

Oracle® WebCenter Content

Application Administrator's Guide for Content Server

11g Release 1 (11.1.1)

E10978-02

November 2011

This guide describes how to administer applications and components to extend Oracle WebCenter Content Server functionality including how to create custom metadata fields, schemas, and profiles, how to configure workflows and PDF watermarks, how to configure alternative folio, folders, and WebDAV interfaces, and how to configure Content Tracker and Content Categorizer components.

Oracle WebCenter Content Application Administrator's Guide for Content Server, 11g Release 1 (11.1.1)

E10978-02

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

Primary Author: Robert Lies

Contributor: Sandra Christiansen, Karen Johnson, Jean Wilson

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 licensed through X/Open Company, Ltd.

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	xix
Audience	xix
Documentation Accessibility	xix
Related Documents	xix
Conventions	xx
1 Introduction	
1.1 About This Guide	1-1
1.2 What's New	1-2
1.2.1 Release 11g (11.1.1.6.0)	1-2
1.2.2 Release 11g (11.1.1)	1-2
1.3 Administration Applications	1-3
1.3.1 User Types	1-3
1.3.2 Accessing Administration Applications	1-3
1.3.3 Running Administration Applications as Applets	1-4
1.3.4 Running Administration Applications in Standalone Mode	1-4
1.3.4.1 On Windows Systems	1-5
1.3.4.2 On UNIX Systems	1-5
2 Managing Repository Content	
2.1 Content Types	2-1
2.1.1 Managing Content Types	2-2
2.2 Custom Fields	2-2
2.2.1 About Custom Fields	2-2
2.2.1.1 Application Fields	2-3
2.2.1.2 Custom Metadata Fields	2-3
2.2.1.3 Standard Metadata Fields	2-3
2.2.2 Adding or Editing a Custom Field	2-5
2.2.3 Rebuilding the Database or the Search Index	2-6
2.2.4 Defining an Option List	2-7
2.2.4.1 Defining Option List Storage	2-8
2.2.4.2 Adding or Editing Option List Content	2-8
2.2.4.3 Editing View Values	2-8
2.2.4.4 Using Tree Values	2-9
2.3 Native Content Conversion	2-9

2.3.1	Identifying MIME Types	2-10
2.3.2	Native Applications and Content Conversions	2-10
2.3.3	Associating File Types with Conversion Programs.....	2-10
2.3.4	Thumbnails.....	2-11
2.4	Managing Content and Revisions	2-12
2.4.1	Managing the Content List.....	2-12
2.4.1.1	Changing Column and Filter Settings	2-12
2.4.1.2	Changing Default Sort Order.....	2-13
2.4.2	Managing Content.....	2-13
2.4.2.1	Adding a New Content Item	2-13
2.4.2.2	Managing Content Metadata with Repository Manager.....	2-14
2.4.2.3	Managing Expired Content with Repository Manager.....	2-14
2.4.3	Managing Revisions	2-15
2.4.3.1	Check In and Checkout a Revision	2-15
2.4.3.2	Undo a Checkout or Resubmit a Revision.....	2-16
2.4.3.3	Deleting Revisions.....	2-16
2.4.3.4	Managing Workflow Revisions.....	2-16
2.5	Signing Content Electronically.....	2-17
2.5.1	About Electronic Signatures.....	2-17
2.5.2	Custom Electronic Signature Metadata.....	2-18
2.5.3	Adding or Editing a Custom Electronic Signature Field	2-18
2.6	Subscribing to Content.....	2-19
2.6.1	Using Subscriptions.....	2-20
2.6.1.1	Adding or Editing a Criteria Subscription.....	2-20
2.6.1.2	Adding or Unsubscribing Users.....	2-21
2.6.1.3	Viewing Subscription Information	2-21
2.6.1.4	Deleting a Criteria Subscription	2-22
2.7	Managing Linked Content with Link Manager	2-22
2.7.1	The Link Extraction Process.....	2-23
2.7.1.1	File Formats and Conversion.....	2-24
2.7.1.2	Link Status	2-24
2.7.2	Configuring Link Manager.....	2-25
2.7.2.1	Link Patterns	2-25
2.7.2.2	Database Tables	2-26
2.7.2.3	Link Manager Filters.....	2-27
2.7.3	Site Studio Integration	2-28
2.7.4	Link Administration.....	2-29
2.7.4.1	Alternative Refresh Methods.....	2-29
2.7.4.2	Recomputing and Refreshing Links in the ManagedLinks Table.....	2-29

3 Managing Schemas and Profiles

3.1	Using Schemas to Customize Metadata	3-1
3.1.1	Schema Structure	3-1
3.1.1.1	Tables.....	3-2
3.1.1.2	Views	3-3
3.1.1.3	Relationships	3-4
3.1.1.4	Schema Directory Structure	3-4

3.1.1.5	Sample Schema-Based Lists	3-5
3.1.2	Creating Schemas.....	3-5
3.1.2.1	Selecting Tables for the Schema	3-6
3.1.2.2	Creating the Schema View	3-6
3.1.2.3	Creating the Schema Relationships	3-6
3.1.2.4	Adding Metadata Fields	3-7
3.1.2.5	Enabling the Schema	3-7
3.1.2.6	Modifying the Publishing Cycle Interval.....	3-7
3.1.3	Schema Example: Dynamic Lists.....	3-8
3.1.4	Schema Example: Recursive Table for Multiple Trees	3-9
3.2	Using Profiles to Customize Content Screens	3-11
3.2.1	Content Profile Elements	3-11
3.2.1.1	Using a Profile Link.....	3-12
3.2.2	Content Profile Rules	3-12
3.2.2.1	Metadata Fields and Attributes in Rules.....	3-13
3.2.2.2	Activation Conditions in Rules	3-13
3.2.2.3	Restricted Lists in Rules.....	3-14
3.2.2.4	Regular Expressions	3-14
3.2.2.5	Using Rules to Group Metadata Fields	3-17
3.2.3	Display Results of Reordered Metadata Fields	3-20
3.2.3.1	General Sequence of Grouped Metadata Fields.....	3-20
3.2.3.2	Positioning Metadata Fields Within a Group.....	3-21
3.2.3.3	Display Results of Grouped Metadata Fields.....	3-22
3.2.3.4	Moving Fields.....	3-23
3.2.4	Managing Rules	3-23
3.2.4.1	Creating or Editing a Rule.....	3-24
3.2.4.2	Creating, Editing, or Deleting a Global Rule.....	3-24
3.2.4.3	Adding Metadata Fields in a Rule	3-24
3.2.4.4	Adding, Editing or Deleting Activation Conditions in Rules.....	3-27
3.2.4.5	Custom Conditions and Side Effects	3-28
3.2.4.6	Setting Default Values, Derived Values and Restricted Lists	3-29
3.2.4.7	Editing Default or Derived Values and Restricted Lists.....	3-30
3.2.4.8	Setting the Display of a Required Field.....	3-30
3.2.5	Content Profile Triggers	3-31
3.2.5.1	Selecting a Profile Trigger Field	3-31
3.2.5.2	Disabling a Profile Trigger Field	3-32
3.2.6	Creating and Using Content Profiles	3-32
3.2.6.1	Creating, Editing, or Deleting a Profile	3-32
3.2.6.2	Previewing a Profile	3-33
3.2.6.3	Troubleshooting a Profile	3-34
3.2.7	Content Profile Examples	3-35
3.2.7.1	Department-Based Content Profile.....	3-35
3.2.7.2	Black-Hole Resume Check In.....	3-39
3.2.7.3	Global Rule to Restrict Content Check-In Based on User Role.....	3-46
3.2.7.4	Global Rule Restricting Content Type Metadata Changes.....	3-47

4 Using Workflows

4.1	Introduction to Workflows	4-1
4.1.1	Workflow Steps	4-2
4.1.1.1	Events	4-4
4.1.1.2	Workflow Files	4-4
4.1.2	Workflow Step Evaluation Process	4-5
4.1.3	Workflow Participation	4-6
4.2	Planning a Workflow	4-6
4.2.1	Choosing a Workflow Type	4-7
4.2.1.1	Security Issues	4-8
4.2.2	Designing a Workflow	4-8
4.2.3	Modifying Workflows	4-9
4.3	Creating a Criteria Workflow	4-10
4.3.1	Criteria Workflow Process	4-10
4.3.1.1	Criteria Workflow Tips	4-12
4.3.2	Setting Up a Criteria Workflow	4-12
4.3.3	Changing a Criteria Workflow or Sub-workflow	4-15
4.3.4	Disabling a Criteria Workflow or Sub-workflow	4-15
4.4	Creating a Basic Workflow	4-16
4.4.1	Basic Workflow Process	4-16
4.4.2	Basic Workflow Tips	4-17
4.4.3	Setting Up a Basic Workflow	4-18
4.4.4	Changing a Basic Workflow	4-21
4.5	Customizing Workflows	4-22
4.5.1	Idoc Script Functions and Variables	4-22
4.5.2	Workflow Tokens	4-23
4.5.2.1	Token Syntax	4-24
4.5.2.2	Creating, Editing, or Deleting a Token	4-24
4.5.2.3	Token Examples	4-25
4.5.3	Workflow Jumps	4-26
4.5.3.1	Jumps and Events	4-26
4.5.3.1.1	Rejected Content	4-27
4.5.3.1.2	Side Effects	4-28
4.5.3.1.3	Jump Variables and Steps	4-28
4.5.3.2	Creating a Jump	4-29
4.5.3.2.1	Setting Up Jump Side Effects	4-30
4.5.3.2.2	Setting the Conditional Statement	4-30
4.5.3.2.3	Completing the Jump	4-30
4.5.3.2.4	Testing the Script	4-31
4.5.3.3	Changing a Jump	4-31
4.5.3.4	Jump Examples	4-32
4.5.3.5	Jump Errors	4-33
4.6	Workflow and Script Templates	4-33
4.6.1	Creating or Modifying a Workflow Template	4-33
4.6.2	Creating a Script Template	4-34
4.6.2.1	Setting Up Jump Side Effects	4-34
4.6.2.2	Setting Up Script Template Conditional Statements	4-35

4.6.2.3	Testing the Script	4-35
4.6.2.4	Changing a Script Template.....	4-35
4.6.2.5	Deleting a Script Template	4-36
4.7	Workflow Scenarios.....	4-36
4.7.1	Scenario 1: Criteria Workflow.....	4-36
4.7.2	Scenario 2: Tokens	4-37
4.7.3	Scenario 3: Jump Based on Metadata.....	4-37
4.7.4	Scenario 4: Time-Dependent Jump	4-38
4.8	Workflow Tips and Tricks	4-38
4.8.1	Requiring Step Authentication	4-38
4.8.2	Setting Up Parallel Workflows	4-39
4.8.3	Adding Ad Hoc Step Users	4-40
4.8.4	Customizing Criteria Workflow E-mails.....	4-40
4.8.4.1	Customizing E-mail Templates	4-41
4.8.4.2	Customizing the Subject or Message Line	4-41
4.8.4.2.1	Modifying Strings.....	4-41
4.8.4.2.2	Changing Idoc Variables	4-41
4.8.5	Workflow Escalation	4-42
4.8.5.1	Setting Up a Workflow Escalation	4-42
4.8.6	Other Customizations	4-45
4.8.6.1	Setting Approval by Non-Reviewers.....	4-45
4.8.6.1.1	Scenarios	4-45
4.8.6.2	Automatic Replication of Workflow Items.....	4-46
4.8.6.2.1	Potential Conflicts	4-46
4.8.6.2.2	Scenarios	4-47
4.8.7	Triggering Criteria Workflows from Folders	4-47
4.8.8	Searching Within a Workflow Step.....	4-48
4.8.9	Suppressing Workflow Notifications	4-48
4.9	Workflow Troubleshooting	4-49
4.9.1	Workflow Item Stuck in EDIT or GENWWW Status	4-49
4.9.2	Workflow Item Stuck in REVIEW Status	4-50
4.9.3	Workflow Item Entered in Wrong Workflow	4-51

5 PDF Watermark

5.1	PDF Watermark Overview	5-1
5.1.1	Static Watermarks.....	5-1
5.1.2	Dynamic Watermarks	5-2
5.1.3	Types of Watermark.....	5-2
5.1.4	Templates.....	5-2
5.1.4.1	Watermark Metadata Configuration	5-3
5.1.4.2	Template Security	5-3
5.1.4.3	Password Encryption.....	5-3
5.1.5	Dynamic Watermark Rules	5-4
5.1.6	PDF Optimization.....	5-4
5.1.7	Watermark Placement.....	5-4
5.2	Watermarking Scenarios.....	5-5
5.2.1	Static Watermarking Scenario.....	5-5

5.2.2	Dynamic Watermarking Scenario	5-6
5.3	Managing PDF Watermark.....	5-7
5.3.1	Specifying the Classpath for an Encryption Library	5-7
5.3.2	Starting PDF Watermark Administration	5-8
5.3.3	Setting Template Metadata Defaults.....	5-8
5.3.4	Adding or Editing Templates	5-8
5.3.4.1	Setting Security	5-9
5.3.4.2	Add or Edit a Text Watermark	5-9
5.3.4.3	Add or Edit an Image Watermark	5-10
5.3.4.4	Add or Edit an Electronic Signature Watermark.....	5-11
5.3.5	Creating and Editing Rules	5-12

6 Using Folders and WebDAV

6.1	Using Folders.....	6-2
6.1.1	The Folders Interface.....	6-2
6.1.2	Folders and Files	6-3
6.1.3	Shortcuts and Links	6-3
6.1.3.1	Folders and Shortcuts	6-3
6.1.3.2	Content Item Links	6-4
6.1.4	Query Folders and Folder Search.....	6-4
6.1.5	Folders Retention	6-5
6.1.6	Personal Folder	6-6
6.1.7	Security and User Access.....	6-6
6.1.8	Content Item Versioning	6-6
6.1.9	Folder and Content Item Metadata	6-6
6.1.9.1	Default Metadata	6-7
6.1.9.2	Metadata Propagation.....	6-7
6.1.9.3	Metadata Profiles.....	6-8
6.2	Managing Folders	6-8
6.2.1	Setting Configuration Variables	6-8
6.2.1.1	Folder Variables	6-8
6.2.1.2	Folders Migration Variables.....	6-9
6.2.1.3	Folders WebDAV Variables	6-10
6.2.2	Working with Retention Scheduling	6-10
6.2.2.1	Specify Retention Rules	6-10
6.2.2.2	Configure Retention Schedule	6-11
6.2.3	Migrating to the Folders Structure	6-12
6.3	Using Contribution Folders.....	6-13
6.3.1	Usage and Structure	6-13
6.3.2	Contribution Folders Component Security.....	6-14
6.3.3	Trash Bin	6-15
6.3.4	Metadata Propagation and Default Values.....	6-15
6.3.5	Latest Version versus Latest Released Version	6-16
6.3.6	Local Contribution Folders	6-16
6.3.7	Contribution Folder Archiving and Searching.....	6-17
6.3.8	Optimizing Performance	6-18
6.3.9	Metadata Inheritance.....	6-19

6.4	Managing Contribution Folders	6-20
6.4.1	Configuring Contribution Folders	6-20
6.4.1.1	Setting Folder and File Limits.....	6-20
6.4.1.2	Enabling and Disabling System Folders	6-20
6.4.1.3	Disabling the Trash Bin	6-21
6.4.1.4	Defining System Default Metadata.....	6-21
6.4.1.5	Configuring Metadata Propagation.....	6-21
6.4.1.6	Hiding Metadata Fields Globally Except for Specific Folders	6-21
6.4.2	Managing Local Folders	6-22
6.4.2.1	Specifying Local Folders.....	6-22
6.4.2.2	Rebuilding Local Folders.....	6-23
6.4.2.3	Removing Local Folders	6-23
6.4.3	Archiving Contribution Folders	6-23
6.4.3.1	Exporting an Archive.....	6-23
6.4.3.2	Importing an Archive.....	6-24
6.4.4	URL-Mapped Folders.....	6-24
6.5	WebDAV Interface.....	6-25
6.5.1	WebDAV Clients.....	6-25
6.5.2	WebDAV Architecture.....	6-26
6.5.3	WebDAV Folders.....	6-27
6.5.4	Multiple Concurrent Language Support.....	6-27
6.6	Administering WebDAV	6-28
6.6.1	WebDAV Connection Strings	6-28
6.6.2	Default Content Item Naming	6-28
6.6.3	Security and WebDAV.....	6-29
6.7	WebDAV Troubleshooting.....	6-29
6.7.1	Zero-Byte Files.....	6-30
6.7.1.1	Cause	6-30
6.7.1.2	Solution	6-30
6.7.2	No Connection to WebDAV Folder	6-30
6.7.2.1	Cause	6-30
6.7.2.2	Solution	6-30
6.7.3	Other Connection Issues.....	6-31
6.7.4	Double-Byte Characters in File Name	6-31
6.7.4.1	Cause	6-31
6.7.4.2	Solution	6-31
6.7.5	Number Sign in Virtual Folder Name or File Name	6-31
6.7.5.1	Cause	6-31
6.7.5.2	Solution	6-31
6.7.6	ExtranetLook Component Problem	6-31
6.7.6.1	Cause	6-31
6.7.6.2	Solution	6-32
6.7.7	Content Item "Stuck" in Auto-Contribution Workflow Step.....	6-32
6.7.7.1	Cause	6-32
6.7.7.2	Solution	6-32
6.7.8	Deleting Content From Contribution Folders for Site Studio Web Site	6-32
6.7.8.1	Cause	6-32

6.7.8.2	Solution	6-32
6.7.9	WebDAV Drag and Drop Does not Work With Windows 2000	6-33
6.7.9.1	Cause	6-33
6.7.9.2	Solution	6-33
6.7.10	Folder Shortcuts Do Not Show Latest Changes	6-33
6.7.10.1	Cause	6-33
6.7.10.2	Solution	6-33
6.7.11	Profile Rule for All WebDAV Requests.....	6-33
6.7.11.1	Solution	6-33

7 Managing Content Folios

7.1	Using Content Folios	7-1
7.2	Managing Content Folios.....	7-2
7.2.1	Creating and Editing Folio Templates.....	7-2
7.2.1.1	Creating a Folio Template	7-3
7.2.2	Adding Custom Viewers and Renderers	7-4

8 Using Content Tracker

8.1	Content Tracker Functionality	8-1
8.1.1	Content Tracker and Content Tracker Reports	8-2
8.1.2	Data Recording, Reduction, and Reporting.....	8-2
8.1.3	Content Tracker Terminology.....	8-3
8.1.4	Installation Considerations	8-4
8.2	Operational Details.....	8-4
8.2.1	Data Collection.....	8-4
8.2.1.1	Service Handler Filter	8-5
8.2.1.2	Web Server Filter Plug-in	8-5
8.2.1.3	Logging Service.....	8-5
8.2.1.4	Enabling or Disabling Data Collection.....	8-5
8.2.2	Data Reduction.....	8-6
8.2.2.1	Standard Data Reduction Process	8-6
8.2.2.2	Data Reduction Process with Activity Metrics.....	8-7
8.2.2.3	Data Reduction Cycles.....	8-7
8.2.2.4	Access Modes and Data Reduction.....	8-8
8.2.2.5	Reduction Sequence for Event Logs	8-8
8.2.2.6	Reduction Schedules	8-9
8.2.2.7	Running Data Reduction Manually	8-9
8.2.2.8	Setting Data Reduction to Run Automatically	8-10
8.2.2.9	Deleting Data Files	8-10
8.2.3	Content Tracker Event Logs.....	8-11
8.2.4	Combined Output Table	8-11
8.2.5	Data Output.....	8-13
8.2.5.1	Content Item Metadata	8-14
8.2.5.2	User Metadata Tables.....	8-14
8.2.5.3	Reduction Log Files.....	8-15
8.2.6	Tracking Limitations	8-15
8.2.6.1	Tracking Limitations in Single-Box Clusters	8-15

8.2.6.2	Static URLs and WebDAV	8-15
8.2.6.2.1	Wrong dID Reported for Access by Saved Static URL	8-16
8.2.6.2.2	False Positive for Access by Saved (stale) Static URL	8-17
8.2.6.2.3	Missed Accesses for Content Repeatedly Requested via WebDAV	8-17
8.2.6.3	Data Directory Protections	8-17
8.2.6.4	ExtranetLook Component	8-18
8.3	Data Tracking Functions	8-18
8.3.1	Activity Snapshots	8-18
8.3.1.1	Search Relevance Metrics	8-18
8.3.1.2	Enabling the Snapshot Function.....	8-19
8.3.1.3	Creating the Search Relevance Metadata Fields	8-19
8.3.1.4	Setting a Check-in Time Value for the Last Access Field	8-20
8.3.1.5	Populating the Last Access Field for Batch Loads and Archives	8-21
8.3.1.6	Linking Activity Metrics to Metadata Fields.....	8-21
8.3.1.7	Editing the Snapshot Configuration	8-22
8.3.2	Service Calls.....	8-22
8.3.3	Web Beacon Functionality	8-23
8.4	Content Tracker Reports	8-24
8.4.1	Report Features and Considerations.....	8-24
8.4.1.1	Oracle and DB2 Case Sensitivity	8-25
8.4.1.2	Access Control Lists and Content Tracker Reports Secure Mode.....	8-25
8.4.1.3	User Authentication/Authorization and Auditing.....	8-25
8.4.1.4	Site Studio Web Site Activity Reporting	8-26
8.4.2	Report Creation Types	8-26
8.4.2.1	Pre-Defined Reports.....	8-26
8.4.2.2	Custom Reports	8-27
8.4.2.3	Generating Reports	8-27
8.4.2.4	Accessing Reports from the Information Page.....	8-27
8.4.2.5	External Report Generators.....	8-28
8.4.2.5.1	Using an External Report Generator	8-28
8.4.3	Security Checks and Query Results	8-28
8.4.3.1	Security Mode Examples	8-29
8.4.3.2	Pre-Defined Reports and Security Modes.....	8-30
8.4.3.3	Custom Reports and Security Modes	8-31
8.4.3.4	Changing the Security Configuration.....	8-31
8.4.3.5	Security Mode Selection	8-31
8.4.3.5.1	Query Type Selection Process	8-31
8.4.3.5.2	Report Query Selection Example	8-32
8.4.3.6	Enabling or Disabling Security Checks for Report Queries	8-33
8.4.3.7	Customization for Report Query Security	8-33
8.4.3.8	Creating Secure Report Queries	8-34
8.4.4	Using Content Tracker Reports	8-34
8.4.4.1	Generating Reports	8-34
8.4.4.2	Accessing Drill Down Reports.....	8-35
8.4.4.3	Accessing Reports from the Information Page.....	8-35
8.4.4.4	Viewing Access Results by Revision	8-35
8.4.4.5	Viewing Access Results for All Versions Combined.....	8-35

8.4.4.6	Creating Custom Report Queries	8-36
8.5	Troubleshooting	8-37
8.5.1	Web Server Filter Plug-in Debugging Support	8-38
8.5.2	Java Code Debugging Support	8-38
8.5.3	DataBinder Dump Facility.....	8-38

9 Using Content Categorizer

9.1	Content Categorizer Functionality	9-1
9.1.1	XML Conversion.....	9-2
9.1.2	Search Rules Overview	9-2
9.1.3	Using Content Categorizer.....	9-2
9.1.3.1	Operating Modes.....	9-3
9.1.3.1.1	Running Batch Mode	9-3
9.1.3.1.2	Interactive Mode Process	9-4
9.2	Setting Up Content Categorizer.....	9-5
9.2.1	Setting XML Conversion Method.....	9-5
9.2.2	Defining Field Properties (Optional)	9-5
9.3	Search Rules.....	9-6
9.3.1	Search Rule Guidelines	9-6
9.3.2	Search Rule Types.....	9-7
9.3.2.1	Pattern Matching Search Rules.....	9-7
9.3.2.2	Abstract Search Rules.....	9-10
9.3.2.3	Option List Search Rule	9-11
9.3.2.4	Categorization Engine Search Rule.....	9-14
9.3.2.5	Filetype Search Rule	9-14
9.3.3	Defining Search Rules	9-15
9.3.3.1	Creating a Search Rule.....	9-16
9.3.3.2	Defining Option List Keywords	9-17
9.3.3.3	Applying Rules to the Type Field	9-18
9.4	Sample doc_config.htm Page	9-18
9.5	XSLT Transformation	9-19
9.5.1	Translation	9-20
9.5.2	Transformation Using XSLT Style Sheets	9-20
9.5.3	SearchML Transformation.....	9-21
9.5.4	Flexiondoc Transformation	9-21

A User Interface

A.1	Content Repository Interface	A-1
A.1.1	Using a Supported Web Browser	A-2
A.1.2	Configuration Manager Page.....	A-2
A.1.2.1	Content Item View Screen.....	A-3
A.1.2.2	User View Screen.....	A-4
A.1.2.3	Define Filter Screen	A-4
A.1.2.4	Show Columns Screen	A-7
A.1.3	Content Type Interface Screens	A-9
A.1.3.1	Content Types Screen.....	A-9
A.1.3.2	Add/Edit Content Type Screen	A-9

A.1.4	Native File Format Interface Screens	A-10
A.1.4.1	File Formats Screen	A-10
A.1.4.2	Add/Edit File Format Screen	A-12
A.1.4.3	Add/Edit File Extension Screen.....	A-12
A.1.5	Configure Thumbnail Options Screen.....	A-13
A.1.6	Custom Fields Interface Screens.....	A-14
A.1.6.1	Configuration Manager: Information Field Tab Screen.....	A-15
A.1.6.2	Add Metadata Field Name Screen.....	A-16
A.1.6.3	Add/Edit Metadata Field Screen	A-17
A.1.6.4	Configure Option List Screen	A-18
A.1.6.5	Option List Storage Screen.....	A-18
A.1.6.6	Edit View Values Screen.....	A-19
A.1.6.7	Option List Screen	A-20
A.1.6.8	Edit Tree Definition Screen	A-21
A.1.6.9	Select Root Node for the Tree	A-22
A.1.6.10	Advanced Search Design Screen	A-22
A.1.6.11	Advanced Options for Field Screen.....	A-23
A.1.6.12	Update Database Design Screen.....	A-24
A.1.6.13	Configuration Manager: Application Fields Tab Screen	A-25
A.1.6.14	Add/Edit Application Field Screen.....	A-26
A.1.7	Electronic Signatures Configuration Screen	A-26
A.1.8	Repository Manager Interface Screens	A-28
A.1.8.1	Repository Manager Main Screen	A-28
A.1.8.2	Repository Manager: Content Tab Screen	A-29
A.1.9	Content Interface Screens	A-30
A.1.9.1	Information Screen	A-31
A.1.9.2	Add New Content Item Screen.....	A-31
A.1.9.3	Update Content Info Screen.....	A-32
A.1.10	Revision Interface Screens	A-32
A.1.10.1	Add New Revision Screen	A-33
A.1.10.2	Check Out Item Screen	A-33
A.1.10.3	Undo Check Out Screen	A-34
A.1.10.4	Resubmit Revision Screen	A-35
A.1.10.5	Delete Revision Screen.....	A-35
A.1.10.6	Delete All Revisions Screen.....	A-36
A.1.11	Workflow Revision Interface Screens	A-36
A.1.11.1	Approve Revision Screen	A-36
A.1.11.2	Reject Revision Screen.....	A-37
A.1.12	Subscription Interface Screens	A-38
A.1.12.1	Repository Manager: Subscriptions Tab Screen.....	A-38
A.1.12.2	Add/Edit Subscription Type Screen	A-39
A.1.12.3	Fields Screen.....	A-39
A.1.12.4	Users Subscribed Screen	A-40
A.1.12.5	Define Subscription Filter Screen	A-41
A.1.12.6	Content Item Subscribed Screen.....	A-41
A.1.12.7	Add Subscription Screen	A-42
A.1.12.8	Select User Screen	A-42

A.1.12.9	Select Alias Screen	A-43
A.1.12.10	Subscribers Screen	A-43
A.1.13	Managed Links Administration Page	A-44
A.1.14	Schema Interface Screens.....	A-45
A.1.14.1	Configuration Manager: Tables Tab Screen	A-45
A.1.14.2	Select Table Screen.....	A-46
A.1.14.3	Create/Edit Table 'name' Screen.....	A-47
A.1.14.4	Add/Edit Column Screen	A-48
A.1.14.5	Configuration Manager: Views Tab Screen.....	A-48
A.1.14.6	Add View Screen: Select Table Screen.....	A-49
A.1.14.7	Add View Screen: Select Columns Screen	A-50
A.1.14.8	Add/Edit View Screen	A-50
A.1.14.9	Edit Values For Views Screen.....	A-54
A.1.14.10	Add/Edit Value Screen	A-55
A.1.14.11	Edit Values: Edit Batch	A-55
A.1.14.12	Configuration Manager: Relations Tab	A-55
A.1.14.13	Add/Edit Relationship Screen	A-56
A.1.14.14	Edit Tree Screen	A-57
A.1.15	Content Profile Interface Screens.....	A-57
A.1.15.1	Configuration Manager: Profiles Tab Screen	A-58
A.1.15.2	Edit Trigger Field Screen.....	A-58
A.1.15.3	Add Profile Screen.....	A-59
A.1.15.4	Add/Edit Profile Screen.....	A-59
A.1.15.5	Profile Links Screen.....	A-60
A.1.15.6	Check In/Search Link Screen: Conditions Tab, Custom Tab	A-61
A.1.15.7	Check In/Search Link: Add Condition Screen	A-61
A.1.15.8	Add Rule in Profile Screen	A-61
A.1.15.9	Preview Profile Screen	A-61
A.1.15.10	Preview Results Screen	A-62
A.1.16	Content Profile Rules Interface Screens.....	A-63
A.1.16.1	Configuration Manager: Rules Tab Screen	A-63
A.1.16.2	Add/Edit Rule Screen.....	A-63
A.1.16.3	Edit Group Header Screen	A-65
A.1.16.4	Edit Activation Condition Screen.....	A-66
A.1.16.5	Add Rule Field Screen	A-71
A.1.16.6	Add/Edit Rule Field 'name' Screen	A-72
A.1.16.7	Edit Default/Derived Value Screens	A-73
A.1.16.8	Edit Default/Derived Value: Select Field Screen.....	A-74
A.1.16.9	Edit Derived Value: Conditions Tab.....	A-74
A.1.16.10	Edit Restricted List Screen.....	A-74
A.2	Workflows User Interface	A-75
A.2.1	The Workflow Admin Screen	A-75
A.2.2	The Criteria Workflow User Interface	A-76
A.2.2.1	Criteria Tab.....	A-77
A.2.2.2	New/Edit Criteria Workflow Screen.....	A-78
A.2.2.3	Add New/Edit Step Screen	A-79
A.2.2.4	Add Alias to Step Screen	A-80

A.2.2.5	Add User to Step.....	A-80
A.2.2.6	Add Token to Step.....	A-81
A.2.2.7	Edit Additional Exit Condition Screen.....	A-81
A.2.3	The Basic Workflow User Interface.....	A-82
A.2.3.1	Workflow Admin: Workflows Tab.....	A-83
A.2.3.2	Add New/Edit Workflow Screen.....	A-84
A.2.3.3	Add Content to Workflow (New Content) Screen.....	A-85
A.2.3.4	Add Content to Workflow (Existing Content) Screen.....	A-85
A.2.3.5	Add Alias to Workflow Screen.....	A-86
A.2.3.6	Add New/Edit Step Screen.....	A-87
A.2.3.7	Add Alias to Step Screen.....	A-88
A.2.3.8	Add User: Basic Workflow.....	A-88
A.2.3.9	Add Token: Basic Workflow.....	A-89
A.2.3.10	Edit Additional Exit Condition Screen.....	A-90
A.2.3.11	Start Workflow Screen.....	A-91
A.2.4	Tokens User Interface.....	A-91
A.2.4.1	Workflow Tokens Screen.....	A-91
A.2.4.2	Add/Edit Token Screen.....	A-92
A.2.4.3	Add Token User Screen.....	A-92
A.2.5	The Jump User Interface.....	A-93
A.2.5.1	Add New/Edit Step Screen: Events Tab.....	A-93
A.2.5.2	Edit Script for <StepName> Screen.....	A-94
A.2.5.3	Script Properties Screen.....	A-94
A.2.5.4	Select Target Step Screen.....	A-97
A.2.5.5	Add/Edit Jump Screen Tabs.....	A-98
A.2.5.6	Content Item View Screen.....	A-100
A.2.6	Workflow Template Interface Screens.....	A-101
A.2.6.1	Workflow Admin: Templates Tab.....	A-101
A.2.6.2	Add/Edit Template Screen.....	A-102
A.2.6.3	Add New/Edit Step Screen.....	A-103
A.2.6.4	Add Alias to Step Screen.....	A-103
A.2.6.5	Add User to Step.....	A-104
A.2.6.6	Add Token: Templates.....	A-105
A.2.6.7	Edit Additional Exit Condition Screen.....	A-105
A.2.7	Workflow Scripts User Interface.....	A-106
A.2.7.1	Workflow Scripts Screen.....	A-106
A.2.7.2	Add/Edit Script Screen.....	A-107
A.2.7.3	Add/Edit Script Screen: Jumps Tab.....	A-107
A.2.7.4	Add/Edit Script Screen: Custom Tab.....	A-109
A.2.7.5	Add/Edit Script Screen: Test Tab.....	A-109
A.2.7.6	Add/Edit Jump Screen.....	A-110
A.2.7.7	Add/Edit Jump Screen: Side Effects Tab.....	A-111
A.2.7.8	Add/Edit Jump Screen: Message Tab.....	A-112
A.2.7.9	Content Item View Screen.....	A-113
A.2.7.10	Select Workflow Step Screen.....	A-114
A.3	PDF Watermark Interface.....	A-114
A.3.1	PDF Watermark Administration Screen.....	A-115

