checked in if the field is empty.

Because copying and pasting or dragging and dropping into a folder often does not require any additional user interaction, the checkin will not complete successfully unless the administrator configures the Records system 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 is an overview of the more commonly used configuration variables. For details about each variable, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

- `AllowRetentionPeriodWithoutCutoff`: Used to specify retention periods for triggers.
- `dodSkipCatFolderRequirement`: Allows items to be checked in without specifying a category or folder for the checkin. If a DoD configuration is in use, this causes non-conformance with DoD regulations.
- `HideVitalReview`: Used to hide the Subject to Review fields.
- `RecordsManagementDenyAuthorFreePassOnRMSecurity`: Allows the author of content to delete content they authored regardless of the user's security settings.
- `RecordsManagementNumberOverwriteOnDelete`: Sets the number of disk scrubbing passes used for a destroy action.
- `RmaAddDocWhereClauseForScreening`: 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.

- `RmaAllowKeepOrDestroyMetadataOption`: Allows the option to keep or destroy metadata when using the following disposition actions: Delete All Revisions, Accession, Archive, Move, and Transfer.
- `RmaEnableWebdavPropPatchOnExport`: Enables WebDAV support of a `PropPatch` method to assign metadata values to a file that has been uploaded to a WebDAV server.
- `RmaEnableFilePlan`: Enables the File Plan folder structure.
- `RmaEnableFixedClone`: Enables the fixed clone functionality that allows the creation of record clones of content revisions.
- `RmaEnablePostFilterOnScreening`: 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.
- `RmaFilePlanVolumePrefix` and `RmaFilePlanVolumeSuffix`: Defines the naming convention for volumes.
- `RmaFixedClonesTitleSuffix`: Used to set the suffix that is automatically appended to a fixed clone content item.
- `RMAHideExternalFieldsFromSearchInfo` and `RMAHideExternalFieldsFromCheckInUpdate`: Used to hide external fields on the noted pages. The default setting is `TRUE`, so External fields are hidden on those screens.
- `RmaNotifyDispReviewerAndCatAuthor`: Used to control who is notified about disposition actions.
- `RmaNotifyReviewerAndAlternateReviewer`: Used to control what reviewers are notified about actions.
- `ShowContentForStorageBrowse`: Used to show content items in the storage browse screens.
- `SimpleProfilesEnabled`: Used to enable Simple Profile functionality.
- `UieHideSearchCheckboxes`: Used to show or hide the metadata field checkboxes on the search page, which limit the number of metadata fields initially shown on the page.

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:

- [Section 8.1, "Physical Content Management"](#)
- [Section 8.2, "Configuring Chargeback Processing"](#)
- [Section 8.3, "Configuring Location Types"](#)
- [Section 8.4, "Configuring Object Types"](#)
- [Section 8.5, "Configuring Media Types"](#)
- [Section 8.6, "Configuring Default Metadata Values: Offsite and Reservations"](#)

8.1 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.

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 are 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, this is used to create barcode labels for items, storage, and customers.

- **Retention management:** Sets up retention schedules for external items and freezes them, sends e-mail 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 WebCenter Content Administrator's Guide for Records* 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, "Security Overview,"](#) 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). For details, see [Section 8.2, "Configuring Chargeback Processing."](#)
- **Configure location types,** which define the locations that hold physical content. Location types can include warehouses, rooms, bays, shelves, and other storage areas. For details, see [Section 8.3, "Configuring Location Types."](#)
- **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. For details, see [Section 8.4, "Configuring Object Types."](#)
- **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 such as mixed, CD, Disc, or DVD. For details, see [Section 8.5, "Configuring Media Types."](#)
- **Configure default reservation information.** Default metadata values can be set for reservations and for items that are stored offsite (as discussed in the *Oracle WebCenter Content Administrator's Guide for Records*). For details, see [Section 8.6, "Configuring Default Metadata Values: Offsite and Reservations."](#)
- **Create barcode labels for content, storage and users.** Default values are provided for users but barcode labels can also be designed. See the *Oracle WebCenter Content Administrator's Guide for Records* 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. Physical Content Management 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 WebCenter Content User's Guide for Records* 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. The following topics are discussed in this section:

- [Section 8.3.1, "Predefined Location Types"](#)
- [Section 8.3.2, "Location Type Icons"](#)
- [Section 8.3.3, "Creating or Editing a Location Type"](#)
- [Section 8.3.4, "Viewing Location Type Information"](#)
- [Section 8.3.5, "Deleting a Location Type"](#)
- [Section 8.3.6, "Reordering Location Types"](#)
- [Section 8.3.7, "Example: Creating a Location Type"](#)

8.3.1 Predefined Location Types

The default 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
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 [Section 8.3.7, "Example: Creating a Location Type."](#)

1. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.

The [Configure Location Types Page](#) opens

2. Click **Add**.

The [Create or Edit Location Type Page](#) opens.

3. Specify the properties of the location type:
 - Location Type ID: An identifier for the location type displayed in the location type hierarchy. Maximum characters: 30.
 - Location Name: Name for the type. Maximum characters allowed: 30.
 - Description: A brief description of the type.
 - Tooltip: Text that appears if the mouse cursor is held over the option in the location type selection list. Maximum characters: 30
 - Allow storage of content (default): Select to allow the location type to 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 that 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: available only if **Allow storage of content (default)** is selected. This 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.
4. Click **OK** when done. The new location type is now added to the bottom of the list on the [Configure Location Types Page](#). If required, click 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 choose **Edit** from the **Actions** 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.
The [Configure Location Types Page](#) opens.
2. Select the location type and click the **Info** icon.
The information page opens. 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.

The [Configure Location Types Page](#) opens.

2. Select the location type to delete and click **Info**.

The information page opens. Choose **Delete** from 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.

The [Configure Location Types Page](#) opens.

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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.

The [Configure Location Types Page](#) opens.

2. Click **Add**.

The [Create or Edit Location Type Page](#) opens.

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 **Allow storage of content (default)** 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](#) opens 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. 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](#).

The following topics are discussed regarding object types:

- [Section 8.4.1, "Predefined Object Types"](#)
- [Section 8.4.2, "Creating or Editing an Object Type"](#)
- [Section 8.4.3, "Viewing Object Type Information"](#)
- [Section 8.4.4, "Deleting an Object Type"](#)
- [Section 8.4.5, "Editing Object Type Relationships"](#)

8.4.1 Predefined Object Types

Physical Content Management 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. For details, see [Section 8.5, "Configuring Media Types."](#)

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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**.
The [Configure Object Types Page](#) opens.
2. Click **Add** in the Object Types Table area.
The [Create or Edit Object Type Page](#) opens.
3. Specify the properties of the object type and click **Create**.
A message 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, choose **Edit Object Type** from the item's **Actions** 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**.
The [Configure Object Types Page](#) opens.
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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**.
The [Configure Object Types Page](#) opens.
2. In the list of existing object types, choose **Delete Object Type** from the **Actions** menu for the object. To delete multiple types, select the checkbox for the type then choose **Delete** from 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**.
The [Configure Object Types Page](#) opens.
2. In the list of existing object types, select the item to edit and choose **Edit Object Type Relationships** from the **Actions** menu.
The [Edit Object Type Relationships Page](#) opens.
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 information page opens again with updated values for the **Object Type Hold** field.

8.5 Configuring Media Types

Media types are an extension to object types 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.

The following topics are discussed regarding media types:

- [Section 8.5.1, "Predefined Media Types"](#)
- [Section 8.5.2, "Creating or Editing a Media Type"](#)
- [Section 8.5.3, "Viewing Media Type Information"](#)
- [Section 8.5.4, "Deleting a Media Type"](#)

8.5.1 Predefined Media Types

Physical Content Management 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 BluRay	Optical
Mixed Audio Data Visual	Tape

Predefined Media Types	Object Type
Mixed	All
Audio	
Box	
CD	
Data	
Disc	
Dvd	
BluRay	
Fax	
Folder	
Microfiche	
Microfilm	
Paper	
Photo	
Visual	

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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Media Types**.

The [Configure Media Types Page](#) opens.

2. Click **Add** in the Media Types area.

The [Create or Edit Media Type Page](#) opens.

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, choose **Edit** from the media type's **Actions** 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Media Types**.

The [Configure Media Types Page](#) opens.

2. In the list of existing media types, click **Info** for the type to view.

The Information Page opens. 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. Choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Media Types**.

The [Configure Media Types Page](#) opens.

2. Choose **Delete Media Type** from the **Actions** menu for the item to be deleted. To delete multiple items, select the checkbox for the item and choose **Delete** from 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. For details about creating and enabling the reservation workflow, see [Section 7.3, "Setting Up Workflows."](#)

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, choose **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. Choose **Physical** then **Configure** from the Top menu. Choose **Metadata** then **Reservation Default Metadata**. To configure offsite storage, choose **Physical** then **Configure** then **Offsite** then **Offsite Default Metadata**.

The [Default Metadata for Checked-in Reservation or Offsite Entries Page](#) opens.

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.

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:

- [Section 9.1, "Storage Space Considerations"](#)
- [Section 9.2, "Browsing the PCM Storage Space"](#)
- [Section 9.3, "Managing Storage Spaces"](#)
- [Section 9.4, "Example: Creating a Single Storage Location"](#)
- [Section 9.5, "Example: Creating a Batch of Storage Locations"](#)

See the *Oracle WebCenter Content Administrator's Guide for Records* for details about setting up offsite storage.

9.1 Storage Space Considerations

Storage space is discussed in more detail in the *Oracle WebCenter Content User's Guide for Records*. See that document for background and conceptual information.

Consider the following issues concerning 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 or 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 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 that 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 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

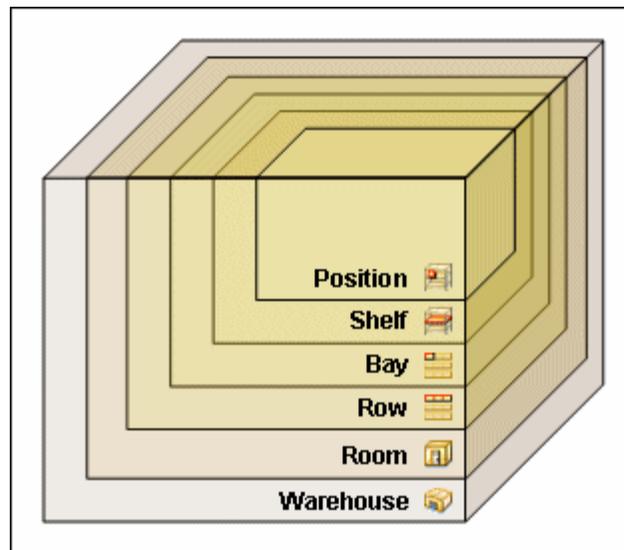
PCM uses a defined space environment to keep track of the storage and retention of physical items. When working with a physical item, assign the item to a storage location, so PCM knows where it is stored and can track it.

This section describes browsing the defined storage environment in PCM. It covers the following topics:

- [Section 9.2.1, "Storage Space Hierarchy"](#)
- [Section 9.2.2, "Storage Location Properties"](#)

9.2.1 Storage Space Hierarchy

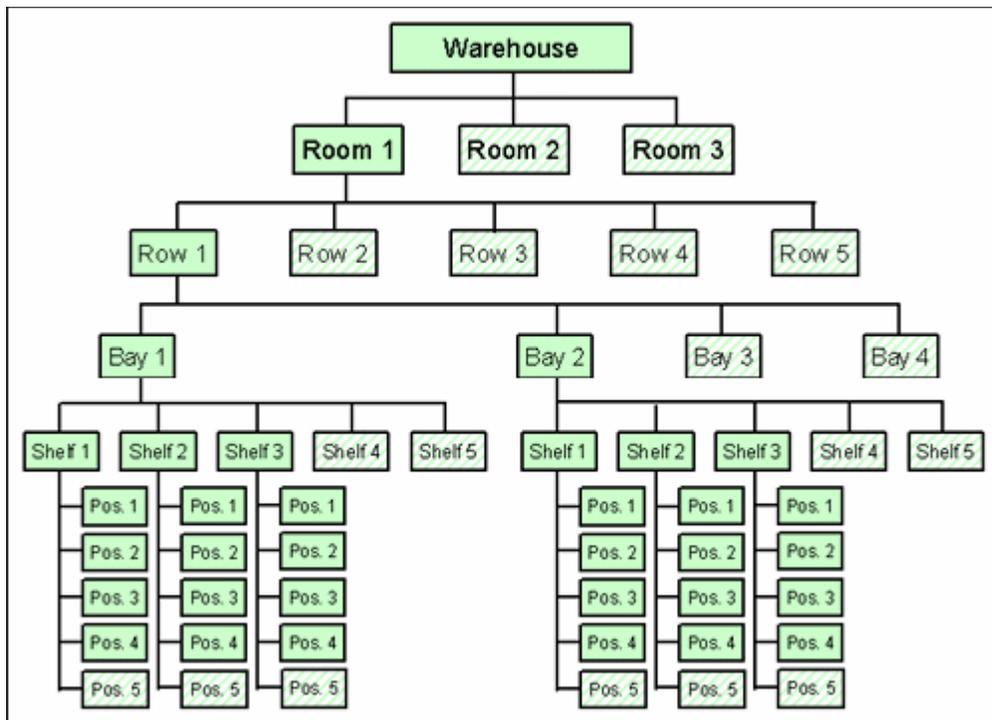
Storage space in PCM is set up hierarchically. Storage locations contain other, smaller storage locations that contain still smaller storage locations, and so on. The following storage space hierarchy (from large to small) is provided by default:

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 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:

- [Section 9.2.2.1, "Location Type"](#)
- [Section 9.2.2.2, "Object Type"](#)
- [Section 9.2.2.3, "Media Type"](#)
- [Section 9.2.2.4, "Storage Status"](#)

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 [Section 8.3, "Configuring Location Types,"](#) [Section 8.4, "Configuring Object Types,"](#) and [Section 8.5, "Configuring Media Types."](#)

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 following predefined location types (in hierarchical order) are provided:

- Warehouse
- Room
- Row
- Bay
- Shelf
- Position

Storage of content applies to a particular level, not to lower levels. For example, shelves have a number of 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).

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, etc.

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 following predefined object types are provided:

- 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.

Several predefined media types are provided, 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. For details, see [Section 9.2.2.2, "Object Type."](#) 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
Optical	Mixed CD Disc DVD BluRay
Tape	Mixed Audio Data Visual
All	Mixed Audio Box CD Data Disc Dvd BluRay 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:

- [Section 9.3.1, "Creating a Storage Location"](#)
- [Section 9.3.2, "Batch Creating Storage Locations"](#)
- [Section 9.3.3, "Editing a Storage Location"](#)
- [Section 9.3.4, "Viewing Information about a Storage Location"](#)
- [Section 9.3.5, "Deleting a Storage Location"](#)
- [Section 9.3.6, "Blocking a Storage Location"](#)
- [Section 9.3.7, "Reserving or Canceling a Reservation for a Storage Location"](#)
- [Section 9.3.8, "Viewing All Items in a Storage Location"](#)
- [Section 9.3.9, "Printing Labels for Storage Locations"](#)

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 opens.

2. To create a location at the topmost level of the hierarchy, choose **Create** then **Define Storage Location** from the page **Actions** menu. You can also choose **Create Storage Location** from the **Actions** menu for a storage location in the list to add a new child storage location at that level.

The [Create or Edit Storage Page](#) opens.

3. Specify the storage location properties:
 - **Storage Name:** Name for this storage area. Maximum characters allowed: 30.
 - **Description:** A brief description of the location. Maximum characters allowed: 30.
 - **Location Type:** The type of storage location. Select a type from the list. The available types depend on where the storage area is created in the storage hierarchy.
 - **Allow Storage of Content:** If selected, 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 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 selected, all fields (except Requestor) below it become available.

- Status: Available only for locations that can hold items. The status of the location (for example, *Available*).
 - Requestor: Available only for locations that can storage content and if the storage status is set to Reserved. Specifies the user who reserved the storage location.
 - Location Holds: Available for locations that can hold items. The type of physical items stored in the storage location. If an object type is not specified, 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 locations that can hold items. Specifies the maximum number of items the location can hold, 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 locations that can hold items. The barcode for the item. If not specified, a random 19 digit number is assigned.
 - Addressing Information: Address, city, state, zip code and other information for offsite storage location.
 - Offsite Ship To Code: Only available when Offsite Storage is enabled. The Ship To code for offsite storage.
4. 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 defines 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.

For an example of this process, see [Section 9.5, "Example: Creating a Batch of Storage Locations."](#)

1. Choose **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

The [Create Batch Storage Import File Page](#) opens.

2. Click **Browse**.

The [Select Storage Location Dialog](#) opens.

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:

- **Location Type:** Choose a location from the list of location types.
- **Name Prefix:** A prefix for the storage name. This prefix is included in the name and the description of the storage location. If not specified, the name and description will contain only numbers (for example, 003).
- **Start Number:** The starting number for the number sequence that is included in the name and description of the storage location. If not specified, 1 (one) is assumed.
- **Number of Items:** 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, which will result in names such as Warehouse_NNN (for example, Warehouse_003).

The `AutoStorageNumberWidth` parameter in the `storagecreationutility_environment.cfg` file can be modified to change this. Restart Content Server after changing the parameter value.

- **Allow Content:** If selected, items can 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 select this option and set the position location to allow storage.

- **Number of Content Items Allowed:** Available if **Allow Content** is selected. 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. This designates 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.

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 that 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 appear 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 Content Server after changing the parameter value.
6. Click **OK**.
- The Exploring Page opens 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 opens.
2. Choose **Edit** then **Edit Storage Location** from the **Actions** menu of the item to edit.
The [Create or Edit Storage Page](#) opens.
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. Choose **Physical** then **Storage** from the Top menu.
The Exploring Page for the top level of the storage hierarchy opens.
2. Click the **Info** icon for the storage location or choose **Information** then **Storage Information** from the location's **Actions** menu.
The Storage Information Page opens listing the current storage location properties.

3. Click **OK** when done.

The Exploring Page opens 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 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 opens.

2. Navigate to the storage location to delete, and choose **Delete** then **Delete Storage Location** from the item's **Actions** menu.

To delete multiple storage locations from the exploring pages select their checkboxes and choose **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 opens.

2. Navigate to the storage space level to block and choose **Edit** then **Block Storage** from the level's **Actions** menu.

The initial Exploring Page opens 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. For details, see [Section 9.3.3, "Editing a Storage Location."](#) 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 opens.

2. Navigate to the storage space level that includes the storage location to reserve.
3. Choose **Edit** then **Reserve Storage** on the location's **Actions** menu.
4. Select the requestor reserving the space from the list of users.
5. The initial Exploring Page opens 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 **Actions** 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 opens.

2. Navigate to the storage space level that includes the storage location with items to view. Choose **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. Choose **Information** on the **Actions** 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 opens.

2. Navigate to the storage space level.
3. Depending on the current storage location, choose **Create Reports** from the **Actions** 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. Choose **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. Choose **Browse Content** then **Browse Storage** from the Top menu.

The Exploring Page for the top level of the storage hierarchy opens.

You can also access the top-level storage Exploring Page from the [Configure Physical Settings Page](#).

2. Choose **Create Storage Item** on the menu bar at the top of the page.

The [Create or Edit Storage Page](#) opens.

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. Choose **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

The [Create Batch Storage Import File Page](#) opens.

2. Click **Browse** to select the highest point of the hierarchy. If not selected, the 'Storage' level is defaulted.

The [Select Storage Location Dialog](#) opens. 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 opens.

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

The Import/Export Content and Record Archive Page opens.

2. Unselect all items (including those under **Show External Sources**) except for **Include Storage**.
3. Click **Browse** next to **Archive File** 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 WebCenter Content Administrator's Guide for Records*.

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:

- [Section 10.1, "Retention Schedule Overview"](#)
- [Section 10.2, "Using a Series"](#)
- [Section 10.3, "Retention Categories"](#)
- [Section 10.4, "Record Folders"](#)

10.1 Retention Schedule Overview

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 that 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.

Note that if the RoleEntityACL component is enabled on the Content Server system, that component does not affect any retention objects such as categories or folders. Therefore, the ability to use ACLs on a URM role is not enabled on category creation pages or folder creation pages even if the RoleEntityACL component is enabled. The use of role ACLs is enabled on the checkin page if the component is enabled.

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 life cycle. It is not intended to check content into the repository.

This section discusses the following topics:

- [Section 10.1.1, "Retention Schedules and MoReq2 File Plans"](#)
- [Section 10.1.2, "Retention Schedules and Folders Retention Functionality"](#)
- [Section 10.1.3, "Planning a Retention Schedule"](#)
- [Section 10.1.4, "Creating and Navigating Object Levels"](#)

10.1.1 Retention Schedules and MoReq2 File Plans

In previous versions of Oracle WebCenter Content: Records the term *file plan* was used to denote disposition schedules. It is now synonymous with *retention schedule* to designate 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 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 Records software has been configured to allow Create access only to those items that 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 Retention Schedules and Folders Retention Functionality

Folders Retention functionality is not available if DoD Baseline or DoD Classified is enabled.

The Folders Retention functionality is enabled when the FrameworkFolders component is enabled. Folders Retention allows you to group content items in a retention query folder then apply a retention action to the content in the folder. It does not apply the retention action to the folder itself.

If a content item has dispositions defined in both Content Server and in Oracle WebCenter Content: Records, only the disposition and schedule defined by the Records system is used.

Important: Because the life cycle information is not viewable when using Retention Folders, it is recommended that you use this functionality for less important items that do not need to be retained or tracked, such as drafts of documents or temporary items. More important documents that need to be tracked and retained should be handled using the Records retention schedules.

Retention actions include the following:

- Retention By Revision: used to specify how many revisions of an item to keep. For example, if a content item in the query folder has 8 revisions, when the retention rule is run, the first 3 revisions are deleted and the latest 5 revisions are retained. Note that if the Records system is installed, an item will not be deleted if it is frozen.
- Retention By Age: used to specify how long an item exists before it is deleted. If the Records system is installed, the options for periods are the periods specified in the Records configuration. If the Records system is not installed, all default periods except for fiscal periods are included.
- Retention By Category (only available if the Records system is installed and enabled): used to specify a category disposition to apply to a query folder. This is similar to specifying a category ID on a content item.

When specifying this option, you can also specify if the action requires approval. Approval is performed in the same manner as approvals in the Records system.

The following list summarizes the actions available with Retention Folders:

- If Oracle WebCenter Content: Records *is not* installed and enabled:
 - Retention By Category is not available for use
 - Retention By Revision AND Retention By Age can be combined
- If Oracle WebCenter Content: Records is installed and enabled:
 - Retention By Category is available for use

Note that delete dispositions in Folders Retention are treated differently than deletions in the Records system. The shortest delete interval is used in Folders Retention instead of the longest interval as is used in Oracle WebCenter Content: Records.

Folders Retention differs from using a Records retention schedule in that the life cycle of content that is managed by Folders Retention is not visible to the user. When content is managed via the Records system, the life cycle of the disposition schedule is

displayed by browsing for the folder then clicking **Information** then **Life Cycle** from the folder's **Actions** menu.

This feature uses scheduled jobs to run the retention rules. The following intervals can be specified:

- **Weeks/Days:** the job runs daily between the specified start and end time. It runs any Retention by Age rules that specify an age in days or weeks or any category dispositions that are defined as days or weeks.
- **Calendar Months:** the job runs monthly on the specified start day, and the specified start and end time. It runs any Retention By Age rules with an age specified in months (Calendar Months, Calendar Quarters, and so on). It also runs any category dispositions that are defined as months.
- **Calendar Years:** the job runs yearly on the specified month and day, and the specified start and end time. It runs any Retention By Age rules that specify an age in years and runs any category dispositions that are defined as years.
- **Fiscal Months:** the job is only created if Oracle WebCenter Content: Records is installed. This functions similarly as Calendar Months.
- **Fiscal Years:** the job is only created if Oracle WebCenter Content: Records is installed. It functions similarly as Calendar Years.
- **Retention Revisions:** the job is run periodically, determined by the interval specified. The default is one month. Specify the intervals of days, weeks, months, and years. This job runs all Retention By Revisions rules.

Folders Retention functionality can only be set up and managed by users with Content Server administrative privileges. A user with Records Administrator privileges cannot set up Folders Retention functionality unless that user also has Content Server administrative privileges.

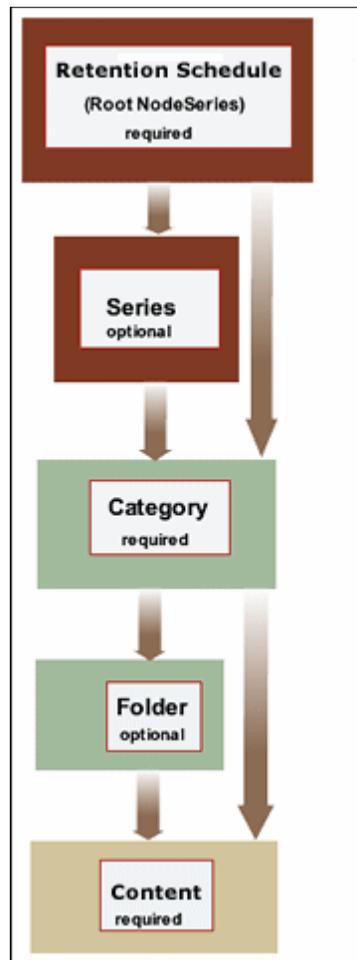
For details about accessing and setting up the Folders Retention functionality, see the *Oracle WebCenter Content Application Administrator's Guide for Content Server*.

10.1.3 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.

10.1.3.1 Retention Schedule Hierarchy

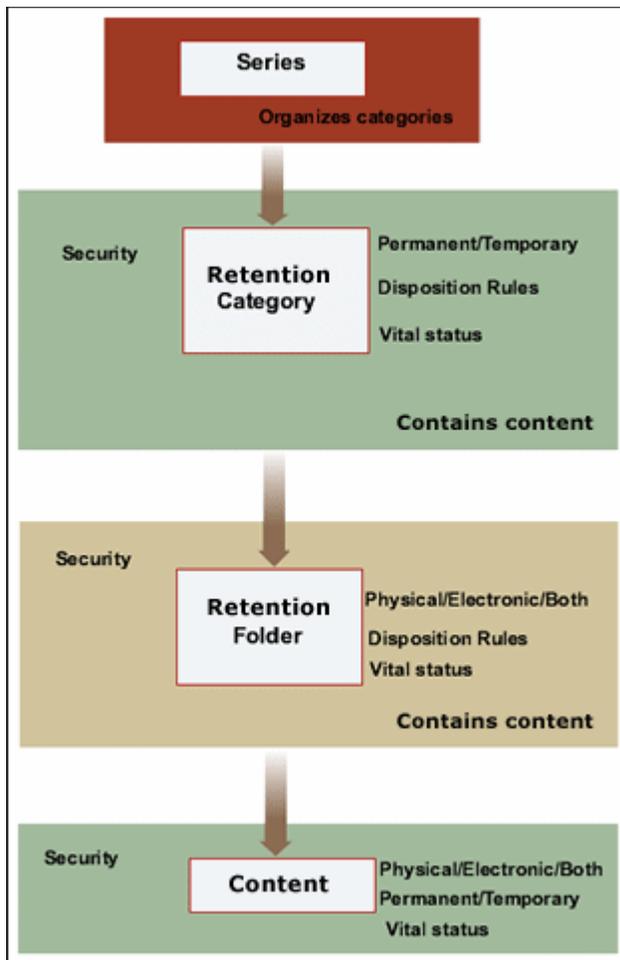
A typical hierarchy of a retention schedule consists of series, categories, and/or record folders. Series are optional top-level nodes that can be nested. A retention category cannot be nested, due to the nature of its disposition schedules. Record folders can be nested. The following figure shows the 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.