A.3.2	Rules Tab.....	A-115
A.3.3	Add New/Edit Rule Screen.....	A-116
A.3.4	Add New/Edit Criteria Screen.....	A-116
A.3.5	Templates Tab.....	A-117
A.3.6	Add New/Edit Template Screen.....	A-117
A.3.7	Add New/Edit Text Watermark Window.....	A-118
A.3.8	Add New/Edit Image Watermark Window.....	A-120
A.3.9	Add New/Edit Signature Watermark Window.....	A-121
A.3.10	Configuration Tab.....	A-122
A.3.11	Edit Default Value Screen.....	A-123
A.4	Contribution Folders Interface.....	A-123
A.4.1	Virtual Folder Administration Configuration Screen.....	A-123
A.4.2	System Folder Configuration Screen.....	A-124
A.4.3	System Default Information Field Configuration Page.....	A-125
A.4.4	Local Folders Page.....	A-126
A.4.5	Information Field Inherit Configuration Page.....	A-127
A.5	Create/Edit Folio Template Page.....	A-128
A.5.1	Structure Tab.....	A-129
A.5.1.1	Folio Structure Pane.....	A-130
A.5.1.2	Element Info Pane.....	A-130
A.5.1.3	Source Items Pane.....	A-132
A.5.2	Properties Tab.....	A-132
A.6	Content Tracker Interface.....	A-134
A.6.1	Data Engine Control Center.....	A-134
A.6.1.1	Collection Tab.....	A-135
A.6.1.2	Reduction Tab.....	A-135
A.6.1.3	Schedule Tab.....	A-136
A.6.1.4	Snapshot Tab.....	A-136
A.6.1.5	Services Tab.....	A-137
A.6.1.6	Extended Services Tracking Screen.....	A-138
A.6.1.7	Field Map Screen.....	A-139
A.6.2	Content Tracker Report Generator Main Page.....	A-139
A.7	Content Categorizer Interface.....	A-140
A.7.1	Content Categorizer Administration Page.....	A-141
A.7.2	Configuration Tab.....	A-142
A.7.2.1	Property Config Screen.....	A-143
A.7.3	Rule Sets Tab.....	A-143
A.7.3.1	Add Ruleset Screen.....	A-144
A.7.3.2	Add/Edit Rule for <i>Field</i> Screen.....	A-145
A.7.4	Option Lists Tab.....	A-145
A.7.5	Filetype Maps Tab.....	A-146
A.7.5.1	Add/Edit Filetype Map Screen.....	A-147
A.7.6	Categorizer Engines Tab.....	A-148
A.7.6.1	Add/Edit Categorizer Engine Screen.....	A-149
A.7.7	Query Trees Tab.....	A-150
A.7.7.1	Build Query Tree Screen.....	A-150
A.7.7.2	Delete Query Tree Screen.....	A-151

A.7.8	Field Properties Tab.....	A-151
A.7.8.1	Field Properties Screen	A-152
A.7.9	Batch Categorizer Screen	A-153
A.7.10	Categorize Existing Screen	A-154
A.8	Web Layout Editor Interface	A-154
A.8.1	Web Layout Editor Page	A-155
A.8.1.1	Web Page Hierarchy Pane.....	A-156
A.8.1.2	Page Properties Pane.....	A-156
A.8.1.3	Page Links Pane	A-157
A.8.2	Add Page Link Screen.....	A-158
A.8.3	Add Web Page Screen	A-159
A.8.4	Edit Local Page Link Screen.....	A-160
A.8.5	Edit External URL Screen	A-160
A.8.6	Edit Page Properties Screen.....	A-161
A.8.7	Edit Active Report Query Screen	A-162
A.8.8	Create Historical Report Screen.....	A-163
A.8.9	Query Link Definition Screen	A-164
A.8.10	Add/Edit Query Results Page.....	A-165

B Building a Web Site

B.1	Planning a Web Site.....	B-1
B.1.1	The Web Layout.....	B-1
B.1.2	Defining the Site Structure and Displaying Criteria.....	B-2
B.1.3	Task Sequence	B-2
B.2	Working with Web Pages	B-3
B.3	Managing Web Pages	B-4
B.3.1	Adding a New Web Page	B-4
B.3.2	Editing Web Page Properties	B-4
B.3.3	Creating a Local Page Link.....	B-5
B.3.4	Creating an External URL Link	B-5
B.3.5	Editing a Hierarchical Web Page Structure	B-5
B.4	Working with Reports.....	B-6
B.4.1	About Reports	B-6
B.4.2	Defining an Active Report.....	B-7
B.4.3	Defining a Historical Report	B-7
B.4.4	Editing a Query Expression in an Active Report	B-7
B.5	Writing Queries.....	B-8
B.5.1	Creating a Query Link	B-9
B.5.2	Editing the Query Expression in a Query Link.....	B-9
B.5.3	Adding a Query Results Page.....	B-9
B.5.4	Editing a Query Results Page	B-9
B.5.5	Deleting a Query Results Page	B-10

Index

Preface

This guide provides concepts, procedures, and reference information for administrators to manage applications for Oracle WebCenter Content Server.

Audience

This guide is intended for people who administer applications for Oracle WebCenter Content Server. Administrators set up, maintain, and manage users, content, and system configurations. Administrator configure the system to manage and index files, archive and replicate information, work with security, adjust system properties, review log files, and so on.

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

Oracle WebCenter Content Server is documented in the following manuals:

- *Oracle WebCenter Content Concepts Guide*
- *Oracle WebCenter Content Quick Installation Guide*
- *Oracle WebCenter Content Installation Guide*
- *Oracle WebCenter Content User's Guide for Content Server*
- *Oracle WebCenter Content Application Administrator's Guide for Content Server*
- *Oracle WebCenter Content System Administrator's Guide for Content Server*
- *Oracle WebCenter Content Developer's Guide for Content Server*
- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

The software also ships with release notes, in both printed and PDF formats, which list new and enhanced features of each new software release. Release notes also provide special, up-to-the-minute considerations for installing and using the software. The release notes are important documents. Always make sure to read them before installing or updating Oracle software.

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 entered.
Forward slashes (/)	Forward slashes are used to separate the directory levels in a path to a UNIX server, directory, or file. Forward slashes are also used to separate parts of an Internet address. A forward slash is always included after a UNIX directory name and might or might not be included after an Internet address.
Backward slashes (\)	Backward slashes are used to separate the levels in a path to a Windows server, directory, or file. A backward slash is always included after a Windows server, directory, or file path.
<i>DomainHome</i>	The variable used to indicate the user-specified directory where an Oracle WebCenter Content server is deployed to run on an Oracle WebLogic Server. DomainHome is a term used in Oracle WebLogic Server deployment, and it is provided here only because IntradocDir refers to it.
<i>IntradocDir</i>	<p>The variable used to indicate the root directory for actual configuration and data files specific to an instance deployed on the Oracle WebCenter Content domain on Oracle WebLogic Server. The files include startup files (intradoc.cfg and executables). This variable is configured for one type of instance: Content Server, Inbound Refinery or Records.</p> <p>The specified directory must be an absolute path to the instance directory, and it must be unique to a specific server or node. For install in a cluster, the instance directory must be in a network share accessible to all nodes in the cluster.</p> <p>The default location for the instance directory is specified as <i>DomainHome/ucm/short-product-id</i> where <i>short-product-id</i> can be:</p> <ul style="list-style-type: none"> ■ cs (Oracle WebCenter Content Server) ■ ibr (Oracle WebCenter Content: Inbound Refinery) ■ urm (Oracle WebCenter Content: Records)

Introduction

Oracle WebCenter Content Server helps you build secure content repositories with check in/check out, revision control, and automated publishing in web-ready formats. It also provides a number of optional applications and components that you can configure and use to provide extended functionality. This guide describes how to administer these applications.

This section provides an introduction to the information in this guide. It covers the following topics:

- [Section 1.1, "About This Guide"](#)
- [Section 1.2, "What's New"](#)
- [Section 1.3, "Administration Applications"](#)

1.1 About This Guide

This guide provides information about administration concepts and tasks for the following Oracle WebCenter Content Server applications:

- **Repository Manager:** Describes how to display or handle content, such as how to create customized content types, how to work with subscriptions, and how to manage revisions.
- **Metadata:** Describes how to use metadata and how to create schemas, rules, and content profiles.
- **Workflows:** Describes how to route content for review, approval, and release to the system.
- **PDF Watermark:** Describes how to add watermarks to PDF files generated by the component PDF Converter.
- **Folders and WebDAV:** Describes the folder interface options for organizing and accessing content in Oracle WebCenter Content Server.
- **Content Folios:** Describes how to assemble, track, and access logical groupings of multiple content items from within the secure environment of Oracle WebCenter Content Server.
- **Content Tracker:** Describes how to track system usage to understand which content items are accessed most frequently and which content items have the highest value for specific users or groups.
- **Content Categorizer:** Describes how to use search rules to set metadata values for new documents checked in to Oracle WebCenter Content Server and for existing documents that have or do not have metadata values.

1.2 What's New

This section provides a brief overview of changes to the functionality discussed in this book for this release of Oracle WebCenter Content Server.

1.2.1 Release 11g (11.1.1.6.0)

- **Folders:** This component (FrameworkFolders component) is installed but disabled by default. It provides a hierarchical folder interface within the browser, similar to a conventional file system, for organizing, locating, and managing repository content and content item metadata. This is a scalable, enterprise solution and is a replacement for the earlier Contribution Folders interface.

This document describes how to configure and administer the component. For information about migrating content from the earlier Contribution Folders interface see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

- **FoldersRetention:** With Folders, you can perform basic content retention scheduling by creating a retention query folder, assigning retention attributes to the folder, and then configuring the retention schedule. You can assign retention rules based on the age of the content item or on the number of revisions. If you have a license for Oracle WebCenter Content: Records, you can also define retention rules based on categories defined in Records.
- **Electronic Signatures:** You can optionally sign a content item with an electronic signature that uniquely identifies the contents of the file at a particular revision and associates the revision with a particular user. You can sign a content item as part of a workflow approval step or as an independent content item and you can include signature metadata in a PDF Watermark.

This document describes how to define custom metadata fields for electronic signature metadata and how to use electronic signatures when you define workflows and PDF Watermarks. For more information about signing documents electronically, see the *Oracle WebCenter Content User's Guide for Content Server*.

- Electronic signatures extends the functionality of PDF Watermark to include the *cover* modifier in the page range option. This modifier creates a new cover sheet that includes the electronic signature watermark information.
- PDF Watermark also now provides the \$PAGE_COUNT\$ symbol which is replaced by the total number of pages in the content item when the watermark is rendered.

1.2.2 Release 11g (11.1.1)

- This guide combines information that was previously contained in the following 10g version of the documents:
 - *Managing Repository Content*
 - *Content Server Workflow Implementation Guide*
 - *Content Categorizer System Administration Guide*
 - *Content Tracker Administration Guide*
 - *PDF Watermark*
 - *Folders/WebDAV Administration Guide*
 - *Folios Administration Guide*

- Administration Applets: All Administration Applets in the user interface have been converted to Java Swing and are now accessible.
- Content Tracker: New preferences have been set to provide maximum efficiency in high volume production environments. In addition, event log file locking within and between Java Virtual Machines is now managed using object synchronization and parallel log files.
- Content Categorizer: Several enhancements have been made. Export conversion parameters are now available for user customization. Dynamic metadata field length checks are now used so a server restart is not necessary. The Batch Categorizer executable is no longer on the Start menu but has been relocated to the `contentcategorizer` subdirectory in the instance.
- PDF Watermark: The installation now includes five variants of the Albany font set. In addition the iText Common Library is now distributed in the iText Component.
- See the *Oracle WebCenter Content System Administrator's Guide for Content Server* for a detailed description of changes to security for this release and for information about other changes to the product.

1.3 Administration Applications

This section covers the following topics:

- [Section 1.3.1, "User Types"](#)
- [Section 1.3.2, "Accessing Administration Applications"](#)
- [Section 1.3.3, "Running Administration Applications as Applets"](#)
- [Section 1.3.4, "Running Administration Applications in Standalone Mode"](#)

1.3.1 User Types

Oracle WebCenter Content Server provides for two types of users and two types of administrators:

User	Description
Consumers	Users who find, view, and print files based on their security credentials.
Contributors	Users who have the additional ability to create and revise files based on their security credentials.
Administrators	Administrators who oversee an entire server instance.
Subadministrators	Administrators who oversee a functional subset of an instance.

1.3.2 Accessing Administration Applications

The system provides administration applications to configure and maintain user access.

Note: Oracle recommends using Sun's JDK version 1.6 Java plug-in when opening any Java applets (such as an administration applet or the multiple-file upload applet) from a browser.

The Administration page provides access to administration applets and configuration tools page. To access this page, log on as an administrator or subadministrator, and choose **Administration** then **Admin Applets** from the Main menu.

Figure 1–1 Admin Applets Menu



You can start all applications as a standalone application at the server. You can run several applications as applets through a browser, or from the Apps menu in each of the tools.

1.3.3 Running Administration Applications as Applets

You can run several administration applications as applets from any browser with access to Oracle WebCenter Content Server. Applets are convenient for remote administration.

You cannot run the Batch Loader, Component Wizard, System Properties, and Analyzer utilities as applets; for security reasons, they must be run in standalone mode from the computer where the software is installed. For details, see [Section 1.3.4, "Running Administration Applications in Standalone Mode."](#)

Some functions available in the standalone version of an application are not available from the applet version. See the documentation for each application for more information.

To run an administration application as a Java applet within a Java-enabled browser:

1. Open a browser window.
2. Log on as an administrator.
3. Choose the **Administration** tray link.
4. Choose the **Admin Applets** link.

1.3.4 Running Administration Applications in Standalone Mode

You can run all administration applications in standalone mode from the computer where the software is installed. The method required to start these programs differs slightly between Windows and UNIX installations.

Running the standalone version of an application offers greater security than browser applets, and enables sending passwords without the risk of having them captured or copied from the Web or a network.

1.3.4.1 On Windows Systems

To run a standalone administration application on a Windows operating system:

1. Select the application from the Windows Start menu:
 - To run a configuration application, select **Start, Programs, Oracle WebCenter Content Server, instance, application**.
 - To run an administration Utility, select **Start, Programs, Oracle WebCenter Content Server, instance, Utilities, utility**.

For all applications except for Component Wizard and System Properties, a login screen opens. For Component Wizard and System Properties, the main screen of the application opens.

Tip: It may take several seconds for the login screen or the application screen to appear, and the screen may be hidden by other windows.

2. Enter the administrator login name and password.
3. Click **OK**.

The main screen of the application opens.

1.3.4.2 On UNIX Systems

To run a standalone administration application on a UNIX operating system:

1. Navigate to the *DomainHome*/ucm/cs/bin/ directory.
2. Enter the following

```
% ./application_name
```

where *application_name* is the name of an executable file. If an application is not listed, you can enter it as a parameter to the IntradocApp application, as in this example:

```
% ./IntradocApp Workflow
```

3. Press **Enter**.

For all applications except for Component Wizard and System Properties, a login screen opens. For Component Wizard and System Properties, the main screen of the application opens.

4. Enter the administrator login name and password.
5. Click **OK**.

The main screen of the application opens.

Managing Repository Content

While managing repository content, you may have to create a new content type to group files or you may have to convert files into a content format that the Oracle WebCenter Content Server can more effectively manage. You can also create custom application fields and custom metadata to tailor input forms and searching to a site's needs.

This chapter covers the following topics about managing repository content:

- [Section 2.1, "Content Types"](#)
- [Section 2.2, "Custom Fields"](#)
- [Section 2.3, "Native Content Conversion"](#)
- [Section 2.4, "Managing Content and Revisions"](#)
- [Section 2.5, "Signing Content Electronically"](#)
- [Section 2.6, "Subscribing to Content"](#)
- [Section 2.7, "Managing Linked Content with Link Manager"](#)

2.1 Content Types

Files are grouped in directories designated by *content types*.

- Content types become the names of the subdirectories in which documents are stored in the *weblayout* and *vault* directories.
- Content types can correspond to departments (such as ENG, MKTG, and HR), document types (such as MEMO, FORM, and SPREADSHEET), or any other model needed.
- Several content types are defined by default (Document, Binary, Digital Media, and so on), but you can modify or delete these.
- Each content type is assigned an image, which helps users identify the content type on search result pages. Several images are provided or you can create and assign your own images.
- Create a manageable number of content types, typically no more than 50. Too many content types increases the amount of effort required to maintain the system, and makes it difficult for contributors to assign the correct content types to their files.
- When configuring content types, consider using the same prefix in a content type when grouping similar information. For example, the prefix MEMO is used in the following content types: MEMO_INT, MEMO_EXT, MEMO_EXEC.

2.1.1 Managing Content Types

The following typical tasks are performed when working with content types:

- Creating a new content type
- Editing an existing type
- Deleting a content type

Follow these steps to perform those tasks:

1. Choose **Administration** then **Admin Applets** from the Main menu.
2. Click **Configuration Manager**.
The [Configuration Manager Page](#) opens.
3. Choose **Options** then **Content Types** from the Page menu.
The [Content Types Screen](#) opens.
4. To add a new type, click **Add**. To edit a type, highlight a type name and click **Edit**. To delete a type, highlight the type name and click **Delete**. Click **OK** when the confirmation screen opens.

Note: You cannot delete a content type if content still exists with that type. Make sure no content is using the type before attempting to delete it.

When adding or editing a type, the [Add/Edit Content Type Screen](#) opens.

5. Enter or edit the name and description of the type. Select an image from GIF list to associate with the content type.
6. Click **OK** when done.

2.2 Custom Fields

This section covers the following topics:

- [Section 2.2.1, "About Custom Fields"](#)
- [Section 2.2.2, "Adding or Editing a Custom Field"](#)
- [Section 2.2.3, "Rebuilding the Database or the Search Index"](#)
- [Section 2.2.4, "Defining an Option List"](#)

2.2.1 About Custom Fields

This section covers the following topics:

- [Section 2.2.1.1, "Application Fields"](#)
- [Section 2.2.1.2, "Custom Metadata Fields"](#)

If you use the Electronic Signature component, you can also define custom fields for use with the electronic signature metadata. For more information, see [Section 2.5.2, "Custom Electronic Signature Metadata."](#)

2.2.1.1 Application Fields

Application fields are custom fields that you can use to customize forms and screens. With application fields, you can add features such as dependent lists to forms. You can also use application fields in custom components, HCSP (Hypertext Content Server Page) files, and HCSF (Hypertext Content Server Form) files.

By default, application fields do not appear on the standard check-in and search forms, but are used by custom templates. You can use application fields as placeholders or with schema views to enable dependent lists without creating an associated metadata field. For details, see [Section 3.1, "Using Schemas to Customize Metadata."](#)

You can specify in a content profile that application fields are displayed on the standard check-in and search pages. For details, see [Section 3.2, "Using Profiles to Customize Content Screens."](#)

Application fields are not indexed and are not searchable. Changes to application fields do not affect the database or the index.

2.2.1.2 Custom Metadata Fields

For each content item, the system maintains a set of information about the content, or *metadata*. Metadata is similar to a card in a library's card catalog, while the actual files are similar to library books. As with the card catalog, metadata consists of information about a file (title, reference number, author, subject, publishing date, book location, and so forth).

In addition to the standard metadata fields provided with the system, you can create new fields to accommodate unique content or system design requirements. It is important to create only the necessary amount of additional metadata necessary to help locate or manage a content item.

When you create a custom field name, the system automatically prefixes the name with an 'x' to ensure that it is unique and does not conflict with any reserved names. Similarly, when you create custom user information (metadata) fields, the system prefixes the name with a 'u' to ensure that it is also unique and does not conflict with any reserved names. For more information about adding custom user information fields, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

Metadata fields are indexed and searchable. Changes to custom metadata fields can affect the database (where information about metadata fields is stored) or the search index (where the metadata values are stored).

2.2.1.3 Standard Metadata Fields

The following are standard fields provided with the system. You cannot edit or delete these fields.

Field Caption	Entry Method	Required?	Definition
Content ID	Text Entry or Automatic Generation	Yes	<p>The unique identifier for each content item.</p> <ul style="list-style-type: none"> ■ Duplicate names are not allowed. ■ Maximum field length is 30 characters. ■ Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. ■ The Content ID can be automatically generated. See the General Options tab of the System Properties Utility. <p>If using an Oracle or DB2 database, all Content IDs are converted to uppercase letters automatically.</p>
Type	List	Yes	<p>An identifier used to group content.</p> <ul style="list-style-type: none"> ■ Types become subdirectories in the <i>weblayout</i> directory. ■ Maximum field length is 30 characters. ■ Use only letters, numbers, and underscores (_). Do not use spaces or other special characters.
Title	Text Entry	Yes	<p>A descriptive title for the content item.</p> <ul style="list-style-type: none"> ■ Maximum field length is 80 characters.
Author	List or Text Entry	Yes	The user who checked in the content item.
Security Group	List	Yes	<p>The security group for which users must have permission to access the content item.</p> <ul style="list-style-type: none"> ■ Duplicate names are not allowed. ■ Maximum field length is 30 characters. ■ Use only letters, numbers, and underscores (_). Do not use spaces or other special characters.
Account	List or Text Entry	No	<p>The account for which users must have permission to access the content item.</p> <p>This field is available only if accounts are enabled.</p>
Primary File	Text Entry or Browse to File	Yes	<p>The complete path to the native file being checked in. Maximum file name length is 80 characters, including the directory path and file extension. Maximum file extension length is eight characters.</p> <p>The Folders option modifies this maximum file name length on installation to 255 characters.</p>
Alternate File	Text Entry or Browse to File	No	<p>The path name to another Web-viewable file format of the native document, or one that can be converted to a Web-viewable format.</p> <p>For example, when checking in a FrameMaker or Quark document that has several files that comprise the document, you would check in a zipped file as the native format (or Primary File) and a Postscript, PDF, or viewable file as its Alternate File. The zipped file is not viewable on the Web, but Inbound Refinery converts the Postscript file to its Web-viewable format, PDF.</p> <p>Maximum file name length is 80 characters, including the directory path and file extension. Maximum file extension length is eight characters.</p> <p>The Folders option modifies this maximum file name length on installation to 255 characters.</p>

Field Caption	Entry Method	Required?	Definition
Revision	Automatic Generation or Text Entry	Yes	A label (such as 1, 2, 3,... or A, B, C,...) that represents the number of times the content item has gone through its life cycle (the number of revisions). You can customize the Revision label for your revision scheme.
Comments (optional)	User Text Entry	No	A field for additional information about the file. Maximum field length is 255. This field is considered a custom field and can be deleted.
Release Date	Automatic Generation or Text Entry	Yes	The date the file is to be released so it is available for searching and viewing. The Release Date defaults to the date and time the file is checked in.
Expiration Date	Text Entry	No	The date the file is no longer available for searching or viewing. All revisions of the content item expire when the current revision expires. When a content item expires, revisions are retained, but only an administrator can access from the Repository Manager, unless you use <i>Notification of Expiration</i> .

2.2.2 Adding or Editing a Custom Field

Follow these steps to add or edit a custom field, either application or metadata field:

1. Choose **Administration** then **Admin Applets** from the Main menu.
2. Click **Configuration Manager**.
The [Configuration Manager Page](#) opens.
3. Click **Information Fields** to add a metadata field. Click **Application Fields** to add or edit an application field.
Click **Add** to add a new field or highlight a field and click **Edit** to change a field.
4. When adding a metadata field, a dialog opens where you can enter the name. Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. Click **OK** when done.

The [Add/Edit Metadata Field Screen](#) or [Add/Edit Application Field Screen](#) opens (depending on the type of field being used).

When adding an application field, you can enter the name on the Add/Edit Field Page.

5. Enter or edit the information for the field:
 - Field Caption: The label for the field displayed to users.
 - Field Type: The size indicated is the character input length, not an indication of the actual number of bytes needed to store the field.
 - Integer: -2^{31} to 2^{31} (-2 billion to +2 billion). By definition, an integer is a natural number, so decimal values and commas are not permitted.
 - Memo: 2000 characters.
 - Date: Date format (such as *dd/mm/yyyy* or *dd/mm/yy* for the English-US locale).
 - Long Text: 200 characters.
 - Text: 30 characters.

- Field Order (metadata fields only): Sequence in which the field is displayed on pages. Starting at 2, the number automatically increments as new fields are added. However, it is recommended to manually increment the numbers by 5, such as 15, 20, 25, and so on to accommodate fields added in the future.
 - Default Value (metadata field only): Any default value for the field.
 - Require Value (metadata field only): Prevents files from being checked in if the field does not have a value.
 - Placeholder: If selected, the field is not stored or indexed. Placeholders are often used for the parent level of a dependent list.
 - Enable on User Interface (metadata field only): If selected, the field is displayed. If deselected the field is hidden.
 - Enable for Search Interface (metadata field only): If selected, the field is indexed and thus used for searching. If deselected the field is not indexed nor does it appear on search pages.
 - Enable Option List: Enables the use of user-selectable list on a page. For details, see [Section 2.2.4, "Defining an Option List."](#)
 - View Only (application field only): If selected, the field is only used in a schema view. For details, see [Section 3.1, "Using Schemas to Customize Metadata."](#)
6. Click **OK**.
 7. Update the database design and rebuild the search index if necessary.

2.2.3 Rebuilding the Database or the Search Index

The following table lists the events after which a database update or search index rebuild is required depending on the search engine that is used.

Event	Action Required
Add metadata field	Update database
Edit metadata field	Update database
Delete metadata field	Update database
Enable or disable <i>Enable for Search Index</i> for metadata field	Rebuild search index
Add metadata field with <i>Enable for Search Index</i> selected	Rebuild search index

Rebuilding the Database

If changes were made that must be saved to the database, the **Update Database Design** button on the **Information Fields** tab of the **Configuration Manager** page becomes active. To update the database:

1. Click **Update Database Design**.
A screen opens listing the information fields that are added and any fields that are marked for deletion.
2. To retain a field, deselect the box next to the field name. The field remains hidden but still exists in the database.
You cannot remove added or edited fields using this screen. They must be added then deleted later.

3. Click **OK** when done.

Rebuilding the Index

If changes were made that require rebuilding the search index, the **Rebuild Search Index** button on the **Information Fields** tab of the **Configuration Manager** page becomes active. To rebuild the search index:

1. Click **Rebuild Search Index**.
2. If a message asks to update the database design before rebuilding the search index, click **Update Database Design** to save changes to the database before proceeding.
3. When the message *Rebuild initiated* is displayed, click **OK**.

Caution: Depending on the size of the search index and available system resources, the search index rebuild process can take several days. If rebuilding is necessary, rebuild at times of non-peak system usage.

2.2.4 Defining an Option List

Lists are used with custom fields to provide a selection from which users can choose a value. Follow these steps to define a list:

1. Create the custom field and click **Enable Option List**, then click **Configure**. For details, see [Section 2.2.2, "Adding or Editing a Custom Field."](#)

The [Configure Option List Screen](#) opens.

2. Choose what type of list to use:
 - Multiselect List: Provides a list from which users can select multiple items.
 - Edit and Multiselect List: Provides both a text field and a data entry box. Contributors can enter values that are not in the list and they can select or enter multiple values.
 - Edit and Select List: Provides both a text field and a data entry box. Contributors can enter values that are not in the list.
 - Select List Not Validated: For Batch Load and Archiver purposes, this option permits check in of files whose specified values are not current options.
 - Select List Validated: For Batch Load and Archiver, this option ensures that only files whose specified values are current options for this field are checked in.

Click **Advanced** to display the Option List Storage screen where information about the list's display and storage are specified. For more details, see [Section 2.2.4.1, "Defining Option List Storage."](#)

3. Choose how to access the values in the list:
 - Use Option List: Create a new list or edit an existing values. The name of the new list, taken from the name of the field, is inserted. For more details, see [Section 2.2.4.2, "Adding or Editing Option List Content."](#)
 - Use View: Uses values in a stored view instead of a list. Click **Edit Values** to change the values saved in the view. For more details, see [Section 2.2.4.3, "Editing View Values."](#)

- Use Tree: Uses values stored in a tree rather than a view or a list. Click **Edit Definition** to change how the tree is viewed or stored.
4. Determine the dependencies for the list:
 - Dependent field: Check if the metadata field is subordinate to another field. This option is only available when using a view.
 - Depends on: If you select the Dependent Field, this becomes active. Enter a field name or choose the field from the list of fields.
 - Relationship: If a relationship has been defined for the view in use, select it from the list. For more details, see [Section 3.1, "Using Schemas to Customize Metadata."](#) If you select a list or view, you must specify a relationship.
 5. Click **OK** when done.

2.2.4.1 Defining Option List Storage

One part of creating a list is to determine the storage options. To define storage, click **Advanced** next to the Option List Type on the [Configure Option List Screen](#). Enter the following information:

- Storage type: Choose to either permanently store list keys or store a localized list.
- Multiselect options: Choose options to customize the appearance of a multiselect list:
 - Pad ends: Pad the length of the separator for multiselect values.
 - Storage Separator: Change the separator used to store values.
 - Display Separator: Change the separator used in the display of values.

Click **OK** when done.

2.2.4.2 Adding or Editing Option List Content

The contents of a list are created on the Option List screen. To open this screen, click **Edit** next to the Use Option List field on the [Configure Option List Screen](#). Enter the following information:

- Option list values: The items to select. Each value must be on a separate line, with a carriage return between values.
- Sort order (ascending or descending): Sorts the list in alpha-numeric order. If ascending, capital letters precede lowercase letters. If descending, the reverse is done. If **Ignore Case** is selected, the list is sorted and the case of the letters is ignored.
- Sort Now: Sorts the list in the manner specified (ascending, and so on).

2.2.4.3 Editing View Values

A view displays the items available in a list. To edit a view, click **Edit View** next to the Use View field on the [Configure Option List Screen](#). Make the following selections:

- Filter: Select a filter to alter which values are displayed on the screen.
- Show Columns: Limits the number of columns to display.
- Add, Edit: Displays a screen where you can add or edit new values for those currently in the view.
- Delete: Prompts to confirm the deletion of a value from the view.

- **Edit Batch:** Displays a screen you can use to edit values in a line editor. To add values, enter the data in the appropriate columns separated by a pipe symbol (|). Each row in the table should begin on a new line.

2.2.4.4 Using Tree Values

A tree displays the items available in a list. If you use this method, a screen opens where you can enter a tree definition. Make the following selections:

- **Select relationship:** Choose a relationship between options in the list.
- **Remove view:** Click to remove the selected view from the level in the tree.
- **Selection path:** Choose to display the complete path when the option is selected or to save the complete path when the option is selected.
- **Separator:** Specify the separator used between values.

2.3 Native Content Conversion

Note: Unless Oracle WebCenter Content Server is configured to work with an Inbound Refinery instance, files are all passed through to the Web site in their native format.

When Oracle WebCenter Content Server is configured as a provider for an Inbound Refinery instance, you must specify what file formats to pass to the refinery for conversion, based on the file extension. You can do this in the following ways:

- You can use the File Format Wizard, accessed from the Refinery Administration folder in the Administration tray
- You can use the File Formats option of the Configuration Manager applet to map file extensions (.doc, .txt, and so on) to file formats and then map the file formats to the conversion option on the refinery. This option provides more flexibility in mapping different file extensions to different conversion options
- You can create a custom component to base the conversion on the value of specified metadata fields for the content item, including the file format or custom fields.

After the job passes from Oracle WebCenter Content Server to Inbound Refinery, the refinery configuration determines how to convert and return the native file.

File formats are automatically configured during installation or can be added and changed as needed.

See the *Oracle WebCenter Content Administrator's Guide for Conversion* for more details about conversions.

This section covers these topics:

- [Section 2.3.1, "Identifying MIME Types"](#)
- [Section 2.3.2, "Native Applications and Content Conversions"](#)
- [Section 2.3.3, "Associating File Types with Conversion Programs"](#)
- [Section 2.3.4, "Thumbnails"](#)

2.3.1 Identifying MIME Types

When you define new file formats, specify the MIME (Multipurpose Internet Mail Extensions) type corresponding to the file extension (for example, the format mapped to the doc file extension is application/msword).

When a content item is checked in to the repository, the content item's format is assigned according to the format mapped to the file extension of the native file. If the native file is not converted, Oracle WebCenter Content Server includes this format when delivering the content item to clients. Using the MIME type for the format assists the client in determining what type of data the file is, the associated helper applications, and so on.

Check MIME types and the list of registered MIME types at <http://www.iana.org/assignments/media-types/index.html>.

2.3.2 Native Applications and Content Conversions

The native applications used to convert content must meet the following requirements:

Native Application	Requirements
MS Word	Verify that the native application is installed if needed by Inbound Refinery for the conversion. Associate the file type to a conversion process on the File Formats tab. For Word and PowerPoint applications, use the Native Options tab on the Local Inbound Refinery Configuration screen to specify whether to process links.
MS Project	
Lotus Freelance	
MS Excel	
Lotus 123	
Corel WordPerfect	
MS PowerPoint	
Lotus WordPro	
MS Visio	
iGrafx Designer	
MS Publisher	Verify that the native application is installed.
FrameMaker	Configure the file path in Inbound Refinery. To check in FrameMaker books, use the Upload Multiple Files option, which must be first enabled in System Properties.
PhotoShop	
PageMaker	
Other	Verify that the native application is installed (if required). Install the custom conversion program in Inbound Refinery. Configure the file path in Inbound Refinery. Associate the file type to a conversion process on the File Formats tab.

2.3.3 Associating File Types with Conversion Programs

Associating file types with conversion programs is a two-stage process.

Add the file format and associate the file extension with the format:

1. Choose **Administration** then **Admin Applets** from the Main menu.
2. Click **Configuration Manager**.

The [Configuration Manager Page](#) opens.

3. Choose **Options** then **File Formats** from the Page menu.
The [File Formats Screen](#) opens.
4. Click **Add** in the File Formats pane to add a file format.
The [Add/Edit File Format Screen](#) opens.
5. Enter the necessary information:
 - **Format:** Usually the MIME type.
 - **Conversion type:** Associates the format name with a conversion program. Select from the following:
 - **Passthru:** Documents with extensions mapped to PASSTHRU are not converted, but are displayed on the Web site in their native file format. The client computer must have the native applications.
 - **Legacy Custom:** Documents with extensions mapped to CUSTOM execute a conversion program not included in the set of standard conversions. This option is not supported in this release.
 - **Description:** A brief description of the file format.
6. Click **OK**.

Enter the file extension to associate with the format:

1. Click **Add** in the File Extensions pane.
The Add/Edit File Extension Screen opens.
2. Enter the necessary information:
 - **Extension:** The three-character designation for the file format. A file with this format is converted using the conversion program specified by the Map to Format field.
 - **Map To Format:** A list of the available formats with specified conversions (defined in the File Formats pane). Select a format to directly relate all files with that extension to a specific conversion program.
3. Click **OK**.

2.3.4 Thumbnails

Thumbnails are small preview images of content. They are used on search results pages and typically link to the web-viewable file they represent. This means that users do not need to rely solely on text information such as the title to tell if a file is the one for which they are looking. A thumbnail provides consumers with a visual sample of a file without actually opening the file itself. This enables them to check a file before committing to downloading the larger, original file.

You can automatically generate thumbnails for supported file types with options provided by Content Server. For more information about thumbnail configuration options, see [Section A.1.5, "Configure Thumbnail Options Screen."](#)

Content Server provides a basic set of thumbnail creation options. Oracle WebCenter Content: Inbound Refinery provides a more extensive set of options for file conversion and thumbnail generation. For more information, see *Oracle WebCenter Content Administrator's Guide for Conversion*.

2.4 Managing Content and Revisions

The Repository Manager is used to manage content items, revisions, subscriptions, and the Indexer. To access the Repository Manager as an applet, choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager**. Repository Manager can also be run in standalone mode. For more details, see [Section 1.3.4, "Running Administration Applications in Standalone Mode."](#)

Use the Functions menu of the Repository Manager to perform a variety of administrative functions on specific revisions. For example, you can check in, check out, view and update metadata, approve and reject revisions in a workflow, and delete revisions. Right-click a revision when displaying the revisions with the filter to open a shortcut menu, which includes all of the options on the Functions menu.

This section covers these topics:

- [Section 2.4.1, "Managing the Content List"](#)
- [Section 2.4.2, "Managing Content"](#)
- [Section 2.4.3, "Managing Revisions"](#)

2.4.1 Managing the Content List

Administrators and subadministrators with RepMan rights can display a list of content item revisions in the Repository Manager. Administrators can display all content items; subadministrators with RepMan rights can display only content items for which they have Admin permission to the security group and account (if applicable). You can search the revision list by specifying metadata fields and revision status as filter criteria.

This section covers these topics:

- [Section 2.4.1.1, "Changing Column and Filter Settings"](#)
- [Section 2.4.1.2, "Changing Default Sort Order"](#)

2.4.1.1 Changing Column and Filter Settings

To filter the Content list by revision:

1. On the **Content** tab of the Repository Manager application, select the **Use Filter** check box, then click **Define Filter**.

The [Define Filter Screen](#) opens.

2. Select the check boxes for the filter criteria to use and add values for the fields.
3. Click **OK**.

To filter revisions by Release Date:

1. On the **Content** tab of the Repository Manager application, select **Release Date Since**.
2. Select a predefined date range.
3. Click **OK**.

To change the columns displayed on the Content tab:

1. On the **Content** tab of the Repository Manager application, click **Show Columns**.
The [Show Columns Screen](#) opens.
2. Select the columns to be displayed. Custom fields are at the bottom of the list.

3. Click OK.

2.4.1.2 Changing Default Sort Order

When the Repository Manager application is started, it runs a default query against the database that returns all content released the previous day. By default, the query sorts the results by the ContentID of the content items.

Ordering by ContentID is advantageous because the order is predictable when the Repository Manager has a long list of content items. But sorting by ContentID can take a long time to return the results. It may be preferable to have faster query results without the predictable order.

To change the order, disable the `DoDocNameOrder` configuration setting. When the value is set to true (the default), content items are sorted by ContentID. When set to false, content items are not sorted. When you change the sort order to optimize the query, enable the JDBC Query Trace to log trace information to the console log where you can view database queries.

To disable the `DoDocNameOrder` configuration setting:

1. In a text editor, open the `IntradocDir/config/config.cfg` file.
2. Add the following configuration setting:
`DoDocNameOrder=false`
3. Save and close the `config.cfg` file.
4. Restart Oracle WebCenter Content Server.

To enable Query Tracing:

1. Choose **Administration** then **System Audit Information** from the Main menu.
The System Audit Information page opens.
2. Scroll to the bottom of the **Edit Active Console Output Tracing** section.
3. Select **systemdatabase** from the Active Sections list.
The `systemdatabase` is added to the list of active sections.
4. Click **Update**.
5. Restart Oracle WebCenter Content Server.

See the *Oracle WebCenter Content System Administrator's Guide for Content Server* for more details about tracing reports and restarting Oracle WebCenter Content Server.

2.4.2 Managing Content

Several common tasks are done when managing content and revisions:

- [Section 2.4.2.1, "Adding a New Content Item"](#)
- [Section 2.4.2.2, "Managing Content Metadata with Repository Manager"](#)
- [Section 2.4.2.3, "Managing Expired Content with Repository Manager"](#)

2.4.2.1 Adding a New Content Item

To add a new content item using the Repository Manager:

Note: You cannot add new content items using the Repository Manager launched as a Java applet from a browser. Use the standalone application.

1. Start the Repository Manager in standalone mode. Click the **Content** tab.
2. Click **Add New**.
The [Add New Content Item Screen](#) opens.
3. Enter the required and optional information for the content item.
4. Click **OK**. The specified file is checked in as a new content item.

2.4.2.2 Managing Content Metadata with Repository Manager

To **view** the metadata for a revision using the Repository Manager:

1. Choose **Administration** then **Admin Applets** from the Main Menu. Click **Repository Manager** then the **Content** tab.
2. Highlight the revision for metadata review.
3. Choose **Functions** then **Info** or right-click and click **Info**.
The [Approve Revision Screen](#) opens.
4. Click **OK** to close the screen.

To **update** the metadata for a revision using the Repository Manager:

1. Choose **Administration** then **Admin Applets** from the Main Menu. Click **Repository Manager** then the **Content** tab.
2. Select the revision to update.
3. Choose **Functions**, **Update**, or right-click and select **Update**.
The [Update Content Info Screen](#) opens.
4. Enter new metadata as necessary.
5. Click **OK**.
The metadata is updated without checking in a new revision.

2.4.2.3 Managing Expired Content with Repository Manager

To **review** expired content from Repository Manager:

1. Choose **Administration** then **Admin Applets** from the Main Menu. Click **Repository Manager** then the **Content** tab.
2. From the **Content** tab, select **Define Filter**.
The [Define Subscription Filter Screen](#) opens.
3. Select **Enable Revision Status**, and select **Expired**.
A list of expired content is displayed.

To automate e-mail notification for the author and administrator when the content expires:

1. Edit `IntradocDir/config/config.cfg` in a text editor and enter the following:
`EnableExpirationNotifier=1`

2. Adjust optional configuration entries which are described in detail the *Oracle WebCenter Content Idoc Script Reference Guide*:
 - `NotificationQuery`: Defines the criteria for the automatic query that searches for expired content.
 - `NotifyExtras`: Defines the users who receive a list of expired content.
 - `NotificationIntervalInDays`: Defines how often a notification query is run.
 - `NotifyTime`: Defines the time of day the query is run.
 - `NotificationMaximum`: Defines the maximum number of content items to be returned by the query.

By default, an e-mail message is sent to the administrator at midnight, seven days before a piece of content is set to expire. And, an *Expired Content* link is added for the author and system administrator on their respective Content Management trays.

3. Restart Oracle WebCenter Content Server.

2.4.3 Managing Revisions

A revision is a new or revised version of a content item. By default, revisions are numbered sequentially starting with Revision 1, and every time the content item is checked out and checked in again, the revision number is incremented by one and Oracle WebCenter Content Server creates a new revision of that file. The new revision has the same content ID as the previous revision, but the native file and the metadata can be the same or different. The system stores the previous versions of a file, which can be reviewed as necessary. This section covers the following topics:

- [Section 2.4.3.1, "Check In and Checkout a Revision"](#)
- [Section 2.4.3.2, "Undo a Checkout or Resubmit a Revision"](#)
- [Section 2.4.3.3, "Deleting Revisions"](#)
- [Section 2.4.3.4, "Managing Workflow Revisions"](#)

2.4.3.1 Check In and Checkout a Revision

Follow these steps to check in a new revision or check out a revision using the Repository Manager:

Note: These tasks must be performed using the standalone application.

1. Start the Repository Manager in standalone mode. Click the **Content** tab.
2. Select the item to be revised.
3. Click **Functions** then **Add Revision** or **Check Out**. You can also right-click and choose the appropriate option.

The [Add New Revision Screen](#) or [Check Out Item Screen](#) opens.

4. Enter the information for the revision to be checked in.
5. Click **OK**.

2.4.3.2 Undo a Checkout or Resubmit a Revision

Follow these steps to undo a checkout or resubmit a revision using the Repository Manager:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager** then the **Content** tab.
2. Select one or more revisions to use.
3. Choose **Functions** then **Undo Check Out** or **Resubmit**. You can also right-click and select the appropriate option.
The appropriate screen opens.
4. To exclude a revision from the list, clear the check box next to the revision.
5. Click **OK**.

2.4.3.3 Deleting Revisions

To delete a **particular revision** using the Repository Manager:

1. Choose **Administration** then **Admin Applets**. Click **Repository Manager** then the **Content** tab.
2. Select one or more revisions to delete.
3. Click **Delete Revision**. You can also choose **Functions** then **Delete Revision** or right-click and select **Delete Revision**.
The [Delete Revision Screen](#) opens.
4. To exclude a revision from the list, clear the check box next to the revision.
5. Click **OK**.

To delete **all revisions** of a content item follow the same steps, choosing **Delete All Revisions** from the appropriate menus.

2.4.3.4 Managing Workflow Revisions

A workflow specifies how content is routed for review and approval before it is released to the system. Users are notified by e-mail when they have a file to review.

From a workflow participant's point of view, there are two types of workflows:

- A **basic** workflow defines the review process for specific content items, and must be initiated manually.
- In a **criteria** workflow, a file enters the workflow automatically upon check in when its metadata matches predefined criteria.

When you approve a workflow revision using the Repository Manager, you bypass any approval steps in the workflow. The workflow may complete normally, but bypassing approval steps can have unanticipated consequences. For example, if a workflow step requires an electronic signature and you approve the associated revision through the Repository Manager, there will be no record of an electronic signature, even though the workflow completes and the revision is approved.

Note: Be sure you understand the consequences of approving a workflow revision using the Repository Manager before doing so.

For more information about electronic signatures, see [Section 2.5, "Signing Content Electronically."](#)

To approve or reject a revision in a workflow using the Repository Manager:

1. Choose **Administration** then **Admin Applets**. Click **Repository Manager** then the **Content** tab.
2. Select one or more revisions to approve.
3. Choose **Functions** then **Approve** or **Reject**. You can also right-click and choose **Approve** or **Reject**.
The appropriate screen opens.
4. To exclude a revision from the list, clear the check box next to the revision.
5. Click **OK**.

2.5 Signing Content Electronically

With the Electronic Signatures component (ElectronicSignatures), you can sign a content item with an electronic signature that uniquely identifies the contents of the file at a particular revision and associates the revision with a particular user.

Electronic signatures are used and managed in several different contexts:

- **Workflow:** You can specify that a particular step requires an electronic signature for approval.
Because electronic signatures are stored separately from both the content item and from its metadata, multiple users can sign a particular content item revision. For more information about using electronic signatures in workflow, see [Section 4.3.2, "Setting Up a Criteria Workflow."](#)
- **Content Item:** You can sign a content item electronically and compare a local file against a signed content item (or against all repository content) to see if the local file matches. For more information, see the *Oracle WebCenter Content User's Guide for Content Server*.
- **PDF Watermark:** You can apply a watermark that uses electronic signature metadata. For more information, see [Section 5.3.4, "Adding or Editing Templates."](#)

This section covers the following topics:

- [Section 2.5.1, "About Electronic Signatures"](#)
- [Section 2.5.2, "Custom Electronic Signature Metadata"](#)
- [Section 2.5.3, "Adding or Editing a Custom Electronic Signature Field"](#)

2.5.1 About Electronic Signatures

An electronic signature is a unique identifier computed from the binary content of a content item and associated with other metadata such as the name of the user who signs the content item. Unlike a digital signature, which uniquely identifies both the document and the signer and encrypts the information with the document, an electronic signature is not stored with the document.

When you check in a content item, Content Server generates the identifier and stores it with the revision metadata for the content item. When you "sign" a content item, a copy of the identifier is stored with the electronic signature metadata. When you check in a modified revision of the content item, a new identifier is calculated.

Content Server can compare the identifier stored with the content item to the identifier stored with the electronic signature to help you determine if a signed content item has changed and if existing signatures for a content item are valid.

Note: The identifier is computed from the content only, not the associated metadata. A change in the metadata for a content item does not invalidate the electronic signature for the content item.

Because electronic signatures are stored separately from both the content item and from its metadata, multiple users can sign a particular content item revision. For example, in a workflow approval process, multiple reviewers may sign a revision of a content item. For more information, see [Section 4.3.2, "Setting Up a Criteria Workflow."](#)

Any user with access to the Document Information page for a content item can sign the content item. For more information about signing a content item, see the *Oracle WebCenter Content User's Guide for Content Server*.

When using the Archiver with the Electronic Signatures component, make sure to use the table archive feature to move the ElectronicSignatures table. If archived content is restored without the associated signature metadata, errors can occur. For more information about archiving content, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

2.5.2 Custom Electronic Signature Metadata

When you sign a content item electronically, the signature includes standard metadata about the user, such as the user name and password, and metadata about the content item itself, such as the name (dDocName) and revision (dRevisionID). The Electronic Signature component also provides the xESigHasElectronicSignatures field which is automatically set to 1 (True) when a content item is signed.

You can define additional metadata fields that are stored as part of the metadata for the electronic signature. Electronic signature information is stored and managed in a separate ElectronicSignatures table in the database.

When you create a custom metadata field, you select a basic data type, and optionally specify a choice-list of comma-delimited values. You can also designate one or more fields as required fields. The fields you define are displayed when the user signs a content item and when the user displays detailed signature information about a content item. For more information about these windows, see the *Oracle WebCenter Content User's Guide for Content Server*.

2.5.3 Adding or Editing a Custom Electronic Signature Field

To create or edit a custom Electronic Signature field, perform the following steps:

Note: Consider your metadata requirements carefully before you create and use custom metadata fields. After you create a field (click **Save Changes**), you cannot change the field name, the data type, or the required status. To change these values, you must delete the existing field and create a new one. When you delete a custom field, any stored data associated with that field is deleted.

1. Click the **Administration** tray and click **Electronic Signatures**.

The [Electronic Signatures Configuration Screen](#) opens.

2. To add a new field, click the Add New Field icon (the green plus sign).
3. Specify an internal field **Name**. This is the field name in the data table.
Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). The name must start with a letter. Do not use special characters.
4. Specify a **Display Label**. This is the label displayed for the field on pages and dialogs.
5. Specify a data type. The default data type is **Text**.
For more information about the specific data types, see [Section A.1.7, "Electronic Signatures Configuration Screen."](#)
6. To specify a choice list for a field, select the check box in the associated **Choice List** column and specify the choices as a comma-delimited list of values.
 - Make sure the values match the data type selected for the field.
 - Values are displayed in the specified order on pages and in windows. The first value in the list is the default value.
 - To provide no default value, enter a space followed by a comma as the first value in the choice list.
7. To specify that the custom field is itself a check box, select **Checkbox**. A check box field is automatically designated a required field. The user must select the check box to complete the electronic signature. The Display Label field contains acknowledgement text to display next to the check box.
8. To specify that the user must supply a value in the associated field to complete the electronic signature, select **Required**.
9. Repeat steps 2 through 8 for each field you want to add.
10. Fields are displayed on pages and in windows in the order listed in this table. To change the order of one or more fields, select the check box next to the field or fields and use the Move Up and Move Down icons at the top of the table to move the fields up or down in the order.
11. To delete one or more field from the table, select the check box next to the field or fields and use the Delete Fields icon to remove the field or fields and all associated field data. Fields are not permanently deleted until you click **Save Changes**.
12. To commit the changes you made, click **Save Changes** then click **OK** on the confirmation window.

2.6 Subscribing to Content

A subscription is a function that notifies users by e-mail when a particular content item has been revised.

Note that an e-mail message buffer is 20000 bytes. If a large number of subscription e-mail notices are sent at one time (for example, 40 content items with 40 subscribers each), the buffer can be overloaded and the e-mail messages are not sent. The limit to the total size of a subscription notification e-mail sent is 1GB. The total number of subscription notification e-mails that can be included in one e-mail sent to n users is 1GB divided by the size of the subscription notification e-mail.

Tip: To change the subscription notification message, use Component Architecture to customize the following:

- `subscription_mail_subject` include (in `std_page.htm` file)
 - `wwSubscriptionMailSubject` string (in `ww_strings.htm` file)
 - `subscription_mail.htm` template
-
-

You can create subscriptions in two ways:

- **Basic subscription:** Users manually subscribe to individual content items. This type of subscription is predefined.
- **Criteria subscription:** Users can subscribe to a group of content items based on metadata criteria. Administrators can set up a Criteria subscription in two ways: with users or with aliases. If a subscription is set up with users, users can unsubscribe if they want. If aliases are used, users cannot unsubscribe.

You can subscribe to content items in two ways:

- **Open subscription:** Users voluntarily subscribe to a content item through a Basic or Criteria subscription.
- **Managed subscription:** An administrator assigns users and aliases to a particular subscription. If individual users are assigned, each user can unsubscribe if they want. If an alias is assigned, the users in that alias cannot unsubscribe.

2.6.1 Using Subscriptions

These are common tasks in managing subscriptions.

- [Section 2.6.1.1, "Adding or Editing a Criteria Subscription"](#)
- [Section 2.6.1.2, "Adding or Unsubscribing Users"](#)
- [Section 2.6.1.3, "Viewing Subscription Information"](#)
- [Section 2.6.1.4, "Deleting a Criteria Subscription"](#)

2.6.1.1 Adding or Editing a Criteria Subscription

To specify subscription criteria:

1. Choose **Administration** then **Admin Applets** from the Main menu. Select **Repository Manager** then the **Subscription** tab.
2. Click **Add**.

The [Add/Edit Subscription Type Screen](#) opens.

3. Enter the subscription information:

Important: If criteria fields are changed, all current subscriptions are deleted. Use care when working with this feature.

- **Name:** Name for the subscription.
- **Description:** A brief description.
- **Notifications:** If selected, enables e-mail notifications to users.

The `PrimaryWorkQueueTimeout` configuration variable sets the number of seconds until workflow and subscription notification e-mails are sent. For more information about configuration variables, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

- **Criteria fields:** To add fields, click **Fields**. The [Fields Screen](#) opens. Select the boxes of fields to be used as criteria for triggering the subscription. The values for these fields are set later when users are added.
4. Click **OK**. Confirm enabling the subscription.

2.6.1.2 Adding or Unsubscribing Users

Tip: If any of the users added to subscription do not have a correct e-mail address, notification fails. The system quits after it encounters five errors in the work queue log and does not notify the rest of the subscribers.

To add users to a Criteria subscription:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager** then the **Subscription** tab. Select the subscription to use.
2. Click **Subscribers**.
The [Users Subscribed Screen](#) opens.
3. Click **Add**.
The [Add Subscription Screen](#) opens.
4. Select **User** or **Alias** then click **Select**.
The [Select User Screen](#) or [Select Alias Screen](#) opens.
5. Choose the users or aliases to be subscribed. Click **OK**.
6. Set the values for the criteria fields specified earlier.
7. Click **OK**.

Follow these steps to unsubscribe a user:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager** then the **Subscription** tab. Select the subscription to use.
2. Select the revision to unsubscribe.
3. Click **Function** then **Subscribers**, or right-click and select **Subscribers**.
The [Subscribers Screen](#) opens.
4. Select the user alias to unsubscribe.
5. Click **Unsubscribe**.
A confirmation screen opens.
6. Click **OK**.

2.6.1.3 Viewing Subscription Information

To view subscription information for a revision using the Repository Manager:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager** then the **Subscription** tab. Select the subscription to use.
2. Select the revision to view the subscription information for.
3. Select **Functions, Subscribers**, or right-click and select **Subscribers**.
The [Subscribers Screen](#) opens.
4. To narrow the Subscriptions list:
 - a. Select the **Use Filter** check box.
 - b. Click **Define Filter**.
The Subscription Detail screen opens.
 - c. Enter the filter criteria.
 - d. Click **OK**.
5. To view all subscription details for a particular user or alias, select the user or alias and click **View Details**.
The Subscription Detail screen opens.

2.6.1.4 Deleting a Criteria Subscription

To delete a Criteria subscription:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager** then the **Subscription** tab. Select the subscription to use.
2. Select a subscription.
3. Click **Delete**.
A confirmation screen opens.
4. Click **Yes**.

2.7 Managing Linked Content with Link Manager

Link Manager is an optional component bundled with and automatically installed with Oracle WebCenter Content Server. If enabled, it evaluates, filters, and parses the URL links of indexed content items before extracting them for storage in a database table (ManagedLinks). After the ManagedLinks table is populated with the extracted URL links, the Link Manager component references this table to generate link search results, lists of link references for the Content Information page, and the resource information for the Link Info page. The Link Manager component enables users to:

- View lists of links using specific search criteria
- View detailed information about a specific link
- Recompute and refresh links to reevaluate and validate them
- View the links to other content in a specific content item
- View the links back to a specific content item.

The search results, link references lists, and Link Info pages are useful to determine what content items are affected by content additions, changes, or revision deletions. For example, before deleting a content item, you can verify that any URL references contained in it are insignificant. Another use might be to monitor how content items are being used.

The Link Manager component extracts the URL links during the indexing cycle, so only the URL links of released content items are extracted. For content items with multiple revisions, only the most current released revision has entries in the database table. If the Link Manager component is installed after content items are checked in, perform a rebuild to ensure that all links are included in the ManagedLinks table.

Link Manager does all of its work during the indexing cycle and it increases the amount of time required to index content items and to rebuild collections.

The amount of time required depends on the type and size of the content items involved. That is, if the file is converted, this requires more time than text-based (HTML) files.

For information about disabling Link Manager during the rebuild cycle, see `LkDisableOnRebuild` and `LkReExtractOnRebuild` in the *Oracle WebCenter Content Idoc Script Reference Guide*. For more information about file formats, conversion, and link extraction, see [Section 2.7.1, "The Link Extraction Process"](#) and [Section 2.7.1.1, "File Formats and Conversion."](#)

This section covers the following topics:

- [Section 2.7.1, "The Link Extraction Process"](#)
- [Section 2.7.2, "Configuring Link Manager"](#)
- [Section 2.7.3, "Site Studio Integration"](#)
- [Section 2.7.4, "Link Administration"](#)

2.7.1 The Link Extraction Process

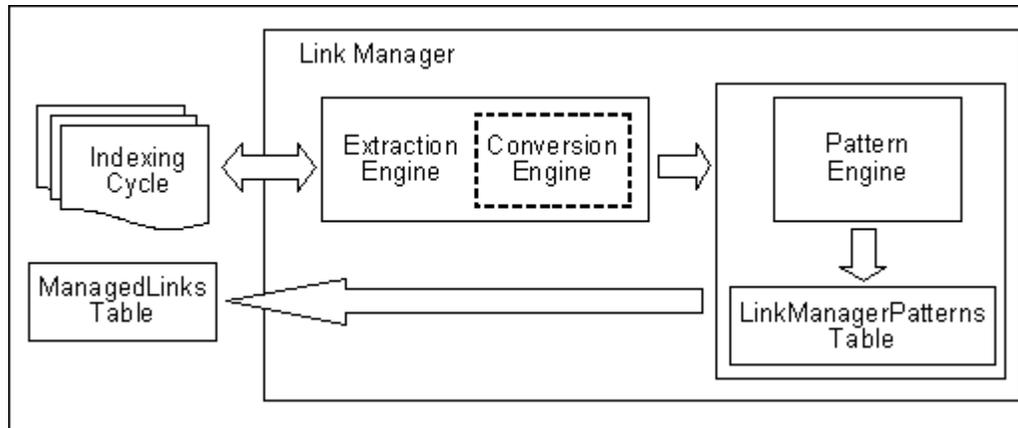
Caution: The Link Manager component uses `HtmlExport 8` for file conversion. A link extractor template file is included with the Link Manager component. `HtmlExport 8` requires this template. Do not edit this file.

The Link Manager consists of an extraction engine and a pattern engine. The extraction engine includes a conversion engine (`HtmlExport`). The conversion engine is used to convert files that the extraction engine cannot natively parse to a text-based file format (HTML).

Link Manager does not use `HtmlExport` to convert files that contain any of the following strings in the file format: `hcs`, `htm`, `image`, `text`, `xml`, `jsp`, and `asp`. These text-based files are handled by Link Manager without need for conversion.

During the indexing cycle, the Link Manager component searches the checked-in content items to find URL Links as follows:

1. The extraction engine converts the file using the conversion engine (if necessary).
2. The extraction engine then uses the pattern engine to access the link evaluation rules defined in the Link Manager Patterns table.
3. The evaluation rules tell the extraction engine how to sort, filter, evaluate, and parse the accepted URL links in the content items.
4. The accepted URL links are inserted or updated in the ManagedLinks table.



Important: To execute successfully, HtmlExport requires either a virtual or physical video interface adaptor (VIA). Most Windows environments have graphics capabilities that provide HtmlExport access to a frame buffer. UNIX systems, however, may not have graphics cards and do not have a running X-Windows Server for use by HtmlExport. For systems without graphics cards, you can install and use a virtual frame buffer (VFB).

2.7.1.1 File Formats and Conversion

Various file formats (such as Word) must be converted by the conversion engine (HtmlExport) before links can be extracted. Because Link Manager can extract links in text-based files (HTML) without requiring conversion, Link Manager does not use HtmlExport to convert files that contain any of the following strings in the file format: hcs, htm, image, text, xml, jsp, and asp.

Link Manager also handles all the variations of these file formats. For example, the hcs string matches the dynamic server page strings of hcst, hcsp, and hcsf. The image string matches all comparable variants such as image/gif, image/jpeg, image/rgb, image/tiff, and so on. To prevent other types of files from being converted, use the `LkDisallowConversionFormats` configuration variable. For more information, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

Link Manager recognizes links in the following file formats:

- Text-based formats (txt, html, xml, jsp, asp, csv, hcst, hcsf, and hcsp)
- E-mail (msg and eml)
- Microsoft Word
- Microsoft Excel
- OpenOffice Writer
- OpenOffice Calc

2.7.1.2 Link Status

All new and existing links are managed during the indexing cycle. When content items are checked in, the accepted links in the content items are added to or updated in the Managed Links table. Existing links are evaluated for changes resulting from content items being checked in or deleted. As links are added or monitored, they are marked as valid or invalid.

When one content item in the system references another content item in the system, the resulting link is marked as valid. When an existing link references a deleted content item, the link is reevaluated and the status changes from valid to invalid. Statuses are recorded as Y (valid) or N (invalid) in the *dLkState* column of the Managed Links table and displayed for the user in the *State* column of the Link Info page as *Valid* or *Invalid*.

2.7.2 Configuring Link Manager

You can specify the following Link Manager configuration variables in the *IntradocDir/config/config.cfg* file:

- AllowForceDelete
- HasSiteStudio
- LkRefreshBatchSize
- LkRefreshErrorsAllowed
- LkRefreshErrorPercent
- LkRefreshErrorTHreshold
- LkDisableOnRebuild
- LkDisallowConversionFormats
- LkReExtractOnRebuild
- LkIsSecureSearch

See the *Oracle WebCenter Content Idoc Script Reference Guide* for details about using these configuration variables.

2.7.2.1 Link Patterns

The Link Manager component uses an extraction engine that references the link patterns defined in a resource table. These link patterns are rules that tell the extraction engine how to sort the different links, which links to filter out, which links to accept, and how to parse the links for more information.

To customize the *DomainHome/ucm/LinkManager/resources/linkmanager_resource.htm* resource table, you can add new rules or edit the existing default rules. Customize the table using standard component architecture. The table includes the following columns:

Column Name	Description
lkpName	The name of the pattern and the primary key of the table. Used mainly in error handling and to allow other components to directly target the override of a specified rule.
lkpDescription	An explanation of the purpose of the pattern.

Column Name	Description
lkpType	<p>The initial screening of the URL:</p> <ul style="list-style-type: none"> Prefix: If the path begins with a specified parameter, the condition is met. Contains: If the path contains a specified parameter, then the condition is met. Service: If the URL contains a value for IdcService and if this value matches a parameter, the condition is met. <p>The extraction engine is a two-step engine. The 'prefix' and 'contains' types are used on the path part of the URL, while the 'service' type is used on the query string part of the URL.</p>
lkpParameters	<p>A comma-delimited list of patterns or parameters used by the type. The parameters are Idoc Script capable and are initially evaluated for Idoc Script. The engine uses the following rules for extracting the patterns from the parameters:</p> <ul style="list-style-type: none"> The parameter string is evaluated for Idoc Script. The parameters are parsed using the comma separator. The result is a list of patterns. Each pattern is XML decoded. <p>One rule looks for a URL that begins with the resolved value for <code><\$HttpRelativeWebRoot\$></code> by setting <code>lpkParameters</code> to <code><\$HttpRelativeWebRoot\$></code>.</p> <p>A later rule can look for a URL that literally begins with <code><\$HttpRelativeWebRoot\$></code> by setting the parameter to <code>&lt;\$HttpRelativeWebRoot\$&gt;</code>.</p>
lkpAccept	<p>Determines if the URL is accepted if the pattern is matched:</p> <ul style="list-style-type: none"> Pass: No determination is made. The 'action' is used to determine how this URL is processed. Filter: the URL is rejected. This value is usually combined with <code>lkpContinue=false</code> to stop the processing. Accept: The URL is accepted.
lkpContinue	<p>Determines if the pattern processing engine continues to parse the URL. If true, the processing continues. If false, processing stops.</p>
lkpLinkType	<p>Specifies the URL type determined for this link.</p>
lkpAction	<p>A function defined in the LinkHandler class referring to a method in the LinkImplementor class used to further parse and evaluate the URL.</p> <p>LinkImplementor can be class aliased or extended.</p>
lkpOrder	<p>The order in which the patterns are to be evaluated.</p>
lkpEnabled	<p>Determines if this rule is evaluated. It is calculated and evaluated during start up when the patterns are loaded.</p>

You can add new rules or edit the existing default rules using standard component architecture.

2.7.2.2 Database Tables

Two database tables are maintained with Link Manager:

- Managed Links Table: A link is stored in the Managed Links table if the pattern engine successfully processes it and determines that the link is acceptable. Each link in the table is assigned a unique class id (`dLkClassId`) and each row in the

table has a unique GUID (dLkGUID). A single link can consist of multiple rows in the table if multiple resources define the link and each resource can independently break the link.