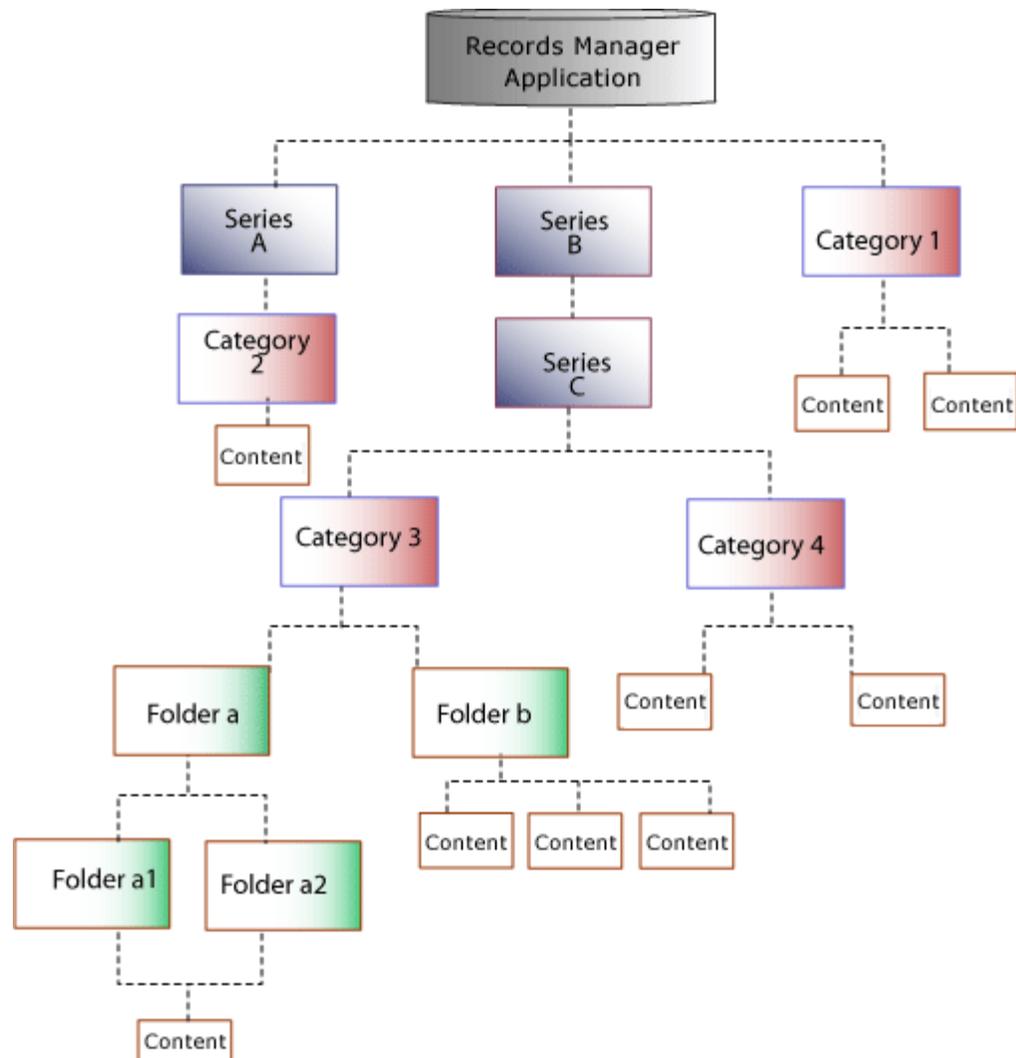
The figure below shows the main characteristics of each retention schedule object at a glance. Series do not have security set directly on the series object, whereas retention categories, record folders, and content all have a variety of security options, including Access Control Lists (ACLs), supplemental 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.

10.1.3.2 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, "Security Overview"](#).

10.1.3.3 Review Status Attributes

Review status, which includes the review period and reviewer, can be set at the retention category level, 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. If the shorter review period is removed or changed, the longer review period is used 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. 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.

10.1.3.4 Permanent Status Attributes

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.

10.1.3.5 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"](#).

10.1.3.6 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.

10.1.4 Creating and Navigating Object Levels

To use any retention objects, choose **Browse Content** from 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** menu 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	<ul style="list-style-type: none"> ■ Series ■ Retention category
Retention category	<ul style="list-style-type: none"> ■ Record folder ■ Content item
Record folder	<ul style="list-style-type: none"> ■ Record folder ■ Content item

10.1.4.1 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 that may appear depending on the location in the hierarchy. These options may appear on an individual item's **Actions** menu or on the Page menu.

Information in parenthesis indicates the area of the hierarchy where the information appears.

- **Information**
 - Category Information (Category level): Opens the [Retention Category Information Page](#).
 - Series Information (Series level): Opens the [Series Information Page](#).
 - Folder Information (Folder level): Opens the [Record Folder Information Page](#).
 - Metadata History (Category level and Folder level): Opens the [Metadata History Page](#).

- Disposition Information (Category level): Opens the [Disposition Information Page](#).
- Life Cycle (Folder level): Opens Life Cycle information. See the *Oracle WebCenter Content Administrator's Guide for Records* for details.
- Recent Reviews (Folder level): Opens review history information. See the *Oracle WebCenter Content Administrator's Guide for Records* 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): Opens the [Create or Edit Retention Category Page](#).
 - Edit Disposition (Category level): Opens the [Disposition Instructions Page](#).
 - Edit Review (Category level and Folder level): Opens the Edit Review information screen. See the *Oracle WebCenter Content Administrator's Guide for Records* for details.
 - Edit Series (Series level): Opens the [Create or Edit Series Page](#).
 - Move (all): Opens the [Select Retention Series, Record Folder or Category Dialog](#).
 - Hide (Series level): Opens 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): Opens the [Create or Edit Record Folder Page](#).
 - Check In Content (Category level and Folder level): Opens the Content Checkin Page.
 - Check in Physical Item: Opens the Create Physical Item Page.
 - Create Series (Series level): Opens the [Create or Edit Series Page](#).
 - Create Retention Category (Series level): Opens the [Create or Edit Retention Category Page](#).
- **Change View**
 - Thumbnail: Presents a icon-based view.
 - Headline: Presents a horizontal, textual view.

In addition, the following options may be available on the individual item's **Actions** 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. Note that to undo the obsolete status for content items, you must search for the items, select the checkboxes for those items to be marked, then select **Clear Dates** then **Obsolete** from the Set Dates menu.
- **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:

- [Section 10.2.1.1, "Creating or Editing a Series"](#)
- [Section 10.2.1.2, "Viewing Series Information"](#)
- [Section 10.2.1.3, "Hiding and Unhiding a Series"](#)
- [Section 10.2.1.4, "Moving a Series"](#)
- [Section 10.2.1.5, "Deleting a Series"](#)

The retention schedule can be accessed in two ways:

- Choose **Browse Content** then **Retention Schedule** from the Main menu.
- Choose **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. Choose **Create** then **Create Series** from the **Actions** menu in an existing series or from the Page menu.
The [Create or Edit Series Page](#) opens.
3. Enter an identifier for the series.
4. Enter a name for the series.
5. Click **Create**. The series is shown 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. Choose **Edit** then **Edit Series** in the **Actions** menu for the series to edit.
The [Create or Edit Series Page](#) opens.
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](#) opens. 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. Choose **Edit** then **Hide Series** from the **Actions** 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 choose **Unhide Series** in the item's **Actions** 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. Choose **Edit** then **Move Series** from the **Actions** menu for the item to move. To move multiple items, select the checkbox for the series and choose **Move** from the Table menu.

The [Select Retention Series, Record Folder or Category Dialog](#) opens.

2. Click to expand the tree, and click the series that will contain the item. The location field populates with the new location.
3. Click **OK**. The Exploring Series Page shows 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, select the checkbox for the items and choose **Delete** from the Table menu.

1. Access the retention schedule. Choose **Delete** then **Delete Series** from the **Actions** 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, select 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:

- [Section 10.3.1, "Managing Retention Categories"](#)
- [Section 10.3.2, "Retention Category Example"](#)

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:

- Choose **Browse Content** then **Retention Schedule** from the Main menu.
- Choose **Records** then **Retention Schedules** from the Top menu.

10.3.1 Managing Retention Categories

The following tasks are involved in managing retention categories:

- [Section 10.3.1.1, "Creating or Editing a Retention Category"](#)
- [Section 10.3.1.2, "Viewing Retention Category Information"](#)
- [Section 10.3.1.3, "Viewing Category Metadata History"](#)
- [Section 10.3.1.4, "Copying a Retention Category"](#)
- [Section 10.3.1.5, "Moving a Retention Category"](#)
- [Section 10.3.1.6, "Deleting a Retention Category"](#)

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. Choose **Browse Content** then **Retention Schedules**. Choose **Create** then **Create Retention Category** from the Table menu.
The [Create or Edit Retention Category Page](#) opens.
2. (Optional) Accept the default security group or select a group from the **Security Group** list. The **Default Content Server security** checkbox must be selected on the [Configure Retention Settings Page](#).
3. (Optional) If Accounts are enabled, choose the associated account for the category.
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.
6. Enter a name for the category.
7. Enter a description with a maximum of 1000 characters.
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, select **Restrict Revisions**.
10. To restrict deletions of items in the category, select **Restrict Deletes**.
11. To restrict edits of items in the category, select **Restrict Edits**.
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. Select **Subject to Review**.
 - 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.
 - 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** near **Group Permissions**. The Select Alias page opens.
 - 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 for which to set permissions, and click **OK**. The alias and its permissions show 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 opens.
 - 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 for whom to set permissions, and click **OK**. The user and their permissions show in the User Permissions text box of the Create Retention Category page.
15. Click **Create**. The Dispositions Instructions Page opens. 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. Choose **Edit** then **Edit Retention Category** from the item's **Actions** menu.
The [Create or Edit Retention Category Page](#) opens.
2. Enter changes to the available fields.
3. Click **Submit Update**. The successfully updated retention category message is displayed.
4. Click **OK**. The [Exploring Retention Schedule Page](#) opens.

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](#) opens. 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 shows 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. Choose **Information** then **Metadata History** from the item's **Actions** menu.
2. The [Metadata History Page](#) opens, 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 choose **Copy** from the item's **Actions** 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 opens. 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. Choose **Edit** then **Move** from the item's **Actions** menu.
2. The [Select Retention Series, Record Folder or Category Dialog](#) opens.
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 show 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. Choose **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, select 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. Choose **Browse Content** then **Retention Schedules**.
The [Exploring Retention Schedule Page](#) opens.
2. Choose **Create** then **Create Retention Category** from the Table menu.
The [Create or Edit Retention Category Page](#) opens.
3. Enter RCV-101 for the Retention Category Identifier.
4. Enter `Operational for Review` for the Retention Category Name.
5. Enter RCV-101 for the Retention Category Description.
6. (Required for U.S. Government Agencies) Enter RCV-101 as the code of the authority for the Disposition Authority.
7. Select **Subject to Review**.
8. Specify a Reviewer and a Review Period.
9. Click **Create**.
The [Disposition Instructions Page](#) opens.
 - a. Click **Add**. The [Disposition Rule Page](#) opens.
 - b. Select **Retention Period Cutoff** for the After field (alternate label: Triggering Event).
 - c. Enter `3 Calendar Months` in the Wait For field (alternate label: Retention Period).
 - d. Select **Notify Authors** from the Do list (alternate label: Disposition Action).
 - 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 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:

- [Section 10.4.1, "About Record Folders"](#)
- [Section 10.4.2, "Managing Record Folders"](#)
- [Section 10.4.3, "Folder Examples"](#)

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 but 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. For details, see the *Oracle WebCenter Content Idoc Script Reference Guide*. 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 do 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:

- [Section 10.4.2.1, "Creating a Record Folder"](#)
- [Section 10.4.2.2, "Creating a Volume Folder"](#)
- [Section 10.4.2.3, "Editing a Record Folder"](#)
- [Section 10.4.2.4, "Changing the Disposition Applied to a Folder"](#)
- [Section 10.4.2.5, "Moving a Record Folder"](#)
- [Section 10.4.2.6, "Deleting a Record Folder"](#)

For details about viewing folder information, see the *Oracle WebCenter Content Administrator's Guide for Records*.

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. Choose **Create** then click **Create Records Folder** from the Page **Actions** menu.
The [Create or Edit Record Folder Page](#) opens.
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 WebCenter Content 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. Select **Subject to Review**.

- 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 [Section 10.1.3.2, "Attribute Inheritance."](#)
10. External information: If the item is external to the Records system, add its location, container, and applicable dates. 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.
- You can also enter a deactivation date corresponding to a content item but external to the Records system. 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 the Records system after deactivation. Content expired in Oracle WebCenter Content cannot be accessed after expiration.
- 11. Delete Approval Date: A date after which the folder can be deleted.
 - 12. (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 [Section 6.4.1, "Supplemental Markings Details."](#)
 - 13. (Optional, for ACL-enabled implementations) Set up ACL access at the alias level or user level. For details, see [Section 5.8.1, "Setting ACLs During Software Use."](#)
 - 14. Click **Lifecycle Preview** to view the disposition instructions associated with the category and thus the folder.
 - 15. Click **Create**. The record folder is shown 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. Choose **Create** then **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:

- A 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. Choose **Edit** then **Record Folder** from the Page **Actions** menu.
The [Create or Edit Record Folder Page](#) opens.
3. Make changes to the available fields.
4. Click **Submit Update**. The successfully updated folder message and the edits are shown 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. Choose **Edit** then **Edit Disposition** in the folder's **Actions** menu.
The [Disposition Instructions Page](#) opens.
3. Click the **Edit** icon (a pencil) in the row for the disposition to change.
The [Disposition Rule Page](#) opens.
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 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 **Move** from the item **Actions** menu.
The [Select Retention Series, Record Folder or Category Dialog](#) opens.
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 show 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 WebCenter Content Administrator's Guide for Records*.

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. Choose **Delete** then **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, select **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:

- [Section 10.4.3.1, "Creating a Record Folder That is Subject to Review"](#)
- [Section 10.4.3.2, "Creating Record Folders Subject to Recurring Audit Triggers"](#)

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 WebCenter Content Administrator's Guide for Records*.

1. Open the retention category or record folder where the record folder will be created.
2. From the **Actions** menu, choose **Create Record Folder**.
The [Create or Edit Record Folder Page](#) opens.
3. Enter RFV-101 as the Record Folder Identifier.
4. Enter RFV-101 as the Record Folder Name.
5. Select **Subject to Review**.
6. Select 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 opens 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 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 [Section 11.1, "Trigger Overview."](#) The Audit Periods must already be defined in the Configuration Manager utility. For further information about configuring audit period lists, see the *Oracle WebCenter Content 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** menu, choose **Create Record Folder**.
The [Create or Edit Record Folder Page](#) opens.
3. Enter RFA-101 as the Record Folder.
4. Enter RFA-101 as the Record Folder Name box.
5. Select **Subject to Audit** and select 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 the corresponding Audit Period.

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:

- [Section 11.1, "Trigger Overview"](#)
- [Section 11.2, "Managing Triggers"](#)
- [Section 11.3, "Trigger Examples"](#)

11.1 Trigger Overview

Two types of triggers are provided 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:

- [Section 11.1.1, "System-Derived Triggering"](#)
- [Section 11.1.2, "Custom Triggers"](#)
- [Section 11.1.3, "Global Triggers"](#)
- [Section 11.1.4, "Custom Direct Triggers"](#)
- [Section 11.1.5, "Indirect Triggers"](#)

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 and 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 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 that **Subject to Audit** 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 WebCenter Content User's Guide for Records*.

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 WebCenter Content System Administrator's Guide for Content Server*.

11.2 Managing Triggers

Several tasks are involved in managing triggers:

- [Section 11.2.1, "Creating or Editing a Trigger"](#)
- [Section 11.2.2, "Viewing Trigger Information"](#)
- [Section 11.2.3, "Viewing Trigger References"](#)
- [Section 11.2.4, "Deleting a Trigger"](#)
- [Section 11.2.5, "Setting Up Indirect Triggers"](#)
- [Section 11.2.6, "Deleting an Indirect Trigger Date Entry"](#)
- [Section 11.2.7, "Disabling an Indirect Trigger Period"](#)

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 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.

Note that custom triggers are not usually created using a PCM field for the trigger. To use a PCM field for a trigger, you must first create a field to be used. The field must be prefixed with an x (for example, xPhysicalDateField). A similar field must be created in the Configuration Manager with the same name, with no prefix (for example, PhysicalDateField). After the fields are created, the field can be selected for use with the trigger.

See [Chapter 13, "Creating Custom Metadata"](#) for details about creating a custom metadata field. See *Oracle WebCenter Content System Administrator's Guide for Content Server* for details about using the Configuration Manager to create custom fields.

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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Select the type of trigger to create (Global, Custom Direct, or Indirect). Choose **Add**.
The [Create or Edit Trigger Type Page](#) opens.
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 to a maximum of 100 characters.
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 and a folders field on which the indirect trigger is based.

The New Revision Date option is available only if **Enable New Revision Date Trigger Field** 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.

7. Synchronize on Period Start Date: If selected, the start date is 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.
8. (Optional) If ACL-based security is enabled, click **Group** and **User Permissions** for the trigger. This limits who can edit the trigger. For details, see [Section 5.8.1, "Setting ACLs During Software Use."](#)
9. Click **Create**.

A message is displayed saying the trigger was created successfully.

10. 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Select the type of trigger to edit (Global, Custom Direct, or Indirect).
3. Choose **Edit** then **Edit Trigger** from the item's **Actions** menu for the trigger to edit.
The Create or Edit Trigger Type Page opens.
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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Select the type of trigger to view (Global, Custom Direct, or Indirect).
3. Click the trigger name to view.
The [Trigger Information Page](#) opens.
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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Select the type of trigger to view (Global, Custom Direct, or Indirect).
3. Click the trigger name to view.
The [Trigger Information Page](#) opens.
4. From the Page menu, choose **References**.
The Trigger References Page opens. 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 opens.
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 [Section 14.8.2, "Creating or Editing a Disposition Rule."](#)

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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.

The [Configure Triggers Page](#) opens.

2. Select the type of trigger to view (Global, Custom Direct, or Indirect). Navigate to the trigger to delete.
3. Choose **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, select the trigger checkboxes and choose **Delete** from 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.

The [Configure Triggers Page](#) opens.

2. Click the Indirect tab. Choose **Trigger Dates Info** from the **Actions** menu for the Audit Approval trigger.
3. Choose **Trigger Dates Info** on the Page menu.

The [Indirect Trigger Date Entries Page](#) opens.

4. Click **Add**. The [Create or Edit Indirect Trigger Date Entries Page](#) opens.
5. Select the trigger period that 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Choose **Delete** from the trigger's **Actions** menu.

11.2.7 Disabling an Indirect Trigger Period

Use this procedure to disable 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers** from the Page menu.
The [Configure Triggers Page](#) opens.
2. Choose **Edit** then **Edit Trigger** from the trigger's **Actions** menu.
The [Create or Edit Trigger Type Page](#) opens.
3. Select the trigger period to disable from the trigger period list, and click **Info**. The [Create or Edit Indirect Trigger Date Entries Page](#) opens.
4. Deselect **Enabled**, and click **Submit Update**. The Enabled field for the Trigger Period that was edited now displays No. Click the **Configure Retention Schedule Components** 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:

- [Section 11.3.1.1, "Delayed Global Trigger"](#)
- [Section 11.3.1.2, "Dormant Global Trigger"](#)
- [Section 11.3.1.3, "Activating a Dormant Global Trigger"](#)
- [Section 11.3.2, "Custom Direct Trigger"](#)

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. Choose **Records** then **Configure** then **Triggers** from the Top menu.
The [Configure Triggers Page](#) opens.
2. In the Global Triggers area, click **Add**. The [Create or Edit Trigger Type Page](#) opens.
3. Enter `Case 123 Closed` as the name.
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 [Section 11.3.1.3, "Activating a Dormant Global Trigger."](#)

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 the Records system, 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. Choose **Admin Applets** from the **Administration** menu.
The Administration Applets open.
2. Click **Configuration Manager**.
The Configuration Manager utility starts.
3. Click the **Information Fields** tab and click **Add**.
The Add Custom Info Field page opens.
4. Enter `EETermDate` as the Field Name and click **OK**.
The Edit Page for the field opens.
5. Enter `Employee Termination Date` as the Field Caption.
6. In the **Field Type** list, select **Date**.
7. Make sure **Required** is not selected and **User Interface** and **Search Index** are selected (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. Choose **Records** then **Configure** then **Triggers** from the Top menu.
The [Configure Triggers Page](#) opens.
2. In the Custom Direct Trigger area, click **Add**.
The [Create or Edit Trigger Type Page](#) opens.
3. Enter `EE Term Date` as the Trigger Name.
4. Enter `Employee Termination Date` as the Brief Description.
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. Choose **Browse Content** then **Retention Schedules**. The [Exploring Retention Schedule Page](#) opens.
2. Choose **Create** then **Create Retention Category** on the Page menu.
The [Create or Edit Retention Category Page](#) opens.
3. Enter EE-RC-1 as the Retention Category Identifier.
4. Enter Employees as the Retention Category Name.
5. Enter Employee Retention Category as the Retention Category Description.
6. (Required for U.S. Government Agencies) Enter EE-RC-1 as the code of the authority for the disposition.
7. Click **Create**. The [Disposition Instructions Page](#) opens.
8. Create the first rule:
 - a. Click **Add**. The [Disposition Rule Page](#) opens.
 - b. In the **Triggering Event** list select the new custom direct trigger called EE Term Date.
 - c. In the **Disposition Action** list, select **Cutoff**.
 - d. Click **OK**.
9. Create the second rule:
 - a. Click **Add**. The [Disposition Rule Page](#) opens.
 - b. In the **Triggering Event** list, select **Preceding Action**.
 - c. In the Retention Period field, enter 3 and click **Calendar Years**.
 - d. In the **Disposition Action** list, select **Destroy**.
 - e. Click **OK**.
 - f. Click **Submit Update**. A 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 with the **Update** option in the **Actions** menu 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.

Configuring Time Periods

Periods define a length of time to use in retention schedules and dispositions. They are associated with retention periods for dispositions and with review periods for cycling subject-to-review content.

This chapter covers the following topics:

- [Section 12.1, "Using Time Periods"](#)
- [Section 12.2, "Managing Time Periods"](#)

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:

- [Section 12.2.1, "Creating or Editing a Custom Time Period"](#)
- [Section 12.2.2, "Viewing Period Information"](#)
- [Section 12.2.3, "Viewing Period References"](#)
- [Section 12.2.4, "Deleting a Custom Period"](#)

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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.

The [Configure Periods Page](#) opens.

2. Click **Add**.

The [Create or Edit Period Page](#) opens.

3. Enter a name for the period.
4. Select the type of time period, either Calendar, Fiscal, or Custom. The start date of the fiscal year is defined on the [Configure Retention Settings Page](#). 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.
5. Click the calendar icon and select or edit a custom start time.
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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.

The [Configure Periods Page](#) opens.

2. Choose **Edit Period** from the item's **Actions** menu for the period to edit.

The [Create or Edit Period Page](#) opens.

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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.
The [Configure Periods Page](#) opens.
2. Click the period to view from the **Period Name** list.
The [Period Information Page](#) opens.
The Built-in label indicates if a period was predefined. 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** menu is not available to any users other than those with the Admin.RecordManager right.
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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.
The [Configure Periods Page](#) opens.
2. Click the period to view from the list.
The [Period Information Page](#) opens.
3. Choose **References** from the Page **Actions** menu. The [Period Reference Page](#) opens. 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 opens.

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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.

The [Configure Periods Page](#) opens.

2. Choose **Delete Period** from a period's **Actions** 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.

The [Configure Periods Page](#) opens.

2. In the Period Name area, click **Add**. The [Create or Edit Period Page](#) opens.

3. Enter `School year 2010-2011` as the Period Name.

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 of `September 7, 2010`. The date and default time show 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 9. Make sure you specify the date according to the format used by your system locale.

6. Enter 9 as the Length and select Months from the list.
7. Enter End of School year 2010–2011 as the label for end of period.
8. Click **Create**.

A message is displayed saying the period was created successfully.

9. Click **OK**.

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. Depending on the field characteristics, the new custom fields are displayed on 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 that 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 auxiliary 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.

This chapter covers the following topics:

- [Section 13.1, "Managing Custom Metadata"](#)
- [Section 13.2, "Example: Creating a Custom Category Metadata Field"](#)

13.1 Managing Custom Metadata

The following tasks are used when managing custom metadata:

- [Section 13.1.1, "Creating or Editing Custom Metadata Fields"](#)

- [Section 13.1.2, "Viewing Custom Metadata Field Information"](#)
- [Section 13.1.3, "Deleting a Custom Metadata Field"](#)

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 WebCenter Content System Administrator's Guide for Content Server* for details about creating option lists.

13.1.1 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. Choose **Records** then **Configure** from the Top menu. Choose **Metadata** then **Metadata Sets**.

The [Metadata List Page](#) opens.

2. To create a **new auxiliary metadata set**, choose **Create Auxiliary Metadata** from the Page menu.

The [Create or Edit Auxiliary Metadata Set Page](#) opens. Enter the auxiliary metadata set name, display name, name of the new table being created to house the metadata set, and column prefix for that table.

To **add fields to an existing metadata set**, either auxiliary or standard set (Retention Categories, Record Folders, or Physical), choose **Update Fields** from the auxiliary set's individual **Actions** menu on the [Metadata List Page](#). The [Create or Edit Standard Metadata Field Page](#) opens.

3. Add the field information for the new metadata field.
 - **Name:** Name for the field in the database. Maximum of 30 characters is allowed. Do not use special characters (question mark, punctuation, and so on).
 - **Caption:** Caption for the field that will appear in the user interface. Maximum of 30 characters allowed.
 - **Type:** The data type for the field. Options include:
 - **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 allowed: 30.