For example, in Site Studio, you can define a single link by both a node and a content item. If the node is missing, the link breaks. If the content item is missing, the link breaks. In this case, there are two resources that do not depend on each other and each can break the link. Consequently, each resource is managed separately in the ManagedLinks table. For additional information about Site Studio links, see [Section 2.7.3, "Site Studio Integration."](#)

To improve query execution performance, standard indexes are added to the dDocName and dLkResource columns in the Managed Links table. System administrators are responsible for adjusting these indexes to accommodate specific database tuning requirements in various system environments.

- **Link Reference Count Table:** This table maps the content items to the number of times each is referenced in the ManagedLinks table. A content item in this table might not be a content item that is currently managed by Oracle WebCenter Content Server. If there is an entry for a content item in this table, it only indicates that a link in the ManagedLinks table, as parsed by the pattern engine, has referenced the content item as a 'doc' resource.

When a content item is checked in and a link references it, the link is marked as valid. When a link references a deleted content item, the link is marked as invalid. Notice that the dLkState column indicates the link's status as Y (valid) or N (invalid).

2.7.2.3 Link Manager Filters

The Link Manager component provides filters for parts of the pattern engine that allow customization of some very specific behavior. In general, the rules of the pattern engine are usually the ones to be modified. In certain circumstances Link Manager explicitly creates and uses filters to augment its standard behavior.

- **extractLinks Filter:** Used during the extraction process when the extraction engine parses the accepted URL links. As links are extracted, Link Manager looks for specific HTML tags. However, other HTML tags might also contain relevant links. If so, use this filter to extract the additional links.

The tag is passed to the filter as a cached object with the key HtmlTag. The value (or link) is passed back to the parse with the key HtmlValue. If the filter extracts extra information, be aware that the passed-in binder is flushed before being passed to the pattern engine. The service.setCachedObject and service.getCachedObject methods should pass and retrieve the extra information, respectively.

By default, it looks for the following HTML tags: <a>, <link>, <iframe>, , <script>, and <frame>.

- **linkParseService Filter:** Used during the extraction process when the pattern engine evaluates links that use the IdcService parameter. After evaluation, the link binder and service are provided for the linkParseService filter.

The service contains the binder for the parsed URL and information map. Customize the values in the parsed URL binder by adjusting certain parameters or customize the information map (which tells the parseService method what parameters to extract from the URL binder and how to map the data to resource types).

- `sortAndDecodeLinks` filter: Only available from the 'refresh' option. It is only called when users are refreshing the links. The service contains the 'LinkSetMap' which includes a sorted list of links contained in the ManagedLinks table. The refresh validates the Site Studio links and the existence of all links referring to 'doc' resources. You can create a component that augments the standard validation.

2.7.3 Site Studio Integration

Important: When using Site Studio, set the `HasSiteStudio` configuration variable value to true. This variable enables the Site Studio-specific patterns for parsing 'friendly' URLs for the pattern engine. For more information about the `HasSiteStudio` variable, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

When configured to work with Site Studio, Link Manager obtains links from Site Studio by directly requesting a parsing of the links that Site Studio has identified. In return, Site Studio provides information about the links pertaining to its operation and components. In particular, Site Studio provides information about the node/section, if a content item is used, the state of the content item, the type of link (friendly, page, or node), and if the link is valid.

Site Studio does not load its project information when the Standalone applications are launched. Therefore the Site Studio links are not properly evaluated if a rebuild or index update cycle is started and completed by a standalone application.

When a user changes links using the Site Studio designer, Link Manager checks filter events. If a node is deleted, Link Manager marks all links using the deleted node as invalid, thus managing links that directly reference the node ID. Additionally, with information provided by Site Studio, Link Manager can accurately determine the state of the link.

Friendly URLs (links that do not reference the node ID or `dDocName`) are more difficult to manage and validate. When a node property changes, Link Manager marks all friendly links (both relative and absolute) that use the node as invalid and broken. Link Manager cannot retrace the parent chain to determine what part of the link was changed, how to fix it, or determine if it is actually broken.

Site Studio uses two types of managed links:

- **Completely Managed Links:** These are any links using the `SS_GET_PAGE` `IdcService` or links to nodes that include the following:
 - `javascript:nodelink(Node,Site)`
 - `javascript:nodelink(Node)`
 - `ssNODELINK/Site/Node`
 - `ssNODELINK/Node`

Also links to pages that include the following:

- `ssLINK/Doc`
- `ssLINK/Node/Doc`
- `ssLINK/Site/Node/Doc`
- `ssLink(Doc)`

- ssLink(Doc,Node)
- ssLink(Doc,Node,Site)
- javascript:link(Doc)
- javascript:link(Doc,Node,Site)
- Provisionally Managed Links: The following Site Studio links are managed up to Site Studio node changes. Use the 'refresh' option from the [Managed Links Administration Page](#) to determine state of the links. If the majority of links are of this form and nodes have changed dramatically, you should refresh or recompute the links.
 - Absolute (or full URLs): http://site/node/doc.htm
 - Friendly links to nodes
 - <!--\$ssServerRelativeSiteRoot-->dir/dir/index.htm
 - [!--\$ssServerRelativeSiteRoot--]dir/dir/index.htm
 - <%=ssServerRelativeSiteRoot%>dir/dir/index.htm
 - Friendly links to pages
 - <!--\$ssServerRelativeSiteRoot-->dir/dir/doc.htm
 - [!--\$ssServerRelativeSiteRoot--]dir/dir/doc.htm
 - <%=ssServerRelativeSiteRoot%>dir/dir/doc.htm

2.7.4 Link Administration

This section covers the following topics:

- [Section 2.7.4.1, "Alternative Refresh Methods"](#)
- [Section 2.7.4.2, "Recomputing and Refreshing Links in the ManagedLinks Table"](#)

2.7.4.1 Alternative Refresh Methods

In addition to the refresh activities available on the [Managed Links Administration Page](#), you can use alternative methods to update the Managed Links and Link Reference Count tables:

- Using the Repository Manager, perform a collection rebuild. This process rebuilds the entire search index, and the old index collection is replaced with a new index collection when the rebuild successfully completes.

If Repository Manager is opened as a standalone application, the alternate refresh method can only be used when the `HasSiteStudio` configuration variable is disabled. When information is requested from Site Studio and the Repository Manager is in standalone mode, Site Studio is not initialized completely and does not return accurate information. This issue does not occur if the Repository Manager applet is used.

- If custom fields have been added while content is in the system, use the Configuration Manager **Rebuild Search Index** to rebuild the search index.

2.7.4.2 Recomputing and Refreshing Links in the ManagedLinks Table

Use this method to reevaluate the links in the ManagedLinks table:

1. Choose **Administration** then **Managed Links Administration** from the Main menu. The [Managed Links Administration Page](#) opens.

2. Use an option to manage links:

- To recompute links: Click **Go** next to the Recompute links option. This refresh activity resubmits each link in the ManagedLinks table to the patterns engine. The link is evaluated according to the pattern rules and updated in the table. A link can be reclassified as another type of link depending on which patterns have been enabled or disabled. Use this option if the pattern rules have changed.

- To refresh links: Click **Go** next to the Refresh links option. This activity checks each link in the ManagedLinks table and attempts to determine if the link is valid. For Site Studio links, the links are sent to the Site Studio decode method to determine what nodes and content items are used by the link. It also determines if the link is valid and is indeed a Site Studio link.

Use this option after many changes to Site Studio node/section properties. LinkManager cannot completely track the changes to 'friendly' Site Studio links. By refreshing or forcing a validation on the links, Link Manager can more accurately determine which links are broken and which are valid.

- To refresh the references counts: Click **Go** next to the Refresh option. This activity flushes the LinkReferenceCount table and queries the ManagedLinks table for the content item references. Both the 'recompute' and 'refresh' table activities try to maintain the LinkReferenceCount table. However, on occasion, this table can become out-of-sync and this option, when used on a quiet system, rebuilds this table.
- To cancel a refresh activity: Click **Go** next to the Abort activity option. Only one refresh activity can be active at any one time.

The Status area indicates how many links have been processed and how many errors have been encountered.

Only one refresh activity can be active at any one time. Wait until the refresh activity completes and the 'Ready' status is displayed before attempting another refresh activity.

Managing Schemas and Profiles

This chapter discusses managing repository metadata with schemas, rules, and profiles. You can create metadata schemas to manage dependent lists that are localized for specific sites. You can create content profiles to customize what metadata fields appear on different screens.

This chapter discusses the following topics:

- [Section 3.1, "Using Schemas to Customize Metadata"](#)
- [Section 3.2, "Using Profiles to Customize Content Screens"](#)

3.1 Using Schemas to Customize Metadata

To create custom metadata fields that present a list of values, use the **Information Fields** tab of the Configuration Manager. You can also make the associated list dependent on the value of another field. This organization is called a *dependent choice list* (DCL).

For example, assume there are Country and State information fields. The country you select determines the choices available in the State list.

You can also use metadata schema mapping to create field lists. With metadata schema mapping, you can easily adjust option list views to accommodate localization requirements.

This section covers these topics:

- [Section 3.1.1, "Schema Structure"](#)
- [Section 3.1.2, "Creating Schemas"](#)
- [Section 3.1.3, "Schema Example: Dynamic Lists"](#)
- [Section 3.1.4, "Schema Example: Recursive Table for Multiple Trees"](#)

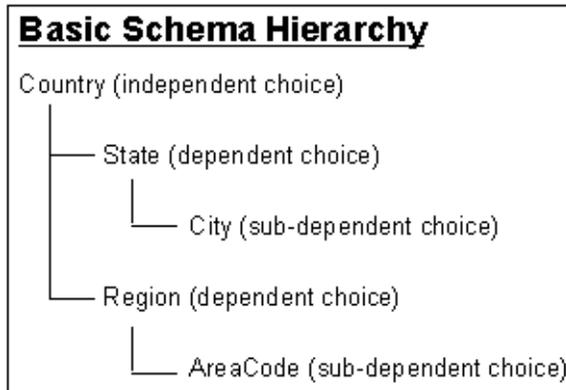
3.1.1 Schema Structure

A *schema* is a collection of related schema objects. The term *schema* also refers to a graphical depiction of the database hierarchy that is created to support the Oracle WebCenter Content Server metadata schema mapping feature. The schema hierarchical structure consists of tables and their respective columns (or fields), views of the data, and the relationships between them.

Let's add City, Region, and Area Code information fields to the Country and State example to illustrate a three-tiered dependency structure.

In [Figure 3-1](#), the sample basic schema hierarchy, one independent field has two dependent fields. Each dependent field also has a dependent field. These dependencies are also referred to as *Parent/Child relationships*.

Figure 3-1 Basic Schema Hierarchy Example



This three-level schema hierarchy produces five distinct metadata fields: **Country**, **State**, **City**, **Region**, and **Area Code**. Each field presents a specific list to the user.

The contents of the lists are contingent on whether the information field is dependent or not. Thus, the following lists result from the sample basic Country/State/Area Code schema hierarchy:

- The Country list is independent and the choices remain constant.
- The choices available in the State list are variable and depend on which country the user selects from the Country list.
- The choices available in the City list are variable and depend on which state the user selects from the State list.
- The choices available in the Region list are variable and depend on which country the user selects from the Country list.
- The choices available in the Area Code list are variable and depend on which region the user selects from the Region list.

Schemas are comprised of [Tables](#), [Views](#), and [Relationships](#), as discussed in the following sections.

3.1.1.1 Tables

Schema tables are database tables that store the choices displayed in information field (metadata) lists. Tables and their columns are created using the **Tables** tab of the Configuration Manager. You can have multiple columns in each table but at least two are essential for producing dependent choice lists:

- The common column name used to create the dependency between one list and a second list that is dependent on the choice made from the first (for example, Country and State, respectively).
- The column that stores the choices for metadata lists.

Figure 3–2 Schema Tables Example

Schema Tables				
Country	State	City	Region	AreaCode
countryID	stateID	cityID	regionID	areacodeID
countryName	countryID	stateID	countryID	regionID
	stateName	cityName	regionName	areacode

Using the geographical example (Country, State, City, Region, Area Code) in the three-tiered schema hierarchy, a table must be created for each *branch* in the schema tree structure. Additionally, the dependent tables (child tables) must contain a column that corresponds to an identical column in the table to which it is subordinate (the parent table). These corresponding columns are used to create the dependencies between the two tables and are ultimately used to generate the dependent choice lists.

For example, the tables in [Figure 3–3](#) illustrate how the Country and State table columns might be populated. The data in each **name** column provides the choices available on the lists. The relationship that is created between the corresponding columns in the Country and State tables (countryID) determines what choices are displayed in the State metadata list.

Figure 3–3 Populated Schema Tables

Country		State		
countryID	countryName	countryID	stateID	stateName
1	United States	1	1A	Minnesota
2	Canada	1	1B	Wisconsin
		2	2A	Manitoba
		2	2B	Ontario

3.1.1.2 Views

A view is a tailored presentation of the corresponding table. Views do not contain data, but they derive data from their tables. Views are used to simplify a database for use and to present data in a different perspective.

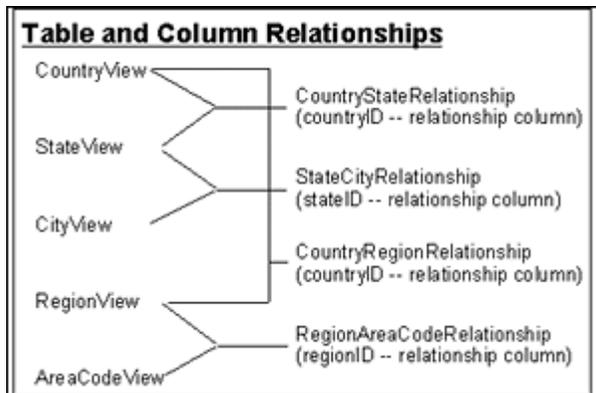
A view consists of a list of properties and associated display rules. Each table in the schema must have an associated view. Views provide information about these items:

- Specific columns in the table included in the schema. The selected columns are used to establish the dependencies between tables and also to generate the dependent choice lists.
- Internal and external column names.
- User interface display characteristics.
- Editing and sort order criteria.

3.1.1.3 Relationships

Relationships define the dependencies between tables and are essential in generating the appropriate dependent choice lists. Each defined relationship establishes the correspondence between parent and child tables. This correspondence is created by specifying the column in the child table that is dependent on the column in the parent table. Thus, the choices displayed using column data from the child table are contingent on the choice made from the corresponding column data from the parent table.

Figure 3–4 Table and Column Relationships



For example, in [Figure 3–4](#), the CountryView (Country table) and the StateView (State table) use the countryID column to create a relationship that generates a parent country list and a child state list. The choices available in the State metadata list are dependent on the choice made in the Country metadata list.

3.1.1.4 Schema Directory Structure

Three subdirectories are associated with the Schema function, located in the /weblayout/resources directory:

- schema
- schema.work
- schema.old

The schema.work directory is usually not listed because it is a temporary directory. When the schema creation process completes, the working directory is renamed. If this directory exists it indicates one of the following:

- A large schema rebuild is in progress
- The schema is created, but there is a problem with the schema structure.

Caution: If working inside the directory structure to review the Schema files and directories, be sure to close all open applications accessing these files. The directories are renamed on completion of processing. However, if external applications, such as text editors, are using these files the schema.work directory cannot be renamed.

3.1.1.5 Sample Schema-Based Lists

After the schema tables, views, and relationships are created and properly established, the lists display the appropriate choices. For example, in [Figure 3–5](#), the Country list now displays two choices: United States and Canada.

Figure 3–5 List Example

Because the State metadata field is contingent on the Country field, the State list contains items based on the choice made in the Country list. In this case, if the United States choice is selected, the State list displays Minnesota and Wisconsin as choices. If Canada had been selected, then the State list would display Ontario and Quebec.

Figure 3–6 Dependent List Example

3.1.2 Creating Schemas

The **Tables**, **Views**, and **Relations** tabs in the Configuration Manager are used to create the schema structure.

- The **Table** tab is used to select or create the database tables.
- The **Views** tab is used to manipulate the views used in the schema.
- The **Relations** tab is used to manipulate the dependencies.

The **Information Fields** tab is used to create the metadata fields used on Oracle WebCenter Content Server pages. The metadata fields must be correlated to the tables and views to properly display the lists.

New or modified schemas are automatically updated during each scheduled publishing cycle. Because the default interval between each publishing cycle is set to four hours, immediate results for new or modified schemas are not visible. To adjust the interval between each publishing cycle, change the default value of the associated configuration variable. For more information, see [Section 3.1.2.6, "Modifying the Publishing Cycle Interval."](#)

This section provides an overview of a simple sequence using the applicable Configuration Manager tabs to create a schema structure.

This section covers the following steps in creating a schema:

- [Section 3.1.2.1, "Selecting Tables for the Schema"](#)
- [Section 3.1.2.2, "Creating the Schema View"](#)
- [Section 3.1.2.3, "Creating the Schema Relationships"](#)

- [Section 3.1.2.4, "Adding Metadata Fields"](#)
- [Section 3.1.2.5, "Enabling the Schema"](#)
- [Section 3.1.2.6, "Modifying the Publishing Cycle Interval"](#)

3.1.2.1 Selecting Tables for the Schema

To select tables for the schema:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Tables** tab.
The [Configuration Manager: Tables Tab Screen](#) opens.
2. To add tables to the schema, click **Add Tables** and select the tables to add to the schema from the [Select Table Screen](#). When creating a new table, click **Create Table**.

Important: You can use core system tables such as Revisions, Alias, Documents, and Users, but you cannot edit them (remove columns, alter column length, and so on.)

3. After you select tables, the [Create/Edit Table 'name' Screen](#) opens with Table Column names filled in.
4. Select the column to be used as a primary key to establish a dependency and select **Edit**. The [Add/Edit Column Screen](#) opens.
5. Select the box labeled Primary Key and click **OK**. Select **Add Recommended** to add recommended columns to the table.

Repeat these steps for all tables to be used in the schema. When finished, click **OK**.

3.1.2.2 Creating the Schema View

To create the schema view:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Views** tab.
The [Configuration Manager: Views Tab Screen](#) opens.
2. To create a view, click **Add** to open the [Add View Screen: Select Table Screen](#).
3. Select the table to use in the view and click **Next**. The [Add View Screen: Select Columns Screen](#) opens.
4. Choose the columns to include in the view, and click **Finish**. The [Add/Edit View Screen](#) opens.
5. Select a name for the view and add information for the description. Choose the internal column (name in the database) to use in the view and choose the visible column that is displayed to end users. You can specify a display expression (text and Idoc script) that is displayed in place of the actual field value. When done, click **OK**.
6. Repeat these steps for all tables to be included in the view.

3.1.2.3 Creating the Schema Relationships

To create the schema relationships:

1. After the tables and associated views are completed, click **Relationships** to establish the dependencies between tables and columns. A list of the currently existing schema relationships is displayed.
2. Click **Add** to set up a new schema relation. The [Add/Edit Relationship Screen](#) opens.
3. Enter the name of the relationship (for example, Country_State to indicate the relationship between the Country and the State tables). In the Parent Info box, select the table where the parent information resides (for example, the Country table) and the column to be used to establish the dependencies (for example, the countryID). Do the same for the Child Info field (for example, select State as the table name and countryID as the relationship).
4. Click **OK** when done. The new relationship is now displayed on the **Relations** list.

3.1.2.4 Adding Metadata Fields

The final phase in schema creation is to set up the metadata fields to use the columns and to configure them to use the Views and Relations created previously. For an overview of the procedure, see [Section 2.2.2, "Adding or Editing a Custom Field"](#) and [Section 2.2.4, "Defining an Option List."](#)

3.1.2.5 Enabling the Schema

After you configure the schema, the views, and the relationships, click the button on the Configuration Manager screen to update your database design. Click **Options** then **Publish Schema** from the Configuration Manager Page menu.

Republishing (updating) of schema takes place automatically based on these things:

- Existence of the data/schema/publishlock/publish.dat file.
- The internal schedule of automatic publishing times. For details on how to modify this schedule, see [Section 3.1.2.6, "Modifying the Publishing Cycle Interval."](#)
- How long it took to publish schema last time.

Do not select **Options** then **Publish Schema** unless it is necessary to see the new Content Type quickly. The system can be overloaded when large lists are republished.

3.1.2.6 Modifying the Publishing Cycle Interval

New or modified schemas are automatically updated during the automatic schema publishing cycle. However, by default, the interval between publishing cycles is set to four hours. New schemas or changes to existing schemas are not seen in the corresponding menu lists until the completion of the next publishing cycle. Adjust the publishing cycle interval by changing the value of the SchemaPublishInterval configuration variable.

To change the interval of schema publishing cycles:

1. In a text editor, open the IntradocDir/config/config.cfg file.
2. Add the following configuration variable and value:

```
SchemaPublishInterval=300
```

The value is specified in seconds. In this configuration example, the lists are republished every 300 seconds (that is, 5 minutes).

Note: Depending on the number of lists in addition to the size and complexity of each list, automatically republishing (updating) your schemas frequently can have a significant impact on your system's performance.

3. Save and close the config.cfg file.
4. Restart Oracle WebCenter Content Server to apply the changes.

The queries for schema publishing are cached for up to five minutes. Publishing more frequently does not retrieve new values until the current cache expires.

If a new value is added to a metadata field, that value is not displayed on the content item's Content Information page until the next publishing cycle is complete.

If one content item is checked in with a unique value in a dynamic list and a second item is checked in with the same value but using a different case, the value is treated as one value in the list. The case used is dependent on the database sorting scheme.

For more information about creating dynamic lists, see [Section 3.1.3, "Schema Example: Dynamic Lists."](#)

3.1.3 Schema Example: Dynamic Lists

Creating a *dynamic* list enables users to add values to metadata lists. For example, if a value exists in a list, users can select the value from the list. However, if it is a new value, users can enter the value into a text field and it becomes available as an option following the next publishing cycle.

To create a dynamic list, first create a view into the table in the database. The list values are pulled directly from the metadata columns where they are stored. As content items are checked in, revised, and removed, the list values change or are updated accordingly.

The following is an example of creating a dynamic list:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Information Field** tab.
The [Configuration Manager: Information Field Tab Screen](#) opens.
2. Click **Add**.
The [Add Metadata Field Name Screen](#) opens.
3. Enter the name of the metadata field that has the dynamic list. For example, TestMetadata.
4. Click **OK**.
The [Add/Edit Metadata Field Screen](#) for TestMetadata opens.
5. Complete the fields as necessary but do not select **Enable Option List**.
6. Click **OK**.
The screen closes and the Field Info list on the [Configuration Manager: Information Field Tab Screen](#) shows the added metadata field.
7. Click **Update Database Design**.
The [Update Database Design Screen](#) opens and lists the TestMetadata field to add.
8. Click **OK**.

9. Open the [Configuration Manager: Views Tab Screen](#) and click **Add**.
The [Add View Screen: Select Table Screen](#) opens.
10. Click **Add Table**.
The [Select Table Screen](#) opens.
11. Select the **DocMeta** table.
12. Click **OK**.
The [Select Table Screen](#) closes and the DocMeta table is added to the Tables list on the [Add View Screen: Select Table Screen](#).
13. Click **Next**.
The [Add View Screen: Select Columns Screen](#) with column names opens.
14. Select the column to use to create the list for TestMetadata.
15. Click **Finish**.
The [Add/Edit View Screen](#) page opens.
16. Enter a view name. For example, `TestMetadata_view`.
17. Click **OK**.
18. Open the **Information Fields** tab on the [Configuration Manager: Information Field Tab Screen](#) and select TestMetadata.
19. Click **Edit**.
The [Add/Edit Metadata Field Screen](#) for TestMetadata opens.
20. Select **Enable Option List**.
21. Click **Configure**.
The [Configure Option List Screen](#) for TestMetadata opens.
22. Select **Edit and Select List** from the Option List Type list.
23. Click **Use View** and select a view from the list. For example, `TestMetadata_view`.
24. Click **OK**.
The [Configure Option List Screen](#) closes.
25. Click **OK**.
The [Add/Edit Metadata Field Screen](#) closes.
26. Select **Publish schema** from the Options menu on the [Configuration Manager: Information Field Tab Screen](#).

Test this list by checking in a document and entering a value into the new dynamic metadata field. Initially, the list is empty because no documents have been checked in that contain data in the TestMetadata field. However, as documents are checked in with values entered in TestMetadata, the list includes the specified values.

3.1.4 Schema Example: Recursive Table for Multiple Trees

Creating a recursive table enables the use of the data for multiple schema trees.

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Information Field** tab.

- The [Configuration Manager: Information Field Tab Screen](#) opens.
2. Create a database table with two columns (`id`, `parent`):
 - a. Open the **Tables** tab and click **Create table**.
The [Create/Edit Table 'name' Screen](#) opens.
 - b. Enter the table name. For example, `TreeTest`.
 - c. In the Columns pane, click **Add**.
The [Add/Edit Column Screen](#) opens.
 - d. Enter the first column name (`id`) and its length. Click **OK**.
 - e. Enter the second column name (`parent`) and its length. Click **OK**.
 - f. Click **OK** to create the table.
 3. Create a view on the table that includes both columns:
 - a. Open the **Views** tab and click **Add**.
The [Add View Screen: Select Table Screen](#) opens.
 - b. In the Tables pane, select `TreeTest` and click **Next**.
 - c. In the Columns pane, select the `id` and `parent` check boxes and click **Finish**.
The [Add/Edit View Screen](#) opens.
 - d. Enter the view name. For example, `TreeTestView`. Add display, options, and security configurations as applicable.
Display tab: used to create rules for the relationship.
Option tab: used to establish the sort order and criteria for the data in the schema.
Security tab: used to define security rules for the schema.
 - e. Click **OK** to create the view.
 4. Create a relationship on the view:
 - a. Open the **Relations** tab and click **Add**.
The [Add/Edit Relationship Screen](#) opens.
 - b. Enter the relationship name. For example, `TreeTestRecursive`.
 - c. From the Parent Info table list, select `TreeTest` and in the corresponding column list, select `id`.
 - d. From the Child Info table list, select `TreeTest` and in the corresponding column list, select `parent`.
 - e. Click **OK** to create the relationship.
 5. Open the **Information Fields** tab and click **Add**.
The [Add Metadata Field Name Screen](#) opens.
 6. Enter the custom metadata field's name and click **OK**.
The [Add/Edit Metadata Field Screen](#) opens.
 7. Select **Enable Option List** and click **Configure**.
The [Configure Option List Screen](#) screen opens.

8. Click **Use Tree** and click **Edit Definition**.
The [Edit Tree Definition Screen](#) opens.
9. In the Building level pane: Select view for level1 list, select **TreeTestView**.
TreeTestView is entered as Level 1 in the Tree Definition pane.
10. In the Building level pane: Select relationship between the 1st and 2nd level list, click **TreeTestRecursive**.
TreeTestRecursive is added under TreeTestView in the Tree Definition pane.
11. In the Building level pane: Select view for level 2 list, click **TreeTestView (recursive to level 1)**.
TreeTestView (recursive to level 1) is entered as Level 2 in the Tree Definition pane and the **Select root** button is added.
12. Click **Select root**.
The Select Tree Root dialog opens.

3.2 Using Profiles to Customize Content Screens

Administrators can use Content Profiles to selectively include or reorder metadata fields to produce targeted Check In, Update, Content Information, and Search pages.

Content profiles do not create or modify any Oracle WebCenter Content Server tables. They are simply used as a type of filter for what information is displayed. All information for the Content Profile is stored in the *IntradocDir/data/profiles/document/* directory.

After you create a content profile, it is always active. You can disable the link on the user interface, but the profile rules remain functional unless the profile is deleted.

This section covers these topics:

- [Section 3.2.1, "Content Profile Elements"](#)
- [Section 3.2.2, "Content Profile Rules"](#)
- [Section 3.2.3, "Display Results of Reordered Metadata Fields"](#)
- [Section 3.2.4, "Managing Rules"](#)
- [Section 3.2.5, "Content Profile Triggers"](#)
- [Section 3.2.6, "Creating and Using Content Profiles"](#)
- [Section 3.2.7, "Content Profile Examples"](#)

3.2.1 Content Profile Elements

A profile is composed of rules and a trigger value, which are set up on the **Profiles** and **Rules** tabs of the Configuration Manager screen. Administrators can create multiple content profiles and all are available to the end user. For each profile, the end user has a distinct check-in page and search page available. Although all profiles are visible to all users, each user can configure their user interface to hide or display links to specified profiles.

Note: Documents cannot be associated with multiple profiles in the system.

Content profiles are composed of the following:

- **Rules:** A rule consists of a set of metadata fields that determine if fields are editable, required, hidden, excluded, or read-only based on their criteria when specific conditions are met. You can change a rule's behavior based on an input, or *activation condition*. You can evaluate a rule for every profile (*global*), or you can evaluate the rule for specific profiles. For ease of use, you can use rules to group metadata fields under an optional header.

For example, a profile's rules can determine the user type and, depending on the document type being checked in, ensure that only specific metadata fields are displayed. Rules must be established before a profile is created.

- **Triggers:** A *trigger field* is a metadata field that is defined on the [Configuration Manager: Profiles Tab Screen](#). If a document matches a *trigger value* for a profile, then that profile is evaluated for the document. There can be an unlimited number of profiles, but only one trigger value per profile.

Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

3.2.1.1 Using a Profile Link

When a profile is enabled on the Edit Content Profile Links page, the profile is available from the Search and New Check In menus on the toolbar. If no profiles are enabled for display, the Search and New Check In menus become direct links to the Advanced Search page and standard Content Check In Form, respectively.

After a profile has been created, it appears in the Search and New Check In menus on the toolbar after refreshing the browser session. By default, all profiles are listed as options under both menus. However, not every user is authorized to use all of the listed profiles. On the Edit Content Profile Links page, select or clear applicable check boxes to specify the profiles to display.

For example, a marketing employee does not have the necessary privileges to use an accounting profile. In this case, the user can clear the check boxes for the accounting profile and it does not display under Search and New Check In menus. For more information about the user interface in general and the content profile links in particular, see the *Oracle WebCenter Content User's Guide for Content Server*.

3.2.2 Content Profile Rules

Note: Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

A profile consists of one or more rules and a trigger value. The rules determine how metadata fields are displayed on the Check In, Update, Content Information, and Search pages and if a rule is used (depending on how it is evaluated). Each rule consists of the following:

- A set of metadata fields. See [Section 3.2.2.1, "Metadata Fields and Attributes in Rules."](#)
- An optional activation condition. See [Section 3.2.2.2, "Activation Conditions in Rules."](#)
- An option that indicates if it is a global rule and has a specified priority.

- An option that indicates if the metadata fields in the rule are grouped and if an optional header is used.

Global rules are always 'on' (always evaluated). A global rule automatically affects the metadata fields displayed on the Check In, Update, Content Information, and Search pages even if it is not included in a profile or even if no profiles have been created. It is not necessary for a profile to exist in the system for any defined global rules to take effect and be applied to events, actions, or workflow states. However, you cannot preview the effects of a global rule unless it is associated with a profile.

Global rules are evaluated first and can be superseded by specific profile rules. The priority for the global rule can be set to increase its precedence. It can then have a higher priority than specific rules and produce different profile results. View those results by previewing the profile and seeing the consequence of rule selection.

A global rule obeys the following guidelines:

- It is always on, is independent of a profile, and is always evaluated.
- For documents and searches with profiles, the global rule is evaluated first. The specific profile rules are evaluated after the global rule. Global rules have a lower priority than profile rules.
- Global rules have a priority number. The priority determines the order in which the rule is evaluated. Lower priority rules are executed earlier and rules with higher priority can override changes made by rules with lower priority.

This section covers these topics about rules:

- [Section 3.2.2.1, "Metadata Fields and Attributes in Rules"](#)
- [Section 3.2.2.2, "Activation Conditions in Rules"](#)
- [Section 3.2.2.3, "Restricted Lists in Rules"](#)
- [Section 3.2.2.4, "Regular Expressions"](#)
- [Section 3.2.2.5, "Using Rules to Group Metadata Fields"](#)

3.2.2.1 Metadata Fields and Attributes in Rules

Each metadata field in a rule has the following attributes:

- **Field position** (required): Adjusts the general placement order of the metadata field. Values are *top*, *middle*, and *bottom*.
- **Display type** (required): Determines how the metadata field is displayed on the Check In and Search pages. Values can be *Edit*, *Info Only*, *Hidden*, *Excluded*, or *Required*. If required, a message is also required.
- **Use Default value** (optional): Displays a default value for the metadata field.
- **Is Derived value** (optional): Enables the metadata field to be set to a specified value on update or check in.
- **Has Restricted list** (optional): Allows the list metadata field to be restricted to either a specific list of values or to a filtered list of values.

3.2.2.2 Activation Conditions in Rules

An activation condition allows a change in the profile behavior based on different inputs. For example, a rule is not active for the search page or for a contributor, or certain fields are hidden or overridden on check in. Also, because profiles are activated during any check-in process, distinctions are made between a browser check in and a batch-load check in.

You can preview profiles to assess the validity of the activation conditions. The previewing screen is used to check the existing profile and perform what-if scenarios by changing activation condition choices and evaluating the results.