- Usage: Select a checkbox to enable usage. Options include:
 - Required: If selected the column will be required.
 - Enabled: If selected, the field is enabled on pages.
 - Searchable: If selected, the field is added to those fields that are searchable.
 - Option List Key: The field used for the option list. Click **Choose** to select a key from a list. Note that an option list must be created and populated before it can be used.
 - Option List Type: The kind of option list to use, selectable from a list.
4. Click **Add** (a plus sign) to add the field to the Field list. Click **Delete** (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.
 5. Click **Apply** after adding or editing all the fields.

13.1.2 Viewing Custom Metadata Field Information

Use this procedure to view information about the custom fields added to metadata sets:

1. Choose **Records** then **Configure** from the Top menu. Choose **Metadata** then **Metadata Sets**.
The [Metadata List Page](#) opens.
2. Choose **Fields Information** from the **Actions** menu of the metadata set to view.
The [Fields for Metadata Page](#) opens showing the specific fields created for that metadata set.

13.1.3 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. Choose **Records** then **Configure** from the Top menu. Choose **Metadata** then **Metadata Sets**.
The [Metadata List Page](#) opens.
2. Choose **Update Fields** from the set's individual **Actions** menu on the [Metadata List Page](#). The [Create or Edit Auxiliary Metadata Set Page](#) opens.
3. Select the field name in the Field list and click **Delete** (an X).
4. Click **Apply** after deleting the fields.

13.2 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. Choose **Records** then **Configure** from the Top menu. Choose **Metadata** then **Metadata Sets**.
The [Metadata List Page](#) opens.
2. Choose **Update Fields** in the **Actions** menu for Retention Categories. The [Create or Edit Standard Metadata Field Page](#) opens.
3. Complete the metadata fields as follows:
 - a. Enter DeptSKU as the Name.
 - b. In the Type list, select **Integer**.
 - c. Enter Department SKU as the Caption.
 - d. Select **Enabled**.
 - e. Select **Searchable**.
4. Click **Add** (the plus symbol).
5. Click **Apply**. To view the new field, browse content, and choose **Create Retention Category** from the **Actions** menu. The new custom metadata field is displayed.

The Department SKU field is added to the Create Retention Category page.

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.

Dispositions are defined using disposition instructions. A disposition instruction is typically constructed as follows:

1. When a specified triggering event occurs (see [Section 14.3, "Triggering Events"](#)),
2. Wait a specified period (the retention period, described in [Section 14.4, "Retention Periods"](#)), if required, and then
3. Perform a specified disposition action (see [Section 14.5, "Disposition Actions"](#)).

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.

This chapter discusses setting up and administering disposition scheduling. It covers the following topics:

- [Section 14.1, "Disposition Types"](#)
- [Section 14.2, "Category Rule Review Using Workflows"](#)
- [Section 14.3, "Triggering Events"](#)
- [Section 14.4, "Retention Periods"](#)
- [Section 14.5, "Disposition Actions"](#)
- [Section 14.6, "Cutoff Guidelines"](#)
- [Section 14.7, "Disposition Precedence"](#)
- [Section 14.8, "Managing Dispositions"](#)

- [Section 14.9, "Disposition Examples"](#)

14.1 Disposition Types

The following types of dispositions are available:

- [Section 14.1.1, "Event Dispositions"](#)
- [Section 14.1.2, "Time Dispositions"](#)
- [Section 14.1.3, "Time-Event Dispositions"](#)

14.1.1 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.

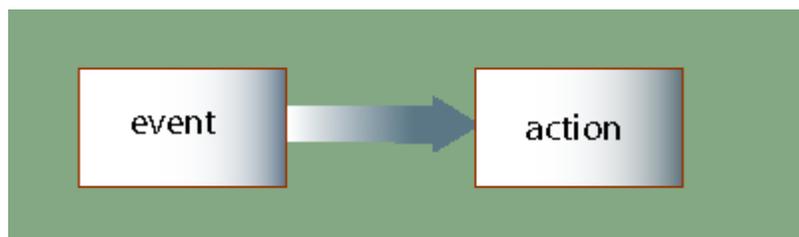
- Content that is tracked for DoD purposes use actions like Destroy and Retain, and the states of the items are Obsolete and Declassified, respectively.
- Non-DoD content uses actions like Delete Revision and Delete All Revisions.

To view an example step-by-step procedure for creating an event disposition, see [Section 14.9.1, "Event Disposition."](#)

If classification is used (an optional security feature that 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



14.1.2 Time Dispositions

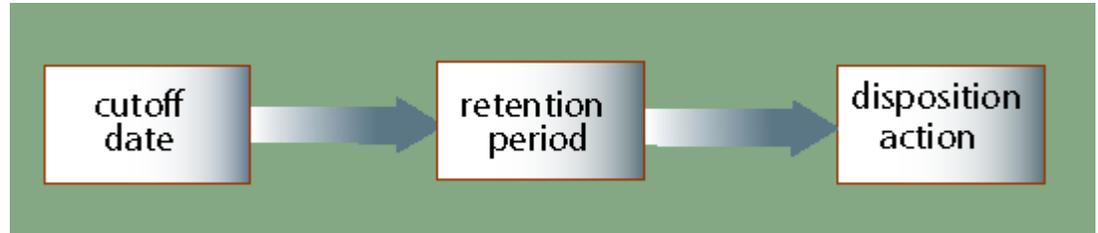
A *time disposition* has a fixed retention period and begins with a user-defined file cutoff. The retention period must transpire before the disposition instruction takes action on the content item. Typical examples include the following:

- Cutoff at the end of the (fiscal or calendar) year
- Retain for three years, then destroy
- Cut off at declassification, retain for ten years, then destroy (DoD classified items)

To view an example step-by-step procedure for creating a time disposition, see [Section 14.9.3, "Time Disposition."](#)

To summarize, time dispositions have retention periods and explicitly defined cutoffs.

Figure 14–2 Time Disposition



14.1.3 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 [Section 14.9.4, "Time-Event Disposition."](#)

To summarize, time-event dispositions have explicitly defined events, cutoffs, and retention periods.

Figure 14–3 Time-event Disposition



14.2 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 variables must be set:

- Select **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. The default is 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. For more details, see [Section 7.3, "Setting Up Workflows."](#)

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 stay in the workflow and 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.

14.3 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"](#). The following types of triggering events are discussed:

- [Section 14.3.1, "Preceding Actions Triggering Event"](#)
- [Section 14.3.2, "Content State Triggering Event"](#)
- [Section 14.3.3, "Indirect Triggers"](#)
- [Section 14.3.4, "Custom Triggers"](#)

14.3.1 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.

14.3.2 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.

14.3.3 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).

14.3.4 Custom Triggers

- **Custom triggers** are also supported. For more information, see [Section 11.2.1, "Creating or Editing a Trigger."](#)

14.4 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. For details, see [Section 12.2.1, "Creating or Editing a Custom Time Period."](#)

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

14.5 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).

The following actions are discussed:

- [Section 14.5.1, "Classified Records Actions"](#)
- [Section 14.5.2, "Dispose Actions"](#)
- [Section 14.5.3, "Other Actions"](#)
- [Section 14.5.4, "Transfer/Move Actions"](#)

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.

14.5.1 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.

14.5.2 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.

14.5.3 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.

14.5.4 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)**.

14.6 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 record revisions 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` variable is enabled. It is disabled by default.

14.6.1 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.

14.6.2 Time-Event Retention Periods

On the date the event or action is completed, perform the cutoff, then apply the retention period.

14.7 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.

14.8 Managing Dispositions

The following tasks are involved in managing dispositions:

- [Section 14.8.1, "Enabling or Disabling User-Friendly Captions"](#)
- [Section 14.8.2, "Creating or Editing a Disposition Rule"](#)
- [Section 14.8.3, "Copying a Disposition Rule"](#)
- [Section 14.8.4, "Viewing Disposition Information"](#)
- [Section 14.8.5, "Deleting a Disposition Rule"](#)

14.8.1 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Settings**.
The [Configure Retention Settings Page](#) opens.
2. Expand the User Interface section if necessary. Select **User-Friendly Disposition**.
3. Click **Submit Update**. A message is displayed saying the configuration was successful.
4. Click **OK**.

14.8.2 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 [Section 14.9, "Disposition Examples."](#)

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 Retention Schedule Page](#) opens.
2. In the row for the retention category, choose **Edit** then **Edit Disposition** from the item's **Actions** menu.
The (initially blank if creating a disposition) [Disposition Instructions Page](#) opens.
3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
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 for Retention Period (Wait for) and select the corresponding period from the Retention Period list.

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.*

6. Select an action for the rule from the Disposition Action (Do) list. The system sends an e-mail message to the person responsible for performing this action.
7. (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, either the specified user and the category author (the default) or the specified user only.
8. If the item should go through an external approval process, select the checkbox. 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).
9. (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.
10. (Optional) If the disposition instruction applies only to other retention objects, select an object from the list. Otherwise it will apply to all objects.
11. (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. For details, see [Section 7.5, "Configuration Variables."](#)

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 transferred 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 opens. Click **Edit** in the User Workspace section. You can set default locations, passwords, and other details for the location types there.

12. If necessary, choose a physical container for an external record folder, such as a barcode or some other means of identification. Maximum characters: 30.
13. If necessary, map fields when exporting data to another system that 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.
14. 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.
15. Click **Submit Update**. A message is displayed with the disposition information.
16. 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 Retention Schedule Page](#) opens.
2. Navigate to the appropriate retention category.
3. Choose **Edit** then **Edit Disposition** from the item's **Actions** menu. The [Disposition Instructions Page](#) opens.
4. In the Disposition Instructions list, select the rule to edit, and click the **Edit** icon (an image of a pencil).
5. The [Disposition Rule Page](#) opens.
6. Make changes to the rule, and click **OK**. The Disposition Rule page closes.
7. Click **Submit Update**. A message is displayed with the disposition information.

8. Click **OK**.

14.8.3 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 Retention Schedule Page](#) opens.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, choose **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 opens. 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](#) opens.
5. If needed, edit the rules in the same manner as described earlier.
6. Click **Submit Update**. A 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.

14.8.4 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 Retention Schedule Page](#) opens.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click the **Info** icon.
The [Disposition Information Page](#) opens.
4. When done, click **OK**.

14.8.5 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 Retention Schedule Page](#) opens.
2. Navigate to the appropriate retention category.
3. In the row for the retention category, click **Edit** then **Edit Disposition**.
The [Disposition Instructions Page](#) opens.
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**. A confirmation 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 appropriate action by choosing **Records** then **Batch Services** from the Top menu.

14.9 Disposition Examples

This section includes the following disposition examples:

- [Section 14.9.1, "Event Disposition"](#)
- [Section 14.9.2, "Simple Time/Event Disposition"](#)
- [Section 14.9.3, "Time Disposition"](#)
- [Section 14.9.4, "Time-Event Disposition"](#)
- [Section 14.9.5, "Disposition Rules for Specific Folders"](#)
- [Section 14.9.6, "Multi-Phased Disposition"](#)

All of the examples in this section use the default (that is, non user-friendly) disposition captions.

14.9.1 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, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the Page menu on the [Retention Category Information Page](#).

The (initially blank) [Disposition Information Page](#) opens.

3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
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**. A confirmation message is displayed.

14.9.2 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, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the Page menu on the [Retention Category Information Page](#).

The [Disposition Instructions Page](#) opens.

3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
4. In the Triggering Event list, select **No Longer Latest Revision**. The Retention Period field becomes available.
5. In the Retention Period fields, enter 1 and select **Weeks** 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**. A completion message is displayed.

14.9.3 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, choose **Edit** then **Edit Disposition** from the item's **Actions** menu or click the **Info** icon and choose **Edit** then **Edit Disposition** from the Page menu on the [Retention Category Information Page](#).

The [Disposition Instructions Page](#) opens.

3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
4. In the Triggering Event list, click the **Retention Period Cutoff** option. The Retention Period field becomes available.

5. In the Retention Period field, enter 3 and select **Fiscal Years** on the Retention Period list.
6. In the Disposition Action list, select the **Destroy** option.
7. Click **OK**. The disposition rule is displayed in the **Disposition Instructions** box.
8. Click **Submit Update**. A confirmation 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.

14.9.4 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, choose **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the Info icon and choose **Edit** then **Edit Disposition** from the Page menu on the [Retention Category Information Page](#).
The [Disposition Instructions Page](#) opens.
3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
4. Define the first disposition rule.
 - a. In the Triggering Event list, select the **Case closed** option under the Custom Triggers sublist.
 - b. In the Disposition Action list, select 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, select 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, select 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**. A completion message is displayed.

14.9.5 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, choose **Edit** then **Edit Disposition** from the item's **Actions** menu. You can also click the **Info** icon and choose **Edit** then **Edit Disposition** from the Page menu on the [Retention Category Information Page](#).
The [Disposition Instructions Page](#) opens.
3. In the Disposition Instructions area, click **Add**.
The [Disposition Rule Page](#) opens.
4. Define the first disposition rule for record folder 1.
 - a. In the Triggering Event list, select **Program ABC Canceled**, the custom trigger you created for the folder.
 - b. In the Disposition Action list, select the **Destroy** action.
 - c. In the Advanced Options section, select **Folder 1**, the folder which will have the rule applied.
 - 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 **Program BBC Expired**, the custom trigger you created for the folder.
 - c. In the Disposition Action list, select the **Destroy** action.
 - d. In the Advanced Options section, select **Folder 2**, the folder which will have the rule applied.
 - 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 **Program CDB Rescinded**, the custom trigger you created for the folder.
 - c. In the Disposition Action list, select the **Destroy** action.

- d. In the Advanced Options section, select **Folder 3**, the folder which will have the rule applied.
 - e. Click **OK**. The rule is displayed in the Disposition Instructions box.
7. Click **Submit Update**. A completion message is displayed. Notice there are rules drawn between the multiple instructions.

14.9.6 Multi-Phased Disposition

This example demonstrates defining a disposition instruction that has more phases than is typical in a disposition instruction. This example contains the disposition actions of 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](#) opens.
3. In the Disposition Instructions area, click **Add**. The [Disposition Rule Page](#) opens.
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, select the **Retention Period Cutoff** option. The Retention Period field becomes available.
 - b. In the Retention Period fields, enter 1 in the text box and select **Calendar Years** from the Retention Period list.
 - c. In the Disposition Action list, select the **Move** option to move the content to offline storage.
 - d. In the Destination Location box, select **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, select the **Preceding Action** option.
 - c. In the Retention Period fields, enter 1 and select **Calendar Years** from the Retention Period list.
 - d. In the Disposition Action list, select 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, select the **Preceding Action** option.
 - c. In the Retention Period field, enter 10 in the text box and select **Calendar Years** from the Retention Period list.
 - d. In the Disposition Action list, select 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**. A completion message is displayed.
8. Click **OK**.

Setting Up Freezes

A freeze (sometimes called a *dynamic hold*) inhibits disposition processing for an item. This can be used to comply with legal or audit requirements, such as when a legal hold must be placed on information. 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 WebCenter Content Administrator's Guide for Records*.

Important: Creating custom disposition actions requires in-depth technical knowledge of Oracle WebCenter Content. To define custom disposition actions, contact Consulting Services.

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.

Recurring freezes can also be scheduled for selected items of content. See the *Oracle WebCenter Content Administrator's Guide for Records* for details about that process.

This chapter covers the following topics:

- [Section 15.1, "Managing Freezes"](#)
- [Section 15.2, "Example: Creating a Freeze"](#)

15.1 Managing Freezes

The following tasks are involved in managing freezes:

- [Section 15.1.1, "Creating or Editing a Freeze"](#)
- [Section 15.1.2, "Viewing Freeze Information"](#)
- [Section 15.1.3, "Deleting a Freeze"](#)
- [Section 15.1.4, "Freezing Items, Folios or Folders"](#)
- [Section 15.1.5, "Unfreezing Frozen Items or Folders"](#)
- [Section 15.1.6, "Searching for Frozen Content and Folders"](#)
- [Section 15.1.7, "Re-sending an E-Mail Notification for a Freeze"](#)

15.1.1 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.
The [Freeze Configuration Page](#) opens.
2. Click **Add**.
The [Create or Edit Freeze Page](#) opens.
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](#). For details, see [Section 5.8.1, "Setting ACLs During Software Use."](#)
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 e-mail address of people to receive the freeze notification and the e-mail address of the person initiating the e-mail. If left blank, the send of the notification is the user who created the freeze.

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.

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** is selected. Maximum characters: 3,000.

The e-mail is (re)sent when **Create** (on the Create Freeze page) or **Submit Update** (on the Edit Freeze page) is clicked. 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.

12. Enter an e-mail message. Maximum characters allowed: 3000.
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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Choose **Edit** then **Edit Freeze** from a freeze's **Actions** menu.

The [Create or Edit Freeze Page](#) opens.

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**.

15.1.2 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Click a freeze name to view.

The [Freeze Information Page](#) opens.

3. When done, click **OK**.

This page also has menu options to perform the following actions:

- **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:** Displays a list 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:** Display a list 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:** Display a list 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:** Display a list 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.

15.1.3 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Choose **Delete** from a freeze **Actions** menu.

To delete multiple freezes, select the freeze checkbox and choose **Delete** from the Table menu on the [Freeze Configuration Page](#).

15.1.4 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 opens.

2. Select the item to freeze by selecting 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. Choose **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. To view frozen items after a freeze is executed from the Search Results Page, click the **Refresh** button or execute a new search.

5. Click **OK**.

15.1.5 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Choose **Edit** then **Unfreeze** from a freeze's **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**.

15.1.6 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Click the **Actions** menu for a freeze. In the **Information** Page menu, choose 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](#) opens, which lists all content or folders meeting the criteria of the selected screening option.

15.1.7 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. 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. Click a freeze name.

The [Freeze Information Page](#) opens.

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](#).

Notifications can also be set by searching for a freeze. On the [Freeze Information Page](#), click **Edit** then **Renotify**.

15.2 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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

The [Freeze Configuration Page](#) opens.

2. In the Freeze area, click **Add**.

The [Create or Edit Freeze Page](#) opens.

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, select **Send Notification** and provide the e-mail properties (recipients, from-address, and message text).
10. Click **Create** when you finish.

The Oracle Content Server Adapter

An *adapter* provides a bridge between Oracle WebCenter Content: Records (which contains the record management policies) and an 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 Records 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 WebCenter Content: Record Adapter for Content Server (hereafter abbreviated as the Content Server Adapter) obtains these policies from the server and applies them to the content items stored in the vault.

Multiple adapters can be used with the Records system to manage an enterprise's content needs. This chapter discusses how to configure and use one specific adapter, the Content Server Adapter.

This chapter contains the following topics:

- [Section 16.1, "Content Server Adapter Overview"](#)
- [Section 16.2, "Adapter Configuration"](#)
- [Section 16.3, "Synchronizing Data"](#)

16.1 Content Server Adapter Overview

This section provides an overview of the Content Server Adapter and its components. It contains the following topics:

- [Section 16.1.1, "Architecture"](#)
- [Section 16.1.2, "Oracle WebCenter Content: Records and the Content Server Adapter"](#)

16.1.1 Architecture

The major components involved in a typical Content Server Adapter installation include:

- the Records system: 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 Content Server Adapter.
- Oracle WebCenter Content: Stores and manages content in a repository.

- Content Server Adapter: Communicates between Records and the Content Server Adapter's content vault. The Content Server Adapter provides common retention functionality as follows:
 - Identifying the content in the repository that is of interest to the Records system.
 - Performing searches and declaring the applicable content items to the Records system.
 - 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 WebCenter Content: Records and the Content Server Adapter

Oracle WebCenter Content: Records 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 Content Server 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 Content Server Adapter ensures that the record remains unalterable during the retention period. Upon request, the Content Server Adapter's content vault can purge the content at the end of the retention period.

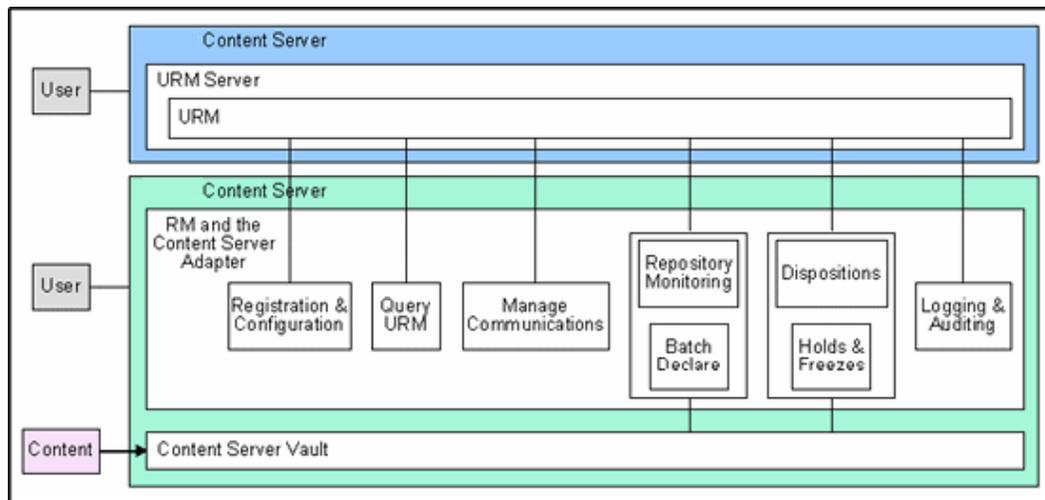
The Content Server Adapter vault may also hold content that does not need to be retained. When retention of this content is no longer necessary, it can be disposed of according to the disposition processes stored within the Records system.

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 Content Server Adapter enables the Records system 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 the Records system. Instead, these documents remain in the Content Server Adapter vault and only their metadata is stored in the Records system.

The Content Server Adapter is the communications intermediary between the Records system and the Content Server Adapter repository. Content is stored in and remains in the Content Server Adapter vault while the Records system simultaneously enforces corporate retention policies, disposition processes, and legal holds on the stored content.

Figure 16–1 Content Server Adapter Retention Functions Overview



The Content Server Adapter can be configured to provide the following basic retention functions:

- **Registration:** The Content Server Adapter self-registers with the Records system, ensuring that the Records system knows about the Content Server Adapter vault and is thus ready to manage the stored content within the repository.
- **Configuration:** Content Server Adapter configuration includes collecting the proper identification and credentials information for the Records system security and communications. Configuration information also includes mapping metadata fields and defining synchronization schedules.
- **Query the Records system:** The Content Server Adapter queries the Records system for certain information. For example, it may need to retrieve retention schedules for specific items of interest. Or the Content Server Adapter may need to request Records metadata for content items and obtain life cycle information.
- **Manage Communications:** The Content Server Adapter monitors batch processes, handles communication errors with the Records system, and handles large work requests by grouping them into communication blocks and processing the response in chunks.
- **Repository Monitoring and Batch Declare:** The Content Server Adapter monitors its server's content vault by periodically searching the repository and informing the Records system of any changes in the repository that may affect disposition processes or audit holds. For example, the Content Server Adapter will inform the Records system about new content checkins that need to be managed.
- **Perform Oracle WebCenter Content: Records Tasks:** The Content Server Adapter periodically checks the Records system for tasks to be performed within the repository. These tasks enable the Records system to abide by the corporate retention policies and disposition processes. Typical tasks include:
 - the Records system may use the Content Server Adapter to perform a search within the Content Server Adapter vault and provide a list of items matching the search criteria.
 - When a litigation hold applies to managed content within the Content Server Adapter vault, the Records system may use the Content Server 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 Content Server 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 Content Server Adapter provides consistent logging for the activities it coordinates. It contributes event information to the log files that are then uploaded to the Records system, consolidated, and stored.

16.2 Adapter Configuration

The initial step in setting up the Content Server Adapter is to access the **Administration** menu on the remote server where the adapter will reside. Choose **Administration** then **Configure Record Settings** then **Adapter** from the Top menu. Select the Adapter option.

When the Adapter option is chosen on the [Configure Retention Settings 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 Content Server Adapter server and register the repository source. The documents in that repository are managed using the Records system retention policies.

After registration of the source, a check is automatically made to compare content on the Content Server Adapter and the the Records system repository. A list is presented of items that do not match. At that time the items on the Content Server Adapter repository can be deleted to make sure the two systems are in sync.

Next metadata fields should be mapped. The Content Server Adapter repository may contain a wide variety of documents and may have custom fields that do not directly correlate to those on the the Records system repository. When 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 repositories must be mapped so the content is categorized correctly.

The Content Server Adapter does not synchronize security groups with the Records system. If you are using WebCenter Content: Imaging with the Content Server Adapter and later plan to synchronize data with the Records system, the security groups will not match. The Imaging system creates new security groups dynamically, as needed for applications. Therefore, plan to set up the same security groups on the Imaging system and the Content Server Adapter that are used on the Records system.

The Access Control List (ACL) settings are also not synchronized between the Content Server Adapter and the Records system. This means that it is possible to have a higher ACL security setting on one system than on the other, or to have ACLs disabled on one system. The administrators for the systems should ensure that ACLs are set appropriately for the site's needs.

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 WebCenter Content System Administrator's Guide for Content Server*.

Important: Revisioning of external items differs from revision of items stored on Oracle WebCenter Content. For example, if an item is created on the adapter system and is synchronized to the Records system, it appears as a single item. However, if that item is revised on the adapter system then synchronized to the Records system, 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 Content Server Adapter:

- [Section 16.2.1, "Configuring Sources and Providers"](#)
- [Section 16.2.2, "Managing Fields"](#)

16.2.1 Configuring Sources and Providers

Use these procedures to configure the source and provider.

- [Section 16.2.1.1, "Defining a New Outgoing Provider"](#)
- [Section 16.2.1.2, "Editing an Outgoing Provider"](#)
- [Section 16.2.1.3, "Disabling the Adapter's Outgoing Provider"](#)
- [Section 16.2.1.4, "Deleting the Adapter's Outgoing Provider"](#)
- [Section 16.2.1.5, "Registering an External Source"](#)
- [Section 16.2.1.6, "Unregistering and Removing an External Source"](#)
- [Section 16.2.1.7, "Viewing External Source Configuration Settings"](#)
- [Section 16.2.1.8, "Viewing Outgoing Provider Configuration Settings"](#)

16.2.1.1 Defining a New Outgoing Provider

Use this process to define an outgoing provider:

1. Choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Source Registration**.

The [Register Source Page](#) opens.

2. Click **Add**.

The [Add or Edit New Provider Page](#) opens.

3. Enter the required information in the appropriate fields:

- **Provider Name:** The name of the outgoing provider. Special characters are not allowed.
- **Provider Description:** A description of the provider.
- **Server Host Name:** Host name of the instance on the Records system server.
- **HTTP Server Address:** The URL of the instance.
- **Server Port:** The port on which the provider communicates with the instance.
- **Instance Name:** Name of the instance on the Records system server.
- **Relative Web Root:** The relative root of the instance.

4. Click **Add** when done.

To use a 10g adapter with Oracle WebCenter Content: Records 11g, a connection string must be changed. Previous connection strings were similar to the following example:

```
http://myhost.mycompany.com:myport/URMinstance/idcplg
```

The new connection string should be similar to the following example:

```
http://myhost.mycompany.com:myport/_dav/URMinstance/idcplg
```

The addition of the `_dav` string is all that changes.

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 WebCenter Content: Records source. You must first undo this link before editing the outgoing provider.

1. Choose **Administration** then **Providers** from the Main menu.
The [Provider List Page](#) opens.
2. Navigate to the provider to edit and click **Info**.
The [Provider Information Page](#) opens.
3. Click **Edit**.
The [Add or Edit New Provider Page](#) opens. 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. Choose **Administration** then **Providers** from the Main menu.
The [Provider List Page](#) opens.
2. Navigate to the provider to disable and click **Info**.
The [Provider Information Page](#) opens.
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 WebCenter Content: Records source. You must first undo this link before deleting the outgoing provider.

1. Choose **Administration** then **Providers** from the Main menu.
The [Provider List Page](#) opens.
2. Navigate to the provider to delete and click **Info**.
The [Provider Information Page](#) opens.
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. Choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Source Registration**.
The [Register Source Page](#) opens.
2. Enter the required information in the appropriate fields:
 - Provider Name: Name of the outgoing provider that was configured for communication between the Adapter server and the Records system server.
 - Source Name: The name of the Records system source to be created on the Records system **server**.
 - Source Display Name: Name used in the user interface to identify the source.
 - Source Table Name: Prefix of the database tables created for the source.
 -
3. Click **Register** when done. Registration ensures that the Records system is aware of the Adapter and is ready to manage the stored content in the Adapter server's repository.

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. Choose **Records** then **Record Adapter** from the Top menu. Choose **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. Choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Remove External Sources**.

The Remove External Source page opens.

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), select **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 source configuration settings, choose **Records** then **Record Adapter** from the Top menu. Choose **Configuration Information**. The [Source Configuration Information Page](#) opens.

16.2.1.8 Viewing Outgoing Provider Configuration Settings

Follow this procedure to view outgoing provider configuration settings:

1. Choose **Administration** then **Providers** from the Main menu.

The [Provider List Page](#) opens.

2. Navigate to the provider to delete and click **Info**.

The [Provider Information Page](#) opens.

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 Records system local source. If fields do not exist that match those on the Adapter, create a custom metadata field to accommodate the Adapter data.

This section describes the tasks needed to map custom fields:

- [Section 16.2.2.1, "Mapping a Custom Metadata Field"](#)
- [Section 16.2.2.2, "Editing a Mapped Metadata Field"](#)

16.2.2.1 Mapping a Custom Metadata Field

Use this procedure to add a custom metadata field to a remote source:

1. Choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Custom Fields**.

The [Map Custom Fields Page](#) opens.

2. Click **Add**.

The [Map/Edit Custom Field Dialog](#) opens.

3. A list of custom metadata from the remote source is available in a list. Select a metadata field for use from the list and enter a name and caption for that field to be stored in the Records system database table. You can also enter a different name. If entering a new name, the Adapter automatically creates a corresponding custom metadata field for the name.
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

Use this procedure to edit a previously mapped field:

1. Choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Custom Fields**.
The [Map Custom Fields Page](#) opens.
2. Select a metadata field from the list, and click **Edit**.
The [Map/Edit Custom Field Dialog](#) opens.
3. Alter information as needed and click **Update**.
The [Map Custom Fields Page](#) opens.
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 the Records system, determine a synchronization schedule to ensure that content on both systems, the Adapter and the Records 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 Content Server 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 Oracle WebCenter Content. For example, if an item is created on the adapter system and is synchronized to the Records system, it appears as a single item. However, if that item is revised on the adapter system then synchronized to the Records system, 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 that have been frozen or unfrozen.
- **Content Dates:** Synchronizes any date field that 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 Records system 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:

- [Section 16.3.1, "Performing As-Needed Synchronization"](#)
- [Section 16.3.2, "Scheduling Synchronization"](#)
- [Section 16.3.3, "Viewing Synchronization Logs"](#)

16.3.1 Performing As-Needed Synchronization

Follow this procedure to synchronize content based on specific synchronization operations:

1. Choose **Records** then **Record Adapter** from the Top menu. Choose **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. For details, see [Section 16.3.3, "Viewing Synchronization Logs."](#)

16.3.2 Scheduling Synchronization

Follow this procedure to set up a schedule to perform regular synchronization:

1. To access this page, choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Scheduled Events**.
The [Configure Scheduled Events Page](#) opens.
2. Choose the unit of time measurement from the list and the amount of time to elapse between synchronizations.
3. Choose a time for synchronization that 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. Choose **Records** then **Record Adapter** from the Top menu.

2. Choose **Logs** then choose the type of log file to view.
The [Synchronization Log Page](#) opens.
3. To view additional details about the logged event, choose **View Items** from the operation's **Actions** menu.
4. To rerun the operation, choose **Rerun Task** from the operation's **Actions** menu.

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:

- [Section A.1, "Initial Features Pages"](#)
- [Section A.2, "Configure Retention Settings Page"](#)
- [Section A.3, "Configure Physical Settings Page"](#)
- [Section A.4, "Security Interface"](#)
- [Section A.5, "PCM Configuration Interface Screens"](#)
- [Section A.6, "Retention Schedule Interface Screens"](#)
- [Section A.7, "Triggers Interface"](#)
- [Section A.8, "Time Period Interface"](#)
- [Section A.9, "Custom Metadata Interface"](#)
- [Section A.10, "Disposition and Freeze Interface"](#)
- [Section A.11, "Disposition Interface Screens"](#)
- [Section A.12, "Adapter Interface"](#)
- [Section A.13, "Report Interface"](#)

A.1 Initial Features Pages

After installation of the software, two screens are available with options that must be configured before setting up retention policies and procedures:

- [Section A.1.1, "Enabled Features Page"](#)
- [Section A.1.2, "Setup Checklist Page"](#)

A.1.1 Enabled Features Page

This page is used to determine which components are enabled for use.

Configure : Enabled Features

Select a preset configuration below, or use the Custom option to choose your own settings. Note that you will need to restart the server after making any changes here.

Installation levels

Minimal [i](#)
 Typical [i](#)
 DoD Baseline [i](#)
 DoD Classified [i](#)
 Custom [i](#)

Features

<input checked="" type="checkbox"/> Related Content	<input checked="" type="checkbox"/> Audit Trigger	<input checked="" type="checkbox"/> Subject to Review
<input checked="" type="checkbox"/> Revision Dates	<input checked="" type="checkbox"/> Security Markings	<input checked="" type="checkbox"/> Email Fields
<input checked="" type="checkbox"/> DoD Configuration	<input checked="" type="checkbox"/> Classified Topics	<input type="checkbox"/> FOIA-Privacy Act

Disposition Actions

<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Obsolete	<input checked="" type="checkbox"/> Cancel
<input checked="" type="checkbox"/> Rescind	<input checked="" type="checkbox"/> Expire	<input checked="" type="checkbox"/> Cutoff
<input checked="" type="checkbox"/> Approve Deletion	<input checked="" type="checkbox"/> Destroy	

The page depiction here shows all options.

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Enabled Features**.

After making selections or if configuration options are changed (for example, switching from Baseline to Classified), restart Oracle WebCenter Content and rebuild the index. See the *Oracle WebCenter Content 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 include: <ul style="list-style-type: none"> ■ Minimal ■ Typical ■ DoD Baseline ■ DoD Classified ■ Custom

Element	Description
Features	<p>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.</p> <p>These features include:</p> <ul style="list-style-type: none">■ Related Content■ Audit Trigger■ Subject to Review■ Revision Dates■ Security Markings■ E-mail Fields■ DoD Configuration■ Classified Topics■ FOIA/Privacy Act
Disposition Actions	<p>This section contains the disposition actions for content. They include:</p> <ul style="list-style-type: none">■ 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.

Note that this is a checklist to be used as a reminder. The system does not verify that these items have been appropriately set.

Configure : Setup Checklist

Records Management Setup Checklist

Use this page as a reminder of items that must be set up before using your system. Use the active links below or choose these options from the main Records menu. Use the check boxes to mark items that have been completed.

Detailed documentation is available for each option. Click the Quick Help button then navigate to the appropriate chapter for more information.

[Expand All Details](#)

> Configure Installation	<input type="checkbox"/>
> Configure Report Library	<input type="checkbox"/>
> Define Defaults : (refresh the page once the action is executed)	
Install Data Resource Files (Schema etc.)	Done
Install Default Templates (Category Defaults, Reports , Dashboards etc.)	Done
Checked-in Audit Entries Default Metadata	Not Done
Checked-in Screening Reports Default Metadata	Not Done
Install DoD Content	Not Done
> Configure Security Settings (User Admin Applet)	<input type="checkbox"/>
> Configure Retention Management Settings	<input type="checkbox"/>
> Configure Fiscal, Calendar, and Custom Periods	<input type="checkbox"/>
> Configure Global, Direct, and Indirect Triggers	<input type="checkbox"/>
> Create Retention Schedule or Import Retention Schedule	<input type="checkbox"/>
> Configure Freeze Reasons	<input type="checkbox"/>
> Configure Workflows (Workflow Admin Applet)	<input type="checkbox"/>
> Configure Default Reviewers (User Admin Applet)	<input type="checkbox"/>
> Configure Related Content Types	<input type="checkbox"/>
> Configure 'Profile Trigger' as Trigger Field for:	
Content	Done
Retention Categories	Done
Records Folders	Done

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 page, choose **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 open 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, if 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 Oracle WebCenter Content and rebuild the index.

See the *Oracle WebCenter Content 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 the Records system, you must set up the File Store Provider first and then check in the templates. See the *Oracle WebCenter Content 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 also be available, depending on the installation being performed.

Element	Description
Configure Installation	Used to configure optional components and metadata fields.
Configure Report Library	See Section A.1.2.1, "Configuring the Report Library" for details about configuring the necessary report library.
Define Defaults	Used to define the default 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 checkin page where the fields to be used as defaults can be edited. This option is also used to check in report templates, dashboard panels, and category defaults.
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. Selecting this option opens the Configure Retention Settings Page .
Configure Fiscal, Calendar, and Custom Periods	Used to set periods used for disposition processing. Selecting this option opens the Configure Periods Page .
Configure Global, Direct, and Indirect Triggers	Used to set up the triggers used for disposition processing. Selecting this option opens the Configure Triggers Page .
Create Retention Schedule or Import Retention Schedule	Used to set up retention schedules. Selecting Create Retention Schedule opens the Exploring Retention Schedule Page . Selecting Import Retention Schedule opens the Import/Export Screen. See the <i>Oracle WebCenter Content Administrator's Guide for Records</i> for details about importing and exporting files.
Configure Freeze Reasons	Used to set up freezes. Selecting this option opens 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 as default reviewers.
Configure Related Content Types	Used to set up links. Selecting this option opens the Configure Links Type Page. Links are discussed in the <i>Oracle WebCenter Content User's Guide for Records</i> .

Element	Description
Configure Federated Search Default Category	Used to indicate a default category and default folder to use for Federated searches. Selecting this option opens the Admin Server page where the appropriate configuration variables can be entered: <ul style="list-style-type: none"> ■ FederatedSearchDefaultCategory=<i>categoryId</i> ■ FederatedSearchDefaultFolder=<i>folderId</i>
Configure Profile Triggers	Used to determine the trigger for profiles used in searching and checking in content and physical items.

A.1.2.1 Configuring the Report Library

If you plan to configure the Records Management feature in Content Server, you need to add the `oracle.xdo.runtime.ear` library manually.

For complete details on the configuration process, see the *Oracle WebCenter Content Installation Guide*.

Follow these instructions to load the library from the **WebSphere Integrated Solutions Console** after the server node is created for Oracle WebCenter Content.

1. From the Integrated Solutions Console, click **Shared Libraries** under **Environment**, on the left.
2. In the shared libraries display, select the scope value as the Oracle WebCenter Content node that needs the library.
3. If the `oracle.xdo.runtime.ear` library does not already exist in the Shared Libraries list, click **New**, and enter these values:

```
Name=oracle.xdo.runtime_1_11.1.1.3.0
Classpath=
WC_CONTENT_ORACLE_HOME/ucm/idc/components/ReportPublisher/lib/APP-INF/lib
```
4. Click **Apply**.
5. In the Servers section on the left, under Server Types, click **WebSphere application servers**.
6. In the table on the Application servers screen, click **Oracle WebCenter Content**.
7. In the installed applications display, click **WebCenter Content**.
8. In the application configuration display, under References, click **Shared library references**.
9. Select the **Oracle WebCenter Content** application, and click the **Reference Shared Libraries** button.
10. In the Shared Library Mapping display, select `oracle.xdo.runtime_1_11.1.1.3.0` on the left, move the selection to the right, and click **OK**.
11. In the Reference Shared Libraries display, click **OK**.
12. Under Messages at the top, click **Save** to save the local configuration to the master configuration.

Follow these instructions to configure the library from the **Oracle WebLogic Server Administration Console** after creating the domain that includes the WebCenter Content Managed Server and before starting it for the first time. You also need to add a reference to this library in the `weblogic-application.xml` file of the WebCenter Content EAR file before starting the Managed Server.

1. After a domain is created, start only the Administration Server. If the WebCenter Content Managed Server has already been started, then you will have to perform additional steps to add a reference to the deployed WebCenter Content instance later.
2. Open the Administration Console in browser, click **Deployments** on the left, and browse the pages to check if there is already an `oracle.xdo.runtime` file. If it is already present, then no more steps need to be performed.
3. If the file does not already exist, click **Install** on the Deployments display. A file selection dialog opens. Browse the available file system, and select `oracle.xdo.runtime` in the following path:

```
MW_HOME/WC_CONTENT_ORACLE_  
HOME/ucm/idc/components/ReportPublisher/lib/oracle.xdo.runtime.ear
```
4. Click **Next**. The option page to select the file as library opens. Select **Install this deployment as a library**, and click **Next**.
5. The Target Selection Screen opens. Select all targets, and click **Next**.
6. The Deployment Name screen opens. In the Security section, select **DD Only: Use only roles and policies that are defined in the deployment descriptors**. In the Source accessibility section, select **Copy this application onto every target for me**, and click **Next**.
7. In the Additional Configuration section, select **Yes, Take me to the deployment's configuration screen**, and click **Finish**. The library is now deployed in the environment.

A.2 Configure Retention Settings Page

This page is used 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.

Configure : Settings

General

Record Definition

Security

Notification

Scheduling

User Interface

DoD Config

Classified Topics

Permissions: The Admin.RecordManager right is required to use this page. This right is assigned by default to the Records Administrator role. If the **Run Auto Computation of Declassification Date** option is selected, the user must have the highest security classification as well.

To access this page, choose **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. Default: April 1.

Element	Description
Archive Meta Data Format	<p>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):</p> <ul style="list-style-type: none"> ▪ hda: Proprietary HDA file format, specific to Oracle WebCenter Content. ▪ xml: (initial default): eXtensible Markup Language (XML) format. ▪ csv: Comma-separated values format.
Log Metadata Changes	If selected, enables tracking item-level metadata changes. Default: enabled.
Enable Category Dispositions Review	If selected, enables the workflow to review category dispositions. The workflow must be set up prior to enabling.
Enable Report Exclude Search Options	If selected, report templates and reports are excluded from search results and options are available for use on the Configure Reports Settings Page .
Disable Lifecycle Update	If selected, prevents life cycle updates
Always restrict revisions/Never restrict revisions	If selected, allows or prevents revisioning of content.
Always restrict deletions/Never restrict deletions	If selected, allows or prevents deleting of content.
Always restrict edits/Never restrict edits	If selected, allows or prevents editing of content.
Display record icon	<p>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 when a deletion is restricted or when revisions are restricted. Options include:</p> <ul style="list-style-type: none"> ▪ Deletes Restricted ▪ Edits Restricted ▪ Revisions Restricted ▪ Deletes and Edits Restricted ▪ Deletes and Revisions Restricted ▪ Edits and Revisions Restricted ▪ Deletes, Edits, and Revisions Restricted
ACL-based security	If selected, enables security based on Access Control Lists (ACLs) and enables the Group and User Permissions fields on pages where ACLs can be created to assign security permissions. The initial default is dependent on the features enabled. If DoD Baseline or DoD Classified is enabled, this feature is enabled.
Default Content Server security on Retention Schedule objects	<p>If selected, enables default security on retention categories, record folders, and triggers. Default: enabled.</p> <p>IMPORTANT: If your organization requires a change to this feature after your production environment is running, call Technical Support for assistance.</p>

Element	Description
Supplemental Markings	If selected, enables supplemental marking security on content, record folders, and users. This must be selected to enforce user matching of at least one supplemental marking. Default: enabled.
User must match all Supplemental Markings	If selected, forces a user to match <i>all</i> supplemental markings to access an item. When not selected, a user must match at least <i>one</i> supplemental marking to access an item within a marked record folder. Default: enabled.
Custom Security Fields	If selected, enables the creation of custom security fields. Only available if the DoD Baseline configuration is used. Default: not enabled.
Classified Security	If selected, enables the classified security feature (required for conformance to the Chapter 4 Classified Records section of DoD 5015.2 specification). Default: enabled/disabled, depending if the Classified Enhancements option was selected during configuration.
Do Not Notify Authors	If selected, prevents e-mail notifications from being sent for pending events, reviews, and the Notify Authors disposition action. Default: not enabled.
Only allow scheduled screening	If selected, 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. Default: not enabled.
User-friendly disposition	If selected, enables user-friendly language for disposition rules. If unselected, standard DoD 5015 labels are used. Default: not enabled.
Show Export Date	If selected, enables users to export items in the retention schedule that changed since a specific date. Default: not enabled.
Use Page Navigation	If selected, displays more elaborate page navigation controls on screening results lists and disposition record folder lists. Default: enabled.
Paginate Navigation Tree	If selected, displays the number of pages and page location on screening results lists and disposition record folder lists. Default: enabled.
Enable Custom Script Evaluation	If selected, allows the creation of custom scripts. This field is only displayed if classified security features are enabled. See the <i>Oracle WebCenter Content Administrator's Guide for Records</i> for details about custom scripts. Default: enabled.
Maximum years before declassifying	The number of years after which content is declassified. 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.

Element	Description
Run Auto Computation of Declassification Date	<p>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. The user must also have the highest security setting (for example, Top Secret).</p> <p>When selected, records with a <i>publication date</i> plus the <i>Maximum years before declassifying</i> value that is less than the current date are automatically declassified.</p> <p>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.</p> <p>Default: not enabled.</p>

Important: Enabling or disabling ACLs affects existing ACL settings system-wide. For example, if ACLs are enabled in Oracle WebCenter Content and the Records system is configured to one of the DoD settings (which re-enables ACLs), the Oracle WebCenter Content ACLs are overridden. And if the **Typical** or **Minimal** Oracle WebCenter Content: Records 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.

A.3 Configure Physical Settings Page

This page is used to configure many aspects of Physical Content Management.

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, choose **Physical** then **Configure** then **Settings** from the Top menu.

Element	Description
Default Transfer Method	<p>The default transfer method for reserved physical items:</p> <ul style="list-style-type: none"> ■ 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 (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	<p>The default priority for reservation requests:</p> <ul style="list-style-type: none"> ■ No Priority (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)	<p>The number of days a reserved physical item can be checked out. Administrators can override this value when processing a reservation. Default: 30 days.</p>
Delete completed requests	<p>If selected, completed reservation requests are automatically deleted from the reservations history after a defined number of days. A reservation request is considered completed if no request items are still pending (in process), on a waiting list, or checked out. Default: not enabled.</p>
Request History Period (days)	<p>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.</p> <p>This option is available only if Delete completed requests is selected.</p>
Check in internal content item for reservation workflow	<p>If selected, 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.</p> <p>If unselected, users can still make reservations, but no e-mail notifications about them are received. Default: enabled.</p>
Do not notify users when checked out items are overdue	<p>If selected, users who check out a reservation item receive an e-mail notification if the item is past its due date.</p>
Allow reservation requestors to modify/delete their reservations	<p>If selected, users creating reservation requests can modify or delete their open reservation requests, even if they do not have the PCM.Reservation.Delete and/or PCM.Reservation.Edit rights.</p> <p>When enabled, users 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. Default: not enabled.</p>
Automatically update request waiting lists	<p>If selected, waiting lists for requests are updated automatically. If unselected, the administrator must manually change the status on any of the reservation pages. Default: enabled.</p>

Element	Description
Show batch services	If selected, batch services are available on 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). Default: not enabled.
Enable offsite functionality	If selected, external content offsite storage is enabled.

The Batch Services option is only available 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.

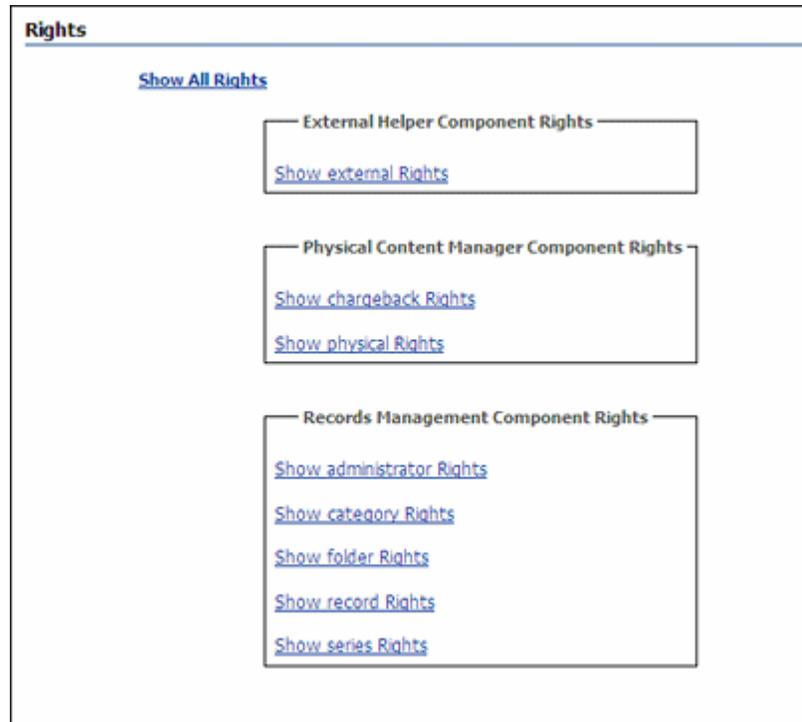
A.4 Security Interface

The following screens are used to view security settings and to set security for classification.

- [Section A.4.1, "Assigned Rights Page"](#)
- [Section A.4.2, "Access Control Edit Section"](#)
- [Section A.4.3, "Edit Rights Page"](#)
- [Section A.4.4, "Classification Interface"](#)
- [Section A.4.5, "Custom Security Interface"](#)
- [Section A.4.6, "Classification Guide Interface"](#)
- [Section A.4.7, "Supplemental Markings Interface"](#)

A.4.1 Assigned Rights Page

This page shows the rights assigned to a specific user.



To access this screen, choose **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

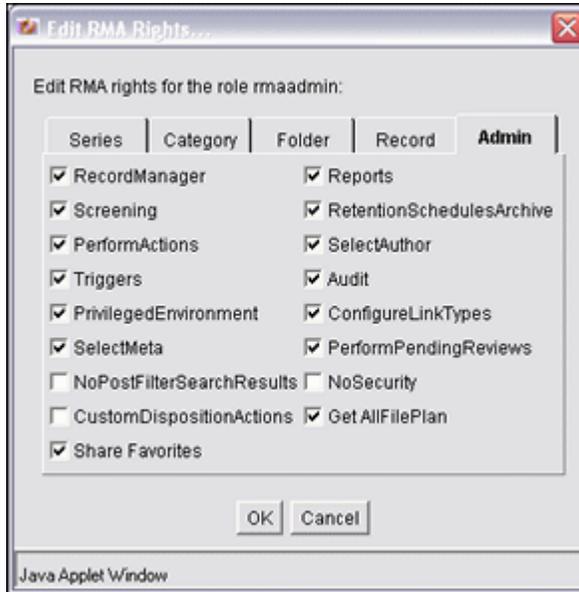
Use this portion of a page to adjust the permissions given to individuals and groups.



This functionality appears on several different pages such as [Create or Edit Trigger Type Page](#) and the [Create or Edit Freeze Page](#).

A.4.3 Edit Rights Page

This page is used to assign management rights to roles.



To access this page, choose **Admin Applets** from the **Administration** menu. Click the User Admin icon. Choose **Security** then choose **Permissions by Role**. Select a role to view the rights. Highlight any role then click **Edit RMA Right** or **Edit ECM Right**.

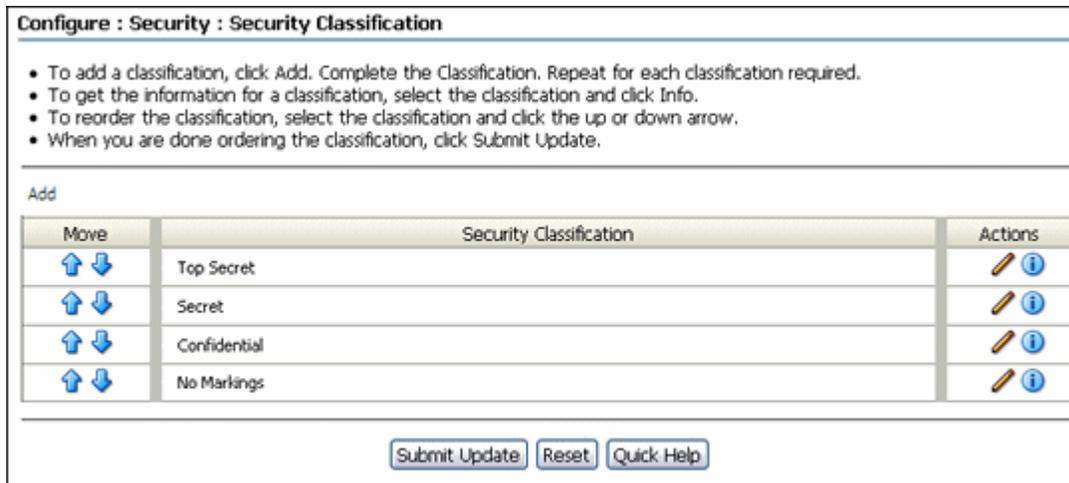
A.4.4 Classification Interface

The following screens are used to manage classifications:

- [Section A.4.4.1, "Configure Security Classification Page"](#)
- [Section A.4.4.2, "Create or Edit Security Classification Page"](#)

A.4.4.1 Configure Security Classification Page

This page is used to create security classifications and set the classification hierarchy.