You can base an activation condition for a rule on:

- A system event: These include on-request events, on-submit events, and on-import events.
- A user action: These include check in new, check in selected, content information, content update, and search.
- A workflow state: These are contingent on if the content item is in a workflow.
- A document type: These can use components based on document metadata fields.
- A user type: These can use components based on user metadata fields.

Caution: Be very careful when using activation conditions that include one or more combinations of condition choices. Not all combinations of activation condition choices are valid and some can be mutually exclusive. For example, if an activation condition requires the event to be an import and the action to be a document information page request, the activation is never true and the rule is never active.

3.2.2.3 Restricted Lists in Rules

The restricted list is an optional attribute for a metadata field in a rule. You can modify the user interface for metadata fields defined as lists in two ways:

- Specifying a fixed list: An explicit set of values that override the actual master list for the metadata field that was defined as a list. Only those items in the master list are displayed in the user interface list.
- Using regular expression evaluation: The list can include wildcards and other special characters for string pattern matching and evaluation processes. The items displayed in the user interface list are those values satisfying the regular expression.

3.2.2.4 Regular Expressions

Regular expressions are ideal for text manipulation and describe the format of strings. In its simplest form, a regular expression specifies the text to match.

For example, the regular expression 'ABC' matches the string ABC but not the string DEF. You can use wildcard characters, such as the asterisk (*), to match more strings. The asterisk (*) specifies zero or more instances of the preceding character or characters. For example, the regular expression 'A*B' matches the strings B, AB, AAB, AAAB, and so on.

This section provides a brief overview of using regular expression evaluation to generate modified user interface lists. Because of the complexity of regular expressions, system administrators must be familiar with regular expressions, building patterns, and implementing regular expression methods. If not, use Oracle Consulting Services to assist in defining restricted lists.

The following table lists the most commonly used modifiers, metacharacters, and special characters used in building patterns for regular expression evaluation.

Modifiers

Element	Definition
g	Global pattern matching.
i	Case-insensitive pattern matching.
m	Allows the special characters ^ and \$ to match multiple times within a string.
s	Allows the special character . to match newlines.
x	Ignores whitespace within a pattern.

Metacharacters

Element	Definition
\s	Matches whitespace (including tabs and newlines).
\S	Matches anything that is not whitespace.
\b	Matches only a word boundary.
\B	Matches only nonword boundaries.
\d	Matches digits 0 through 9.
\D	Matches only nonnumeric characters.
\w	Matches only letters, numbers, or underscores.
\W	Matches only characters that are not letters, numbers, or underscores.
\A	Matches the beginning of a string only.
\Z	Matches the end of a string only.

Special Characters

Element	Definition
*	Matches zero or more occurrences of the preceding character.
+	Matches one or more occurrences of the preceding character.
?	Matches zero or one occurrence of any character.
.	Matches any one character, except newlines.
^	Matches the beginning of a string, like the \A metacharacter.
\$	Matches the end of a string, like the \Z metacharacter.
	Imposes either, or.

The following examples illustrate the results displayed in the user interface lists depending on how the [Edit Restricted List Screen](#) is completed. The restricted lists being defined use a metadata field defined to be a list. Its master list values are the US states in alphabetical order. The two dependencies include:

- The items or expression entered into the text pane.
- The Allow Java Regular Expressions check box (selected or unselected).

Example 1

In this example, text values are entered into the text pane and the Allow Java Regular Expressions check box is not selected. In this case, the options 'NoState' and 'Carolina' are not included in the resulting list because they are not full names of states. Note that the order is maintained as typed into the text area.

If the following values are entered into the text pane:

- Alabama
- Minnesota
- NoState
- Utah
- Carolina

The results displayed in the user interface list are:

- Alabama
- Minnesota
- Utah

Example 2

In this example, the same text values are entered into the text pane as in Example 1. However, the Allow Java Regular Expressions check box is selected.

If the following values are entered into the text pane:

- Alabama
- Minnesota
- NoState
- Utah
- Carolina

The results displayed in the user interface list are:

- Alabama
- Minnesota
- Utah
- North Carolina
- South Carolina

In this case, both 'North Carolina' and 'South Carolina' are included in the resulting list because they match the regular expression 'Carolina'.

Example 3

In this example, the Allow Java Regular Expressions check box is selected and instead of entering similar text values (as in the previous examples) the ^ special character is used with alphabet characters.

In this case, there are two regular expressions. The first expression specifies choosing everything in the master list beginning with C and the second expression specifies choosing everything beginning with A. Notice that the results order is dictated by how the list was entered in the text pane.

If the following values are entered into the text pane:

- ^C
- ^Al

Then the results displayed in the user interface list are:

- California
- Colorado
- Connecticut
- Alabama
- Alaska

Example 4

In this example, the same values are entered into the text pane as in Example 3. However, both values are entered on the same line and separated with the pipe (|) special character which is evaluated as 'or'. In this case, the expression retains the values in order because the list is filtered exactly one time for values that begin with either Al or C.

If the following values are entered into the text pane:

- ^C | ^Al

The following results are displayed in the user interface list:

- Alabama
- Alaska
- California
- Colorado
- Connecticut

3.2.2.5 Using Rules to Group Metadata Fields

You can group and arrange metadata fields and label them with an appropriate header. The fields are shown on the Check In, Update, Content Information, and Search pages as specified in the group.

To create metadata groups, select **Is Group** on the [Add/Edit Rule Screen](#). Use the **Fields** tab to add metadata fields to the group. Use the **Up** and **Down** buttons to rearrange the fields.

For example, [Figure 3-7](#) shows a rule on the left that results in the metadata field list on the Check In page on the right. In this example, Content ID is the group leader because it is the first element in the group list. The metadata fields included after Content ID are the group associates.

Figure 3-7 Metadata Fields Generated from Rule

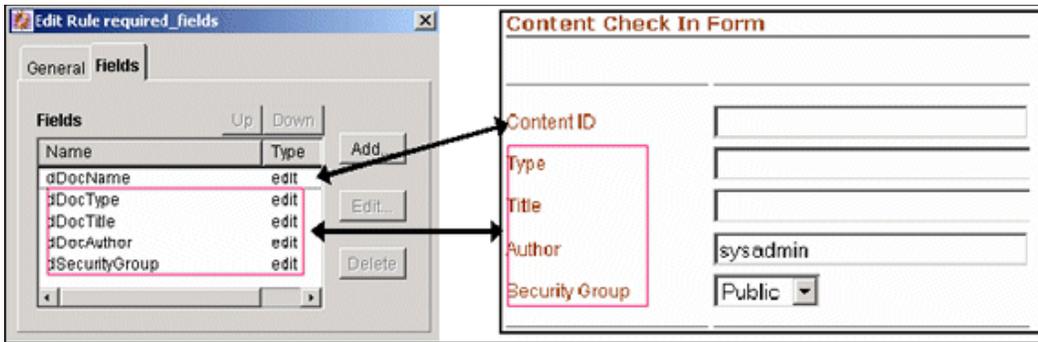
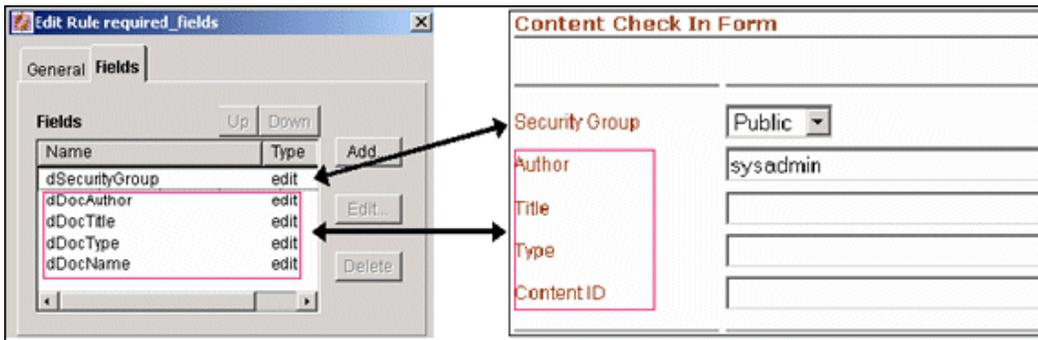


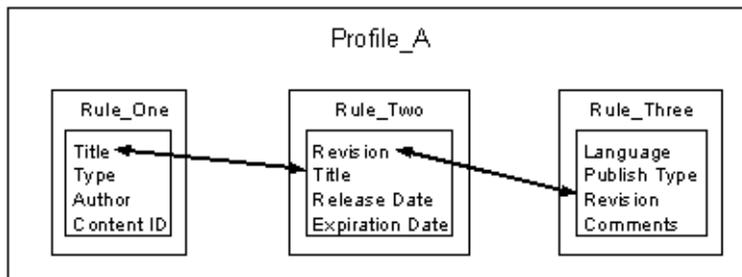
Figure 3-8 shows the same rule but the metadata fields in the group have been rearranged using the **Up** and **Down** buttons. This reorganization results in a different listing of the same metadata fields on the Check In page. In this case, Security Group becomes the group leader and the other fields are now the group associates.

Figure 3-8 Reorganized Metadata Fields



In Figure 3-9, a single profile contains three rules that have grouped metadata fields. Each group has one field that belongs to another group. In this situation, the system uses resolution rules to reconcile any conflicts.

Figure 3-9 Profile with Rules Grouping Metadata Fields



Caution: System evaluation and implementation of additional profile and global rules that contain one or more of these metadata fields can cause grouping conflicts. Some rules executed later can override earlier rules and affect how grouped metadata fields are resolved.

The following rules resolve conflicts between metadata fields that belong to groups in multiple rules:

1. The first element in the list is the group leader.
2. All elements following the first element are the group associates.
3. If the group leader is not a group leader in another group listing, then assign any group associates to the group, below the group leader.
4. If a group leader is a group associate in a prior group listing, then the new group listing is merged with the prior group listing as follows:
 - a. Find the main group leader (the group leader in the prior group).
 - b. Insert the new group associates after the group leader in the main group leader's group associates list.
5. Ensure that no group associate has multiple group leaders. If so, remove the associate from the prior group leader's list.
6. If a grouping has a group associate that is a group leader in another later grouping, then this rule is invalid, an error is reported, and the rule is not evaluated. (If this were to be allowed, the result would be a non-group leader (a group associate) being promoted to a group leader.)

Example 1

1. **IF:** A,B,C is a metadata group
WHERE: A is the group leader and B and C are group associates to A
2. **AND:** B,D,E is another metadata group
WHERE: B is the group leader and D and E are group associates to B
3. **RESULT:** A,B,D,E,C

Example 2

1. **IF:** A,B,C is a metadata group
WHERE: A is the group leader and B and C are group associates to A
2. **AND:** A,D,E is another metadata group
WHERE: A is the group leader and D and E are group associates to A
3. **RESULT:** A,D,E,B,C

Example 3

Example 3

1. **IF:** A,B,C is a metadata group
WHERE: A is the group leader and B and C are group associates to A
2. **AND:** C,B,D is another metadata group
WHERE: C is the group leader and B and D are group associates to C
3. **RESULT:** A,C,B,D

Example 4

1. **IF:** A,B is a metadata group
WHERE: A is the group leader and B is a group associate to A

2. **AND:** B,A,C is another metadata group
WHERE: B is the group leader and A and C are group associates to B
3. **RESULT:** Theoretically, this situation can resolve to B,A,C but this makes the A,B grouping irrelevant. To avoid confusion for other groupings, this is treated as an error case.

Example 5

1. **IF:** A,B,C is a metadata group
WHERE: A is the group leader and B and C are group associates to A
2. **AND:** D,A,E is another metadata group
WHERE: D is the group leader and A and E are group associates to D
3. **RESULT:** Error. It is impossible to resolve this grouping conflict.

3.2.3 Display Results of Reordered Metadata Fields

You can use content profiles to reorder metadata fields on the Check In, Update, Content Information, and Search pages. You can reorder custom metadata fields and system-specific information fields.

This section provides information about the display results of reordered custom and system information fields.

You can position metadata fields, as described in the following sections:

- [Section 3.2.3.1, "General Sequence of Grouped Metadata Fields"](#)
- [Section 3.2.3.2, "Positioning Metadata Fields Within a Group"](#)
- [Section 3.2.3.3, "Display Results of Grouped Metadata Fields"](#)
- [Section 3.2.3.4, "Moving Fields"](#)

3.2.3.1 General Sequence of Grouped Metadata Fields

The positioning of grouped system and custom metadata fields on Oracle WebCenter Content Server pages is determined by the priority of the first metadata field in the group. When adding a custom metadata field to the system, its positioning sequence (field order) is set.

Add custom metadata fields using the [Configuration Manager: Information Field Tab Screen](#) and assign the sequence number in the Order field on the [Add/Edit Metadata Field Screen](#).

When a custom metadata field is the first field in a group, that group is positioned on the page according to the field order assigned to the custom metadata field. When a system metadata field is the first field in a group, that group is positioned according to their established precedence.

Depending on the specific Oracle WebCenter Content Server page, you can include or exclude specified system metadata fields in the general display order. For example, the Search page displays the Release Date and Expiration Date system metadata fields but excludes Revision.

By default, the general order for system metadata fields is as follows:

- Content ID (dDocName)
- Type (dDocType)

- Title (dDocTitle)
- Author (dDocAuthor)
- Security Group (dSecurityGroup)
- Account (dDocAccount)
- Revision (dRevLabel)

A group with a system metadata field as the first field is usually displayed in default order. For example, if Author is the first field in a group of custom metadata fields, that group is displayed below any group containing Content ID, Type, or Title as its first field.

3.2.3.2 Positioning Metadata Fields Within a Group

[Section 3.2.2.5, "Using Rules to Group Metadata Fields"](#) describes how to define rules to conveniently group custom and system metadata fields on the Check In, Update, Content Information, and Search pages. You can also order metadata fields using the following methods:

- **Option 1: Field Position:** Use the Field Position list, available when adding metadata fields to rules using the [Add Rule Field Screen](#). This option works in a relative manner. For example, you might add the following metadata fields:

- xRegion (Top position)
- xSubDept (Bottom position)

If you add xDept with a field position of Middle, it is added as follows:

- xRegion (Top position)
- xDept (Middle position)
- xSubDept (Bottom position)

If you then add xContinent with a field position of Top, it is added as follows:

- xRegion (Top position)
- xContinent (Top position)
- xDept (Middle position)
- xSubDept (Bottom position)

Similarly, if you add xManager with a field position of Middle, it is added as follows:

- xRegion (Top position)
- xContinent (Top position)
- xDept (Middle position)
- xManager (Middle position)
- xSubDept (Bottom position)

This option produces these display results on the Check In, Update, Content Information, and Search pages if the fields are grouped. When adding the fields to a rule, select **Is Group** on the [Add/Edit Rule Screen](#).

- **Option 2: Up and Down buttons:** Use the **Up** and **Down** buttons to reorder fields. This option is available when adding metadata fields to rules using the **Fields** tab.

It is often useful to reorder fields after they are added, or to reorder fields with the same field position.

For example, if you added three fields with a field position of Top, they are positioned in the order they were added to the rule. However, you can use the **Up** button to move a field to the absolute top. Similarly, if any field is not positioned properly when it was added, you can use the **Up** and **Down** buttons to reposition them.

3.2.3.3 Display Results of Grouped Metadata Fields

The following rules specify how metadata groups are displayed on the Check in, Update, and Check in Selected pages.

- If the first field in a group is a system field (such as Content ID, Type, Title, and so on), the group is always displayed above the Primary File field.
- If automatic Content ID generation is disabled, then the Content ID field is always listed as the first field on the page followed by the remaining fields in the group. Also, if a separate group includes other system fields like Title and Type, that group is listed after the Content ID group but above the Primary File field.
- If automatic Content ID generation is enabled, then the Content ID field functions like a custom metadata field with 1 as its field order. In this case, if Content ID is the first field in a group, then the group is displayed immediately below the Primary File and Alternate File fields. Also, the Revision system metadata field is displayed after the last field in the Content ID group. (Note that, by default, Revision is displayed below the Alternate File field.)
- If the first field of a group is a custom metadata field, then the group is ordered by the field order number of the lead metadata field relative to the lead metadata fields in other groups, even if there are system metadata fields in the group.
- The Release Date and Expiration Date fields are always listed last on the page unless they are grouped with a custom metadata field that has a higher (that is, smaller number) field order value. Or, if Release Date and Expiration Date are grouped with a system metadata field, then they are listed above the Primary File field.

The following rules specify how metadata groups are displayed on the **Search page**.

- The Content ID field is always positioned first unless it is part of a group and it is not the first field. However, if Content ID is the first field of a group, then that group is listed first.
- If a system metadata field (other than Content ID) is the first field in a group, that group is listed after the Content ID field or Content ID group.
- All other groups with custom metadata fields as the first fields are displayed after groups with system metadata fields as the lead fields. When groups have a custom metadata field as the first field, the ordering of these groups is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

In order for a metadata field to be displayed on a search page, the Enable for Search Index must be set on the [Add/Edit Metadata Field Screen](#).

The following rules specify how metadata groups are displayed on the **Content Information page**.

- The Content ID field is always positioned first unless it is part of a group and it is not the first field.
- The Checked Out By, Status, and Formats fields are always listed at the bottom.

- The Security Group field, or any group with Security Group as the first field, is listed above the Checked Out By, Status, and Formats fields unless:
 - The account is disabled. If the account is enabled, then Security Group is displayed above the Checked Out By field. Security Group is displayed above the Account field.
 - The Security Group field is part of a group where it is not the first field, and the lead metadata field has a field order number that positions it above other custom metadata fields. In this case, the Security Group field is displayed in the order that is determined by the field order number of the group's lead metadata field.
- The Release Date and Expiration Date fields are listed as part of the Revision History table at the bottom of the page.
- All other groups with custom metadata fields as the first fields are displayed in the order that is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

The following rules specify how metadata groups are displayed on the **Folder Information** page.

- The Content ID field is not displayed unless it is part of a group. Currently, any group with Content ID as the first field is not displayed. Counteract this by defining another system or custom metadata field in the group as the lead field.
- All the groups are listed that have system metadata fields as their lead field (provided their assigned display attribute is Edit, Label, or Required). If any system or custom metadata field is assigned a Hidden or Excluded display attribute, it is not displayed.
- All other groups with custom metadata fields as the first fields are displayed in the order that is determined by the field order numbers of the lead metadata fields of groups in relation to each other.

3.2.3.4 Moving Fields

Follow these steps to force any **custom metadata field** to **display above the Primary File field**:

1. Add the custom metadata field to a group that includes system metadata fields.
2. Make the first field in the group a system metadata field. Group position is based on which system metadata field is the lead field.

To force any **system metadata field** to **display below the Primary File field**:

1. Add the system metadata field to a group that includes custom metadata fields.
2. Ensure that the first field in the group is a custom metadata field.

The group is displayed below the Primary File field based on the field order number of the lead field.

3.2.4 Managing Rules

The following tasks are included in rule management:

- [Section 3.2.4.1, "Creating or Editing a Rule"](#)
- [Section 3.2.4.2, "Creating, Editing, or Deleting a Global Rule"](#)
- [Section 3.2.4.3, "Adding Metadata Fields in a Rule"](#)

- [Section 3.2.4.4, "Adding, Editing or Deleting Activation Conditions in Rules"](#)
- [Section 3.2.4.5, "Custom Conditions and Side Effects"](#)
- [Section 3.2.4.6, "Setting Default Values, Derived Values and Restricted Lists"](#)
- [Section 3.2.4.7, "Editing Default or Derived Values and Restricted Lists"](#)
- [Section 3.2.4.8, "Setting the Display of a Required Field"](#)

3.2.4.1 Creating or Editing a Rule

To create a rule:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Click **Add**.

The [Add/Edit Rule Screen](#) opens. Click the **General** tab.

3. Enter the name and description information about the new rule.

Click **OK**.

To edit a rule, select the rule from the list on the [Configuration Manager: Rules Tab Screen](#) and click **Edit**. Edit the field values and click **OK** when done.

To **delete a rule**, select the rule from the list on the [Configuration Manager: Rules Tab Screen](#) and click **Delete**. Click **OK** to verify the deletion.

3.2.4.2 Creating, Editing, or Deleting a Global Rule

To create a global rule:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Click **Add** to create a global rule or highlight a rule and click **Edit** to change a rule to a global rule or edit an existing global rule.

The [Add/Edit Rule Screen](#) opens. Click the **General** tab.

3. Select *Is global rule with priority*.

4. Change the default priority number (optional). By default, 10 is the priority number listed. If editing a rule, change other information as needed. A lower priority rule is executed before higher priority rules which higher priority rules to override the changes made by lower priority rules.

5. Click **OK**.

To **edit a rule**, select the rule from the list on the [Configuration Manager: Rules Tab Screen](#) and click **Edit**. Edit the field values and click **OK** when done.

To **delete a rule**, select the rule from the list on the [Configuration Manager: Rules Tab Screen](#) and click **Delete**. Click **OK** to verify the deletion.

3.2.4.3 Adding Metadata Fields in a Rule

To **add metadata fields** to a rule:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Click **Add** to create a global rule or highlight a rule and click **Edit** to change a rule to a global rule or edit an existing global rule.

The [Add/Edit Rule Screen](#) opens.

3. Click the **Fields** tab and click **Add**.

The [Add Rule Field Screen](#) opens.

4. Select the following information:

- **Display Information Field** check box and **Display Application Fields** check box: if selected, lists metadata fields in the field names list, making fields available for display on standard check-in and search pages.

Note that if an application field is selected for display in a rule, the field's behavior (as defined for the application that normally uses the field) is changed.

5. Select a field name from the list.
6. Select a general placement choice for the metadata field from the Field Position list for each metadata field added. The selected option adjusts the general placement order of the metadata fields in the list on the [Add/Edit Rule Screen](#), Field Tab. The position of each field is relevant to its priority in the evaluation process. You can use the **Up** or **Down** buttons to further refine the placement.
 - **Top**: Moves the metadata field to a relatively higher position.
 - **Middle**: Moves the metadata field to a relatively central position.
 - **Bottom**: Moves the metadata field to a relatively lower position.

7. Click **OK**.

The [Add/Edit Rule Field 'name' Screen](#) opens.

8. Enter the following display information about each metadata field which determines how the metadata field is displayed on Check In and Search pages:
 - **Edit**: The field is editable even if a default value is provided.
 - **Label**: The field is read-only (fixed but displayed).
 - **Hidden**: The field does not display but when the user submits a content item, this metadata field value remains on the source page.
 - **Excluded**: The field does not display. Unlike a hidden metadata field, an excluded value does not remain on the source page.
 - **Required**: A required field. If this is used, a message is also required.
9. **Custom Label**: Specify a label for the field. You can use different labels in different profiles.
10. **Use Custom Include**: Used to reposition standard fields. For example, creating a group that includes a placeholder field and the title field moves the title field below the other standard fields on the page. A custom include can then be used for the placeholder field to control how or if it is displayed. Provided files are:
 - **Standard Separator**: Places a standard horizontal rule on the page where the field otherwise would be.
 - **Display Nothing**: hides the field when the page opens.

If **checked**, allows the use of custom fields. Default: deselected.

The standard include options listed in the Start Include and End Include lists are defined in the DpDisplayIncludes table of the std_resources.htm file. To add additional include options, a custom component must be written defining the new includes and merging them into the DpDisplayIncludes table.

11. Exclude field from the group count: Prevents the group header from being displayed while keeping the presentation properties of the placeholder field. If the number of fields in a group is greater than zero, then the group header is displayed. For example, a placeholder field used for presentation purposes is the only field in a group that is displayed. Default: deselected.
12. Use Default Value: Allows display of a default value on the Content Check In page or the Search page. Default values are computed for On Request events. You can use Idoc Script, or schema values if the metadata field is associated with a schema view.

If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the default value is added and its properties defined). If unselected, (default), default values cannot be used.

13. Is Derived: Enables the field to be set to a specified value on update or check-in. Values are computed for On Submit and On Import events. You can use Idoc Script, or schema values if the metadata field is associated with a schema view.

If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the value is added and its properties defined). If unselected (default), default values cannot be used.

14. Has Restricted List: Enables the field to be restricted to either a specific list of values or to a filtered list of values.

If selected, the **Edit** button is activated and the text pane becomes active, displaying the computed Idoc Script for the field (automatically generated after the list is added and its properties defined). If unselected (default), default values cannot be used.

15. Click **OK** when done specifying the attributes of the rule.
16. For each metadata field to be added to the rule, repeat steps 4 through 15.

To group metadata fields and add a header to a group:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Highlight a rule and click **Edit**.

The [Add/Edit Rule Screen](#) opens.

3. On the **General** tab, select **Is group**.
4. Select **Has Group Header**.
5. Click **Edit**.

The [Edit Group Header Screen](#) opens. Provide the following information:

- **Enable Hiding:** If selected, group metadata fields are hidden and a link appears on the page instead of the fields. Pressing the Show link shows the fields. The default is to display the pages with a Hide link, meaning all fields are displayed by default.

- Start and End Include: Specifies how to display the group. Options include:
 - Standard Separator: Inserts a rule above or below the group
 - Start/End HTML Table: Displays the group in an HTML table with borders for each row and the header.
 - Display Nothing: (default): No distinction is made for the group.
 - Header Text: The header string associated with the group of fields.
6. Click **OK** when done.

3.2.4.4 Adding, Editing or Deleting Activation Conditions in Rules

Follow these steps to **add** an activation condition to a rule:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Highlight a rule and click **Edit** to add a condition to a rule or click **Add** to add a new rule.

The [Add/Edit Rule Screen](#) opens.

3. Click the **General** tab then select **Use Rule Activation Condition**.

4. Click **Edit**. The [Edit Activation Condition Screen](#) opens.

5. Click **Add**. In the dialog that opens, enter the name and click **OK**. The **General** tab opens.

6. Enter the following information using the General pane and Clauses pane. For details, see [Section 3.2.4.5, "Custom Conditions and Side Effects."](#)

The following options are available on the **General** pane:

- Use Event check box: If selected, rules can perform differently when events are detected. Events include the following:
 - On Request: Includes an event that results from a user request to view an Oracle WebCenter Content Server page.
 - On Submit: Includes an event that results from a contribution action.
 - On Import: Includes an event that results from a batch loading or archive procedure. The rule is only active for archiver, batch loading, or any other process that uses a special check-in service (for example, Content Publisher).
- Use Action: If selected, rules can perform differently when user actions are detected by the system. User actions include the following (for example, when new contributions are checked in or when a content item is revised):
 - Check in new: Includes the user action of contributing a new content item.
 - Check in selected: Includes the user action of submitting a revision to an item.
 - Content information: Includes the user action of requesting to view the document information page.
 - Content update: Includes the user action of submitting revisions to the document information page.
 - Search: Includes the user action of requesting to view the search page.

- **Workflow flag:** Enables a rule to perform differently based on the workflow state of a document. For example, when a document is in a workflow, it displays a different Content Information page.

The following options are available on the Clauses pane. This pane is an Idoc Script wizard used to automate the process of creating Idoc Script statements:

- **Field List:** A list of metadata options.
 - **Operator List:** The method used for searching metadata fields, including the following:
 - **Matches:** The entire text within the specified metadata field contains the specified metadata Value.
 - **Contains Word:** The text within the specified metadata field contains the metadata Value.
 - **Begins With:** The text within the specified metadata field starts with the metadata Value.
 - **Is Date Before:** The date in the specified metadata field occurs before the Value date.
 - **Is Date After:** The date in the specified metadata field occurs after the Value date.
 - **Value Field:** You can select an editable field to enter data, a list of options, or an editable field that activates the **Select** button. If the field value is Content ID, pressing **Select** opens the Custom pane. If the field is author, a selection screen of users opens.
7. When done configuring the conditions, click **Add** to add the condition to the Clause pane.
 8. Click **OK**.

To **edit an activation condition**, follow the previous steps and on the **Conditions** tab, select the activation condition to edit from the list. Edit the field values and click **OK** when done.

To **delete an activation condition**, follow the previous steps and on the **Conditions** tab, select the activation condition from the list and click **Delete**. Click **OK** to confirm the deletion.

3.2.4.5 Custom Conditions and Side Effects

The **Custom** tab of the [Edit Activation Condition Screen](#) is used to define specific conditions for a rule that, when met, affect the behavior of the profile.

To use this screen, click the **Custom** tab then enter customized text in the text pane. Information that is entered is displayed in the text pane on the [Add/Edit Rule Screen](#).

To define side effects, click the **Side Effects** tab on the [Edit Activation Condition Screen](#). The Side Effects screen is used to:

- Easily add name-value pairs as Idoc Script variables that get pushed to local data using Idoc Script if the activation condition is true.
- Add custom Idoc Script to a rule that is only evaluated if the activation condition is true.

Because the side effect is Idoc Script and evaluated when a rule is activated, you can also include logical statements such as `like`, `if`, `elseif`, and `else`, and can execute any Idoc Script function. For example, you can establish a rule that can control the

activation of other rules. For more information scripting in Idoc Script, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

Add the following information on this screen:

- Key: the name used as the Idoc Script variable.
- Value: a literal string that equates to the variable.

Click **Add** when done. The key and value are converted to Idoc Script and are displayed in the editing pane, where you can edit the text.

3.2.4.6 Setting Default Values, Derived Values and Restricted Lists

Follow these steps to set a **default value field** or a **derived value field**:

1. In step 12 or step 13 of the [Adding Metadata Fields in a Rule](#) task, select the appropriate check box. Click **Edit**.
The appropriate screen opens.
2. On the **Conditions** tab, click **Add**.
In the screen that opens, enter a name for this value attribute and click **OK**. The name is added to the Conditions list.
3. Select a Field value and Operator from the lists. Depending on the selected value from the Field list, the Value field provides:
 - An editable field to enter the data.
 - A list of appropriate options.
 - An editable field with a corresponding **Select** button.
4. Enter or select a value for the upper Value field, as applicable:
 - a. Click **Select**. If:
 - The Field value is Content ID, the [Edit Default/Derived Value: Select Field Screen](#) opens. Select a field for use.
 - The Field value is Author, the [User View Screen](#) opens. Select a user.
 - b. Use the filters to select content. When finished, click **OK**.
The screen closes and the selected content value is added to the upper Value field on the default value **Conditions** tab.
5. Click **Add**.
The statement is added to the expression pane.
6. Click **Compute**.
The [Edit Default/Derived Value: Select Field Screen](#) opens.
7. If the field is linked to a schema view, select a column. Otherwise, click **OK**.
The Select Field screen closes and the computed value is added to the lower Value field on the default value **Conditions** tab.
8. Click **OK**.
The screen closes and the Idoc Script statement is displayed in the default value text pane on the [Add/Edit Rule Field 'name' Screen](#).
9. If finished adding metadata field attributes, click **OK**. Otherwise, continue to include additional attributes.

To use a **restricted list for the metadata field**:

1. In step 14 of the [Adding Metadata Fields in a Rule](#) task, select **Has Restricted List**. Click **Edit**.

The [Edit Restricted List Screen](#) opens.

2. To use a list of values directly associated with rules, select **Is Filtered List**. To use a list of specific values, select **Is Strict List** and enter the specific items in the Restricted Value text pane.
3. Click **OK**.

The Edit Restricted List screen closes. If the strict list option is used, the items are displayed in the text pane on the [Add/Edit Rule Field 'name' Screen](#).

3.2.4.7 Editing Default or Derived Values and Restricted Lists

To edit the attributes of a metadata field:

1. Choose **Administration** then **Admin Applets**. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Click **Add** to create a global rule or highlight a rule and click **Edit** to change a rule to a global rule or edit an existing global rule.

The [Add/Edit Rule Screen](#) opens.

3. Open the **Fields** tab and select the metadata field with attributes to edit. Click **Edit**.

The [Add/Edit Rule Field 'name' Screen](#) opens.

4. Click the corresponding **Edit** button of the attribute to edit. The appropriate screen opens.

5. For either the default value or derived value, select the value to edit in the Conditions text pane.

- a. Select the new Field, Operator or both field values.
- b. To edit the upper Value field value without deleting and redefining the clause, highlight the clause in the Clause pane. Edit the value in the upper Value field, then click **Update**.
- c. Click **Compute**.
- d. Click **OK**.

The screen closes and the revised values are displayed.

6. For the restricted list attribute, on the Edit Restricted List screen, select the list option and edit the text pane as needed. Click **OK**.

The screen closes and the revised list information is displayed.

7. Click **OK**.

3.2.4.8 Setting the Display of a Required Field

Two configuration variables control how required metadata fields appear on the Check In page. For more information, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

- To use red lettering for a required field, use the following configuration variable and value:

```
StyleForRequiredFields=requiredField
```

- To mark the required field with any symbol, use the following configuration variable and value:

```
NotationForRequiredFields=*
```

Note: In this example, an asterisk is used to mark the required fields.

3.2.5 Content Profile Triggers

A *trigger field* is a metadata field defined on the [Configuration Manager: Profiles Tab Screen](#). If a document matches a *trigger value* for a profile, then that profile is evaluated for the document.

An unlimited number of profiles can exist, but only one trigger value per profile is allowed. For example, if the trigger field is `dDocType`, Profile1 can use the trigger value of `ADACCT` and Profile2 can use the trigger value of `ADSALES`.