To access this page, choose **Records** then **Configure** from the Top menu. Choose **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 or Down	Moves a selected security classification upward or downward one step in the hierarchy with each click.
Add	Opens the Create or Edit Security Classification Page , where a security classification can be defined.
Info	Opens 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.4.4.2 Create or Edit Security Classification Page

This page is used to define or change a security classification.

To access the Create page, click **Add** on the [Configure Security Classification Page](#).

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 Custom Security Interface

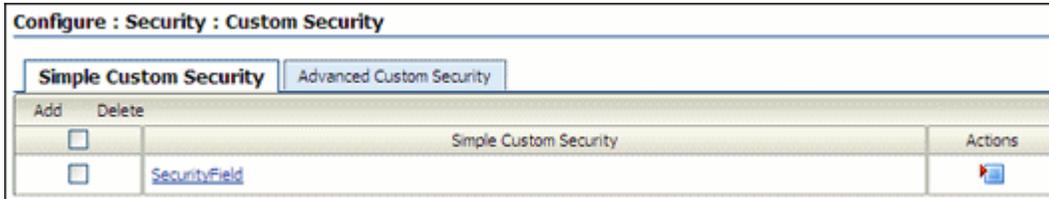
The following screens are used in managing custom security:

- [Section A.4.5.1, "Configure Custom Security Page"](#)
- [Section A.4.5.2, "Create or Edit Simple Custom Security Field Page"](#)

- [Section A.4.5.3, "Advanced Custom Security Option Page"](#)
- [Section A.4.5.4, "Select Security Dialog"](#)

A.4.5.1 Configure Custom Security Page

This page is used to view, delete, or add custom security fields.



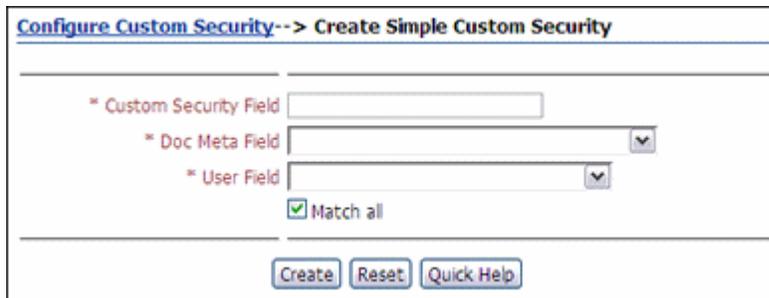
To access this page, choose **Records** then **Configure** from the Top menu. Choose **Security** then **Custom Security**. Two types of security fields can be created:

- 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 **Custom Security** is selected on the [Configure Retention Settings Page](#).

A.4.5.2 Create or Edit Simple Custom Security Field Page

These pages 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, choose **Edit field** from the item's **Actions** 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.

Element	Description
Doc Meta Field	The content field to match against the user field. The list displays all available content fields, custom or otherwise.
User Field	The user field to match against the content field. This field must also be set up in the User Admin utility. Required.
Match all	If selected, forces the user to match all content field entries. When unselected, allows access when a user matches at least one content field.

A.4.5.3 Advanced Custom Security Option Page

This page is used to set the security on individual options in the option list.

Remove	Copy	Option Value	Security Group	Assigned Aliases	Assigned Users	Actions
<input type="checkbox"/>		FOIA Request Review				
<input type="checkbox"/>		Freeze1Test				
<input type="checkbox"/>		Freeze2				
<input type="checkbox"/>		General Litigation				

This page is opened 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	An item in an option list used for the security setting.
Security Group	Security group that can access this option.
Assigned Aliases	Alias that can access this option.
Assigned Users	Users who can access this option.

A.4.5.4 Select Security Dialog

This page is used to select the users, aliases, and security groups who can access the option.



To access this page, choose **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	<p>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.</p> <p>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.</p>
Aliases	<p>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.</p> <p>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.</p>
Security Group	Security group that can access the option.

A.4.6 Classification Guide Interface

The following screens are used to configure classification guides:

- [Section A.4.6.1, "Configure Classification Guide Page"](#)
- [Section A.4.6.2, "Create or Edit Classification Guide Page"](#)

- [Section A.4.6.3, "Administer Classification Topic Page"](#)
- [Section A.4.6.4, "Create or Edit Classification Topic Page"](#)
- [Section A.4.6.5, "Configure Topic Settings Page"](#)

A.4.6.1 Configure Classification Guide Page

This page is used to start setting up classification guides.

The screenshot shows a web interface titled "Configure : Security : Classification Guide". Below the title is a dropdown menu labeled "* Guide Name". To the right of the dropdown are three buttons: "Add", "Info", and "Delete".

To access this page, choose **Records** then **Configure** from the Top menu. Choose **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. Click Info to view information about the selected classification guide or edit it, and click Delete to remove it.
Add	Opens the Create or Edit Classification Guide Page , used to create a new classification guide.
Info	Opens the information page for the selected classification guide. See Classification Guide Information Page .
Delete	Deletes the selected classification guide.

A.4.6.2 Create or Edit Classification Guide Page

This page is used to add or edit the classification guide.

The screenshot shows a web interface titled "Configure Classification Guide--> Create Classification Guide". It contains four input fields: "* Guide ID", "* Guide Name", "Guide Date" (with a calendar icon), and "Originating Organization". Below the fields are three buttons: "Create", "Reset", and "Quick Help".

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, choose **Records** then **Configure** then **Security** from the Top menu. Choose **Classification Guides**. In the menu, select the classification guide to edit and click **Info**. From the Top 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.4.6.3 Administer Classification Topic Page

Use this page to set up and configure classification topics.



To access this page, choose **Edit** then **Configure Topics** from the Page menu on the Classification Guide Information 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 Name	Shows the name of the classification guide the topic is associated with. It cannot be edited.
Topic Name	Contains all defined topics for the current classification guide.
Add	Opens the Create or Edit Classification Topic Page , used to create a new classification topic.
Info	Opens the Classification Topic Information Page.
Delete	Deletes the selected classification topic.

A.4.6.4 Create or Edit Classification Topic Page

This page is used to add or modify classification topics.

The screenshot shows a web form titled "Configure Classification Guide--> Create Classification Topic". The form contains the following elements:

- A label "Guide ID" with the value "JLW1" displayed next to it.
- A label "Topic Name" followed by a single-line text input field.
- A label "Topic Description" followed by a multi-line text input area.
- At the bottom of the form, there are three buttons: "Create", "Reset", and "Quick Help".

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 opens 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	Name of the classification guide with which the topic is associated. It cannot be edited.
Topic Name	Name for the classification topic. Maximum characters: 255.
Topic Description	Description for the topic. Maximum characters: 1,000.
Create (Create Page only)	Opens the Configure Topic Settings Page , where the default metadata field values are specified.

A.4.6.5 Configure Topic Settings Page

This page is used to set or modify the default field values of a classification topic.

The screenshot shows a web form titled "Configure Topics--> Configure Topic Settings for topic 'Editorial Overview'". At the top right, there are "Edit" and "Delete" dropdown menus. The form contains several input fields: "Security Classification" (a dropdown menu), "Reason(s) for Classification" (a text field with a "Select" button), "Declassify Exemption Category" (a text field with a "Select" button), "Declassify on Event" (a text field), "Declassify on Date" (a date picker), and a checked checkbox labeled "Is Auto Declassification Date". Below these is a large text area for "Classification Guide Remarks". At the bottom, there are three buttons: "Submit Update", "Reset", and "Quick Help".

To access this page, choose **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	Default reason(s) for classifications assigned to the topic.
Declassify exemption category	Default declassification exemption category assigned to the topic.
Declassify on event	Default declassification event assigned to the topic.
Declassify on date	Default scheduled declassification date assigned to the topic. If Is Auto Declassification Date is selected, the date for declassification is set according to that setting.
Classification Guide Remarks	Additional remarks about the classification guide to clarify its usage.

A.4.7 Supplemental Markings Interface

The following screens are used when managing supplemental markings:

- [Section A.4.7.1, "Configure Supplemental Markings Page"](#)

- [Section A.4.7.2, "Create or Edit Supplemental Marking Page"](#)

A.4.7.1 Configure Supplemental Markings Page

This page is used to view, delete, or add supplemental markings. It is available when **Use Supplemental Markings** is selected in the [Configure Retention Settings Page](#).

Configure : Security : Supplemental Markings		
Add	Delete	
<input type="checkbox"/>		Supplemental Marking
<input type="checkbox"/>		Audit
<input type="checkbox"/>		Formerly Restricted Data
<input type="checkbox"/>		FOUO
<input type="checkbox"/>		NOCONTRACT
<input type="checkbox"/>		NOFORN
<input type="checkbox"/>		Restricted Data
<input type="checkbox"/>		FGI

To access the page, choose **Records** then **Configure** from the Top menu. Choose **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 WebCenter Content Administrator's Guide for Records* for details about republishing schema.

A.4.7.2 Create or Edit Supplemental Marking Page

This page is used to define or edit supplemental markings.

Configure Supplemental Markings--> Create Supplemental Marking	
* Supplemental Marking	<input type="text"/>
* Brief Description	<input type="text"/>
<input type="button" value="Create"/> <input type="button" value="Reset"/> <input type="button" value="Quick Help"/>	

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 **Actions** 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.

Element	Description
Brief Description	A brief description of the marking. Maximum characters: 30. Required.
Create (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.5 PCM Configuration Interface Screens

The following screens are used to configure PCM.

- [Section A.5.1, "Storage Location and Barcode Configuration Pages"](#)
- [Section A.5.2, "Object Types, Media Types, and Payment Types"](#)

A.5.1 Storage Location and Barcode Configuration Pages

The following screens are used when configuring locations and barcodes:

- [Section A.5.1.1, "Configure Location Types Page"](#)
- [Section A.5.1.2, "Create or Edit Location Type Page"](#)
- [Section A.5.1.3, "Default Metadata for Checked-in Reservation or Offsite Entries Page"](#)
- [Section A.5.1.4, "Create or Edit Storage Page"](#)
- [Section A.5.1.5, "Configuring Custom Barcode Page"](#)
- [Section A.5.1.6, "Create Custom Barcode Dialog"](#)
- [Section A.5.1.7, "Create Batch Storage Import File Page"](#)
- [Section A.5.1.8, "Select Storage Location Dialog"](#)
- [Section A.5.1.9, "Browse Storage Page"](#)
- [Section A.5.1.10, "Physical Items in Storage Page"](#)

A.5.1.1 Configure Location Types Page

This page is used to add, edit, delete, or reorder location types.

Configure : Types : Location Types

To add/remove an object type, select the desired object type and click Add/Remove.
Repeat for each object type required.
When you are done assigning the object types, click Submit Update.

Add		
Move	Location Type	Actions
↑ ↓	Warehouse	i
↑ ↓	Room	i
↑ ↓	Row	i
↑ ↓	Bay	i
↑ ↓	Shelf	i
↑ ↓	Position	i

To access this page, choose **Physical** then **Configure** from the Top menu. Choose **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	Location types in their assigned hierarchical order. 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.
Up or Down	Moves the associated item up or down one level in the storage hierarchy.
Add	Opens the Create or Edit Location Type Page , used to define a new location type.
Info	Opens the 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.5.1.2 Create or Edit Location Type Page

This page is used to define or edit location types to be used in the definition of the storage environment.

Create Location Type

* Location Type ID

* Location Name

Description

Tooltip

Allow storage of content (default)

Maximum Items Allowed

* Image

OK Reset Quick Help

To access this page, choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Location Types**.

To edit a type, choose **Edit Type** from the **Actions** 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	Identifier for the location type displayed in the location type hierarchy. Maximum characters: 30. This field is view-only on the Edit Location Type page. Required.
Location Name	Name of the location type. Maximum characters: 30. Required.
Description	Description for the location type. Maximum characters: 30.
Tooltip	Text for the location type that appears if the mouse cursor is held over the option. Maximum characters: 30.
Allow storage of content (default)	If selected, 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 that enables a user to maintain consistent numbering across parallel objects.
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.
Image	Icon to use for the location type.

A.5.1.3 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.

Configure : Metadata : Reservation Default Metadata

Default Metadata for Checked-in Reservation Entries

Content ID res

* Type PCM Request

Folder

* Title Reservation

* Author wasadmin wasadmin

* Security Group Reservation

Account

* Revision 1

Comments

User Access List

Group Access List

Profile

Template Type

Category or Folders

* Retention Schedules -> rrs admin cat

Record Activation Date

Record Expiration Date

Supplemental Markings

Subject To Audit

Audit

Vital

Vital Reviewer

Vital Period

Watermark Template ID

Watermark Template Type

Release Date 10/3/11 10:49 AM

Expiration Date

To access this page, choose **Physical** then **Configure** from the Top menu. Choose **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.5.1.4 Create or Edit Storage Page

This page is used to create or edit storage locations where physical items can be assigned.

To access this page, choose **Physical** then **Storage** from the Top menu. Select a location for the new storage item and choose **Create** then **Define Storage Location** from the **Actions** 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 choose **Edit** then **Edit Storage Location** from the Page menu. Note that a bar code has been assigned if one wasn't specified during creation.

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	Name for the storage location. Maximum characters: 30. Required.
Description	Description for the storage location. Maximum characters: 30.
Location Type	Location type of the storage location. Required.

Element	Description
Allow storage of content	If selected, 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. If selected, all fields (except Requestor) below it become available.
Status	Available for locations that can hold items. Specifies the 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. Specifies the user who reserved the storage location.
Location Holds	Available for locations that can hold items. Specifies what type of physical items are stored in the storage location. If not specified, the storage location can hold any type of content.
Maximum Items Allowed	Available only for storage locations that can hold items. The maximum number of items the location can hold, used to track space availability. If unspecified, 1 (one) is assumed.
Barcode	Available only for locations that can hold items. The barcode for the location. If not specified, a random 19-digit number is automatically assigned.
Address Information	Addressing information for offsite storage.
Offsite Ship To Code	Available only for offsite storage. The Ship To code for offsite storage.

A.5.1.5 Configuring Custom Barcode Page

This page is used to set a barcode numbering system.

Configure : Function Barcodes				
Add	Delete	Transaction Code	Transaction Name	Is System
<input type="checkbox"/>				
<input type="checkbox"/>	1000		Check Out	Yes
<input type="checkbox"/>	2000		Check In	Yes
<input type="checkbox"/>	3000		Set Home & Actual	Yes
<input type="checkbox"/>	7999		Rene_custom_barcode	No

[Quick Help](#)

To access this page, choose **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	Barcode used for the type of activity or transaction.
Transaction Name	Type of transaction or activity associated with the barcode.

Element	Description
Is System	Indicator of the type of barcode. System barcodes are default barcodes provided with the software.

A.5.1.6 Create Custom Barcode Dialog

This dialog is used to create a new custom barcode.



This dialog opens 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	Code to be associated with the new transaction type. Values must be between 7000 and 9999. Required.
Transaction Name	Activity or event associated with the barcode. Required.

A.5.1.7 Create Batch Storage Import File Page

This page is used to define a new storage hierarchy to be imported by specifying creation rules.

Configure : Batch Storage Creation

Select Storage Start Point

Location Type	Name Prefix	Start Number	Number Of Items	Allow Content	Number of Content Items Allowed	Object Type
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/>	<input type="text" value=""/>	All <input type="text" value=""/>

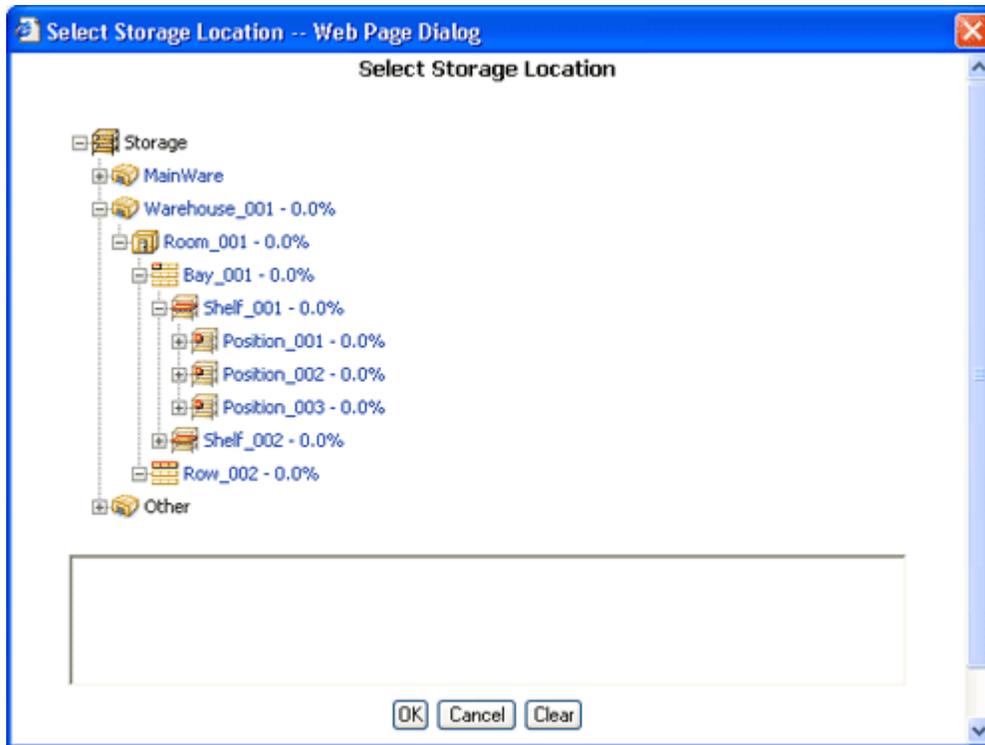
To access this page, choose **Physical** then **Configure** then **Batch Storage Creation** from the Top menu.

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	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	Location type for the storage hierarchy.
Name Prefix	Prefix for the storage location name that is included in the name and description of the storage location.
Start Number	Starting number for the number sequence.
Number Of Items	Number of instances of the storage location to include in the storage space.
Allow Content	If selected, items can 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.
Number of Content Items Allowed	Available if Allow Content is checked. The maximum number of items the storage location can hold.
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.
Create	Creates a <i>StorageImport.hda</i> file, which can be imported into the existing storage hierarchy.

A.5.1.8 Select Storage Location Dialog

This page is used 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, choose **Browse** on the [Create Batch Storage Import File Page](#).

A.5.1.9 Browse Storage Page

This page is used to view all defined storage locations.

Exploring "Storage"

Storage

<input type="checkbox"/>	Storage Name	Location Type	Description	Status	Space Used	Actions
<input type="checkbox"/>	JeremyStore1	Warehouse			41.666667%	
<input type="checkbox"/>	OffSite	Warehouse	Location for items Located at			
<input type="checkbox"/>	Warehouse A	Warehouse				
<input type="checkbox"/>	Other	Misc Storage	Location for unassigned items			

To access this page, choose **Physical** then **Storage** from the Top menu.

A.5.1.10 Physical Items in Storage Page

This page lists physical items contained in a storage location (and its child locations.)

Exploring "JeremyStore1"

Storage --> [JeremyStore1](#)

<input type="checkbox"/>	Storage Name	Location Type	Description	Status	Space Used	Actions
<input type="checkbox"/>	JeremyRoom1	Room			41.666667%	

To access this page, choose **Physical** then **Storage** from the Top menu. Choose the name of a storage location on the [Browse Storage Page](#).

A.5.2 Object Types, Media Types, and Payment Types

The following screens are used to configure object, media, and payment types:

- [Section A.5.2.1, "Configure Object Types Page"](#)
- [Section A.5.2.2, "Create or Edit Object Type Page"](#)
- [Section A.5.2.3, "Edit Object Type Relationships Page"](#)
- [Section A.5.2.4, "Configure Media Types Page"](#)
- [Section A.5.2.5, "Create or Edit Media Type Page"](#)
- [Section A.5.2.6, "Select Media Type Dialog"](#)

A.5.2.1 Configure Object Types Page

This page is used to manage object types.

Configure : Types : Object Types		
Add	Delete	
<input type="checkbox"/>		Object Type Name
<input type="checkbox"/>	All	 
<input type="checkbox"/>	Box	 
<input type="checkbox"/>	Folder	 
<input type="checkbox"/>	Optical	 
<input type="checkbox"/>	Document	 
<input type="checkbox"/>	Microfilm	 
<input type="checkbox"/>	Tape	 

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, choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**.

Element	Description
Object Types	Object types including predefined and custom object types.
Add	Opens the Create or Edit Object Type Page where a new object type can be defined.
Info	Opens the information page for a selected object type where the properties of the object type can be viewed or edited or deleted.

A.5.2.2 Create or Edit Object Type Page

This page is used to add or edit an object type.

To access this page, click **Add** on the [Configure Object Types Page](#). To edit a type, choose **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	Unique identifier for the object type. Maximum characters: 30. This field is view-only on the Edit Object Type page. Required.
Object Type Name	Name for the object type. Displayed in the object type list on the Create Physical Item page. Maximum characters: 30. Required.
Prefix	A prefix to be used to designate this object type.

A.5.2.3 Edit Object Type Relationships Page

This page is used 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, choose **Physical** then **Configure** from the Top menu. Choose **Types** then **Object Types**. Select an object type from the list and choose **Edit Object Type Relationships** from the object's **Actions** 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	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	All object types that cannot be contained in the current object type.
Add or Remove arrow	Moves an object type from one box to the other, to make objects available or unavailable.

A.5.2.4 Configure Media Types Page

This page is used to manage defined media types.

Configure : Types : Media Types		
Add	Delete	
<input type="checkbox"/>		Media Type Name
<input type="checkbox"/>	Audio	 
<input type="checkbox"/>	Blu-Ray	 
<input type="checkbox"/>	Box	 
<input type="checkbox"/>	CD	 
<input type="checkbox"/>	DVD	 
<input type="checkbox"/>	Data	 
<input type="checkbox"/>	Disc	 
<input type="checkbox"/>	Fax	 
<input type="checkbox"/>	Folder	 
<input type="checkbox"/>	Microfiche	 
<input type="checkbox"/>	Microfilm	 
<input type="checkbox"/>	Mixed	 
<input type="checkbox"/>	Paper	 
<input type="checkbox"/>	Photo	 
<input type="checkbox"/>	Visual	 

To access this page, choose **Physical** then **Configure** from the Top menu. Choose **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.

A.5.2.5 Create or Edit Media Type Page

This page is used to create or edit a media type.

Create Media Type	
* Media Type ID	<input type="text"/>
* Media Type Name	<input type="text"/>
* Object Type	<input type="text"/> ▼
<input type="button" value="Create"/> <input type="button" value="Reset"/> <input type="button" value="Quick Help"/>	

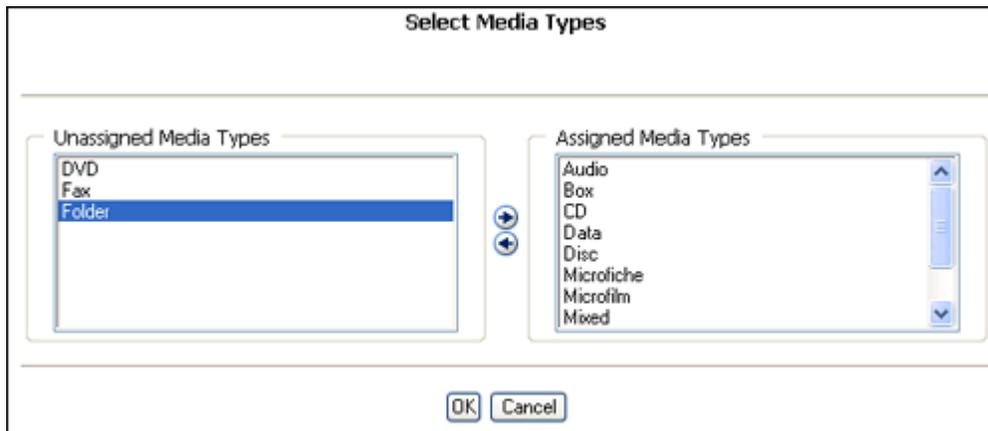
To access this page, click **Add** on the [Configure Media Types Page](#).

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	Identifier for the media type. Maximum characters: 30. This field is view-only on the Edit Media Type page. Required.
Media Type Name	Name for the media type to be displayed in the media type list. Maximum characters: 30. Required.
Object Type	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.5.2.6 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 when managing chargebacks.

A.6 Retention Schedule Interface Screens

The following screens are used to manage Retention Schedules:

- [Section A.6.1, "Exploring Retention Schedule Page"](#)
- [Section A.6.2, "Series Interface Pages"](#)
- [Section A.6.3, "Category Interface Screens"](#)
- [Section A.6.4, "Record Folders Interface Screens"](#)

See the *Oracle WebCenter Content User's Guide for Records* 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.

Exploring Series "Retention Schedules"

Retention Schedules

<input type="checkbox"/>	ID	Name	Date	File	Actions
<input type="checkbox"/>	0031	0031 - COMBATANT COMMA	1/13/10		
<input type="checkbox"/>	0105	0105 - UNIT MANNING DOCL	1/13/10		
<input type="checkbox"/>	0106	0106 - MANPOWER AND PR	1/13/10		
<input type="checkbox"/>	0205	0205 - PAYROLL CORRESPO	1/4/10		
<input type="checkbox"/>	0216	0216 - STANDARDS OF CON	1/13/10		
<input type="checkbox"/>	0220	0220 - LABOR MANAGEMENT	1/13/10		
<input type="checkbox"/>	0239	0239 - TIME AND ATTENDAN	1/4/10		
<input type="checkbox"/>	0414	0414 - LAW LIBRARIES	1/4/10		
<input type="checkbox"/>	0927	0927 - FOIA CONTROL	1/4/10		
<input type="checkbox"/>	0942	0942 - SCIENCE ADVISOR RI	1/4/10		
<input type="checkbox"/>	AuditLogs	Audit Logs	1/4/10		
<input type="checkbox"/>	ReadAccessSeries_AB	ReadAccessSeries_AB	1/14/10	weblogic	
<input type="checkbox"/>	SERIES 0318	REPORTS	1/4/10		
<input type="checkbox"/>	SERIES 0412	MILITARY FILES	1/4/10		
<input type="checkbox"/>	SERIES 0430	CIVILIAN FILES	1/4/10		
<input type="checkbox"/>	SERIES 0950	MISCELLANEOUS FILES	1/4/10		
<input type="checkbox"/>	01KerryTestCat	01KerryTestCat	1/18/10	weblogic	
<input type="checkbox"/>	Accession-DestroyNoSTI	Accession-DestroyNoSTR	1/12/10	weblogic	
<input type="checkbox"/>	AlexCat	Alex_Category	1/7/10	weblogic	
<input type="checkbox"/>	ApproveDeletion	ApproveDeletion	1/11/10	weblogic	

Page 1

To access this screen, choose **Browse Content** then **Retention Schedules** from the Main menu.