The following are true for the selected trigger:

- The trigger field must be a list metadata field. Metadata fields defined as lists are included in the trigger field list.
- After you define the trigger field, you cannot delete it from the system. An Administrator can reset the trigger field to 'none specified', however this disables all profiles.
- If you can change the trigger field, you may invalidate some profiles and have to resolve the situation. User interface hints are provided concerning which profiles are invalid.

Note: Although you create rules before you create triggers and profiles, it is necessary to know what your trigger is before creating rules.

3.2.5.1 Selecting a Profile Trigger Field

You can select only one trigger field for each Oracle WebCenter Content Server instance.

Follow these steps to select or change the current profile trigger field:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Profiles** tab.

The [Configuration Manager: Profiles Tab Screen](#) opens.

2. Click **Select**.

The [Edit Trigger Field Screen](#) opens.

3. Select a new trigger field from the list in the Field Name field.

Click **OK**.

If you change the trigger field after one or more profiles are created, the new trigger field could cause the existing profiles to become invalid.

3.2.5.2 Disabling a Profile Trigger Field

Follow these steps to completely disable the trigger field (essentially disabling all profiles as well):

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Profiles** tab.

The [Configuration Manager: Profiles Tab Screen](#) opens.

2. Click **Select**.

The [Edit Trigger Field Screen](#) opens.

3. Select **none specified** from the list in the Field Name field.
4. Click **OK**.

3.2.6 Creating and Using Content Profiles

This section discusses the tasks involved in creating and using a profile. It covers these topics:

- [Section 3.2.6.1, "Creating, Editing, or Deleting a Profile"](#)
- [Section 3.2.6.2, "Previewing a Profile"](#)
- [Section 3.2.6.3, "Troubleshooting a Profile"](#)

3.2.6.1 Creating, Editing, or Deleting a Profile

Follow these steps to **create a new** profile:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Profiles** tab.

The [Configuration Manager: Profiles Tab Screen](#) opens.

2. Click **Add**. A dialog opens where you can add a name.
3. Enter the name of the new profile and click **OK**.

The [Add/Edit Profile Screen](#) opens.

4. Enter the following information:
 - Display label: Text for the profile on the My Checkin and My Search menu options.
 - Description: brief description of the profile.
 - Trigger list: the list values associated with the trigger.
 - Exclude non-rule fields: Select to exclude all metadata fields that do not belong to the rules included in the profile.
 - Restrict personalization: Select to suppress checkin or search links to a particular user or group of users. Idoc Script code based on user information is entered into the [Profile Links Screen](#) and must evaluate to true before a link is displayed. If deselected (default), all links are displayed for all users by default unless evaluated by another profile. Click Edit to customize the list of users.

5. Click **Add** to include rules in the new profile.

The [Add Rule in Profile Screen](#) opens.

Note: You cannot add rules to the profile until you create and define them using the [Configuration Manager: Rules Tab Screen](#).

6. Select rules from the list and assign them a general placement priority value.

Adjust the placement order of the rules in the list by pressing the **Up** or **Down** button. The position of each rule in the list is relevant to its priority in the evaluation process. The general position (top, middle, or bottom) in the list is established when the rule is initially added to the profile. The buttons further refine the placement by moving the rule to a more precise position.

7. Click **OK**.

The new profile is included in the Profiles list on the **Profiles** tab.

To **edit** a profile, select the profile on the [Configuration Manager: Profiles Tab Screen](#) and click **Edit**. Change the fields as needed and click **OK**.

To **add or edit rules to a profile**, select the profile on the [Configuration Manager: Profiles Tab Screen](#) and click **Edit**. Click **Add** and select a rule and rule placement from the [Add Rule in Profile Screen](#). Click **OK** when done.

To **delete** a profile, select the profile on the [Configuration Manager: Profiles Tab Screen](#) and click **Delete**. Click **OK** to verify the deletion.

3.2.6.2 Previewing a Profile

Follow these steps to review a profile:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Profiles** tab.

The [Configuration Manager: Profiles Tab Screen](#) opens.

2. Select the profile to be previewed from the Profiles list, and click **Preview**.

The [Preview Profile Screen](#) opens.

3. Select options for use in the profile:

- Event list: Specifies when an event is included in the profile evaluation.
 - none specified: An event is not included.
 - On Request: Includes an event that results from a user request to view an Oracle WebCenter Content Server page.
 - On Submit: Includes an event that results from a contribution action.
 - On Import: Includes an event that results from a batch loading or archive procedure. The rule is only active for archiver, batch loading, or any other process that uses a special check-in service (for example, Content Publisher).
- Action list: Specifies when an action is included in the profile evaluation.
 - none specified: A user action is not included in the profile evaluation.
 - Check in new: Includes the user action of contributing a new content item.
 - Check in selected: Includes the user action of submitting a revision to an item.
 - Content information: Includes the user action of requesting to view the document information page.

- Content update: Includes the user action of submitting revisions to the document information page.
 - Search: Includes the user action of requesting to view the search page.
 - Is workflow list: Specifies when a workflow is included in the evaluation.
 - none specified: A workflow state is not included in the evaluation. The document is or is not in a workflow, but its workflow state is not specified.
 - Yes: The document is in a workflow.
 - No: The document is not in a workflow.
 - Content ID: The content used in the evaluation based on the filter criteria.
 - User name: The user name used in the evaluation.
4. To review the compiled results of the current profile, do not change any field values on the Preview Profile screen. Click **Compute results**.
The [Preview Results Screen](#) opens.
 5. To view the page as an end user sees it, make the following selections:
 - Select **On Request** as the Event field value
 - Select an Action value
 - Leave the User Name field blankClick **Show**.
 6. Review the computed results and click **OK**.

3.2.6.3 Troubleshooting a Profile

The [Preview Profile Screen](#) is also used to troubleshoot invalid profiles and perform analysis on any profile.

Troubleshooting using what-if scenarios is an iterative process, composed of trying combinations of inputs to evaluate the profile's rules. In addition to using different input values, you can also use filtered selections of documents.

Changing the different criteria (with or without filters) and computing the results shows how various input combinations affect the evaluation of rules. When the system evaluates the profile's rules, the computed results are displayed either as script string statements (SQL or Idoc Script) in a standard dialog text pane or as simulated Check In or Search pages (if you select On Request as the Event field value). Using the flexibility of the what-if analysis process helps to debug and optimize profiles.

To perform what-if scenarios using diverse combinations of inputs and filters:

1. Select the profile to be reviewed and tested from the Profiles list, and click **Preview**.
The [Preview Profile Screen](#) opens.
2. Select field values, as applicable, from the Event, Action, and Is workflow lists.
3. To include filtered choices for the Content ID field, click the corresponding **Select** button.
The [Content Item View Screen](#) opens.
4. Select content item filter options, as applicable, and click **OK**. The Preview Profile screen opens.

5. To include filtered choices for the User Name field, click the corresponding **Select** button.

The [User View Screen](#) opens.

6. Select user filter options, as applicable, and click **OK**. The Preview Profile screen opens.

To view the evaluated rules as coded statements, click **Compute Results**.

To evaluate results as a simulated page in a browser window, click Request in the Event field. Select other field values then click Show on the [Preview Profile Screen](#).

The system launches a browser window that displays the resulting metadata fields in a simulated Check In or Search page. This window provides a graphic view of what the end user sees.

3.2.7 Content Profile Examples

The following profile examples illustrate several scenarios in which profiles are useful:

- [Section 3.2.7.1, "Department-Based Content Profile"](#)
- [Section 3.2.7.2, "Black-Hole Resume Check In"](#)
- [Section 3.2.7.3, "Global Rule to Restrict Content Check-In Based on User Role"](#)
- [Section 3.2.7.4, "Global Rule Restricting Content Type Metadata Changes"](#)

3.2.7.1 Department-Based Content Profile

This example shows how to plan and create a department-based profile that includes one global rule and one regular profile rule.

The goal is to control how the metadata fields governed by the rules are displayed on the Check In, Update, Content Information, and Search pages. Ideally, only department-specific fields are displayed to minimize the number of metadata fields that users see.

This example creates the applicable rules first then the profile because the rules are added to the profile during the process of creating the actual profile. It is divided into the following main steps:

- Create a global rule with the following characteristics:
 - Ensure that all new and updated content items checked in have comments associated with them. The optional comments metadata field is revised to be a required field.
 - Allow the content item title metadata field to be editable.
- Create a profile rule with the following characteristics:
 - Provide a default value for the comments metadata field but also allow it to be editable. The default message is triggered by marketing-specific documents.
 - Provide default values that are read-only text for the publish type and revision label metadata fields.
- Create a department-based profile with the characteristics:
 - Organize the metadata fields that are hidden or displayed on the Check In, Update, Content Information, and Search pages.
 - Display only those fields that are relevant to the marketing department.
 - Group selected metadata fields using a marketing-based group heading.

Create the Global Rule

1. Open the **Rules** tab on the [Configuration Manager Page](#) and click **Add**.
The [Add/Edit Rule Screen](#) opens.
2. On the **General** tab, enter the name of the global rule in the Name field (for example, `CmtsRqd`).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority**. You can also change the priority number.
5. Add and define the Comments metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
The [Add Rule Field Screen](#) opens.
 - b. Select **Comments** from the Field Name list.
 - c. Select a general position from the Field Position list (for example, `top`).
 - d. Click **OK**.
The [Add/Edit Rule Field 'name' Screen](#) opens.
 - e. Select **Required** from the Type list to ensure that users must enter a comment about the content item being checked in.
 - f. Enter text in the Required Message field. This is optional for all rule field types except the Required type.
 - g. Select **Use default value** and click the corresponding **Edit** button.
The [Edit Default/Derived Value Screens](#) opens.
 - h. On the **Conditions** tab, click **Add**.
The Add Condition screen opens.
 - i. Enter the name of the field condition (for example, `UserMsg`).
 - j. Click **OK**.
The screen closes and the clause-generating fields display on the lower pane of the **Conditions** tab.
 - k. Enter a short statement in the lower Value field, at the far bottom of the screen near the **Compute** button. This statement becomes the default value for the Comment field.
 - l. Click **OK**.
The screen closes and the default value Idoc Script clause for the `UserMsg` field condition is added to the Default Value text pane.
 - m. Click **OK**.
The screen closes and the Comments metadata field is added to the Fields list.
6. Add and define the Document Title metadata field as follows:
 - a. On the **Fields** tab of the Add/Edit Rule screen, click **Add**.
 - b. Select **Title** from the Field Name list.
 - c. Select a general position from the Field Position list (for example, `bottom`).
 - d. Click **OK**.

- e. Select **Edit** from the Type list to allow this metadata field to be editable on the Check In and Search pages.
- f. Enter a note in the Required Message field (optional).
- g. Click **OK**.

The Title metadata field is added to the Fields list.

7. Click **OK**.

The screen closes.

Create the Profile Rule

1. On the **Rules** tab, select **Add**.
2. On the **General** tab, enter the name of the profile rule in the Name field (for example, `DefaultMktComment`).
3. Enter a description for the profile rule (optional).
4. Select **Is group**.
5. Select **Has group header**, and click the corresponding **Edit** button.
The [Edit Group Header Screen](#) opens.
6. Enter the text to use as the header for the grouped metadata fields (for example, `Marketing-Specific Information`).
7. Click **OK**.
8. Add and define the Comments metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
 - b. Select **Comments** from the Field Name list.
 - c. Select a general position from the Field Position list (for example, `top`).
 - d. Click **OK**.
 - e. Select **Edit** on the Type list, allowing this field to be editable on the Check In, Update, Content Information, and Search pages.
 - f. Enter a note in the Required Message field (optional).
 - g. Select **Use default value** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, `CurrentMktgDocs`).
 - j. Click **OK**.
 - k. Enter `These are Current Marketing Docs` into the lower Value field at the bottom of the screen (near the **Compute** button).
 - l. Click **OK**.
The default value `Idoc Script` clause for the field condition is added to the Default Value text pane.
 - m. Click **OK**.
The Comments metadata field is added to the Fields list.
9. Add and define the Publish Type metadata field as follows:
 - a. On the **Fields** tab, click **Add**.

6. Click **OK**.
The [Add/Edit Profile Screen](#) opens.
7. Enter the profile description in the Description field (for example, `Current Mktg docs`).
8. Enter a descriptive label for the profile (for example, `MarketingSpecific`).
9. Select **ADMKT** (or an equivalent marketing option) from the Trigger list.
10. Click **Add** to include the rules in this profile.
The [Add Rule in Profile Screen](#) opens.
11. Select **DefaultMktComment** from the Name list.
12. Select a general priority placement from the Rule Priority list (for example, `top`).
13. Click **OK**.
14. Click **Add**.
15. Click **OK**.
16. Click **OK**.

The screen closes and the profile is added to the list of profiles on the **Profiles** tab.

3.2.7.2 Black-Hole Resume Check In

This example shows how to plan and create a black-hole check in profile used to submit resumes to Human Resources. The goal is to restrict the visible metadata fields available on the Check In, Update, Content Information, and Search pages when using this profile.

After a resume is initially checked in, the derived settings for all the potentially searchable metadata fields prevent unauthorized users from retrieving the document. This example creates the applicable rules first then the profile because the rules are added to the profile during the process of creating the actual profile.

This example is based on the default metadata fields displayed using a non-customized Oracle WebCenter Content Server instance. The visible metadata fields in this profile are limited to Type, Primary File, Alternate File, and Comments. The Type field uses a read-only label. On submission the value is reset to an HR-accessible value to ensure confidentiality of the document. Only the Comments field is editable. The remaining metadata fields are hidden and on submission also have their values reset. In this example, the hidden metadata fields include Title, Author, Security Group, Content ID, Revision, Release Date, and Expiration Date.

If selected, both the Hidden and Excluded display attributes conceal the defined metadata field. Using the Hidden type has the advantage of allowing the field value to remain on the source page. Thus, the contributor does not see the Hidden fields when checking in the document, but the assigned field values are still visible to an authorized viewer. The Excluded type precludes the field values on the source page.

In this type of profile, it is inadvisable to depend on the Exclude non-rule fields check box to hide unnecessary metadata fields. Contributors see only the fields included in the profile's rules, however, it does not prevent default values from being assigned and stored on the source page. Unauthorized users could find a black-hole document by searching on the excluded metadata fields.

This example is divided into the following main steps:

- Create a profile rule that:

- Hides non-essential metadata fields and does not display them on the Check In, Update, Content Information, and Search pages.
- Resets the default values of each hidden metadata field to ensure that unauthorized users cannot search and retrieve documents using the hidden fields.
- Create a profile rule that:
 - Allows the display of specific metadata fields related to checking in a resume.
 - Resets the values of each visible metadata field to ensure that unauthorized users cannot search and retrieve documents using these fields.
- Create a black-hole check-in profile that:
 - Restricts the metadata fields that are hidden or displayed on the Check In, Update, Content Information, and Search pages.
 - Displays only those fields that are relevant to an employee who is checking in a resume for an internal company position.

Create Rule for Hidden Fields

Follow these steps to create a profile rule for hidden metadata fields:

1. Open the **Rules** tab on the [Configuration Manager Page](#) and click **Add**.
The [Add/Edit Rule Screen](#) opens.
2. On the **General** tab, enter the name of the rule in the Name field (for example, NoExtraFields).
3. Enter a description for the global rule (optional).
4. Add and define the Title metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
The [Add Rule Field Screen](#) opens.
 - b. Select **Title** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.
The [Add/Edit Rule Field 'name' Screen](#) opens.
 - e. Select **Hidden** from the Type list to ensure this metadata field does not appear on the Check In, Update, Content Information, and Search pages.
 - f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
The [Edit Derived Value: Conditions Tab](#) opens.
 - h. On the **Conditions** tab, click **Add**.
The Add Condition screen opens.
 - i. Enter the name of the field condition (for example, HRSEYESONLY).
 - j. Click **OK**.
The screen closes and the clause-generating fields appear on the lower pane of the **Conditions** tab.

- f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, HRSEyesOnly3).
 - j. Click **OK**.
 - k. Select **Security Group** from the Field list.
 - l. Select **Matches** from the Operation list.
 - m. Select an applicable choice from the Value list. For example, select HR or any other department that is authorized to view the documents checked in using this profile.
 - n. Click **Add**.
 - o. Click **OK**.
 - p. Click **OK**.
7. Add and define the Content ID metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
 - b. Select **Content ID** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.
 - e. Select **Hidden** from the Type list to ensure that this field does not appear on the Check In, Update, Content Information, and Search pages.
 - f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, HRSEyesOnly4).
 - j. Click **OK**.
 - k. Select **Content ID** from the Field list.
 - l. Select **Begins With** from the Operation list.
 - m. Enter a confidential string or click **Select**.

The Select Field screen opens. Select a content item from the list. For greater security, enter a unique string (for example, Res) to help ensure that unauthorized users cannot search and retrieve these documents using the Content ID metadata field.
 - n. Click **OK** (if you selected a content item from the [Content Item View Screen](#)).
 - o. Click **Add**.
 - p. Click **OK**.
 - q. Click **OK**.
8. Add and define the Revision metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
 - b. Select **Revision** from the Field Name list.

- c. Select a general position from the Field Position list.
 - d. Click **OK**.
 - e. Select **Hidden** from the Type list (to ensure that this metadata field does not display on the Check In, Update, Content Information, and Search pages).
 - f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, `HRSEyesOnly5`).
 - j. Click **OK**.
 - k. Select **Revision** from the Field list.
 - l. Select **Begins With** from the Operation list.
 - m. Enter a confidential string in the upper Value field (for example, **Res**) to ensure that unauthorized users cannot search and retrieve these documents using the Revision metadata field.
 - n. Click **Add**.
 - o. Click **OK**.
 - p. Click **OK**.
9. Add and define the Release Date metadata field as follows:
- a. On the **Fields** tab, click **Add**.
 - b. Select **Release Date** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.
 - e. Select **Hidden** from the Type list to ensure that this field does not appear on the Check In, Update, Content Information, and Search pages.
 - f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, `HRSEyesOnly6`).
 - j. Click **OK**.
 - k. In the lower Value field, enter a confidential string (for example, `No specific release date`) to prevent unauthorized users from using the Release Date field to retrieve the documents checked in using this profile).
 - l. Click **OK**.
 - m. Click **OK**.
10. Add and define the Expiration Date metadata field as follows:
- a. On the **Fields** tab, click **Add**.
 - b. Select **Expiration Date** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.

- e. Select **Hidden** from the Type list to ensure that this field does not display on the Check In, Update, Content Information, and Search pages.
 - f. Enter text in the Required Message field (optional).
 - g. Select **Is derived field** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, HRsEyesOnly7).
 - j. Click **OK**.
 - k. In the lower Value field, enter a confidential string (for example, No specific expiration date) to help prevent unauthorized users from using the Expiration Date metadata field to search for and retrieve the documents checked in using this profile).
 - l. Click **OK**.
 - m. Click **OK**.
11. Click **OK**.
- The screen closes.

Create Rule for Visible Fields

Follow these steps to create a profile rule for visible metadata fields:

1. On the **Rules** tab, select **Add**.
2. On the **General** tab, enter the name of the profile rule in the Name field (for example, VisibleFields).
3. Enter a description for the profile rule (optional).
4. Add and define the Type metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
 - b. Select **Type** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.
 - e. Select **Label** from the Type list to make this a read-only metadata field on the Check In, Update, Content Information, and Search pages.
 - f. Enter text in the Required Message field (optional).
 - g. Select **Use default value** and click the corresponding **Edit** button.
 - h. On the **Conditions** tab, click **Add**.
 - i. Enter the name of the field condition (for example, ResumeType).
 - j. Click **OK**.
 - k. In the lower Value field, enter **Resume**.
 - l. Click **OK**.
 - m. Select **Is derived field** and click the corresponding **Edit** button.
 - n. On the **Conditions** tab, click **Add**.
 - o. Enter the name of the field condition (for example, ResumeType2).
 - p. Click **OK**.

- q. In the lower Value field, select an appropriate document type from the Value list (for example, HRresumes).
- r. Click **OK**.
- s. Click **OK**.
5. Add and define the Comments metadata field as follows:
 - a. On the **Fields** tab, click **Add**.
 - b. Select **Comments** from the Field Name list.
 - c. Select a general position from the Field Position list.
 - d. Click **OK**.
 - e. Select **Edit** from the Type list to allow this metadata field to be editable on the Check In, Update, Content Information, and Search pages.
 - f. Select **Use default value** and click the corresponding **Edit** button.
 - g. On the **Conditions** tab, click **Add**.
 - h. Enter the name of the condition (for example, PositionAppliedFor).
 - i. Click **OK**.
 - j. In the lower Value field, enter an appropriate statement (for example, Please specify the position title).
 - k. Click **OK**.
 - l. Click **OK**.
 - m. Click **OK**.

Create the Profile

To create the black-hole checkin profile:

1. Open the **Profile** tab on the [Configuration Manager Page](#) and click **Select**.
The [Add Profile Screen](#) opens.
2. Select **Type** from the Field Name drip down list.
3. Click **OK**.
4. Click **Add** on the **Profiles** tab.
The [Add Profile Screen](#) opens.
5. Enter the name of the profile (for example, BlackHoleResumeCheckIn).
6. Click **OK**.
The [Add/Edit Profile Screen](#) opens.
7. Enter the profile description in the Description field (for example, For internal user resumes only).
8. Select **HRresumes** (or the equivalent option) from the Trigger list.
9. Click **Add** to include the rules in this profile.
The [Add Rule in Profile Screen](#) opens.
10. Select the **NoExtraFields** rule from the Name list.
11. Select a general priority placement from the Rule Priority list.

12. Click **OK**.
13. Click **Add**.
14. Select the **VisibleFields** rule from the Name list.
15. Select a general priority placement from the Rule Priority list.
16. Click **OK**.
17. Click **OK**.

The screen closes and the profile is added to the list on the **Profiles** tab.

3.2.7.3 Global Rule to Restrict Content Check-In Based on User Role

This example illustrates how to create a global rule that can validate metadata fields when users check in content. The global rule validates the data in a request and returns an error message if the data is incorrect. This example shows how to allow only an administrator to check in content that specifies ADACCT as the Content Type.

Enable Fatal Error for a Global Rule Violation

1. In a text editor, open the *IntradocDir/config/config.cfg* file.
2. Add the following configuration setting:

```
IsDpSubmitErrorFatal=true
```
3. Close and save the file.
4. Restart the Oracle WebCenter Content Server.

Create Global Rule Restricting Content Type Check-ins

This global rule validates the value for dDocType and ensures that an administrator is checking in an ADACCT document. However, the rule is configured to affect only the Check In and Update pages.

1. Open the **Rules** tab on the [Configuration Manager Page](#), and click **Add**.
The [Add/Edit Rule Screen](#) opens.
2. On the **General** tab, enter the name of the global rule in the Name field (for example, *FailOnCheckInError*).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority** and change the priority number if needed.
5. Select **Use rule activation condition** and click the corresponding **Edit** button.
The [Edit Activation Condition Screen](#) opens.
6. Click **Add**.
The Add Condition Screen opens.
7. Enter the name of the condition in the Name field (for example, *CheckIn*).
8. Click **OK**.
The screen closes and the **General** tab opens. The clause-generating tabs display on the lower pane.
9. Select **Use event**.
10. Select **On Submit**.

11. Select **Use** action.
12. Select **Check in new**, **Check in selected**, and **Content update**.
13. Click **OK**.

The screen closes and the activation condition clause is entered into the Use rule activation condition text pane.

14. Click the **Fields** tab.
The [Add/Edit Rule Field 'name' Screen](#) opens.
15. Click **Add**.
The [Add Rule Field Screen](#) opens.
16. Select **Type** from the Field Name list.
17. Select a general position from the Field Position list (optional).
18. Click **OK**.
The [Add/Edit Rule Field 'name' Screen](#) opens.
19. Select **Is derived field** and click the corresponding **Edit** button.
The [Edit Derived Value: Conditions Tab](#) opens.

20. Click the **Custom** tab.

The Custom screen opens.

21. Select **Custom** and enter the following Idoc Script:

```
<$if dDocType like "ADACCT" and not userHasRole("admin")$>
<$abortToErrorPage("Only administrators can use ADACCT.")$>
<$endif$>
```

22. Click **OK**.
23. Click **OK**.
24. Click **OK**.

The rule is added to the list of Rules.

3.2.7.4 Global Rule Restricting Content Type Metadata Changes

This example shows how to create a global rule that can validate metadata fields when users check in content. The global rule validates the data in a request, and returns an error message if the data is incorrect. Specifically, this example shows how to allow only an administrator to change the content type of a checked-in document.

Enable Fatal Error for a Global Rule Violation

1. In a text editor, open the *IntradocDir/config/config.cfg* file.
2. Add the following configuration setting:
`IsDpSubmitErrorFatal=true`
3. Close and save the file.
4. Restart the Oracle WebCenter Content Server.

Create Global Rule to Restrict Content Type Changes

This global rule validates the value for dDocType and ensures that an administrator is changing the content type of a checked-in document. It is configured to affect only the Check In page.

1. Open the **Rules** tab on the [Configuration Manager Page](#) and click **Add**.
The [Add/Edit Rule Screen](#) opens.
2. On the **General** tab, enter the name of the global rule in the Name field (for example, `FailOnCheckInError`).
3. Enter a description for the global rule (optional).
4. Select **Is global rule with priority** and change the priority number if needed.
5. Select **Use rule activation condition** and click the corresponding **Edit** button.
The [Edit Activation Condition Screen](#) opens.
6. Click **Add**.
The Add Condition Screen opens.
7. Enter the name of the condition in the Name field (for example, `CheckIn`).
8. Click **OK**.
The screen closes and the Edit Activation Condition opens. The clause-generating tabs display on the lower pane.
9. Select **Use event**.
10. Select **On Submit**.
11. Select **Use action**.
12. Select **Content update**.
13. Click **OK**.
The screen closes and the activation condition clause is entered into the Use rule activation condition text pane.
14. Click the **Fields** tab.
The Fields Tab opens.
15. Click **Add**.
The [Add Rule Field Screen](#) opens.
16. Select **Type** from the Field Name list.
17. Select a general position form the Field Position list.
18. Click **OK**.
The [Add/Edit Rule Field 'name' Screen](#) opens.
19. Select **Is derived field** and click the corresponding **Edit** button.
The [Edit Derived Value: Conditions Tab](#) opens.
20. Click the **Custom** tab.
The Custom Screen opens.
21. Select **Custom** and enter the following Idoc Script:

```
<$oldType = getValue("DOC_INFO", "dDocType")$>
```

```
<$newType = getValue("#local", "dDocType")$>  
<$if not (newType like oldType) and not (userHasRole("admin"))$>  
<$abortToErrorPage("Only administrators can change dDocType.")$>  
<$endif$>
```

22. Click **OK**.

23. Click **OK**.

24. Click **OK**.

The rule is added to the list of Rules.

Using Workflows

This chapter provides concepts, tasks, and reference information for using the workflow functionality available with Oracle WebCenter Content Server.

This chapter contains the following topics:

- [Section 4.1, "Introduction to Workflows"](#)
- [Section 4.2, "Planning a Workflow"](#)
- [Section 4.3, "Creating a Criteria Workflow"](#)
- [Section 4.4, "Creating a Basic Workflow"](#)
- [Section 4.5, "Customizing Workflows"](#)
- [Section 4.6, "Workflow and Script Templates"](#)
- [Section 4.7, "Workflow Scenarios"](#)
- [Section 4.8, "Workflow Tips and Tricks"](#)
- [Section 4.9, "Workflow Troubleshooting"](#)

4.1 Introduction to Workflows

Workflows are used to specify how content is routed for review, approval, and release to the system.

For example, using a workflow ensures that the appropriate people in the Legal, Human Resource, and Executive teams review and approve new policies before being released on the organization's intranet. Or a workflow could be set up to obtain timely approval and sign-off on marketing material. Users receive e-mail notification when content in a workflow is ready for review.

Designing an effective workflow is an iterative process. After initial planning, workflows are refined as the process is implemented. Good planning in the beginning can reduce the amount of rework. For details, see [Section 4.2, "Planning a Workflow."](#)

There are three types of workflows:

- A *basic workflow* defines the review process for specific content items, and must be initiated manually.
- A *criteria workflow* is used for content that enters a workflow automatically based on metadata that matches predefined criteria.
- A *sub-workflows* is initiated from a step in another workflow and is created in the same manner as criteria workflows. Sub-workflows are useful for splitting large, complex workflows into manageable pieces.

Setting up workflows for your business processes can provide several advantages:

- Workflows provide good reporting metrics; workflows can produce an audit trail of who signed off on content at various points of the life cycle of the content.
- Workflows help you get the right information to the right person.
- Designing a workflow requires you to examine and understand your business processes, helping you find areas that you can improve.

This section provides an overview to workflows, their uses, and the advantages they can provide for your business operation. It discusses the following topics:

- [Section 4.1.1, "Workflow Steps"](#)
- [Section 4.1.2, "Workflow Step Evaluation Process"](#)
- [Section 4.1.3, "Workflow Participation"](#)

4.1.1 Workflow Steps

Steps define the process and the functionality of the workflow. Each workflow can include multiple review and notification *steps* with multiple reviewers to approve or reject the content at each step. For each step in a workflow, you must define a set of users and a *step type*.

The users defined for a step can perform only the tasks allowed for that step type:

Step Type	Description
Contribution	The initial step of a Basic workflow. Administrators define the contributors when the workflow is created.
Auto-Contribution	The initial step of a Criteria workflow. There are no predefined users involved in this step. The contributor who checks in a content item that enters the workflow process automatically becomes part of the workflow.
Review	Users can approve or reject the content; editing is not allowed. You can also specify that the user must approve and sign the content with an electronic signature.
Review/Edit Revision	Users can edit the content if necessary then approve or reject it, maintaining the revision.
Review/New Revision	Users can edit the content if necessary then approve or reject it, creating a new revision.

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.
- 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 can result in a new revision or an updated revision.
- You can release a revision to the system:

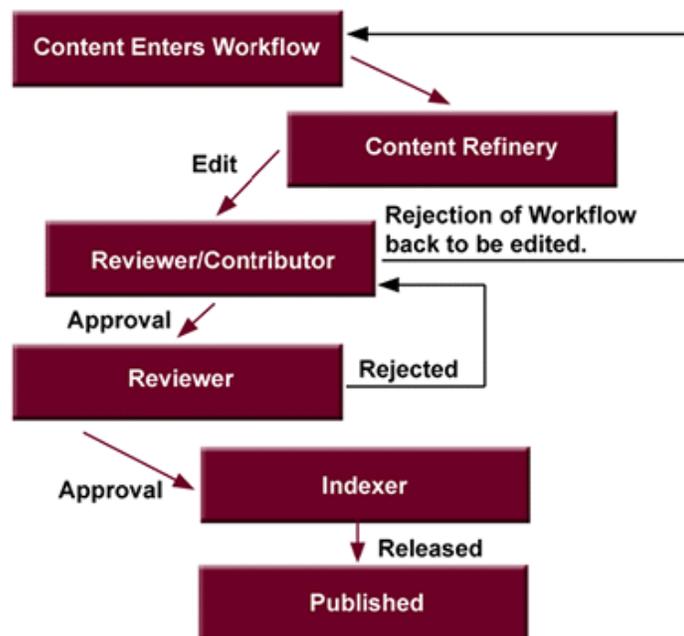
- After it exits the workflow: When content is approved at the last step in the workflow, the content item is released to the system.
- Before it exits the workflow: When you set up a side effect that releases a document from edit state, the document is available for indexing, searching, and archiving. Use this primarily for business routing that does not 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 you release a content item from the edit state as a side effect, you can release that content item without waiting for all items in the Basic workflow.

You can customize the standard workflow process and make it more flexible with *jumps*, *tokens*, and *aliases*. These are discussed fully in [Section 4.5, "Customizing Workflows."](#)

- *Tokens* and *aliases* provide flexibility in specifying users in a workflow. Tokens are variables that you can use to designate unknown users. You can use aliases to include a group of people in a workflow step.
- *Jumps* enable you to create conditional statements that can branch content through different paths in the same workflow, or can send content items from a Criteria or sub-workflow to a different Criteria or sub-workflow.
- *Exit conditions* enable you to create conditional statements that can prevent content from moving to the next step unless certain conditions are met, for example after metadata is changed by an external process during a workflow step.
- You can also create a *custom metadata* field and use it to trigger different workflows.

The following illustration shows a general workflow process.

Figure 4–1 Workflow Process



4.1.1.1 Events

Each step in a workflow has three events: entry, update, and exit.

- An *entry* event script is evaluated when entering the step. If the entry event script does not result in a jump or exit, any users, aliases, and tokens are evaluated and e-mail notifications are sent.
- An *update* event script is evaluated at various points (for example, during the hourly update cycle or on check in of the revision). Extra exit conditions are evaluated each time the update event script is evaluated.
- An *exit* event script is evaluated when a revision has completed the step's approval requirements and the step's extra exit conditions are met.

Jumps are discussed in more detail in [Section 4.5.3.1, "Jumps and Events."](#)

Important: Update and exit event scripts are *not* run when a revision is rejected. Any code to be evaluated on rejection must be in the *entry* event script for the step that the rejected content is sent to.