A.6.2 Series Interface Pages

The following screens are used to manage series:

- [Section A.6.2.1, "Create or Edit Series Page"](#)
- [Section A.6.2.2, "Series Information Page"](#)
- [Section A.6.2.3, "Select Retention Series, Record Folder or Category Dialog"](#)

A.6.2.1 Create or Edit Series Page

This page is used to add or modify a series.

The screenshot shows the 'Create Series' form. At the top, it says 'Create Series' and 'Retention Schedules'. The form has several sections:

- Security Group:** A dropdown menu with 'RecordsGroup' selected.
- Author:** A text field with 'JeanAdmin' and a dropdown menu with 'JeanAdmin' selected.
- Series Identifier:** A text input field.
- Series Name:** A text input field.
- Series Description:** A larger text input area.
- Group Permissions:** A large empty box with an 'Add' button and an information icon below it.
- User Permissions:** A large empty box with an 'Add' button and an information icon below it.

 At the bottom of the form are three buttons: 'Create', 'Reset', and 'Quick Help'.

Use the Create Page to create a new series. To access this page, choose **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, choose **Edit** then **Edit Series** from the item's **Actions** 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	Security group associated with this series. Required.
Author	The creator of the series. Required.
Series Identifier	Identifier for the series. Maximum characters: 100
Series Name	Name for the series. Maximum characters: 100. Required.
Series Description	Description for the series. Maximum characters: 1,000
Group and User Permissions	Groups and users who can access the series.

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:

- [Section A.6.3.1, "Create or Edit Retention Category Page"](#)
- [Section A.6.3.2, "Retention Category Information Page"](#)
- [Section A.6.3.3, "Metadata History Page"](#)

A.6.3.1 Create or Edit Retention Category Page

These pages are used to create or modify retention categories.

To access this page, choose **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, choose **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	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. Only available if default security is enabled.
Account	Account allowed access to the folder/category. This field is only displayed if accounts are enabled.
Filer	Person who initially created the folder/retention category.
Identifier	Identifier for the category. Maximum characters: 100.
Name	Name for the category. Maximum characters: 100.
Description	A description of the folder/retention category. Maximum characters: 1,000. Required.
Disposition Authority	Disposition authority code. When using this software for DoD tracking, the disposition authority code is 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). <ul style="list-style-type: none"> ■ Required for government sector. Private sector organizations can indicate a person or department responsible for the item, or enter None. ■ Maximum characters: 100.
Restrict options	If selected, the category allows revisions, deletions, or edits. If all restricted options are selected, then the Category contains permanent items. Default: not selected.
Transfer or Accession to NARA	If selected, the category is used to transfer data to the National Archives.
Subject to Review (Create Page only)	If selected, a retention category contains items subject to review. All child record folders and items inherit the review status. Default: not selected. After this is selected, the Reviewer and Review Period fields become available.
Reviewer (Create Page only)	Person responsible for reviewing content. 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 .
Review Period text box and list (Create Page only)	Number of periods to cycle the content and corresponding period. Required if Subject to Review is selected.
Group and User Permissions	Groups and users who can access the category.

A.6.3.2 Retention Category Information Page

This page is used to view information about a retention category.

Retention Category Information

Retention Schedules --> Test for JLW

Author: JeanAdmin

Retention Category: JLWTest

Identifier:

Retention Category Name: Test for JLW

Retention Category Used for testing:

Description:

Disposition Authority: Unneeded

Series Identifier: 0

Restrict Revisions: No

Restrict Deletes: No

Restrict Edits: No

Transfer or Accession to: No

NARA:

Disposition Type: No disposition

Subject to Review: No

Reviewer:

Group Permissions: OffSiteRequestReviewGroup

User Permissions: (JeanAdmin)

Security Group: RecordsGroup

OK

To access this page, choose **Information** then **Category Information** from an item's **Actions** menu on the [Exploring Retention Schedule Page](#).

The displayed information depends on the configuration of the system and if optional fields were populated.

A.6.3.3 Metadata History Page

This page is used to view the metadata history for a retention category (a list of all changes made to the editable category properties).

To access this page, choose **Information** then **Metadata History** from the item's **Actions** menu on the [Exploring Retention Schedule Page](#).

A.6.4 Record Folders Interface Screens

The following screens are used to manage record folders:

- [Section A.6.4.1, "Create or Edit Record Folder Page"](#)
- [Section A.6.4.2, "Record Folder Information Page"](#)

A.6.4.1 Create or Edit Record Folder Page

This page is used to add a new folder or modify existing folders.

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. Choose **Edit** then **Edit Record Folder** from the item's **Actions** menu.

The following fields are described in [Section A.6.3.1, "Create or Edit Retention Category Page."](#)

- Security group
- Account
- Filer
- Identifier
- Name
- Description
- Reviewer
- Review period
- Group permissions
- Select (Group)
- User Permissions
- Select (User)

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	A freeze reason can be updated from this location if editing a record folder. Recommended. Maximum characters: 100.
Subject to Review (Create Page only)	If selected, the folder is subject to review. To inherit review information from a parent folder or category, deselect this option and enter a number and select the period from the list. Default: not selected (not subject to review).
Subject to Audit	If selected, the folder is subject to an audit. The Audit Period list becomes available.
Audit Period	Enabled if the folder is subject to audit.
External Information	External location and container for the item if it is external to the Records system.
Activation Date	Date corresponding to a date in a content item but external to the Records system.
Expiration Date	A deactivation date corresponding to a content item but external to the Records system.
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

This page is used to view information about a record folder.

To access this page, choose **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 displayed information 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:

- [Section A.7.1, "Configure Triggers Page"](#)
- [Section A.7.2, "Create or Edit Trigger Type Page"](#)
- [Section A.7.3, "Trigger Information Page"](#)

- [Section A.7.4, "Indirect Trigger Date Entries Page"](#)
- [Section A.7.5, "Create or Edit Indirect Trigger Date Entries Page"](#)

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, choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Triggers**.

This page lists the name of the trigger, the person who created it and an **Actions** menu for each trigger.

A.7.2 Create or Edit Trigger Type Page

This page is used to add or modify triggers.

The screenshot shows the 'Configure Triggers--> Create Custom Direct Trigger' page. It features a header with the page title. Below the header, there are two rows of configuration options: 'Security Group' with a dropdown menu set to 'RecordsGroup', and 'Filer' with a text input 'JeanAdmin' and a dropdown menu also set to 'JeanAdmin'. The main section contains several input fields: 'Custom Direct Trigger Name', 'Brief Description', 'Record Date Field(s)' (with a dropdown arrow), and 'Folder Date Field(s)' (with a dropdown arrow). Below these is a checkbox labeled 'Synchronize on period start date'. There are two large text areas for 'Group Permissions' and 'User Permissions', each with an 'Add Alias' or 'Add User' button and an information icon. At the bottom of the page are three buttons: 'Create', 'Reset', and 'Quick Help'.

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 choose **Edit** then **Edit Trigger** from a trigger's item **Actions** 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	Security group allowed access to the trigger. This field is available if default security is enabled. Default: RecordsGroup.
Account	Account allowed access to the trigger. This field is available if accounts are enabled.
Filer/ Author	Author of the trigger. Default: Current user. This field is only displayed if default security is enabled.
Trigger Name	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.
Brief Description (Custom direct triggers only)	Description of the trigger. Maximum characters: 100.
Content Date Field(s) (Custom direct triggers only)	Date-related content fields. Maximum characters: 100.
Folder Date Field(s) (Custom direct triggers only)	Record folder date fields. All folder date fields are available, including any custom date fields. Maximum characters: 100.
Enabled (Global triggers only)	Activates or disarms the trigger. To disable the trigger, deselect this option. Default: enabled.
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	If selected, the start date is used to synchronize the trigger.
Group and User Permissions	Specific groups and users who can access the trigger.

A.7.3 Trigger Information Page

This page is used to view information about existing triggers.

[Configure Triggers](#) --> **Global Trigger Information**

References Edit Delete

Author: JeanAdmin

Global Trigger Name: JLWTrigger

Activation Date: 3/11/09 12:00 PM

Synchronize on period: No

start date:

Group Permissions: DispositionsReviewGroup R W D A

User Permissions: (JeanAdmin) R W D A
(radmin) R W D A

Security Group: RecordsGroup

Similar pages are used to view information about Global Triggers, Custom Direct Triggers and Indirect Triggers.

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 that 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

This page is used to create, view information about, edit, and delete date entries for indirect triggers.

To access the page, choose **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	A list of Trigger Periods from which a user can add, find information for, or delete.
Enabled	Specifies if the trigger date entry is enabled.
Add	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](#) opens.
- 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

This page is used to define the trigger period, enable or disable the trigger, and set an activation date for an indirect trigger.

To access this page, choose **Records** then **Configure** from the Top menu. Choose **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 access this page, choose **Edit** from a trigger's item **Actions** 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.
Synchronize on Period Start Date	If selected, the start date is used to synchronize the trigger.

A.8 Time Period Interface

The following screens are used when managing time periods:

- [Section A.8.1, "Configure Periods Page"](#)
- [Section A.8.2, "Create or Edit Period Page"](#)
- [Section A.8.3, "Period Information Page"](#)

A.8.1 Configure Periods Page

This page is used to select a period for editing or to add a new period.

Add	Delete	Period Name	Actions
<input type="checkbox"/>		day	
<input type="checkbox"/>		Fiscal Years	
<input type="checkbox"/>		Fiscal Halves	
<input type="checkbox"/>		Fiscal Quarters	
<input type="checkbox"/>		Calendar Years	
<input type="checkbox"/>		Calendar Quarters	
<input type="checkbox"/>		Months	
<input type="checkbox"/>		Weeks	

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Periods**.

A.8.2 Create or Edit Period Page

This page is used to create or modify time periods.

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, choose **Edit Period** from the item's **Actions** 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	Name that appears in the Period options lists. Maximum characters: 30.

Element	Description
Period Type	Type of period: <ul style="list-style-type: none"> ■ Fiscal: Based on the fiscal year as defined by the organization. ■ Calendar: A period based on the calendar year. ■ Custom (default): A period based on organizational factors.
Custom Start Time	Start date and time for a custom period.
Length	Length of the period: <ul style="list-style-type: none"> ■ Years ■ Months ■ Weeks ■ Days
Label for end of period	Label for the end of the period. Maximum characters: 30.

A.8.3 Period Information Page

This page is used to view information about a period.

Period Information

[Edit](#) [Delete](#) [References](#)

Period Name: JLWPromoPeriod

Period Type: Custom

Custom Start Time: 2/1/07 12:00 AM

Length: 6 Months

Label for end of period: End of Promo

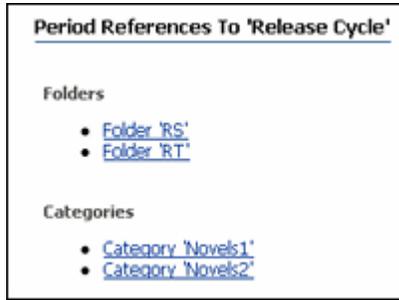
Built-in: No

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](#).

A.8.4 Period Reference Page

This page is used to view those objects that 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:

- [Section A.9.1, "Metadata List Page"](#)
- [Section A.9.2, "Fields for Metadata Page"](#)
- [Section A.9.3, "Create or Edit Standard Metadata Field Page"](#)
- [Section A.9.4, "Create or Edit Auxiliary Metadata Set Page"](#)
- [Section A.9.5, "Metadata Information Page"](#)

A.9.1 Metadata List Page

This page shows the tables used to store metadata.

Configure : Retention : Metadata Sets

Create Auxiliary Metadata Set					
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, choose **Records** then **Configure** from the Top menu. Choose **Metadata** then **Metadata Sets**.

Click **Create Auxiliary Metadata Set** to create a new set. To add fields to an existing metadata set, choose **Update Fields** from the **Actions** menu for the set.

Element	Description
Name	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.
Display Name	Name for the metadata set that appears in the user interface.
Actions	<p>When creating standard metadata sets, this menu contains two options:</p> <ul style="list-style-type: none"> ■ Update Fields: Updates fields in the metadata set. ■ Fields Information: Opens the Fields for Metadata Page, listing information about the metadata fields. <p>If creating an auxiliary metadata set, a third option is available for existing sets:</p> <ul style="list-style-type: none"> ■ Delete set: Delete the set. It is not possible to delete a set that has a value of <i>Yes</i> in the System Metadata column.

A.9.2 Fields for Metadata Page

This page displays metadata fields and is used to add new fields.

To access this page choose **Field Information** in the **Actions** menu of a set on the [Metadata List Page](#).

For details about the information on this screen, see [Section A.9.4, "Create or Edit Auxiliary Metadata Set Page."](#)

A.9.3 Create or Edit Standard Metadata Field Page

This page is used to create or edit a custom metadata field.

Edit 'RetentionCategories' Metadata Set quick help

Metadata Sets --> Edit 'RetentionCategories' Metadata Set

- To add a new field, fill out field information then click the plus (+) sign below the Field List.
- To edit a field, select the field, alter the information, then click the plus (+) sign below the Field List.
- To delete a field, select the field and click the X sign below the Field List.
- When finished with all changes, click the Apply button to save the changes to the database.

Field List

+
+
X

Field Information

Name:

Caption:

Type:

Default Value:

Required

Enabled

Searchable

Option List:

Option List Type:

To access this page, choose **Update Fields** in the **Actions** 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	Name for the field in the database. Maximum characters: 30. Required. Special characters are not allowed.
Caption	A caption for the field displayed on the user interface. Maximum characters: 30. Required.
Type	The data type for the field. Options include Text, Long Text, Integer, Memo, or Date.
Default Value	Default value for an Option List, Text, or Long Text field. Maximum characters: 30.
Required	If selected, the custom metadata field is required.
Enabled	If selected, the field is enabled on Oracle WebCenter Content pages.
Searchable	If selected, the field is indexed in the database and searchable.
Option List Key	Field used for the option list. Click Choose to select a key from a list list.
Option List Type	Type of option list.

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.

Create Auxiliary Metadata Set
[quick help](#)

Metadata Sets --> Create Auxiliary Metadata Set

Auxiliary metadata set information

Metadata can be attached to objects to associate properties to the object. For example, size can be associated with an image or character coding can be associated with a document. Use the Auxiliary Metadata Set to create these types of metadata.

Name:

Display Name:

Table Name:

Column Prefix:

Configure fields

- To add a new field, fill out field information then click the Add button (+) below the Field List.
- To edit a field, select the field, alter the information, then click the Add button (+) below the Field List.
- To delete a field, select the field and click the Delete (X) button below the Field List.
- When finished with all changes, click the Apply button to save the changes to the database.

Field List

+
X

Field Information

Caption:

Type: ▼

Default Value:

Is Required

Is Enabled

Is Searchable

Option List:

Option List Type: ▼

To access this page, click **Create Auxiliary Metadata Set** from the [Metadata List Page](#). To add fields to a current set, choose **Update Fields** from the **Actions** 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	Name for the metadata set. Maximum characters: 30. Special characters are not allowed.
Display Name	Caption for the metadata set. Maximum characters: 30.
Table Name	Name of the table in the database. Required.

Table Information Section	Description
Column Prefix	Prefix for the column housing the field.

See [Section A.9.3, "Create or Edit Standard Metadata Field Page"](#) for details about the other information on this page.

A.9.5 Metadata Information Page

This page displays information about metadata 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:

- [Section A.10.1, "Disposition Interface"](#)
- [Section A.10.2, "Freeze Interface"](#)

A.10.1 Disposition Interface

The following screens are used when managing dispositions:

- [Section A.10.1.1, "Configure Dispositions Page"](#)
- [Section A.10.1.2, "Create or Edit Disposition Action Page"](#)
- [Section A.10.1.3, "Disposition Action Info Page"](#)
- [Section A.10.1.4, "Disposition Actions Configuration Page"](#)

A.10.1.1 Configure Dispositions Page

This page is used to access dispositions and to add new dispositions.

Custom Disposition Actions			
Add	Delete	Custom Disposition Actions	Actions
<input type="checkbox"/>			
<input type="checkbox"/>		dfad	
<input type="checkbox"/>		disposal	

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Disposition Actions** then **Custom**.

A.10.1.2 Create or Edit Disposition Action Page

This page is used to add or edit custom disposition actions.

Configure Custom Disposition Actions--> Create Disposition Action

* Action ID

* Action Name

* Brief Description

* Group Name

* Action Service

Action Service Parameters

Must Be First

Must Be Last

Require Approval

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, choose **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	Name for the custom disposition action. Maximum characters: 30.
Action Name	Name for the custom disposition action. The name is shown in the list of available disposition actions. Maximum characters: 30.
Brief Description	A description of the custom disposition action. Maximum characters: 100. Required.
Group Name	Heading name where the custom disposition action is grouped in the list of available disposition actions on the Disposition Rule Page .
Action Service	Service to be used for the custom disposition action.
Action Service Parameters	Parameter(s) to be used for the selected action service.
Must Be First	If selected, the custom disposition action can only be used as the first action in a disposition instruction.
Must Be Last	If selected, the custom disposition action can only be used as the last action in a disposition instruction.
Require Approval	If selected, approval is required for the disposition action to be performed. Default: selected.

A.10.1.3 Disposition Action Info Page

This page displays the 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

This page is used to disable dispositions actions.

Configure Disposition Actions
Select the disposition actions you want to disable

<input type="checkbox"/> Declassify	<input type="checkbox"/> Downgrade Classification	<input type="checkbox"/> Review Classification
<input type="checkbox"/> Upgrade Classification	<input type="checkbox"/> MSDisposal	<input type="checkbox"/> Test
<input type="checkbox"/> Delete Previous Revision	<input type="checkbox"/> Delete Revision	<input type="checkbox"/> Approve Deletion
<input type="checkbox"/> Delete All Revisions (Destroy Metadata)	<input type="checkbox"/> Delete All Revisions (Keep Metadata)	<input type="checkbox"/> Delete Old Revisions
<input type="checkbox"/> Check in New Revision	<input type="checkbox"/> Accession	<input type="checkbox"/> Accession (Destroy Metadata)
<input type="checkbox"/> Accession (Keep Metadata)	<input type="checkbox"/> Activate	<input type="checkbox"/> Close
<input type="checkbox"/> Cutoff	<input type="checkbox"/> Cutoff and Create Volume	<input type="checkbox"/> Expire
<input type="checkbox"/> Obsolete	<input type="checkbox"/> Mark Related Content	<input type="checkbox"/> No Action
<input type="checkbox"/> Notify Authors	<input type="checkbox"/> Supersede	<input type="checkbox"/> Transfer to OffSite Storage
<input type="checkbox"/> Archive	<input type="checkbox"/> Archive (Destroy Metadata)	<input type="checkbox"/> Archive (Keep Metadata)
<input type="checkbox"/> Create Content Server Archive	<input type="checkbox"/> Create Volume	<input type="checkbox"/> Move
<input type="checkbox"/> Move (Destroy Metadata)	<input type="checkbox"/> Move (Keep Metadata)	<input type="checkbox"/> Transfer
<input type="checkbox"/> Transfer (Destroy Metadata)	<input type="checkbox"/> Transfer (Keep Metadata)	

Submit Update Reset Quick Help

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, choose **Records** then **Configure** from the Top menu. Choose **Disposition Actions** then **Disable**.

A.10.2 Freeze Interface

The following screens are used when managing freezes;

- [Section A.10.2.1, "Freeze Configuration Page"](#)
- [Section A.10.2.2, "Create or Edit Freeze Page"](#)
- [Section A.10.2.3, "Freeze Information Page"](#)
- [Section A.10.2.4, "Frozen Item Page"](#)

A.10.2.1 Freeze Configuration Page

This page is used to add new or access freezes.

Add	Unfreeze	Delete	Add To Favorites	Freeze	Freeze Description	Actions
<input type="checkbox"/>				Freeze		
<input type="checkbox"/>				FOIA Request Review	These are to be used for FOIA requests.	
<input type="checkbox"/>				Freeze1Test		
<input type="checkbox"/>				Freeze2		
<input type="checkbox"/>				General Litigation	These are to be used for pending and general litigation.	

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Retention** then **Freezes**.

A.10.2.2 Create or Edit Freeze Page

This page is used to add or edit freezes.

Configure Freezes--> Create Freeze

Security Group: RecordsGroup

Author: JeanAdmin

Freeze Name: [Text Field]

Freeze Description: [Text Field]

Group Permissions: [List Box] [Add] [Info]

User Permissions: [List Box] [Add] [Info]

End Date: [Date Picker]

Unfreeze Instructions: [Text Field]

Send Notification

Email To: [Text Field]

Email From: [Text Field]

Email Message: [Text Field]

Periodically Resend Notification

Period: [Text Field]

Period Name: [Dropdown]

[Create] [Reset] [Quick Help]

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, choose **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	Security group allowed access to the freeze. Default: RecordsGroup. This field is only displayed if default security is enabled.
Author	Person who created the freeze. Default: Current user. This field is only displayed if default security is enabled.
Freeze Name	Freeze name shown in the user interface. Maximum characters: 30.
Freeze Description	Description for the freeze. Maximum characters: 1,000. Required.
Creation Date (Edit Page only)	Date and time the freeze was created. This field is view-only and is displayed for tracking and documentation purposes.
Group and User Permissions	Groups and users who can access the freeze.
End Date	Date when the freeze ends and when the items should be unfrozen again.

Element	Description
Unfreeze Instructions	Instructions for unfreezing items. 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	If selected, sends e-mail to one or more persons when the freeze is created or edited.
E-mail To	The e-mail address(es) where the notification should be (re)sent (in the form <i>user@domain.com</i>). Required if Send Notification 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. Maximum characters: 100.
E-mail Message	The body text of the e-mail notification (the actual message). Required if Send Notification is selected. Maximum characters: 3,000.
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

This page displays the characteristics of a selected freeze.

To access this page, click a freeze name on the [Freeze Configuration Page](#).

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.

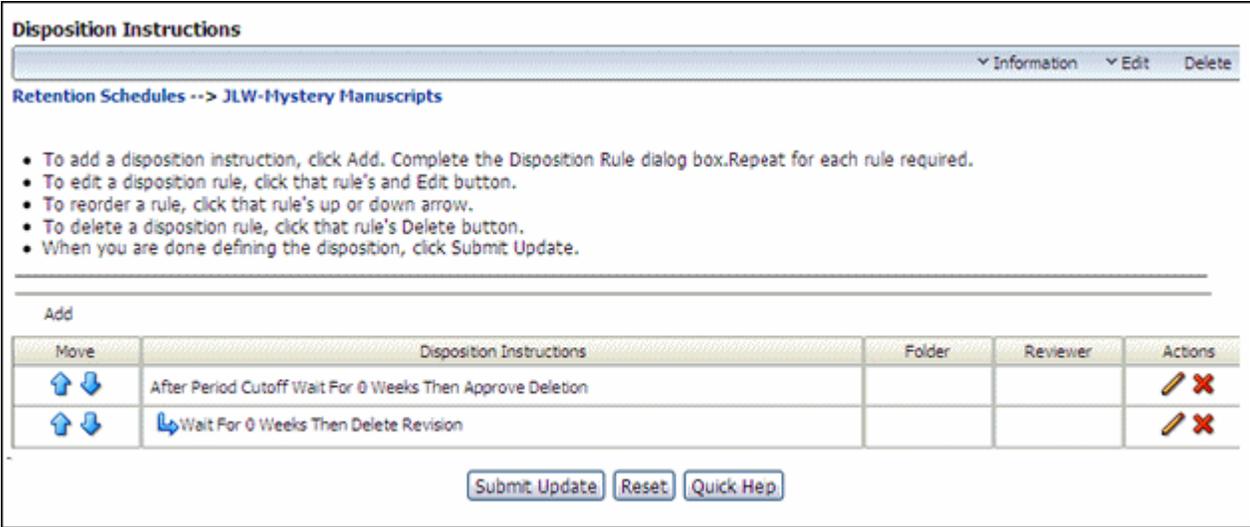
A.11 Disposition Interface Screens

The following screens are used to manage dispositions:

- [Section A.11.1, "Disposition Instructions Page"](#)
- [Section A.11.2, "Disposition Rule Page"](#)
- [Section A.11.3, "Disposition Information Page"](#)

A.11.1 Disposition Instructions Page

This page is used 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, choose **Edit** then **Edit Disposition** from the item’s **Actions** menu.

This page is also opened 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	Moves a selected disposition rule upward or downward one row with each click.
Add	Opens the Disposition Rule Page , where a new disposition rule can be defined.
Edit	Pencil icon. Opens the Disposition Rule Page for the disposition rule selected in the Disposition Instructions box.
Delete	Red X icon. Deletes the disposition rule selected within the Disposition Instructions box.

A.11.2 Disposition Rule Page

This page is used 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 = <i>After</i>)	Triggering events to associate with a disposition rule.
Retention Period text box and list (user-friendly label = <i>Wait for</i>)	The number of periods and period unit to retain scheduled items. The list displays all defined periods.
Is External Approval	If selected, the item must go through an external approval process. This option only appears if an external approval process has been set up on the system.
Disposition Action (user-friendly label = <i>Do</i>)	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.
Notification Reviewer	Specifies who is notified of the event.
Apply to Record Folder (user-friendly label = <i>On Folder(s)</i>)	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.
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.
Location Type	If the disposition action is an option like archive, move, or transfer, choose a location from the Location Type list.

Element	Description
Destination Container (user-friendly label = To Container)	Physical container for an external record folder, such as a barcode or some other means of identification. Maximum characters: 30.
Field mapping	If selected, fields are mapped 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 Oracle WebCenter Content for this setting to take effect.

A.11.3 Disposition Information Page

This page is used to view information about disposition instructions for a retention category.

To view this page, browse to a retention category. Choose **Information** then **Disposition Information** from the item's **Actions** menu or choose **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 Record Adapter.

- [Section A.12.1, "Register Source Page"](#)
- [Section A.12.2, "Add or Edit New Provider Page"](#)
- [Section A.12.3, "Provider List Page"](#)
- [Section A.12.4, "Provider Information Page"](#)
- [Section A.12.5, "Source Configuration Information Page"](#)
- [Section A.12.6, "Map Custom Fields Page"](#)
- [Section A.12.7, "Map/Edit Custom Field Dialog"](#)
- [Section A.12.8, "Configure Scheduled Events Page"](#)
- [Section A.12.9, "Synchronization Log Page"](#)

A.12.1 Register Source Page

This page is used to register the external Adapter source.

To access this page, choose **Records** then **Record Adapter** from the Top menu. Choose **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	Name of the outgoing provider that was configured for communication between the Adapter server and the Records system server.
Source Name	The name of the Records system source to be created on the server.
Source Display Name	Name used to identify the source on the Search page on the Oracle WebCenter Content server.
Source Table Name	Prefix of the database tables that are created for the Records system source.
Register	Registers the Content Server Adapter with the Records system.

A.12.2 Add or Edit New Provider Page

This page is used to define the outgoing provider that enables the Adapter server to connect to the Records system 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 WebCenter Content 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 the Records system in the `config.cfg` file. This can be done during installation of the Records system, but it may be overlooked.

Element	Description
Provider Name	The name of the outgoing provider for the Adapter server. Special characters or hyphens are not allowed.
Provider Description	Description of the provider.
Server Host Name	Server host name of the instance on the Records system server.
HTTP Server Address	URL of the instance on the Records system server.
Server Port	Port on which the provider communicates with the instance on the Records system server.
Instance Name	Instance name on the Records system server.
Relative Web Root	Relative web root of the instance on the Records system server.

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
keepaliveincoming	Configure a keepalive incoming socket provider.	Add
keepaliveoutgoing	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, choose **Administration** then **Providers** from the Main menu.

The top half of this page shows the currently configured providers. The bottom half can be used to add a new provider. See the *Oracle WebCenter Content System Administrator's Guide for Content Server* for details about using this page.

A.12.4 Provider Information Page

This page lists information about an outgoing provider.

To access this page, choose **Administration** then **Providers** from the Main menu. Choose the **Info** link next to an outgoing provider.

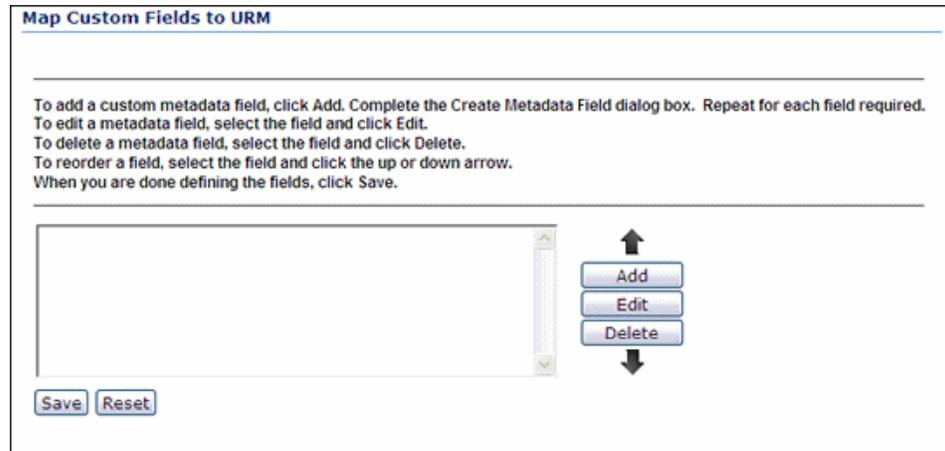
A.12.5 Source Configuration Information Page

This page displays information about a registered source.

To access this page, choose **Records** then **Record Adapter** from the Top menu. Choose **Configuration Information**.

A.12.6 Map Custom Fields Page

This page is used to create and define custom metadata fields for the Records system source.

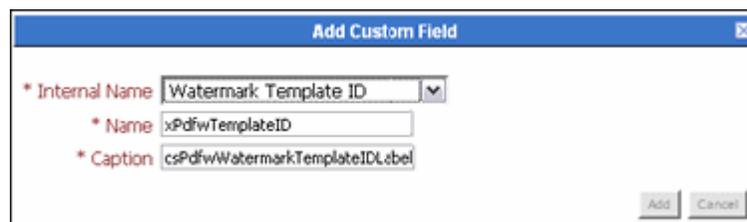


This page is displayed when a source is first registered. It can also be accessed by choosing **Records** then **Record Adapter**. Choose **Configure** then **Custom Fields**.

Element	Description
Custom metadata fields pane	Lists the available custom metadata fields that can be edited or deleted, as necessary.
Add or Edit	Opens the Map/Edit Custom Field Dialog , used to create new custom metadata fields or edit existing fields.
Up or Down	Adjust the 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.

A.12.7 Map/Edit Custom Field Dialog

This dialog is used to add a custom metadata field for use with the Record Adapter.



This dialog is opened when a user clicks **Add** or **Edit** on the [Map Custom Fields Page](#).

Elements	Description
Internal Name	Lists the Adapter's custom metadata fields that can be mapped to the Records system custom metadata fields.
Name	Name of the custom metadata field to be created.
Caption	Name of the field that appears in the user interface.

A.12.8 Configure Scheduled Events Page

This page is used to schedule synchronization activities for the Adapter.

Configure Scheduled Events

Synchronize Retention Schedule
 Run every Day(s) between AM and AM

Synchronize Content
 Run every Day(s) between AM and AM

Synchronize Deleted Content
 Run every Day(s) between AM and AM

Synchronize Content Dates
 Run every Day(s) between AM and AM

Synchronize Mark Complete
 Run every Day(s) between AM and AM

Synchronize Archives
 Run every Day(s) between AM and AM

Synchronize Mark Vital
 Run every Day(s) between AM and AM

To access this page, choose **Records** then **Record Adapter** from the Top menu. Choose **Configure** then **Scheduled Events**.

Elements	Description
Synchronization choices	Each section of this screen displays items that can be synchronized.
Synchronization schedule	Time period for the synchronization.
Synchronization time	Time of day for the synchronization.

A.12.9 Synchronization Log Page

This page displays information about synchronization activities.

To access this page, choose **Records** then **Record Adapter** from the Top menu. Choose **Logs** then the log type. The example shown here is a log for an Archive operation.

Important: Revisioning of external items differs from revision of items stored on Oracle WebCenter Content. For example, if an item is created on the adapter system and is synchronized to the Records system, it appears as a single item. However, if that item is revised on the adapter system then synchronized to the Records system, 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.

- [Section A.13.1, "Configure Reports Settings Page"](#)
- [Section A.13.2, "Configure Report Element Page"](#)
- [Section A.13.3, "Report Checkin Page"](#)
- [Section A.13.4, "Report Templates Page"](#)
- [Section A.13.5, "Configure Report Sources Page"](#)
- [Section A.13.6, "XML Data Dialog"](#)

A.13.1 Configure Reports Settings Page

This page is used to set up reports for retention items, chargebacks, and other functionality.

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

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.

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Reports** then **Settings**. 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.

Element	Description
Template Check In Profile	Profile to use for the template when it is checked in.
Report Check In Profile	Profile to use when the report is checked in.
System Report Format	Default format for reports.
Exclude Report Templates in Search Results	If selected, templates are excluded from search activities. This box is available for selection only if Enable Report Exclude Search Options is selected on the Configure Retention Settings Page .

Element	Description
Exclude Reports in Search Results	If selected, reports are excluded from search activities. This box is available for selection only if Enable Report Exclude Search Options box is selected on the Configure Retention Settings Page .

A.13.2 Configure Report Element Page

This page 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, choose **Records** then **Configure** from the Top menu. Choose **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.

Configure : Reports : Create New Report

Select the Report Type you wish to configure.

- Storage
- Reservation
- Function Barcodes
- Invoices
- Transactions
- Customers
- Payment Methods
- Charge Types
- Physical

To access this page, choose **Physical** then **Configure** then **Reports** from the Top menu. Then choose a report option. After choosing a report option, the [Configure Report Element Page](#) is opened. 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.

Report Content Type

* Report Template

* Report Format

* Report Source Type

* Report Source

Report Source Parameters

Report Scheduled Information

Category or Folders

Content Relations

* Release Date

Expiration Date

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Reports** then **Create New Report**. Choose the type of report to create then choose **Configure**.

Element	Description
Report Template	Template to use for the report. Choose a template from the list or click Add New to create a new template.
Report Format	Format for the report. When creating a report for barcodes, the user must choose PDF as the report type.

Element	Description
Report Source Type	Choose the type of source to use to gather the data for the report. Options include Service, Query, or Dynamic Query. If Services or Query are used, 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	Source for the data. Select from the list 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 reports.

Report Templates for 'InternalContent' Found 8 potential items

Search form --> Report Templates for 'InternalContent'

Select	Security Classification	Content ID	Title	Date	Author	Actions
<input type="checkbox"/>		SEARCHRESULTSTEMPL	Annual Report	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		SEARCHRESULTSTEMPL	Appeals	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		SEARCHRESULTSTEMPL	Denials	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		SEARCHRESULTSTEMPL	Initial Request D	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		INTERNALITEMCLASSIF	Internal Item Cl	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		INTERNALITEMCLASSIF	Internal Item Cl	1/14/10 11:37 AM	sysadmin	
<input type="checkbox"/>		INTERNALITEMDETAILR	Internal Item De	1/4/10 3:56 PM	sysadmin	
<input type="checkbox"/>		INTERNALSEARCHRESU	Search Results	1/4/10 3:56 PM	sysadmin	

To access this page, choose **Records** then **Configure** from the Top menu. Choose **Reports** then **Templates**. Choose a template type then choose **Configure**.

Element	Description
Select	If selected, the template will be used.
Security Classification	Classification associated with a template.
Content ID	Content ID of the template file.
Title	Template title.
Date	Date the template file was created or modified.
Author	Author of the file.
Actions	Actions that 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 is used to perform actions for all template files or only selected files.

A.13.5 Configure Report Sources Page

This page is used to choose queries and service calls to gather data for the report.

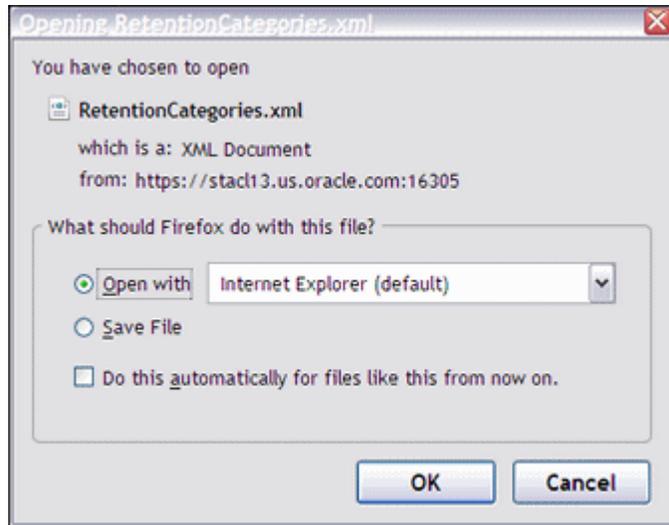


Important: Creating custom report sources requires in-depth technical knowledge of services and queries. Contact Consulting Services for further assistance if needed.

To access this page, click **Add New** on the [Report Checkin Page](#) or choose **Records** then **Configure** from the Top menu. Choose **Reports** then **Report Sources**. A user can also access this page by choosing **Physical** then **Configure** then **Reports** then **Report Sources** from the Top menu.

A.13.6 XML Data Dialog

This dialog opens when the user elects to download an XML data file.



To view the file, select **Open With** and choose a browser type from the menu. To save the file, select **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, select **Do this automatically...**

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 [Section 5.3.4, "Security Classifications Tasks and Defaults for Predefined Roles."](#) It is merely presented in a different manner.

This chapter describes the following topics:

- [Section B.1, "Rights and Roles for Oracle WebCenter Content: Records"](#)
- [Section B.2, "Physical Content Management Rights and Roles"](#)

B.1 Rights and Roles for Oracle WebCenter Content: Records

This section describes the default rights and roles for tasks encountered while using Oracle WebCenter Content: Records.

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 e-mail 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 [Section B.1.12, "Content."](#)

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

Task	Required RM Right	Requestor	Admin
Set up object types	PCM.Admin.Manager		X
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

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:

- [Section C.1, "Custom Disposition Actions"](#)
- [Section C.2, "Using Custom Barcodes"](#)
- [Section C.3, "Adding a Mobile Bar Code Reader"](#)
- [Section C.4, "Creating Custom Reports"](#)

C.1 Custom Disposition Actions

Important: If custom dispositions were previously created using an older version of the Records system, 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 dispositions 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 WebCenter Content 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:

- [Section C.1.1, "Managing Custom Dispositions"](#)
- [Section C.1.2, "Disabling Custom Disposition Actions"](#)
- [Section C.1.3, "Creating a Custom Disposition Action Example"](#)
- [Section C.1.4, "Creating Disposition Rules for Physical Content"](#)

C.1.1 Managing Custom Dispositions

The following tasks are used when managing dispositions:

- [Section C.1.1.1, "Creating or Editing a Custom Disposition Action"](#)
- [Section C.1.1.2, "Viewing Custom Disposition Action Information"](#)
- [Section C.1.1.3, "Deleting a Custom Disposition Action"](#)

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 WebCenter Content. 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](#) opens.
2. Click **Add** in the Custom Disposition Action section.
The [Create or Edit Disposition Action Page](#) opens.
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. The default value for this field is stored in the ww_strings.htm file in the

wwOptGroupLabelCustomDispositionActionsList. It 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 Oracle WebCenter Content. Do not change the suggested default value in the Group Name field.

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 any of the checkboxes as required. Selections include **Must Be First, Must Be Last, Require Approval**. These actions determine when the custom disposition action will be used and how.
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 Parameters
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

Disposition/Event	Service Parameters
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](#) opens.
2. Click **Edit Action** from a disposition **Actions** menu.
The [Create or Edit Disposition Action Page](#) opens.
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](#) opens.
2. Click the disposition name to view.
The [Disposition Action Info Page](#) opens.
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](#) opens.

2. Choose **Delete Action** from a disposition's item **Actions** menu. You can also select the checkbox by the action name and choose **Delete** from the Table menu.

A message is displayed saying the disposition action was deleted successfully.

3. Click **OK**.

To delete multiple dispositions, select the checkbox for the dispositions to delete on the [Configure Dispositions Page](#) and choose **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](#) opens.

2. Select the checkbox next to the actions that should be disabled.
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](#) opens.

2. In the Custom Disposition Action section, click **Add**.

The [Create or Edit Disposition Action Page](#) opens.

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, select `DELETE_ALL_BUT_LAST_N_REVISIONS_SERVICE`.
 - f. In the Action Service Parameters field, type `NumberOfRevisions=3`.
 - g. Click **Require Approval** and **Allow Scheduling**.
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 accommodate 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.

The following topics regarding barcodes are discussed:

- [Section C.2.1, "Adding a Custom Barcode Range"](#)
- [Section C.2.2, "Processing Non-Standard Barcode Data"](#)

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](#) opens.

2. Click **Add**.

The [Create Custom Barcode Dialog](#) opens.

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](#) opens 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 knowledge 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 YYYYMMYYHHMSS 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 Transaction 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 be in 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 Object 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 that 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 is 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 WebCenter Content Administrator's Guide for Records* 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 opens. After logging in, a Direct Scan window opens on the device.
3. Scan items and click the **Process** icon.
4. A Results screen opens, 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 transactions 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 the Records system. 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 Content Server Adapter systems is not included in the report even if the content is managed by the Records system. To generate reports concerning Adapter content, run the reports on the Content Server Adapter system.

This section describes how to create customized reports using Oracle WebCenter Content services and queries. To create reports about users and content using the default reports provided with the software, see the *Oracle WebCenter Content Administrator's Guide for Records*.

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** and choose a report option:

- **Create New Report:** Used to start the process of creating a new report. This option opens a checkin page, used to save the report name and save other detailed report information.

- **Report Sources:** Opens the [Configure Report Sources Page](#), used to choose the criteria to gather data for the report.
- **Templates:** Opens a search results page listing templates for reports.
- **Download BI XML Data:** Opens a dialog where a user can choose to open the XML data used for the reports or save the data.

The [Configure Report Element Page](#) opens.

2. Choose the type of report to create and click **Configure**.

A [Report Checkin Page](#) opens.

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 list or click **Add New** to create a new template. For details about creating a new template, [Section C.4.1, "Creating Custom Templates."](#)
- **Report Format:** Choose a format from the 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 WebCenter Content services to build the report data.
 - **Query:** Use Oracle WebCenter Content 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](#). For details, see [Section C.4.2, "Creating or Editing New Report Sources."](#)

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](#) opens.

2. Choose the type of template you wish to create. Click **Configure**.
A [Report Templates Page](#) opens.
3. The following options are available:
 - To create a new template based on an existing template, click **Get Native File** from the **Actions** 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 **Actions** 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 **Actions** menu of the template with metadata to be copied.

The Table menu on this page is used to perform actions for all template files or for selected files. The options shown depend on the configuration of the system and 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.

Additional options on this page are 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](#) opens.

2. Choose the report whose sources will be altered. Click **Configure**.

The [Configure Report Sources Page](#) opens.

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 are 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](#) opens.

2. Choose the type of XML data file to download. Click **Download**.

The [XML Data Dialog](#) opens.

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. 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 WebCenter Content: Records. Oracle WebCenter Content: Records can 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 WebCenter Content: Records.

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 the term **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

- Access Control List Edit Screen, A-15
- Access Control Lists, 3-12
- access control lists (ACLs), 5-17
- Accession Deletion (disposition action), 14-7
- ACL, 3-12
- ACLs, 5-18
- Activate (disposition action), 14-7
- Activated trigger, 14-4
- Adapter
 - as-needed synchronization, 16-10
 - configuration, 16-4
 - configure providers, 16-5
 - configure sources, 16-5
 - data synchronization, 16-9
 - define outgoing provider, 16-5
 - deleting outgoing provider, 16-6
 - disabling outgoing provider, 16-6
 - editing outgoing provider, 16-6
 - managing fields, 16-8
 - registering external source, 16-7
 - schedule synchronization, 16-10
 - synchronization logs, 16-10
 - unregistering external source, 16-7
 - viewing external URM source configuration settings, 16-8
 - viewing outgoing provider configuration settings, 16-8
- adapter
 - communications, 16-3
 - configuration, 16-3
 - logging, 16-4
 - query function, 16-3
 - registration, 16-3
 - repository monitoring, 16-3
 - retention functions, 16-2
 - role with URM, 16-2
 - tasks
 - disposition holds, 16-3
 - disposition of content, 16-4
 - repository searching, 16-3
 - with URM, 16-2
- Add/Edit New Provider Page, A-66
- Admin rights
 - AllowDispositionUpgrade/Downgrade, 5-23
 - Audit, 5-23
 - Classification Guide, 5-23
 - ClassificationGuide, 5-24
 - ConfigureLinks, 5-23
 - CustomDispositionActions, 5-24
 - GetAllFilePlan, 5-24
 - NoRmaSecurity, 5-24
 - PerformActions, 5-23
 - PerformPendingReviews, 5-22
 - PrivilegedEnvironment, 5-22
 - RecordManager, 5-23
 - Reports, 5-23
 - RetentionScheduleArchive, 5-23
 - Screening, 5-23
 - SecurityClassifications, 5-24
 - SelectAuthor, 5-23
 - SelectMeta, 5-23
 - ShareFavorites, 5-23
 - Triggers, 5-23
- admin rights, 5-22
- Admin Tab, 5-22
- Administer Classification Topic Page, A-22
- Admin.Location.Types right, 5-25
- Admin.Manager right, 5-25
- Admin.PrintLabel right, 5-25
- aliases, 5-17
- AllowDispositionUpgrade/Downgrade right, 5-23
- allowing storage of content, A-28
- Approve Deletion (disposition action), 14-7
- Archive (disposition action), 14-8
- archives
 - rights required for, 5-9
- Assigned Rights Page, A-14
- attribute inheritance, 10-7
 - disposition instructions, 10-8
 - frozen content status, 10-9
 - frozen folder status, 10-9
 - permanent status, 10-8
 - review status, 10-7
- Audit Approval indirect trigger, 11-7
- Audit Approval trigger, 14-5
- Audit right, 5-23
- audit trail
 - rights required for, 5-9
- authentication
 - LDAP, 3-4

AutoStorageNumberWidth parameter, 9-10
Available (storage object status), 9-6

B

barcode
 data files, C-7
 editing data files, C-7
barcode labels
 storage locations, A-31
barcode values for users, 5-25
Barcode.Process right, 5-25
basic concepts, 2-4
 retention schedules, 2-5
basic processes, 2-7
batch services, A-14
Bay, 8-3, 9-2
blocking storage locations, 9-2

C

calendar periods, 12-2
canceling
 trigger, 14-4
canceling the reservation of storage locations, 9-12
categories
 creating, 10-15
 definition, 2-5
 deleting, 10-18
 moving, 10-17
 rights required for, 5-8
 setting up, 10-14
 viewing information about, 10-16
 viewing metadata history of, 10-17
category disposition workflow, 7-5
 creation, 7-7
Category rights
 Create, 5-21
 Delete, 5-21
 Edit, 5-21
 EditReview, 5-21
 Move, 5-21
category rules
 workflow review, 14-3
Category Tab, 5-21
CBC Tab, 5-24
ChargeBacks.Adjust right, 5-24
ChargeBacks.Admin right, 5-24
Chargebacks.Create right, 5-24
ChargeBacks.Delete right, 5-24
ChargeBacks.Edit right, 5-24
ChargeBacks.MarkPaid right, 5-24
ChargeBacks.PrintInvoices right, 5-24
Chargebacks.Read right, 5-24
Checkin New Revision (disposition action), 14-7
checking in internal content item, A-13
checkout period, A-13
classification
 definition, 2-5
classification guide

 definition, 2-6
Classification Guide right, 5-23
classification guides, 6-16
 creating, 6-17
 deleting, 6-18
 overview, 6-16
 rights required for, 5-6
 setting up, 6-16
 viewing information about, 6-18
classification levels, 6-2
 Confidential, 6-3
 Secret, 6-3
 security hierarchy, 6-3
 Top Secret, 6-2
classification markings, see security
 classifications, 6-1
classification topics
 creating, 6-18
 deleting, 6-20
 editing settings, 6-19
 viewing information about, 6-20
ClassificationGuide right, 5-24
classified content, 2-3
classified levels
 security hierarchy, 6-3
classified records, 6-1
classified security
 enabling, 6-4
Close (disposition action), 14-8
completed reservation requests, A-13
Confidential classification level, 6-3
configuration
 assigning rights to user roles, 5-20
 barcode values for users, 5-25
 categories, 10-14
 custom direct triggers, 11-9
 custom security fields, 6-9
 default metadata values, 8-12
 DIS, 7-10
 fiscal calendar, 7-3
 folders, 10-19
 location types, 8-3
 management settings, 7-1, 11-1
 media types, 8-10
 modifying reservations, A-13
 object types, 8-7
 periods, 12-1
 retention schedules, C-6
 security preferences, 5-19
 series, 10-11
 system-wide, 3-12
 triggers, 11-1
configuration settings
 batch services, A-14
 default checkout period, A-13
 default request priority, A-13
 delete completed requests, A-13
 deleting reservations, A-13
 internal content item for reservation
 workflow, A-13

- offsite functionality, A-14
- request history period, A-13
- updating request waiting list, A-13
- configuration variables
 - NumberOfStorageTypeRootsToShow, 9-1
- Configure Classification Guide Page, A-21
- Configure Custom Security Page, A-18
- Configure Dispositions Page, A-58
- Configure Location Types Page, A-26
- Configure Media Type Page, A-37
- Configure Object Types Page, A-35
- Configure Periods Page, A-52
- Configure Physical Settings Page, A-12
- Configure Report Element Page, A-72
- Configure Report Sources Page, A-74
- Configure Reports Settings Page, A-71
- Configure Retention Settings Page, A-7
- Configure Scheduled Events Page, A-69
- Configure Security Classification Page, A-16
- Configure Supplemental Markings Page, A-25
- Configure Topic Settings Page, A-23
- Configure Triggers Page, A-48
- ConfigureLinks right, 5-23
- Configuring Custom Barcode Page, A-31
- configuring dispositions
 - overview, 3-15
- configuring management settings, 7-1, 11-1
- configuring triggers
 - overview, 3-15
- content
 - classified, 2-3
 - declassified, 2-3
 - external, 2-3
 - internal, 2-3
 - life cycle, 2-2
 - overview, 2-1
 - unclassified, 2-3
- content items
 - searching for frozen, 15-5
 - subject to review, 2-4
- Content Items Allowed option, A-28
- content link
 - definition, 2-5
- content state, 11-2
- copying retention category, 10-17
- Create Content Server Archive (disposition action), 14-8
- Create Custom Barcode Dialog, A-32
- Create Storage Page, A-30
- Create Volume (disposition action), 14-8
- Create/Edit Batch Storage Import File Page, A-32
- Create/Edit Classification Guide Page, A-21
- Create/Edit Classification Topic Page, A-22
- Create/Edit Custom Security Field Page, A-18
- Create/Edit Disposition Action Page, A-58
- Create/Edit Freeze Page, A-60
- Create/Edit Indirect Trigger Date Entries Page, A-51
- Create/Edit Location Type Page, A-27
- Create/Edit Media Type Page, A-37
- Create/Edit Metadata Field Page, A-55, A-56
- Create/Edit Object Type Page, A-35
- Create/Edit Period Page, A-52
- Create/Edit Records Folder Page, A-44
- Create/Edit Retention Category Page, A-42
- Create/Edit Security Classification Page, A-17
- Create/Edit Series Page, A-39
- Create/Edit Supplemental Marking Page, A-25
- Create/Edit Trigger Type Page, A-48
- creating
 - calendar periods, 12-2
 - categories, 10-15
 - classification guides, 6-17
 - classification topics, 6-18
 - custom category metadata fields, 13-2
 - custom folder metadata fields, 13-2
 - custom security fields, 6-11, 6-12
 - dispositions rules, 14-10
 - folders, 10-20, 10-21
 - location type, 8-4
 - media types, 8-11
 - object types, 8-8
 - security classifications, 6-4
 - series, 10-11
 - storage locations (batch), 9-8
 - storage locations (single), 9-7
 - supplemental markings, 6-23
 - triggers, 11-4
- creating custom barcodes, C-7
- custom barcodes, C-6, C-7
- custom category metadata fields
 - creating, 13-2
- custom direct triggers
 - examples, 11-9
 - overview, 11-3
 - setting up, 11-9
- custom disposition actions
 - creating, C-2
 - deleting, C-5
- custom dispositions
 - creating, C-2
 - deleting, C-4
 - editing, C-4
 - viewing information about, C-4
- custom folder metadata fields
 - creating, 13-2
- custom metadata field
 - mapping, 16-8
- custom metadata fields
 - creating, 13-2
 - deleting, 13-3
- custom periods
 - deleting, 12-4
 - examples, 12-4
- custom report sources
 - editing, C-12
- custom report templates
 - creating, C-11
- custom reports, C-10
- sources, C-12
- templates, C-11

- XML data files, C-13
- custom security fields, 6-9
 - creating, 6-11, 6-12
 - deleting, 6-13
 - enabling, 6-10
 - examples, 6-14
 - overview, 6-9
 - setting up, 6-9
 - viewing information about, 6-13
- custom supplemental markings, 6-9
- custom triggers, 11-3
- CustomDispositionActions right, 5-24
- customization
 - location type icons, 8-4
- cutoff, 2-3, 14-8
- Cutoff (disposition action), 14-8
- Cutoff and Create Volume, 14-8