4.1.1.2 Workflow Files

The *companion file* is a text file that maintains information about the state of a revision in a workflow. It is only active for the life of the workflow.

- The companion file tracks the steps the revision has been through and maintains the current values of workflow variables.
- Each revision in a workflow has a companion file, which exists while the revision remains in the workflow. When a revision is released from a workflow, its companion file is deleted.
- Companion files are in HDA file format, and are named by Content ID (for example, HR_004.hda).
- Each companion file contains two sets of data:
 - The *LocalData* Properties section defines the Parent List and other workflow variables.
 - The *WorkflowActionHistory* ResultSet section contains a record of the steps, workflow actions, and users that have been involved in the revision's workflow history.

To retain a companion file, add the `IsSaveWfCompanionFiles` configuration variable to your `/config/config.cfg` file and set the parameter to `TRUE`. For more details, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

The companion file uses *keys* to keep track of workflow variables. For example, the following keys define the value of the `EntryCount` and `Last Entry` variables for an Editor step in a workflow called `Marketing Brochures`:

```
Editor@Marketing Brochures.entryCount=1
Editor@Marketing Brochures.lastEntryTs={ts '2001-05-02 16:57:00'}
```

The companion file maintains a *parent list*, which lists the sequence of steps that the revision has been through, starting with the current step and working backward. The parent list is used to determine which step to return to when a file is rejected, when the last step of a workflow is finished, or when an error occurs. For example, the following parent list shows the *Marketing Team*, *Editor*, and *Graphic Artist* steps of the *Marketing Brochures* workflow:

WfParentList=Marketing Team@Marketing Brochures#Editor@Marketing Brochures#Graphic Artist@Marketing Brochures#contribution@Marketing Brochures

An asterisk (*) in front of a step name in the parent list indicates a jump step.

4.1.2 Workflow Step Evaluation Process

When a revision enters a workflow step, it goes through the following process:

1. The entry script is evaluated.
 - The default entry script that keeps track of the entry count and last entry is updated.
 - Actions (such as additional user notification) are executed.
 - If the jump condition is met and a target step is defined, the revision jumps to another step.
 - If the jump condition is not met, reviewers for the current step are notified that the revision is ready for approval.
 - To avoid infinite loops, the entry script of a previously visited step is ignored. The only exception to this is when the step has been restarted using the `wfCurrentStep(0)` symbolic step.
2. When the required number of reviewers have approved the revision, the exit script is evaluated.
 - If there is no exit script, the revision goes to the next step in the workflow.
 - If an exit script jump condition is met and a target step is defined, the revision jumps to another step.
3. After the exit script is evaluated, the current action state (the `wfAction` workflow variable) is set. The following are the possible actions:
 - APPROVE
 - REJECT
 - CHECKIN
 - CONVERSION
 - META_UPDATE
 - TIMED_UPDATE
 - RESUBMIT
4. As a revision moves through the steps of a workflow, each step is added to the parent list. If the revision revisits a step, the parent list returns to the state it was in when the revision first visited that step. For example:

Revision goes to:	Parent list
Step1	Step1
Step2	Step1#Step2
Step3	Step1#Step2#Step3
Step2	Step1#Step2

5. If a revision is rejected, the parent list is checked for the most recent Reviewer/Contributor step, and the revision goes to that step in the workflow.
6. When a revision completes the last step in a workflow, the parent list is checked for the most recent jump step with a defined return step. If a return step is found, the revision goes to that step. If there are no jump steps in the parent list, or none of the jump steps have a return step defined, the revision exits the workflow.

Content items in a workflow can have the following statuses:

Status	Criteria Workflow	Basic Workflow
EDIT	The content item was rejected and returned to the initial contribution step.	The content item is in the initial contribution step, or the content item was rejected and returned.
REVIEW	The content item is in the review process.	The content item is in the review process.
PENDING	N/A	The content item completed all the workflow steps, but other content items in the workflow (if included) are not finished.
DONE	The content item in the workflow is finished.	All of the content items are finished.
GENWWW	The content is being converted to Web-viewable format.	The content is being converted to Web-viewable format.
RELEASED	The revision is available in the Oracle WebCenter Content Server.	The revision is available in the Oracle WebCenter Content Server.

4.1.3 Workflow Participation

E-mail is sent to the participating contributors in a Basic workflow who must check in designated content. E-mail is also sent to reviewers involved in workflow steps. Users can check their necessary actions on the Workflow Content Items page. To access the Workflow Content Items page, choose **Content Management** then **Active Workflows** from the Main menu.

Reviewers can review content, reject or approve content, and view information about the content and the workflow. If the content is rejected, the Reject Content Item page opens where the reviewer can enter a message to explain the reason for rejection. The message is sent to the reviewers assigned to the last step allowing a contribution. Those reviewers can then check out the content, edit it and check the content back in. On the Content Check In form, the reviewer should select the Revision Finished Editing box. The content then goes to the next step in the workflow. If the box is not selected, the content remains in Review status and must be approved before moving on through the workflow.

It is good practice to discuss workflows with the people involved so they are aware of the responsibilities they have in the process. More information about workflow participation is available in the *Oracle WebCenter Content User's Guide for Content Server*.

4.2 Planning a Workflow

This chapter describes the steps to follow to choose a workflow type and plan the workflow. The following topics are discussed:

- [Section 4.2.1, "Choosing a Workflow Type"](#)

- [Section 4.2.2, "Designing a Workflow"](#)
- [Section 4.2.3, "Modifying Workflows"](#)

Before beginning to design a workflow, evaluate how your processes currently operate. You may be able to adapt current processes into the workflow. For example, if you use e-mail loops to manage information between users on a project, can you incorporate that type of scenario into a workflow design?

Is the workflow being used to validate information? Or is it used for collaboration? What specific problem is it addressing? After you understand the current processes and their shortcomings, you can design the workflow to solve the problem.

Ask yourself the following questions when designing a workflow:

- Who is involved in the workflow? What users receive notification that an item is ready for review? Who has edit permissions on an item? Who has final sign-off on an item?
Equally important is to ask who is left out of a workflow?
How do you train the people who are involved in the workflow?
- What happens when an item is in the workflow? What action is taken when an item is approved, rejected, or updated? What should occur when an item stays in a workflow too long?
- When must an item be move to the next stage of a workflow? What is the criteria for determining when a workflow is completed?
- Where do users go to participate in a workflow? Is there a Web interface or some other interface of your design?
- How are approvals and rejections handled? Do you store audit information? Do you require approval or content item revision authentication (an electronic signature)?

4.2.1 Choosing a Workflow Type

Consider the following points when you decide which type of workflow to use.

Use a **Basic Workflow** when you must:

- Specify an 'ad hoc' workflow, one that does not depend on specific criteria to be enabled.
- Route multiple content items to go through the same series of steps. The items go through the steps individually, but are not released until all items are finished in the workflow.
- Notify or remind a user to contribute a content item to the workflow.
- Specify a workflow that is used infrequently.
- Set up the review process for a group of related content items.
- Specify a user to start the workflow. Content can enter a Basic workflow only when a user with Workflow rights starts the workflow.

Use a **Criteria Workflow** when you must:

- Have content enter a workflow automatically based on specific metadata values.
- Route single content items that match specific criteria. You can route multiple items that match the criteria but they do not progress through the workflow as a unit.

- Set up a standardized review process for individual documents.
- Specify a workflow that is used frequently.
- Open the workflow to many users. Users do not need Workflow rights for their content to enter a Criteria workflow.

When deciding which type of workflow to use, keep the following key points in mind:

- If content is checked in with the wrong security group or wrong metadata value, it can enter a Criteria Workflow accidentally.
- If users are frequently processing content through the same Basic workflow, consider setting up a Criteria workflow to automate the process.
- You cannot use the same or overlapping criteria for multiple workflows. If a content item matches the criteria for multiple workflows, it enters the first workflow in the list.

4.2.1.1 Security Issues

Keep the following security issues in mind when administering workflows:

- Each workflow is associated with a security group.
 - For a Criteria workflow, only content items in the same security group enter the workflow.
 - For a Basic workflow, new content items are assigned to the security group of the workflow, and existing content items must belong to the workflow's security group.
- A workflow can only jump to another workflow in the same security group.
- You cannot change the security group of a workflow while a workflow is active but you can change the security group of an item in the workflow process.
- You need Workflow rights and admin permission for the security group of the content to set up a workflow and start it.
- You can use workflow templates to initiate contribution steps.
- You need Write permission to the workflow's security group to be a contributor to the workflow.

4.2.2 Designing a Workflow

To design a workflow:

1. Draw a flowchart of the workflow. For examples, see [Section 4.3.1, "Criteria Workflow Process"](#) and [Section 4.4.1, "Basic Workflow Process."](#)
2. Verify you have all the metadata needed for the workflow. If not, create the necessary metadata before setting up the workflow.
3. Set up the aliases needed for the workflow. Alias creation is discussed in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.
4. Set up the tokens for the workflow. For details, see [Section 4.5.2.2, "Creating, Editing, or Deleting a Token."](#)
5. Set up a Basic or Criteria workflow. If workflow templates are available, consider using a template as a starting point. For details, see [Section 4.6, "Workflow and Script Templates."](#)
6. Set up sub-workflows as necessary.

7. Set up jumps as necessary. For details, see [Section 4.5.3.2, "Creating a Jump."](#)
 - If script templates are available, use them to create the step event scripts.
 - If jumps are used, consider setting up a "master" workflow with sub-workflows for each jump.
8. Test the workflow.
 - For a Criteria workflow, check in a test document that matches the defined security group and metadata field value.
 - For a Basic workflow, define test content and start the workflow.
 - Simulate as many approval/rejection scenarios as possible.
 - For workflows that contain jumps, simulate as many event scenarios as possible.
 - Include reviewers in the workflow testing to verify that people understand their roles.

4.2.3 Modifying Workflows

Keep these points in mind as you design your workflow:

You can:

- Modify the criteria for a Criteria workflow.
- Add or delete content items from a Basic workflow.
- Modify step definitions (including reviewers, exit conditions, and events)

You cannot:

- Change the *order* of the steps. You can delete steps and re-create them in new locations.
- Add steps in the middle of the workflow. New steps are always added to the end of the workflow.

The following tips can help when modifying existing workflows. Altering a workflow in use is a time-consuming and difficult process. Careful design before implementation can help avoid rework. These options are considered a temporary correction until you can rebuild the workflow.

Note: If you disable a Criteria workflow or cancel a Basic workflow to add or delete steps, any revisions in the workflow are released (Criteria workflow) or deleted (Basic workflow).

- Consider the following options to reorder steps in an existing workflow:
 - Create a sub-workflow and add a jump to it from an existing step. You can make this change to an existing step without disabling or canceling the workflow.
 - Add step event scripts to an existing step to define the actions that would normally take place in a separate step. You can make this change to an existing step without disabling or canceling the workflow.
- If you must disable a workflow to modify it (for example, to add a step) all revisions are immediately released from the workflow (Criteria workflow) or

deleted (Basic workflow). Follow these steps to disable a workflow without releasing content:

1. First clone the workflow to a static workflow which has the same step sequence as the original workflow but which has no step logic. The content goes into a step and stays there until moved.
2. Next create an update event in the original workflow. This event is triggered by time and pushes the content into the cloned static workflow at the appropriate step.
3. When the content is out of the original workflow, disable the workflow, make the necessary changes, then re-enable it. Then use the same timed event logic to move the content from the cloned workflow back to the original workflow.

4.3 Creating a Criteria Workflow

Criteria workflows are used to set up a review process for individual documents that enter the workflow automatically when they match predefined criteria. For example, any time a new purchase order is generated, it might be automatically routed to specific reviewers for approval.

A Criteria workflow includes the following:

- Criteria defined by a security group and one metadata field.
- Auto-contribution step with no predefined users.
- One or more reviewer steps with one or more reviewers per step.

Sub-workflows are set up using the same procedure as Criteria workflows with a few minor exceptions which are noted in the procedure for setting up Criteria workflows.

This section discusses the following topics:

- [Section 4.3.1, "Criteria Workflow Process"](#)
- [Section 4.3.2, "Setting Up a Criteria Workflow"](#)
- [Section 4.3.3, "Changing a Criteria Workflow or Sub-workflow"](#)
- [Section 4.3.4, "Disabling a Criteria Workflow or Sub-workflow"](#)

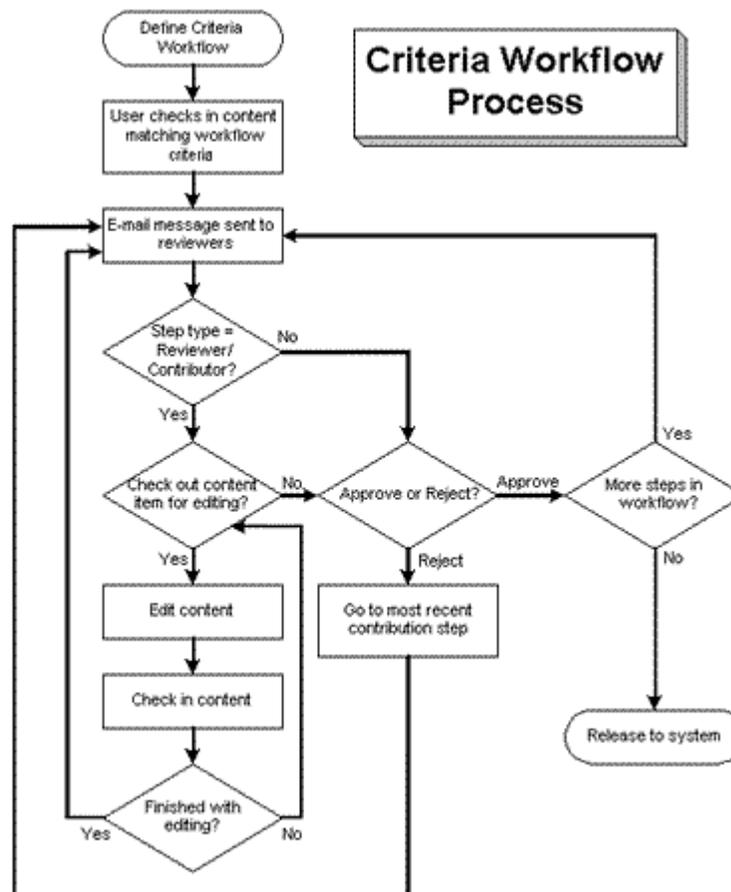
4.3.1 Criteria Workflow Process

The following steps briefly explain the Criteria workflow process:

1. A user with Workflow rights sets up the Criteria workflow by defining the following:
 - Security group
 - Metadata field and value (for example, *ContentType matches PurchaseOrder*). You can use fields of type Text or Long Text.
 - Review steps and reviewers for each step
 - The number of approvals required for each step. For example, must all reviewers approve it before it can move to the next step?
 - Any aliases and the people in the alias group
 - Any tokens needed
2. A user with Workflow rights enables the Criteria workflow.

3. When content is checked in that matches the defined security group and metadata field value, the content enters the workflow.
4. Reviewers for the first step receive e-mail that the revision is ready for review.
5. The reviewers approve or reject the revision.
 - If the step is a reviewer step, the reviewers can optionally sign and approve the content item revision without modification (changing the document produces a different identifier and invalidates any existing electronic signatures).
 - 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, editors can alter the content of an item in the workflow.
 - 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.

Figure 4–2 Criteria Workflow Process



4.3.1.1 Criteria Workflow Tips

Each Criteria workflow must have unique criteria. If a content item matches the criteria for two workflows, it enters the first one in the list of defined workflows.

- All users assigned to the Criteria workflow must have Read permission to the selected security group. Contributors must have Write permission to the selected security group to check the revision in and out.
- You cannot add or delete steps while a Criteria workflow is enabled.
- Any content item checked in while a Criteria workflow is disabled bypasses the workflow process and is released to the system.
- Disabling a Criteria workflow releases revisions in the workflow to the system.
- A Criteria workflow can use jumps to sub-workflows and other Criteria workflows in the same security group, and can jump to other steps in the same workflow.
- Consider making at least one step in the workflow a Reviewer/Contributor step so rejected revisions go to that step rather than back to the original author.
- If the security group of an item does not match the security group of the workflow, the item does not enter the workflow.
- Ensure that the criteria is different from other Criteria workflow.
- If Content ID is used for the Field and if an Oracle database is used, enter all uppercase characters for the Value. All other fields can have mixed case.
- If ContentID is used as the Field, click **Select** below the Value field to choose an existing content item.
- Enter zero (0) in the **At least this many reviewers** field to notify reviewers that the revision has reached the step and to pass it on to the next step automatically. Reviewers cannot approve, reject, or edit the revision at that step.

4.3.2 Setting Up a Criteria Workflow

Follow these steps to create a Criteria workflow or sub-workflow:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Workflow Admin**. Click the **Criteria** tab.
2. Click **Add**.
The [New/Edit Criteria Workflow Screen](#) opens.
3. Enter a name in the **Workflow Name** field. Maximum length is 30 characters. Special characters (; @ &, and so on) are not allowed. You cannot change the workflow name after the workflow is created.
4. Enter a detailed description for the workflow in the **Description** field.
5. Select the Security Group from the list to which the content items in this workflow belong.
6. Select an option from **Original Author Edit Rule**. to specify if the original author can edit the revision or create a new revision if the item is rejected.
7. To use a workflow template, select the **Use Template** check box and select the template name. This box is displayed only if a template currently exists. For details, see [Section 4.6, "Workflow and Script Templates."](#)

8. To create a Criteria workflow, select the **Has Criteria Definition** check box. To create a sub-workflow, clear the check box. You can also change this selection later.
9. For a Criteria workflow, define the criteria by choosing the appropriate **Field**, **Operator**, and **Value**. For example, *Review Process matches HRBenefits*. Field values include Content ID, Author, Type, Account and any custom metadata of type Text or Long Text.
10. Click **OK**.
11. If a template was not used to create steps or to add another step, click **Add** in the right pane of the Workflow Admin screen.
The [Add New/Edit Step Screen](#) opens.
12. Enter an appropriate **Name** for the step. You cannot change the name after the step is created. The name is usually descriptive of the step (for example, *EditorialReview* or *TechnicalReview*).
13. To require that a reviewer provide credentials for an electronic signature, select **Requires signature on approval**. This option is available only if you enabled the Electronic Signatures component.

An electronic signature uniquely identifies the contents of the file at a particular revision and associates the signature with a particular reviewer. If you select this option, the standard **Approve** action is replaced by the **Sign and Approve** action in the list of step options provided to the reviewer.
14. Enter a **Description** for the step.
15. Specify the authority level of the users for the step:
 - Users can review the current revision: Users can approve or reject the revision but cannot edit the revision.
 - Users can review and edit (replace) the current revision: Users can edit the revision, approve it, or reject it. An edit does not update the revision.
 - Users can review the current revision or create new revision: Users can edit the revision, approve it, or reject it. An edit updates the revision. This option preserves the original content and provides an audit trail of changes.
16. Select the type of users to be added to the step. You can define multiple types of user for a step:
 - To add a group of users defined by an alias, click **Add Alias**. The [Add Alias to Step Screen](#) opens. Choose the alias from the displayed list.
 - To add individual user logins, click **Add User**. The [Add User to Step](#) opens.
 - To narrow the list of users, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
 - To select a range of users, click the first user, then press **Shift** and click the last user in the range.
 - To select users individually, press **Ctrl** and click each user name.
 - To add a variable user defined by a token, click **Add Token**. The [Add Token to Step](#) screen opens. See [Section 4.5.2.2, "Creating, Editing, or Deleting a Token"](#) for details about creating tokens.
17. Click **OK**.
18. Click the **Exit Conditions** tab.

19. Specify how many reviewers must approve the revision before it passes to the next step.
 - To require approval by all reviewers, select **All reviewers**.
 - To specify a minimum number of reviewers who must approve the revision, select **At least this many reviewers** and enter the number.
20. Typically, exit conditions are useful when metadata could be changed by an external process during the workflow step. Use the following instructions if the step requires additional exit conditions to pass to the next step:
 - a. Select the **Use Additional Exit Condition** check box.
 - b. Click **Edit**.
The [Edit Additional Exit Condition Screen](#) opens. You can use this screen to select additional criteria from lists.
 - c. Select a workflow condition or a metadata field from the **Field** list.
 - d. Select an operator from the **Operator** list. **Operator** is a dependent choice list that shows operators associated with the Field.
 - e. Select a value from the **Value** list. **Value** is a dependent list based on the option chosen as the Field.
 - f. Click **Add** to add the conditional statement to the Condition Clause. The clause appears in the Condition Clause box. You can append multiple clauses with AND statements.
 - g. Repeat for as many conditions as required. To modify an expression, select it in the Condition Clause box, change the Field, Operator, or Value, and click **Update**.
 - h. To modify the condition expression, select the **Custom Condition Expression** check box and edit the script (for example, use OR not AND for a condition). The additional exit conditions must be Idoc Script statements that evaluate to true or false. Do not enclose the code in Idoc Script tags <\$ \$>.

Caution: If you clear the **Custom Condition Expression** check box, the expression reverts to its original definition; all modifications are lost.

 - i. Click **OK**.
21. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts. For details, see [Section 4.5.3.2, "Creating a Jump."](#)
22. Click **OK**.
23. Add, edit, and delete steps as necessary to complete the workflow.
 - To add another step to the workflow, repeat steps 11 through 22.
 - To edit an existing step, select the step and click **Edit**.
 - To delete an existing step, select the step and click **Delete**.
24. Ensure that the correct workflow is selected in the left pane, and click **Enable**.
A confirmation screen opens.

25. Click **Yes** to activate the selected workflow.

4.3.3 Changing a Criteria Workflow or Sub-workflow

To change an existing Criteria workflow or sub-workflow:

Note: If you disable a Criteria workflow to add or delete steps, any revisions in the workflow are released.

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Workflow Admin**. Click the **Criteria** Tab.
2. Select the workflow you want to change in the left pane.
3. To add or delete steps, click **Disable** to disable the workflow.
4. Click **Add**, **Edit**, and **Delete** in the left and right panes to change the following:
 - workflow description
 - security group
 - type of workflow (Criteria or sub-workflow)
 - criteria
 - step description
 - type of step (reviewer, contributor same revision, contributor new revision)
 - users
 - events
 - number of approvals required
 - exit conditions

You can add users to a step while the Criteria workflow is enabled, but if any revisions are currently at that step in the workflow, the new users are not notified immediately. They are notified after the scheduled workflow system event occurs and performs a `TIMED_UPDATE` on all items in the workflow.

5. If the workflow is disabled, ensure that the correct workflow is selected in the left pane and click **Enable**.

A confirmation screen opens.

6. Click **Yes** to activate the selected workflow.

4.3.4 Disabling a Criteria Workflow or Sub-workflow

To disable a criteria workflow or sub-workflow:

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Workflow Admin**. Select the **Criteria** Tab.
2. Select the workflow.
3. Click **Disable**.
4. If there are any content items still in the workflow process, you are notified that all of the content revisions will be released. If you do not want to release the content, click **No** to cancel the operation. Click **Yes** to release any content and disable the workflow.

The status of the workflow changes to **Disabled**.

4.4 Creating a Basic Workflow

A Basic workflow defines the review process for specific content items. A Basic workflow is set up and initiated manually, and does not require you to define criteria for content to enter the workflow.

A Basic workflow includes the following:

- One or more content items.
- Initial contribution step with one or more contributors.
- Zero or more review steps with zero or more reviewers per step.

This section discusses the following topics:

- [Section 4.4.1, "Basic Workflow Process"](#)
- [Section 4.4.2, "Basic Workflow Tips"](#)
- [Section 4.4.3, "Setting Up a Basic Workflow"](#)
- [Section 4.4.4, "Changing a Basic Workflow"](#)

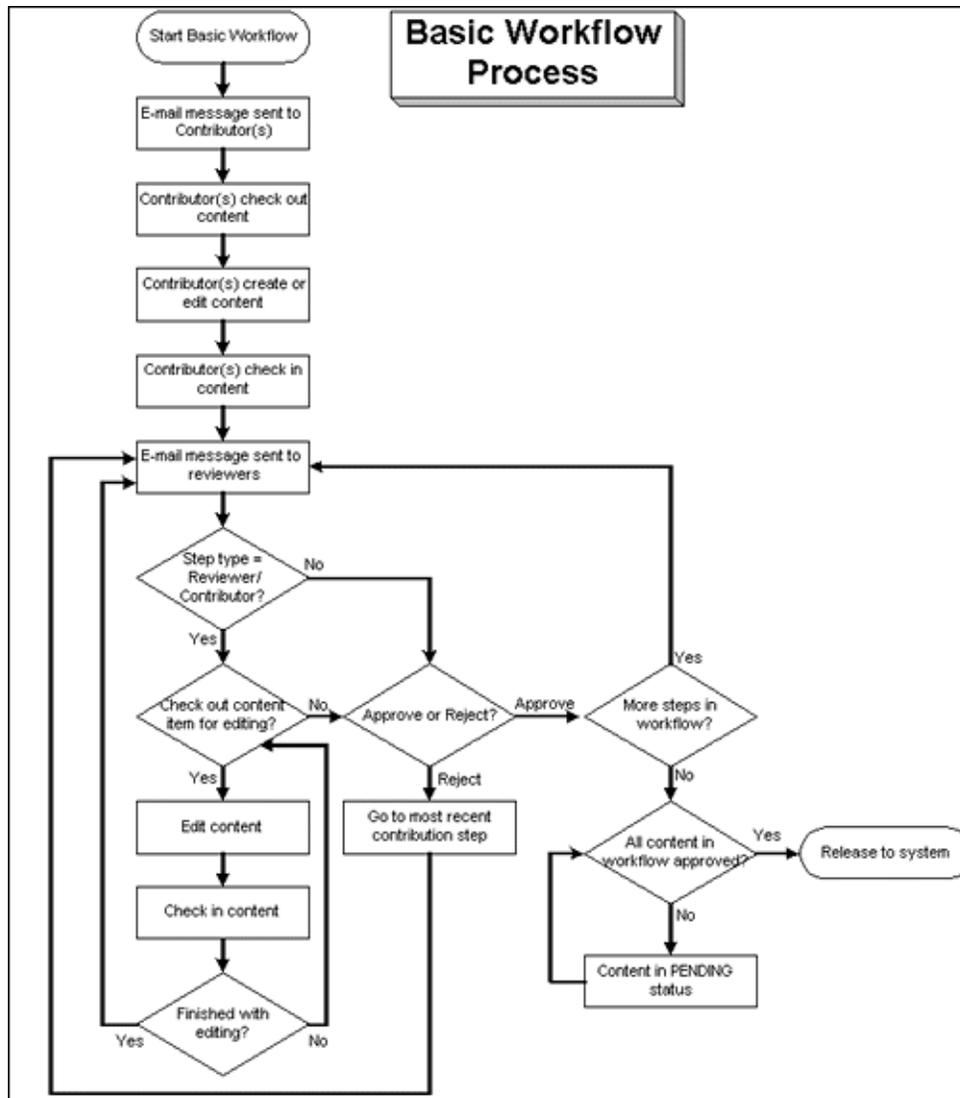
4.4.1 Basic Workflow Process

The following steps explain the Basic workflow process:

1. A user with Workflow rights sets up the Basic workflow by defining the following items:
 - **Content:** You can create new content and select existing content. After going through the workflow, new content is released to the system at revision 1, and existing content is released to the system at the next revision number for that content item.
 - **Initial contributors:** Specify the list of user who can contribute content.
 - **Review steps:** Specify the reviewers for each step and number of approvals required for each step.
2. A user with Workflow rights starts the Basic workflow by enabling it.
3. An e-mail is sent to the contributors.
4. Any of the contributors can check out then check in a file for each content item in the workflow.
5. Reviewers for the first step are notified by e-mail that the revisions are ready for review.
6. The reviewers approve or reject the revisions.
 - If the step permits editing, the reviewers can check out the revisions, edit them, and check them back in before approving it.
 - If a user rejects a revision, the revision 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.)

7. Generally, if a Basic workflow contains multiple files, none of them are released to the system until all of the files have been released from completion of the workflow. Completed content items stay in PENDING status until the last revision is approved. However, if you release a content item from the edit state as a side effect, you can release that content item without waiting for all items in the Basic workflow.
8. When all steps are complete and all revisions are approved, the revisions are released to the system.

Figure 4–3 Basic Workflow Process



4.4.2 Basic Workflow Tips

- For new content, the Content ID defined in the workflow is the Content ID applied when the revision is released to the system. You cannot change the Content ID after you create it.
- You cannot add a content item to multiple basic workflows or an error occurs and the workflow is not enabled.

- New content is assigned to the security group of the Basic workflow.
- The security group of an existing revision must match the security group of the Basic workflow.
- All users assigned to the Basic workflow must have Read permission to the selected security group. Contributors must have Write permission to the selected security group to edit revisions.
- You cannot add, edit, or delete review steps while a Basic workflow is active.
- You can cancel an active workflow, but any revisions in the workflow are deleted from the system. Any edits that have been made to the files are lost unless they have also been saved on a local hard drive.
- You can reuse an inactive Basic workflow, but it must be started manually each time.
- A Basic workflow can use jumps, but only to other steps in the same workflow. A Basic workflow cannot jump to a sub-workflow.

4.4.3 Setting Up a Basic Workflow

Keep these points in mind before creating a Basic workflow:

- All users assigned to the workflow must have Read permission to the selected security group, and Contributors must have Write permission.
- When you use a template, change the reviewers if they are different from those defined in the selected template.
- Do not add a content item to multiple basic workflows or an error occurs and the workflow is not enabled.
- You can enter zero (0) in the **At least this many reviewers** field to notify reviewers that the revision has reached the step, but reviewers cannot approve, reject, or edit the revision at that step. The workflow passes to the next step automatically.

Use the following steps to create a Basic workflow:

1. Display the [Workflow Admin: Workflows Tab](#). The default tab view is that of a Basic workflow.
2. Click **Add**.
The [Add New/Edit Workflow Screen](#) opens.
3. Enter a name in the **Workflow Name** field. The Workflow Name has a maximum field length of 30 characters and cannot contain special characters (; @ &, and so on). You cannot change the **Workflow Name** after you create the workflow.
4. Enter a detailed description for the workflow in the **Description** field.
5. Select the Security Group from the list to which the content items in this workflow belong.
6. Select an option from **Original Author Edit Rule** to specify if the original author can edit the existing revision or create a new revision if the content item is rejected.
7. To use a template, select the **Use Template** check box and select the template name. This box is displayed only if a template exists. For details, see [Section 4.6, "Workflow and Script Templates."](#)
8. Click **OK**.

9. To add a new content item to the workflow, click **New**.

The [Add Content to Workflow \(New Content\) Screen](#) opens.

- a. Enter a Content ID for the new content item. You cannot change the Content ID after you create the content item. A maximum length of 30 characters is allowed. No special characters (\$, #, and so on) are allowed. To change a Content ID, delete the content item from the list and add a new content item. If you are using an Oracle database, all Content IDs are converted automatically to uppercase letters.
- b. Click **OK**.

10. To add an existing content item to the workflow, click **Select**.

The [Add Content to Workflow \(Existing Content\) Screen](#) opens.

- To narrow the list of content items, specify criteria for the filter, release date or both.
- To select a range of content items, click the first content item, then press **Shift** and click the last content item in the range.
- To select content items individually, press **Ctrl** and click each content item.

Existing content items must have the same security group as the workflow.

11. Repeat steps 9 and 10 as necessary to add content items to the workflow.

12. Define one or more contributors for the initial contribution step. You can define multiple types of users for the contribution step.

- To add a group of users defined by an alias, click **Add Alias**. The [Add Alias to Workflow Screen](#) opens.
- To add individual user logins, click **Add User**. The [Add User: Basic Workflow](#) screen opens.
 - To narrow the list of users, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
 - To select a range of users, click the first user, then press **Shift** and click the last user in the range.
 - To select users individually, press **Ctrl** and click each user name.

13. If a template was not used to create review steps, or to add another step, click **Add** in the right pane near the Steps box.

The [Add New/Edit Step Screen](#) opens.

14. Enter an appropriate **Name** for the step. You cannot change the name after the step is created. The name is usually descriptive of the step (for example, *EditorialReview* or *TechnicalReview*).

15. To require that a reviewer provide credentials for an electronic signature, select **Requires signature on approval**. This option is available only if you enabled the Electronic Signatures component.

An electronic signature uniquely identifies the contents of the file at a particular revision and associates the signature with a particular reviewer. If you select this option, the standard **Approve** action is replaced by the **Sign and Approve** action in the list of step options provided to the reviewer.