D

- date entries for indirect triggers, 11-7, 11-8
- declassification time frame, 6-7
- declassified content, 2-3
- Declassified Date trigger, 14-5
- declassified records, 6-1
- Declassify (disposition action), 14-6
- default alias lists, 5-17
- Default Checkout Period setting, A-13
- Default Metadata for Checked-in Reservation Entries Page, A-28
- default metadata values, 8-12
- Default Request Priority setting, A-13
- defaults
 - checkout period, A-13
 - location types, 8-3
 - media types, 8-10
 - metadata for reservations, 8-12
 - object types, 8-7
 - request history period, A-13
 - request priority, A-13
- defining
 - date entries for indirect triggers, 11-7
- definition
 - classification, 2-5
 - classification guide, 2-6
 - content link, 2-5
 - disposition, 2-5
 - disposition instruction, 2-5
 - freeze, 2-6
 - record folder, 2-5
 - retention category, 2-5
 - series, 2-5
 - time period, 2-5
 - trigger, 2-5
- Delete All Revisions (disposition action), 14-7
- Delete Approved trigger, 14-4
- Delete Old Revisions (disposition action), 14-7
- Delete Previous Revision (disposition action), 14-6
- Delete Revision (disposition action), 14-7
- DeleteHistoryFile right, 5-22

- deleting
 - categories, 10-18
 - classification guides, 6-18
 - classification topics, 6-20
 - custom metadata fields, 13-3
 - custom security fields, 6-13
 - date entries for indirect triggers, 11-8
 - dispositions rules, 14-14
 - folders, 10-24
 - location type, 8-6
 - media types, 8-12
 - object types, 8-9
 - periods, 12-4
 - security classifications, 6-6
 - series, 10-13
 - storage location, 9-11
 - supplemental markings, 6-25
 - triggers, 11-7
- Desktop Integration Suite
 - configuration issues, 7-10
- disabling indirect trigger period, 11-8
- disposition
 - definition, 2-5
 - editing for specific item, 10-23
 - event-based, 2-7
 - time-based, 2-7
 - time-event, 2-7
- Disposition Action Info Page, A-59
- disposition actions
 - Accession, 14-7
 - Activate, 14-7
 - Approve Deletion, 14-7
 - Archive, 14-8
 - Checkin New Revision, 14-7
 - Close, 14-8
 - Create Content Server Archive, 14-8
 - Create Volume, 14-8
 - creating, C-2
 - Cutoff, 14-8
 - Cutoff and Create Volume, 14-8
 - Declassify, 14-6
 - Delete All Revisions, 14-7
 - Delete Old Revisions, 14-7
 - Delete Previous Revision, 14-6
 - Delete Revision, 14-7
 - deleting, C-5
 - Downgrade Classification, 14-6
 - Expire, 14-8
 - Mark Related Content, 14-8
 - Move, 14-8
 - No Action, 14-8
 - Notify Authors, 14-8
 - Obsolete, 14-8
 - Review Classification, 14-6
 - Supersede, 14-8
 - Transfer, 14-8
 - Upgrade Classification, 14-6
- Disposition Actions Configuration Page, A-60
- Disposition Information Page, A-65
- disposition instruction

- definition, 2-5
- disposition instructions, 14-1
- Disposition Instructions Page, A-62
- Disposition Rule screen, A-63
- disposition rules, C-6
 - copying, 14-13
 - creating, 14-10
 - deleting, 14-14
 - inheritance, 10-8
 - rights required for, 5-10
- disposition types
 - overview, 3-16
- dispositions
 - cutoffs, 14-8
 - event, 14-2
 - precedence, 14-9
 - retention periods, 14-8
 - time, 14-2
 - time-event, 14-3
 - user-friendly captions, 14-10
 - viewing information about, 14-13
- documentation, 1-4
- Downgrade Classification (disposition action), 14-6
- dyanmic hold, 15-1

E

- ECM Tab, 5-25
- Edit Object Type Relationships Page, A-36
- Edit RMA Rights screen, A-15
- EditIfAuthor right, 5-21
- editing
 - classification topic settings, 6-19
 - folders, 10-22
 - media types, 8-11
 - object types, 8-8
 - storage locations, 9-10
- editing folder disposition, 10-23
- editing location types, 8-5
- e-mail notification for freezes, 15-6
- Enabled Features Page, A-2
- enabling
 - classified security, 6-4
 - custom security fields, 6-10
 - supplemental markings, 6-23
 - user-friendly caption in dispositions, 14-10
- ERM Admin and ERM Requestor rights
 - External.Create, 5-25
 - External.Edit, 5-25
 - External.Read, 5-25
- ERM Admin rights
 - External.Admin, 5-25
 - External.Delete, 5-25
- event dispositions, 2-7, 14-2
- examples
 - custom direct triggers, 11-9
 - custom periods, 12-4
 - custom security fields, 6-14
 - dispositions, 14-14
- Expire (disposition action), 14-8

- Expired trigger, 14-4
- Exploring Retention Schedule Page, A-38
- external authentication provider, 3-4
- external content, 2-3
- external items, 2-6
- external source
 - registering, 16-7
 - unregistering, 16-7
- external URM source
 - viewing configuration settings, 16-8
- External.Admin right, 5-25
- External.Create right, 5-25
- External.Delete right, 5-25
- External.Edit right, 5-25
- External.Read right, 5-25

F

- features of Physical Content Management, 2-6
- Fields for Metadata Page, A-55
- file plans, 10-2
 - and retention schedules, 10-2
 - enabling, 10-2
- filing date, 2-3
- fiscal calendar, 7-3
- Folder rights
 - Create, 5-21
 - Delete, 5-22
 - Edit, 5-22
 - EditIfAuthor, 5-21
 - EditReview, 5-21
 - Freeze/Unfreeze, 5-22
 - Move, 5-21
 - Open/Close, 5-21
 - Read, 5-21
 - UndoCutoff, 5-22
- folder state, 11-2
- Folder Tab, 5-21
- folders
 - creating, 10-20, 10-21
 - definition, 2-5
 - deleting, 10-24
 - disposition inheritance, 10-1
 - editing, 10-22
 - examples, 10-24
 - moving, 10-23
 - overview, 10-19
 - rights, 5-21
 - rights required for, 5-8
 - setting up-, 10-19
- Folders Retention overview, 10-3
- Formerly Restricted Data supplemental marking, 6-27
- freeze, 15-1
 - definition, 2-6
- Freeze Configuration Page, A-60
- Freeze Information Page, A-62
- freezes
 - creating, 15-1
 - deleting, 15-4

- e-mail notification, 15-6
- searching for frozen items, 15-5
- unfreezing, 15-4, 15-5
- viewing information about, 15-3
- freezing
 - folios, 15-4
- freezing items, 15-4
- Frozen Content Page, A-62
- Frozen Item Page, A-62
- frozen items, 15-5

G

- GetAllFilePlan right, 5-24
- glossary, Glossary-1

H

- hiding
 - series, 10-12
- hierarchy
 - classification levels, 6-3
 - retention schedule plan, 10-4

I

- icons
 - customization, 8-4
 - location types, 8-3, 8-4, 9-5
- image of location type, A-28
- Indirect Trigger Date Entries Page, A-50
- indirect triggers
 - date entries, 11-7, 11-8
 - defining date entries, 11-7
 - deleting date entries, 11-8
 - disabling trigger period, 11-8
 - overview, 11-3
 - setting up Audit Approval trigger, 11-7
- information
 - categories, 10-16
 - classification guides, 6-18
 - classification topics, 6-20
 - custom security fields, 6-13
 - dispositions, 14-13
 - items in storage locations, 9-12
 - periods, 12-3
 - series, 10-12
 - storage locations, 9-10
 - supplemental markings, 6-24
 - triggers, 11-6
- inheritance of attributes, 10-7
 - disposition instructions, 10-8
 - frozen content status, 10-9
 - frozen folder status, 10-9
 - permanent status, 10-8
 - review status, 10-7
- interface
 - Access Control Edit Section, A-15
 - Add/Edit New Provider Page, A-66
 - Administer Classification Topic Page, A-22
 - Assigned Rights Page, A-14

- Configure Classification Guide, A-21
- Configure Custom Security Page, A-18
- Configure Dispositions Page, A-58
- Configure Location Types Page, A-26
- Configure Media Type Page, A-37
- Configure Object Types Page, A-35
- Configure Periods Page, A-52
- Configure Physical Settings Page, A-12
- Configure Report Element Page, A-72
- Configure Report Sources Page, A-74
- Configure Reports Settings Page, A-71
- Configure Retention Settings Page, A-7
- Configure Scheduled Events Page, A-69
- Configure Security Classification Page, A-16
- Configure Supplemental Markings Page, A-25
- Configure Topic Settings Page, A-23
- Configure Triggers Page, A-48
- Configuring Custom Barcode Page, A-31
- Create Custom Barcode Dialog, A-32
- Create Object Type Page, A-35
- Create Storage Page, A-30
- Create/Edit Batch Storage Import File Page, A-32
- Create/Edit Classification Guide Page, A-21
- Create/Edit Classification Topic Page, A-22
- Create/Edit Custom Security Field Page, A-18
- Create/Edit Disposition Action Page, A-58
- Create/Edit Freeze Page, A-60
- Create/Edit Indirect Trigger Date Entries Page, A-51
- Create/Edit Location Type Page, A-27
- Create/Edit Media Type Page, A-37
- Create/Edit Metadata Field Page, A-55, A-56
- Create/Edit Period Page, A-52
- Create/Edit Records Folder Page, A-44
- Create/Edit Retention Category Page, A-42
- Create/Edit Security Classification Page, A-17
- Create/Edit Series Page, A-39
- Create/Edit Supplemental Marking Page, A-25
- Create/Edit Trigger Type Page, A-48
- Default Metadata for Checked-in Reservation Entries Page, A-28
- Disposition Action Info Page, A-59
- Disposition Actions Configuration Page, A-60
- Disposition Information Page, A-65
- Disposition Instructions page, A-62
- Disposition Rule screen, A-63
- Edit Object Type Relationships Page, A-36
- Edit RMA Rights screen, A-15
- Enabled Features Page, A-2
- Exploring Retention Schedule Page, A-38
- Fields for Metadata Page, A-55
- Freeze Configuration Page, A-60
- Freeze Information Page, A-62
- Frozen Item Page, A-62
- Indirect Trigger Date Entries Page, A-50
- Map Custom Fields Page, A-68
- Map/Edit Custom Field Dialog, A-69
- Metadata History Page (categories), A-44
- Metadata Information Page, A-58
- Metadata List Page, A-54

- Period Information Page, A-53
- Period Reference Page, A-53
- Physical Items Pages, A-34
- Provider Information Page, A-68
- Provider List Page, A-67
- Records Folder Information Page, A-46
- Register Source Page, A-65
- Retention Category Information Page, A-43
- Select Media Type Page, A-38
- Select Retention Series screen, A-41
- Select Storage Location dialog, A-33
- Series Information Page, A-40
- Setup Checklist Page, A-3
- Source Configuration Information Page, A-68
- Synchronization Log Page, A-70
- Trigger Information Page, A-49
- XML Data Dialog, A-75

internal content, 2-3

L

- labels
 - storage locations, 9-13
- Last New Record Added trigger, 14-5
- layouts supported, 2-6
- layouts supported in product, 2-6
- LDAP, 3-4
- lifecycle of retained content, 2-2
- links
 - rights required for, 5-10
- location types, 9-5
 - allowing storage of content, A-28
 - configuration, 8-3
 - creating --, 8-4
 - customization of icons, 8-4
 - deleting --, 8-6
 - example, 8-6
 - icons, 8-3, 8-4
 - image, A-28
 - predefined --, 8-3
 - reordering --, 8-6
 - viewing information about --, 8-5

M

- Map Custom Fields Page, A-68
- Map/Edit Custom Field Dialog, A-69
- mapped metadata field
 - editing, 16-9
- Maximum Items Allows option, A-31
- media types
 - configuration, 8-10
 - creating --, 8-11
 - deleting --, 8-12
 - editing --, 8-11
 - overview, 8-10
 - predefined --, 8-10
 - viewing information about --, 8-11
- metadata
 - default values for --, 8-12

- metadata field information, 13-3
- metadata for reservations, 8-12
- metadata history
 - categories, 10-17
- Metadata History Page
 - categories, A-44
- Metadata Information Page, A-58
- Metadata List Page, A-54
- mobile bar code reader, C-9
- Move (disposition action), 14-8
- moving
 - categories, 10-17
 - folders, 10-23
 - series, 10-13

N

- names of batch-created --, 9-10
- names of batch-created storage locations, 9-10
- navigating retention schedule, 10-9
- new features, 1-2
- New Revision Date trigger field, 11-5
- No Action (disposition action), 14-8
- No Longer Latest Revision trigger, 14-5
- non-permanent item, 2-4
- NoPostFilterSearch right, 5-23
- NoRmaSecurity right, 5-24
- notification reviewer, A-64
- Notify Authors (disposition action), 14-8
- NumberOfStorageTypeRootsToShow parameter, 9-1

O

- object types
 - configuration, 8-7
 - creating --, 8-8
 - deleting --, 8-9
 - editing, 8-8
 - editing relationships between --, 8-9
 - overview, 8-7
 - predefined --, 8-7
 - viewing information about --, 8-8
- obsolete
 - and content items, 10-11
 - trigger, 14-4
- Obsolete (disposition action), 14-8
- Obsolete and Delete Approved trigger, 14-4
- Occupied (storage object status), 9-6
- offsite processing workflow, 7-5
- offsite storage workflow
 - creation, 7-9
- Oracle Fusion Middleware
 - using single sign-on, 3-5
 - using SSL, 3-4
 - using web services, 3-5
- Oracle Fusion Middleware application
 - using LDAP authentication provider, 3-4
- order
 - location types, 8-6
- order of security classifications, 6-5

- 'Other' storage location, 9-1
- outgoing provider
 - defining, 16-5
 - deleting, 16-6
 - disabling, 16-6
 - editing, 16-6
 - viewing configuration settings, 16-8
- overview, 2-4

P

PCM Admin and PCM Requestor rights

- Physical.Create, 5-24
- Physical.Edit, 5-24
- Physical.Read, 5-24
- Reservation.Create, 5-25
- Reservation.Edit, 5-25
- Reservation.Read, 5-25
- Storage.Read, 5-24
- Storage.Reserve, 5-24

PCM Admin rights

- Admin.Location.Types, 5-25
- Admin.Manager, 5-25
- Admin.PrintLabel, 5-25
- Barcode.Process, 5-25
- ChargeBacks.Adjust, 5-24
- ChargeBacks.Admin, 5-24
- ChargeBacks.Create, 5-24
- ChargeBacks.Delete, 5-24
- ChargeBacks.Edit, 5-24
- ChargeBacks.MarkPaid, 5-24
- ChargeBacks.PrintInvoices, 5-24
- ChargeBacks.Read, 5-24
- Physical.Delete, 5-25
- Physical.Move, 5-25
- Reservation.Delete, 5-25
- Reservation.Process, 5-25
- Storage.Block, 5-25
- Storage.Create, 5-25
- Storage.Delete, 5-25
- Storage.Edit, 5-25

PCM Tab, 5-24

PerformActions right, 5-23

PerformPendingReviews right, 5-22

Period Information Page, A-53

Period Reference Page, A-53

periods

- calendar, 12-2
- deleting, 12-4
- examples, 12-4
- setting up, 12-1
- viewing information about, 12-3
- viewing references to, 12-3

permanent items, 2-4

Physical Content Management

- features, 2-6
- overview, 2-6

Physical Content Manager

- barcode values for users, 5-25
- retention schedules, C-6

physical items

- in storage locations, 9-12

Physical Items Pages, A-34

Physical.Create right, 5-24

Physical.Delete right, 5-25

Physical.Edit right, 5-24

Physical.Move right, 5-25

Physical.Read right, 5-24

Position, 8-3, 9-2

precedence of disposition instructions, 14-9

Preceding Action trigger, 14-4

preceding disposition action, 11-2

printing labels

- storage locations, 9-13

priority of reservation requests, A-13

PrivilegedEnvironment right, 5-22

product

- documentation, 1-4

product overview, 2-4

product processes, 2-7

properties of storage objects, 9-4

Provider Information Page, A-68

Provider List Page, A-67

R

record folder

- overview, 3-14

Record rights

- Create, 5-22

- CreateLink, 5-22

- Delete, 5-22

- DeleteHistoryFile, 5-22

- Edit, 5-22

- EditReview, 5-22

- Freeze/Unfreeze, 5-22

- NoPostFilterSearch, 5-23

- Read, 5-22

- UndoCutoff, 5-22

- UndoRecord, 5-22

- Unlink, 5-22

- Upgrade/Downgrade, 5-22

Record tab, 5-22

RecordManager right, 5-23

records

- classified, 6-1

- declassified, 6-1

- unclassified, 6-1

records classification

- overview, 6-1

Records Folder Information Page, A-46

references

- periods, 12-3

- security classifications, 6-7

- triggers, 11-6

refining ACLs, 5-18

Register Source Page, A-65

relationships between object types, 8-9

reordering

- location types, 8-6

- Report Checkin Page, A-73
- Report Template Page, A-74
- reports
 - rights required for, 5-10
- Reports right, 5-23
- Request History Period setting, A-13
- request priority, A-13
- Rescinded trigger, 14-4
- resending freeze e-mail notification, 15-6
- reservation processing workflow, 7-5
 - creation, 7-7
- Reservation.Create right, 5-25
- Reservation.Delete right, 5-25
- Reservation.Edit right, 5-25
- Reservation.Process right, 5-25
- Reservation.Read right, 5-25
- reservations, A-13
 - default metadata for --, 8-12
 - delete completed requests, A-13
 - deleting --, A-13
 - modifying --, A-13
 - storage locations, 9-12
 - updating waiting list, A-13
- Reserved (storage object status), 9-6
- reserving storage locations, 9-12
- Restricted Data supplemental marking, 6-27
- retention categories, see categories, 10-1
- retention category
 - copy, 10-17
 - overview, 3-14
- Retention Category Information Page, A-43
- retention options, 3-7
- retention period
 - overview, 3-16
- retention period cutoff, 11-2
- Retention Period Cutoff trigger, 14-4
- retention periods, 14-5, 14-8
- retention schedule, 2-5
 - attribute inheritance, 10-7
 - hierarchy, 10-4
 - levels, 10-9
 - management, 3-14
 - menus, 10-9
 - navigation, 10-9
 - object characteristics, 10-5
 - planning, 10-4
 - review status attributes, 10-7
 - setup, 3-13
- retention schedule components
 - classification guides, 6-16
 - custom direct triggers, 11-9
 - periods, 12-1
 - security classifications, 6-1
 - triggers, 11-1
- retention schedules, C-6
- RetentionScheduleArchive right, 5-23
- Review Classification (disposition action), 14-6
- review status
 - inheritance, 10-8
- reviewing category rules, 14-3

- rights, 5-4
 - administration, 5-22
 - archives, 5-9
 - assigning to user roles, 5-20
 - audit trail, 5-9
 - categories, 5-8, 5-21
 - classification guides, 5-6
 - content management, 5-11
 - custom barcode actions, 5-12
 - custom dispositions, 5-12
 - custom reports, 5-12
 - disposition rules, 5-10
 - folders, 5-8
 - links, 5-10
 - reports, 5-10
 - required to perform tasks, 5-4
 - screening, 5-9
 - series, 5-7, 5-21
 - supplemental markings, 6-22
 - viewing assigned, 5-4
- RoleEntityACL, 10-2
- roles
 - assigning rights to, 5-20
 - ermadmin, 5-4
 - ermrequestor, 5-4
 - pcmadmin, 5-3
 - pcmrequestor, 5-3
 - predefined, 5-2
 - rma, 5-3
 - rmaadmin, 5-3
 - rmalocalrecordsofficer, 5-3
 - viewing assigned, 5-4
- Room, 8-3, 9-2
- Row, 8-3, 9-2

S

- Scheduled Declassify Date trigger, 14-5
- Scheduled Downgrade Date trigger, 14-5
- screening
 - rights required for, 5-9
- Screening right, 5-23
- search results
 - unfiltered, 5-23
- search templates, 2-6
- search templates supported in product, 2-6
- Secret classification level, 6-3
- security
 - access control lists (ACLs), 5-17
 - assigning rights to user roles, 5-20
 - rights, 5-4
 - setting preferences, 5-19
- security classifications, 6-1
 - assigning to users, 6-8
 - creating, 6-4
 - deleting, 6-6
 - removing from users, 6-9
 - setting declassification time frame, 6-7
 - setting order of, 6-5
 - setting up, 6-1

- viewing references to, 6-7
- security fields
 - setting up custom, 6-9
- security group
 - defined, 5-16
- security groups, 3-12
- security matrix, 5-18
- security rights, 3-12
- security rights and roles, 3-12
- security roles, 3-11
 - PCM Administrator, 3-12
 - PCM Requestor, 3-12
 - pcmadmin, 3-12
 - pcmrequestor, 3-12
 - Records Administrator, 3-11
 - Records Officer, 3-11
 - Records User, 3-11
 - rma, 3-11
 - rmaadmin, 3-11
 - rmalocalrecordofficer, 3-11
- SecurityClassifications right, 5-24
- Select Media Type Page, A-38
- Select Retention Series screen, A-41
- Select Storage Location dialog, A-33
- SelectAuthor right, 5-23
- SelectMeta right, 5-23
- series
 - categories, 5-21
 - creating, 10-11
 - definition, 2-5
 - deleting, 10-13
 - hiding, 10-12
 - moving, 10-13
 - rights, 5-21
 - rights required for, 5-7
 - setting up, 10-11
 - uses, 10-11
 - viewing information about, 10-12
- series creation
 - overview, 3-14
- Series Information Page, A-40
- Series rights
 - Create, 5-21
 - Delete, 5-21
 - Edit, 5-21
 - Move, 5-21
 - Read, 5-21
- Series Tab, 5-21
- setting ACLs, 5-18
- setting fiscal calendar, 7-3
- setting security preferences, 5-19
- setting up classification guides, 6-16
- setting up custom direct triggers, 11-9
- setting up periods, 12-1
- setting up Physical Content Manager
 - default metadata values, 8-12
 - location types, 8-3
 - media types, 8-10
 - object types, 8-7
 - retention schedules, C-6
 - setting up security classifications, 6-1
 - setting up triggers, 11-1
 - settings, see 'configuration settings'
 - Setup Checklist Page, A-3
 - ShareFavorites right, 5-23
 - Shelf, 8-3, 9-2
 - single sign-on, 3-5
 - Source Configuration Information Page, A-68
 - space management, see 'storage space'
 - space, see 'storage space'
 - SSL, 3-4
 - SSO, 3-5
 - status of storage objects, 9-6
 - Available, 9-6
 - Occupied, 9-6
 - Reserved, 9-6
 - storage location labels, 9-13
 - storage locations, 9-10
 - allowing storage in --, A-28
 - barcode label, A-31
 - batch creation of --, 9-8
 - blocking --, 9-2, 9-11
 - canceling the reservation of --, 9-12
 - creating -- in batch, 9-8
 - creating single --, 9-7
 - deleting --, 9-11
 - editing --, 9-10
 - labels for --, 9-13
 - reserving --, 9-12
 - unblocking, 9-11
 - viewing information about --, 9-10
 - viewing physical items, 9-12
 - storage objects
 - location type, 9-5
 - properties, 9-4
 - storage status, 9-6
 - storage of content in location types, A-28
 - storage space
 - batch creation of --, 9-8
 - considerations, 9-1
 - Storage.Block right, 5-25
 - Storage.Create right, 5-25
 - Storage.Delete right, 5-25
 - Storage.Edit right, 5-25
 - Storage.Import.hda, 9-14, A-32
 - Storage.Read right, 5-24
 - Storage.Reserve right, 5-24
 - subject to review items, 2-4
 - Supersede (disposition action), 14-8
 - Superseded trigger, 14-5
 - Superseded Twice trigger, 14-5
 - supplemental markings, 6-21
 - assigning to users, 6-26
 - creating, 6-23
 - deleting, 6-25
 - enabling, 6-23
 - Formerly Restricted Data, 6-27
 - overview, 6-21
 - Restricted Data, 6-27
 - rights required for, 6-22

- viewing information about, 6-24
- Synchronization Log Page, A-70
- synchronizing data, 16-10
- system-derived triggers, 11-1
 - content state, 11-2
 - folder state, 11-2
 - item state, 11-2
 - preceding action, 11-2
 - retention period cutoff, 11-2

T

- time dispositions, 2-7, 14-2
- time period
 - definition, 2-5
- time-event dispositions, 2-7, 14-3
- Top Secret classification level, 6-2
- Transfer (disposition action), 14-8
- trigger
 - definition, 2-5
- Trigger Information Page, A-49
- triggering event
 - overview, 3-16
- triggering events, 14-4
 - Activated, 14-4
 - Audit Approval, 14-5
 - Canceled, 14-4
 - Declassified Date, 14-5
 - Delete Approved, 14-4
 - Expired, 14-4
 - Last New Record Added, 14-5
 - No Longer Latest Revision, 14-5
 - obsolete, 14-4
 - Obsolete and Delete Approved, 14-4
 - Preceding Action, 14-4
 - Rescinded, 14-4
 - Retention Period Cutoff, 14-4
 - Scheduled Declassify Date, 14-5
 - Scheduled Downgrade Date, 14-5
 - Superseded, 14-5
 - Superseded Twice, 14-5
- triggers
 - creating, 11-4
 - custom, 11-3
 - custom direct, 11-9
 - deleting, 11-7
 - examples, 11-9
 - setting up, 11-1
 - system-derived, 11-1
 - viewing information about, 11-6
 - viewing references to, 11-6
- Triggers right, 5-23
- types of content, 2-3

U

- unblocking storage locations, 9-11
- unclassified content, 2-3
- unclassified records, 6-1
- unfiltered search results, 5-23

- unfreezing
 - content, 15-5
- unregistering external source, 16-7
- Upgrade Classification (disposition action), 14-6
- user labels
 - barcode values for users, 5-25
- user-friendly captions
 - dispositions, 14-10

V

- variables
 - NumberOfStorageTypeRootsToShow, 9-1
 - see configuration variables, 7-10
- viewing information
 - categories, 10-16
 - classification guides, 6-18
 - classification topics, 6-20
 - custom security fields, 6-13
 - dispositions, 14-13
 - items in storage location, 9-12
 - location types, 8-5
 - media types, 8-11
 - object types, 8-8, 8-9
 - periods, 12-3
 - series, 10-12
 - storage locations, 9-10
 - supplemental markings, 6-24
 - triggers, 11-6
- viewing metadata history
 - categories, 10-17
- viewing rights, 5-4
- viewing roles, 5-4

W

- waiting list for reservations, A-13
- Warehouse, 8-3, 9-2
- web services, 3-5
- WNA deployment, 3-3
- workflow
 - category disposition, 7-5
 - offsite processing, 7-5
 - prerequisites, 7-6
 - process, 7-6
 - reservation processing, 7-5
- workflow for reservations, A-13
- workflows
 - needed for URM, 7-4
 - setting up, 7-4

X

- XML Data Dialog, A-75