16. Enter a **Description** for the step.

17. Specify the authority level of the users for the step.

- Users can review the current revision: Users can approve or reject the revision.
 - Users can review and edit (replace) the current revision: Users can edit the revision, approve it, or reject it. Any edit does not update the revision of the content item.
 - Users can review the current revision or create new revision: Users can edit the revision, approve it, or reject it. Any edit updates the revision of the content item which preserves the original content and provides an audit trail of changes.
18. Select the type of users to be added to the step. You can define multiple types of user for a step:
- To add a group of users defined by an alias, click **Add Alias**. The [Add Alias to Step Screen](#) opens.
 - To add individual user logins, click **Add User**. The [Add User: Basic Workflow](#) screen opens. To narrow the list use the **Use Filter** check box; to select a range of users, click the first user, then press **Shift** and click the last user name in the range. To select users individually, press **Ctrl** key and click each user name.
 - To add a variable user defined by a token, click **Add Token**. The [Add Token: Basic Workflow](#) screen opens. For details, see [Section 4.5.2.2, "Creating, Editing, or Deleting a Token."](#)
 - Click the **Exit Conditions** tab.
 - Specify how many reviewers must approve the revision before it passes to the next step.
 - To require approval by all reviewers, select **All reviewers**.
 - To specify a minimum number of reviewers who must approve the revision, select **At least this many reviewers** and enter the number.
19. Typically, exit conditions are useful when metadata could be changed by an external process during the workflow step. Use the following instructions if the step requires additional exit conditions to pass to the next step:
- a. Select the **Use Additional Exit Condition** check box.
 - b. Click **Edit**.
 - c. The [Edit Additional Exit Condition Screen](#) opens. You can use this screen to select additional criteria from lists.
 - d. Select a workflow condition or a metadata field from the **Field** list.
 - e. Select an operator from the **Operator** list. **Operator** is a dependent list that shows operators associated with the Field.
 - f. Select a value from the **Value** list. **Value** is a dependent list based on the option chosen as the Field.
 - g. Click **Add** to add the conditional statement to the Condition Clause. The clause appears in the Condition Clause box. You can append multiple clauses with **AND** statements.
 - h. Repeat for as many conditions as required. To modify an expression, select it in the Condition Clause box, change the Field, Operator, or Value, and click **Update**.
 - i. To modify the condition expression, select the **Custom Condition Expression** check box and edit the script (for example, use **OR** not **AND** for a condition).

The additional exit conditions must be Idoc Script statements that evaluate to true or false. Do not enclose the code in Idoc Script tags <\$ \$> .

Caution: If you clear the **Custom Condition Expression** check box, the expression reverts to its original definition; all modifications are lost.

- j. Click **OK**.
20. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts. For more information, see [Section 4.5.3.2, "Creating a Jump."](#)
21. Click **OK**.
22. Add, edit, and delete steps as necessary to complete the workflow.
 - To add another user to the initial contribution step, repeat step 12.
 - To delete a user from the initial contribution step, click **Delete**.
 - To add another review step to the workflow, repeat steps 13 through 21.
 - To edit an existing review step, select the step and click **Edit**.
 - To delete an existing review step, select the step and click **Delete**.
23. Ensure that the correct workflow is selected in the left pane, and click **Start**.
The [Start Workflow Screen](#) opens.
24. Enter a message to be sent to the contributors.
25. Click **OK**.

4.4.4 Changing a Basic Workflow

Follow these steps to change an existing Basic workflow:

1. Display the [Workflow Admin: Workflows Tab](#).
2. Select the workflow you want to change in the left pane.
3. To change the workflow security group or the number of review steps in an active workflow, first click **Cancel** to cancel the workflow.
4. Click **Edit** in the left pane to change the workflow description or the security group.
5. Click **New**, **Select**, and **Delete** in the Content pane to add or delete content from the workflow.
6. Click **Add Alias**, **Add User**, and **Delete** in the Contributors pane to add or delete contributors from the initial contribution step.

Caution: You can change content items in a Basic workflow after it has been started, but the contributors are not notified automatically. You can also change contributors in a Basic workflow after it has been started, but any new contributors are not notified immediately.

7. Click **Add**, **Edit**, and **Delete** in the **Steps** pane to change the following:

- Requires signature on approval (optional Electronic Signatures option)
- Step description
- Type of step (reviewer or reviewer/contributor)
- Users
- Events
- Number of approvals required
- Exit conditions

4.5 Customizing Workflows

You can use tokens and jumps to customize your workflows to accommodate different business scenarios. A *token* defines variable users in a workflow and a *jump* branches a workflow to a different side effect.

This section describes how to set up and use tokens and jumps. It discusses the following topics:

- [Section 4.5.1, "Idoc Script Functions and Variables"](#)
- [Section 4.5.2, "Workflow Tokens"](#)
- [Section 4.5.3, "Workflow Jumps"](#)

4.5.1 Idoc Script Functions and Variables

Jumps and tokens are created using Idoc script. The interfaces create the correct syntax and usage for you when you create tokens and jumps. However, you can customize your scripts using the following Idoc Script functions. See the *Oracle WebCenter Content Idoc Script Reference Guide* for complete details about usage.

Idoc Script Functions

Function	Description
wfAdditionalExitCondition	Retrieves the exit condition defined for the current step.
wfAddUser	Adds a user, alias, or workflow token to the list of reviewers for a workflow. Use this function only inside a token.
wfCurrentGet	Retrieves a local state value from the companion file.
wfCurrentSet	Sets the local state value of a key in the companion file.
wfCurrentStep	Retrieves the name of a step relative to the current step.
wfDisplayCondition	Retrieves the exit condition for a workflow step.
wfExit	Exits a workflow step. Can be used to exit the workflow.
wfGet	Retrieves a state value from the companion file.
wfGetStepTypeLabel	Takes an internal workflow step value and turns it into a human-readable label.
wfIsReleasable	Indicates if the document is released (as far as the workflow is concerned).
wfJumpMessage	Defines a message to be included in the notification e-mail that is issued when a jump is entered.

Function	Description
wfLoadDesign	Used to retrieve information about the existing steps in a workflow or about the exit conditions in a workflow.
wfNotify	Sends an e-mail to a specified user, alias, or workflow token.
wfReleaseDocument	Causes a workflow to release all outstanding document revisions for a document currently being locked by the workflow.
wfSet	Sets a key with a particular value in the companion file.
wfUpdateMetaData	Defines a metadata value for the current content item revision in a workflow.

Idoc Script Variables

Variable	Description
wfAction	The action currently being performed on the revision.
wfJumpEntryNotifyOff	Turns on/off the jump notification.
wfJumpName	The name of the current jump.
wfJumpReturnStep	The name of the step in the parent workflow that the revision returns to when exiting a workflow after the current jump.
wfJumpTargetStep	The name of the step where the revision jumps if the conditions are met.
wfMailSubject	Defines the subject line of a workflow e-mail notification.
wfMessage	Defines a message to be included in a workflow e-mail notification.
wfParentList	List of the workflow steps that the revision has visited.
wfStart	Sends the revision to the first step in the current workflow.

4.5.2 Workflow Tokens

You can use a token for the following purposes:

- Add a variable to a workflow which is interpreted to be a specific user or class of user when the workflow is run.
- Include users and aliases in workflow jumps.
- Define users with conditional statements.

A token assignment is unique and local to each document in a workflow. The logic used to assign the token of one document does not affect other documents in the workflow.

Several sample workflow tokens are included in the Workflow Admin application. You can use them as-is, or you can modify them to create your own workflow tokens.

Important: If a token does not resolve to any valid user names, the token is ignored. If no valid users are defined for a step, the revision moves to the next step in the workflow. For this reason, it is a good idea to identify at least one defined user for each step.

This section discusses the following information about tokens:

- [Section 4.5.2.1, "Token Syntax"](#)
- [Section 4.5.2.2, "Creating, Editing, or Deleting a Token"](#)
- [Section 4.5.2.3, "Token Examples"](#)

4.5.2.1 Token Syntax

The Idoc Script function for tokens, `wfAddUser`, takes two parameters:

- **User:** The metadata field, alias name, or a variable that resolves to a user name or alias.
- **Type:** The type of token, either user or alias.

All Idoc Script commands begin with `<$` and end with `>$` delimiters. For example:

```
<$wfAddUser(dDocAuthor, "user")$>
<$wfAddUser("MktTeam", "alias")$>
<$wfAddUser("myUserList", "alias")$>
```

See the *Oracle WebCenter Content Idoc Script Reference Guide* for more information about Idoc Script syntax and usage.

4.5.2.2 Creating, Editing, or Deleting a Token

Follow these steps to create a token to represent one or more unspecified users, such as the document author:

1. Choose **Administration** then **Admin Applets** from the Main menu. Choose **Workflow Administration**. Choose **Tokens** from the **Options** menu.
The [Workflow Tokens Screen](#) opens.
2. Click **Add**.
The [Add/Edit Token Screen](#) opens.
3. Enter a token name in the **Token Name** field. You cannot change the **Token Name** after you create the token. Try to use a descriptive name for the token (for example, *GetOriginalAuthor*, or *AuthorManager*).
4. Enter a detailed description in the **Description** field.
5. Click **Add**.
The [Add Token User Screen](#) opens.
6. Select **User** or **Alias**.
7. Enter a metadata field that will resolve to a user or alias.
 - To specify the original author of the content item, enter **dDocAuthor**.
 - To specify an alias, type the alias name. See the **Screen Aliases** tab on the User Admin screen for a list of defined aliases.
8. Click **OK**. The Idoc Script containing the value you specified is shown in the **User** window.
9. Repeat steps 5 through 8 to add another user or alias.
10. To create a conditional token, edit the **Users** field. For an example, see [Section 4.5.2.3, "Token Examples."](#)
11. Click **OK**.

To change an existing workflow token, follow the previous steps and select the token to change. Click **Edit**. Make any necessary changes and click **OK**.

To delete a token, select the token from the list and click **Delete**.

4.5.2.3 Token Examples

The following examples illustrate how you can use tokens in workflows.

Example 4–1 Original Author the Only Contributor

This example assumes that the original author is the only contributor for the file. [Example 4–2](#) addresses the situation where different authors could check out and check in the file during the workflow process.

Suppose you want to notify the original author of each file when their content is released from a workflow into the system. You would first create a token that corresponds to the **Author** metadata field, which is called `dDocAuthor` in Idoc script. When you set up the workflow, you can create a notification step (0 approvals required) and select the token as the user for that step. The token script would look like the following example:

```
<$wfAddUser(dDocAuthor, "user")$>
```

Example 4–2 Workflow with Reviewer/Contributor Steps

If a workflow includes Reviewer/Contributor steps, a user other than the original contributor could check in a revised file, and the `dDocAuthor` would no longer be the original author. In this case, you could set a workflow variable called `OriginalAuthor` in the companion file using custom script in the first workflow step, and specify the custom variable in the token instead of using `dDocAuthor`.

The event script in the first step might look like the following:

```
<$wfSet("originalContributor", dDocAuthor)$>
<$wfSet("type", user)$>
```

And the token script for the notification step would look like:

```
<$wfAddUser(wfGet("originalContributor"), wfGet("type"))$>
```

Example 4–3 Reviewers Selected Based on Jump Criteria

One typical use for tokens is to select reviewers as needed, or based on the conditions of a jump. Suppose you have a workflow set up for standard routing of all marketing materials through the Marketing department. However, you want any changes to your company catalogs to also be reviewed by the Distribution department.

You could create a jump that adds a token to the list of reviewers whenever the Type is `catalog`. The token script would look like:

```
<$wfAddUser("Dist_Dept", "alias")$>
```

Example 4–4 Conditional Token

Rather than creating a jump script for the previous example, you could define a conditional token that adds the `Dist_Dept` alias whenever the Type is `catalog`. The token script would look like the following:

```
<$if dDocType like "catalog"$>
  <$wfAddUser("Dist_Dept", "alias")$>
<$endif$>
```

Example 4–5 Token Specifying Management Chain

Another common use for tokens is specifying the current user's manager as a reviewer. (The manager attribute must be specified as a user information field in Oracle WebCenter Content Server, or as a user attribute in an external directory such as LDAP or ADSI.) The token script would look like:

```
<$wfAddUser (getUserValue("uManager"), "user") $>
```

4.5.3 Workflow Jumps

Jumps enable you to customize workflows for your system, your content, and your users. A jump is usually a conditional statement, written in Idoc Script.

Typical uses of jumps include:

- Specify multiple metadata fields as the criteria to enter a workflow.
- Take action on content automatically after a certain amount of time has passed.
- Define different paths for files to move through the same workflow depending on metadata and user criteria.
- Release a workflow document before approval by using the side effect: *Release document from edit state*.

The following is an example of a jump that exits the workflow if the author is *sysadmin*:

```
<$if dDocAuthor like "sysadmin" $>
  <$wfSet("wfJumpName", "Entry step") $>
  <$wfSet("wfJumpTargetStep", wfExit(0, 0)) $>
  <$wfSet("wfJumpEntryNotifyOff", "0") $>
<$endif $>
```

In most cases, a jump includes a conditional statement. However, you can create a jump that consists of non-conditional code, such as the following:

```
<$wfSet("custom_wf_variable", new_value) $>
  <$wfSet("wfJumpTargetStep", step_1) $>
```

You can use this type of jump to execute code or move a revision to another step automatically.

This section covers the following topics about jumps:

- [Section 4.5.3.1, "Jumps and Events"](#)
- [Section 4.5.3.2, "Creating a Jump"](#)
- [Section 4.5.3.3, "Changing a Jump"](#)
- [Section 4.5.3.4, "Jump Examples"](#)
- [Section 4.5.3.5, "Jump Errors"](#)

4.5.3.1 Jumps and Events

As mentioned in [Events](#) each step in a workflow has an entry, update, and exit event.

You can define a script with one or more jumps for any or all of the events in a step. Any Idoc Script defined for an event is evaluated at a specific time that depends on the type of event:

- An **entry event script** is evaluated upon entering the step. Every time a step is entered, a default script is evaluated in addition to any user-defined custom script. The default script keeps track of the number of times the step has been entered (`entryCount`) and the last time the step was entered (`lastEntryTs`).

If the entry event script does not result in a jump or exit, any users, aliases, and tokens are evaluated, and e-mail notifications are sent.

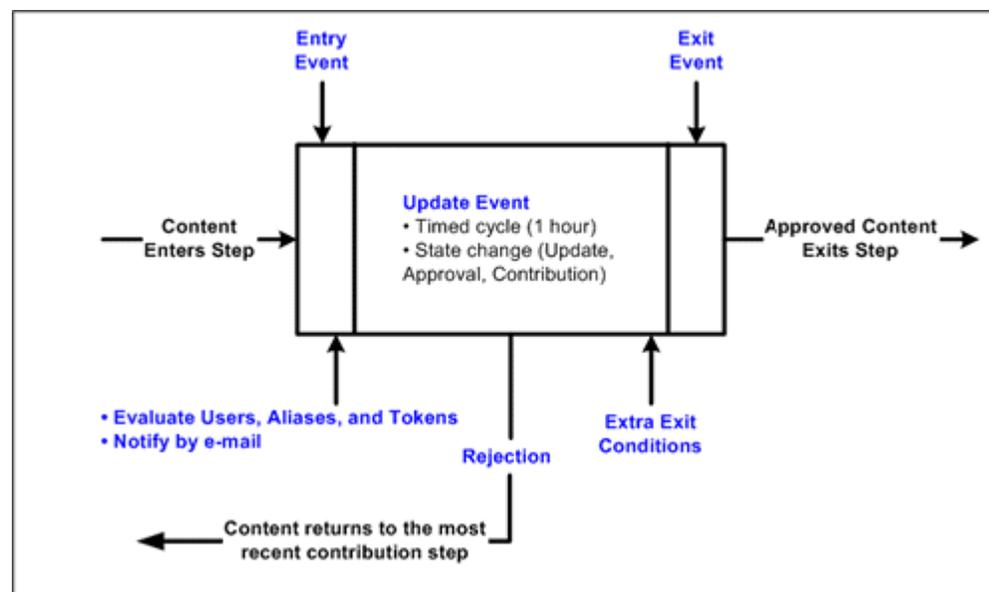
- An **update event script** is evaluated and triggered by a state change of the content, such as the workflow update cycle, the update of the revision's metadata or approval or check in of the revision.

Extra exit conditions are evaluated each time the update event script is evaluated.

- An **exit event script** is evaluated when a revision has completed the step's approval requirements and the step's extra exit conditions are met.

By default, the workflow update cycle occurs hourly. You can increase this cycle time in increments of one hour (using the `WorkflowIntervalHours` configuration setting), but you cannot reduce the to less than one hour. To have update scripts evaluated more often or in response to other events, you can initiate a metadata update cycle without changing any metadata.

Figure 4–4 Jumps and Events



4.5.3.1.1 Rejected Content Within a single workflow, when a reviewer rejects a revision the content item is routed back to the most recent contribution step.

However, when a jump is made to a sub-workflow or other workflow and content is rejected there, different behavior occurs. The process returns to the parent workflow, not to the previous contribution step.

Important: Update and exit event scripts of the current step are not run when a revision is rejected. Any code that is to be evaluated upon rejection must be located in the entry event script for the step that the rejected file is sent to.

4.5.3.1.2 Side Effects Side effects are the actions that take place when a revision in a workflow step meets the jump condition. Side effects can include:

- Jump to another step in the same workflow
- Jump to a step in a sub-workflow or other Criteria workflow (for Criteria workflows only)
- Notify users
- Exit the workflow
- Set state information in the companion file
- Release a workflow document before approval

You can generate side effects automatically with selections on the [Script Properties Screen](#) and [Add/Edit Jump Screen](#), and you can specify custom side effects in the Custom Effects field on the [Add/Edit Jump Screen](#).

4.5.3.1.3 Jump Variables and Steps A jump can include a *target step*, which tells the workflow where to go to if the content meets the jump condition. The following is an example of a target step that sends the content to the next step in the workflow:

```
<$wfSet("wfJumpTargetStep", wfCurrentStep(1))$>
```

A jump can also include a *return step*, which tells the workflow where to go if the content is returning from another workflow. The following is an example of a return step that sends the content to the next step in the workflow:

```
<$wfSet("wfJumpReturnStep", wfCurrentStep(1))$>
```

A *step name* variable, `step_name@workflow_name`, is assigned to each step in a workflow. There are two ways to reference a step in a jump:

- **Explicit** reference is made to a specific step name, such as `Editor@Marketing Brochures`.
- **Symbolic** reference is made relative to the current step and workflow, such as `wfCurrentStep(-1)` (previous step) or `wfStart` (first step in the workflow).

Tip: Use symbolic references rather than explicit step names whenever possible especially when creating a script template.

The *entry count* variable, `entryCount`, keeps track of how many times a step has been entered and is part of the default entry script that is updated each time a step is entered. The following is an example of how an entry count variable is used in a conditional statement:

```
<$if entryCount = 1$>
```

The *last entry* variable, `lastEntryTs`, keeps track of when the step was last entered and is part of the default entry script that is updated each time a step is entered. The following is an example of how the last entry variable is used to specify that action should occur if the step has not been acted on within seven days:

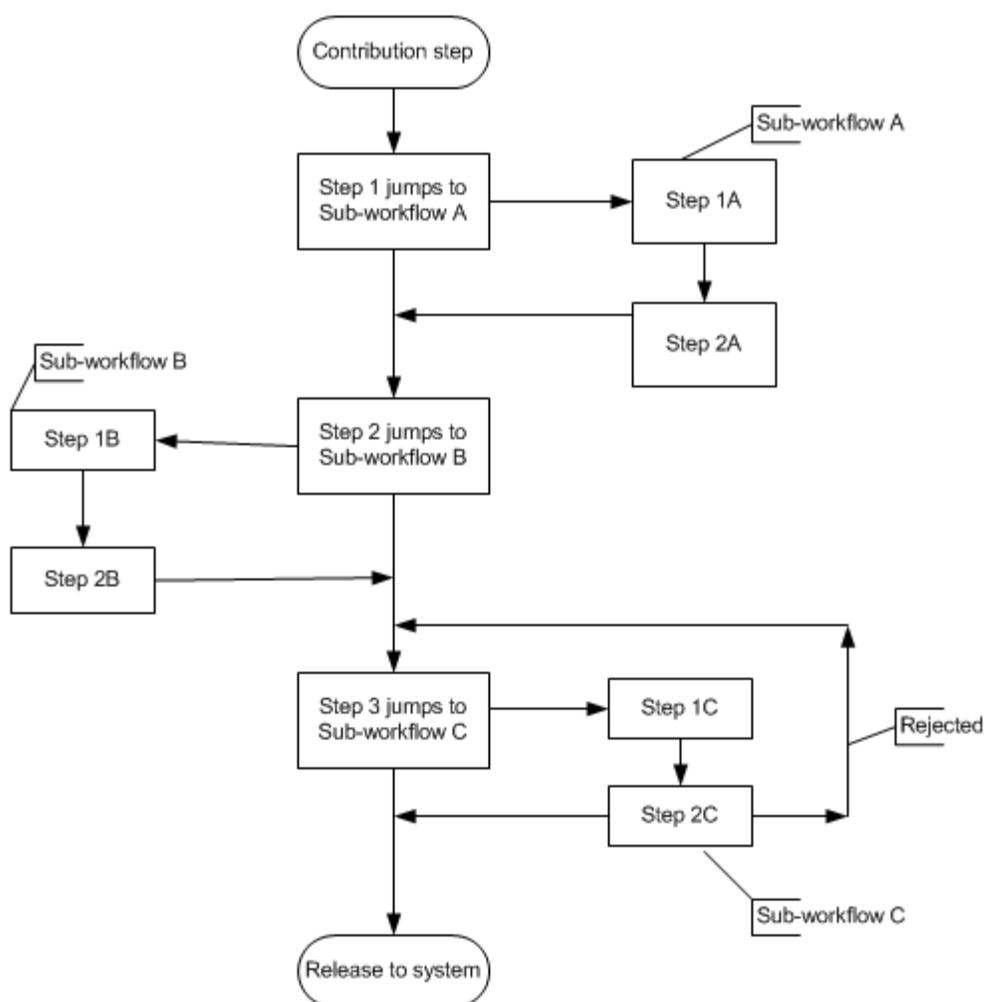
```
<$if parseDate(wfCurrentGet("lastEntryTs")) < dateCurrent(-7)$>
```

4.5.3.2 Creating a Jump

Before you create jumps in a workflow, draw a flowchart and work out all the possible jump scenarios. A recommended method of structuring jumps is to create a main workflow with steps that jump to sub-workflows. See the following example flowchart.

After you have decided what jumps must occur within a workflow, set up the jumps then test them. You can create jumps directly in an existing workflow, or you can create script templates for jumps to be reused in different workflows.

Figure 4–5 Jump Flowchart



Follow these steps to create a jump:

1. Create the workflow that contains jumps. For details, see [Section 4.3.2, "Setting Up a Criteria Workflow"](#) or [Section 4.4.3, "Setting Up a Basic Workflow."](#)
2. Select the workflow on the **Workflow Admin: Criteria Tab** or the **Workflow Admin: Workflows Tab** (depending on the type of workflow).
3. In the Steps pane, click **Add**, or select the step to include the jump and click **Edit**.

The Add New/Edit Step screen for the workflow type (Criteria or Basic) opens.

4. Click the **Events** tab.
5. Click **Edit** next to the event (entry, update, or exit) containing the jump.
 - If a script template does not exist, the [Script Properties Screen](#) opens where you can add properties.
 - If a script template exists, the [Edit Script for <StepName> Screen](#) opens.
 - Select an editing option:
 - To create the script from a blank screen, select **Create New**.
 - To create the script from a script template, select **Use Script Template** then select a template from the list.
6. Click **OK**.

The [Script Properties Screen](#) opens.

4.5.3.2.1 Setting Up Jump Side Effects Follow these steps to test the side effects of a jump.

1. On the **Jumps** tab, click **Add**, or select an existing jump and click **Edit**.
The [Add/Edit Jump Screen Tabs](#) opens.
2. For a new jump, enter a jump name. You cannot change the Jump Name after you create the jump. Try to use a meaningful, descriptive name.
3. If the jump must specify a return point, select the **Has Return Point** check box and select a return point from the list. The possible options are: Current Step, Next Step, Previous Step.
4. If the reviewers for this step should not be notified when the jump is entered, select the **Do not notify users on entry** check box.
5. If the content item is released before approval, select the Release document from edit state check box.
6. Enter any custom side effects in the **Custom Effects** field. For examples, see [Section 4.5.3.4, "Jump Examples."](#)
7. If the reviewers are notified when the jump is entered, click the **Message** tab and enter the notification message.
8. Click **OK**. The Edit Script screen is re-displayed.

4.5.3.2.2 Setting the Conditional Statement Follow these steps to set up conditional statements.

1. Select a metadata field from the **Field** list. This value is the workflow conditions or metadata field to be evaluated.
2. Select an operator from the **Operator** list. **Operator** is a dependent list that shows only the operators associated with the Field.
3. Select a value from the **Value** list. **Value** is the value associated with the specified metadata field.
4. Click **Add** to add the conditional statement to the script.

4.5.3.2.3 Completing the Jump Follow these steps to complete the jump.

1. If the jump must specify a target step:

- To specify a specific step, click **Select**, then select the workflow and step name on the Select Target Step screen. The target step name is displayed in the target step area.
 - To select a symbolic step, such as the current step or exit the workflow, select the step from the **Target Step** list.
2. To modify the script that was just created, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the code.

Caution: If you clear the Custom Script Expression check box, the expression reverts to its original definition. All modifications are lost.

4.5.3.2.4 Testing the Script

- Follow these steps to test the script.
1. Click the **Test** tab.
 2. Click **Select**.
The [Content Item View Screen](#) opens.
 3. To narrow the content list, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
 4. Select a content item to test and click **OK**. Check in and process a test document so that it is in the workflow and at the step you are adding the jump to, then select that content item for testing. If the selected content item is not currently in a workflow, you can still use it to test the script, but it is treated as if it were newly in the workflow.
 5. Click **Load Item's Workflow State**.
If the selected content item is in a workflow, the companion file is loaded in the Input Data field.
 6. Click **Test Script**.
 7. The test results are displayed in the **Results** field.
 - The value of each parameter in the script is displayed.
 - If any Idoc script errors occur, they are displayed with the script containing the errors.
 8. To save the script, click **OK**.
 9. Continue adding jumps as needed to different steps.

4.5.3.3 Changing a Jump

To change an existing jump:

1. Select the workflow on the [The Workflow Admin Screen](#) or the [Workflow Admin: Workflows Tab](#).
2. In the Steps pane, select the step that includes the jump to be changed.
3. Click **Edit** in the Steps pane.
The Add New/Edit Step screen appears for the workflow type (Criteria or Basic).
4. Click the **Events** tab.
5. To delete a jump, click **Clear** in the corresponding event pane.

6. To change a jump, click **Edit** in the corresponding event pane.
The [Edit Script for <StepName> Screen](#) opens.
7. Select an editing option:
 - To edit the existing script, select **Edit Current**.
 - To create a script, select **Create New**.
 - To use a script template, select **Use Script Template** then select a template from the list.
 The [Script Properties Screen](#) opens.
8. Click **Add**, **Edit**, or **Delete** in the Jumps pane to change the jump side effects.
9. Use the Field, Operator, Value fields and **Add** and **Update** buttons in the Script Clauses pane to change the conditional statements for the jumps.
10. Use the **Target Step** list to change the target step for the jump.
11. To change the automatically generated script, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the code.

Caution: If you clear the Custom Script Expression check box, the expression reverts to its original definition and modifications are lost.

12. Test the script before saving it. See [Section 4.5.3.2.4, "Testing the Script."](#)
13. Click **OK** to save the changes.

4.5.3.4 Jump Examples

The following examples describe how to set up different types of jumps.

Example 4–6 Metadata Criteria Jump

Suppose you have a Criteria workflow called *Marketing Brochures* that is defined with the *Marketing* security group and the *MktBrochure* content type. However, any brochures submitted by a graphic artist do not have to go through the first step, which is graphics department approval. You would use the Edit Script screen to create the following entry event script for the first step.

```
<$if dDocAuthor like "bjones" or dDocAuthor like "sjames"$>
  <$wfSet("wfJumpName", "BypassGraphics")$>
  <$wfSet("wfJumpTargetStep", wfCurrentStep(1))$>
  <$wfSet("wfJumpEntryNotifyOff", "0")$>
<$endif$>
```

To change the automatically generated conditional statement from `and` to `or`, you must edit the script on the **Custom** tab of the Edit Script screen.

Example 4–7 Time-dependent Jump

Suppose you want to limit the review period to one week. If the revision has not been approved or rejected, you want to notify the reviewers and process the revision through a sub-workflow called *ApprovalPeriodExpired*. You would use the Edit Script screen to create the following update event script:

```
<$if parseDate(wfCurrentGet("lastEntryTs")) < dateCurrent(-7)$>
  <$wfSet("wfJumpName", "LateApproval")$>
```

```

<$wfSet("wfJumpTargetStep",
  "NotifyAuthor@ApprovalPeriodExpired")$>
<$wfSet("wfJumpMessage", "The review period for content item
  <$eval(<$dDocTitle$>)$> has expired.")$>
<$wfSet("wfJumpReturnStep", wfCurrentStep(0))$>
<$wfSet("wfJumpEntryNotifyOff", "0")$>
<$endif$>

```

4.5.3.5 Jump Errors

Two responses are possible to a jump error:

- An event script that causes an error in execution is treated as if it had never been evaluated. However, the default entry script that keeps track of the entry count and last entry is still evaluated.
- A jump to an invalid step or a step in an inactive workflow results in an error, and the revision is treated as if it has completed the last step of the workflow.

4.6 Workflow and Script Templates

Workflow templates are a quick way to reuse workflows you have created. Each workflow template is an outline for a Basic, Criteria, or sub-workflow that is stored in the Workflow Admin tool. A workflow template is not tied to a security group, and it cannot include step event scripts. You can use *Script templates* to store step event scripts.

The procedure you use to create a template is similar to creating a workflow. This section provides an overview of the process. For details see [Section 4.3.2, "Setting Up a Criteria Workflow"](#) or [Section 4.4.3, "Setting Up a Basic Workflow."](#)

This chapter contains the following topics:

- [Section 4.6.1, "Creating or Modifying a Workflow Template"](#)
- [Section 4.6.2, "Creating a Script Template"](#)

Important: When you use a workflow template, change the reviewers if they are different from those defined in the selected template.

4.6.1 Creating or Modifying a Workflow Template

Follow these steps to create or modify a workflow template:

1. Display the [Workflow Admin: Templates Tab](#).
2. To create a new template, click **Add**. To modify an existing template, select the template and click **Edit**.
The [Add/Edit Template Screen](#) opens.
3. Enter a template name in the **Template Name** field. You cannot change the Template Name after you create the template.
4. Enter a detailed description in the **Description** field.
5. Specify whether to permit the original author to edit the existing revision or create a new revision if the content item is rejected by checking the appropriate box.
6. To Add a step, click **Add**.

7. Enter an appropriate **Name** and **Description** for the step.
8. Specify the authority level of the users for the step: Users can review the current revision, Users can review and edit (replace) the current revision or Users can review the current revision or create new revision.
9. Click **OK**.
10. Select the type of users for the step. You can define multiple types of user for a step.
11. Click **OK**.
12. Click the **Exit Conditions** tab.
13. Specify how many reviewers must approve the revision before it passes to the next step.
14. Specify additional exit conditions if needed.
15. If the workflow requires conditional steps or special processing, click the **Events** tab and add the appropriate scripts.
16. Click **OK**.

4.6.2 Creating a Script Template

Script templates are a quick way to reuse step event scripts you've created. A script template is used as a starting point for creating event scripts. Each script template is a piece of Idoc Script stored in the Workflow Admin tool.

Important: Script templates should use symbolic step names rather than explicit references. For more information, see [Section 4.5.3.1.3, "Jump Variables and Steps."](#)

Follow these steps to create a script template:

1. In [The Workflow Admin Screen](#), select **Script Templates** from the **Options** menu.
2. Click **Add**.
The [Add/Edit Script Screen](#) opens.
3. Enter a script name in the **Script Name** field. You cannot change the **Script Name** after you create the script.
4. Enter a detailed description in the **Description** field.

4.6.2.1 Setting Up Jump Side Effects

1. On the **Jumps** tab, click **Add**.
2. Enter a jump name. You cannot change the Jump Name after you create the jump.
3. If the jump must specify a return point, select the **Has Return Point** check box and select a return point from the list.
4. If users should not be notified when the jump is entered, select the **Do not notify users on entry** check box.
5. If the content item is released before approval, select the Release document from edit state check box.
6. Enter any custom side effects in the **Custom Effects** field.

7. If users are notified when the jump is entered, click the **Message** tab and enter the notification message.
8. Click **OK**.

4.6.2.2 Setting Up Script Template Conditional Statements

1. Select a metadata field from the **Field** list.
2. Select an operator from the **Operator** list.
3. Select a value from the **Value** list.
4. Click **Add** to add the conditional statement to the script.

4.6.2.3 Testing the Script

1. Click the **Test** tab.
2. Click **Select**.
The [Content Item View Screen](#) opens.
3. To narrow the content list, select the **Use Filter** check box, click **Define Filter**, select the filter criteria, and click **OK**.
4. Select a content item to test and click **OK**. If the selected content item is not currently in a workflow, you can still use it to test the script but it is treated as if it were newly in the workflow.
5. Click **Select Workflow**.
The [Select Workflow Step Screen](#) opens.
6. Select a workflow in the Workflows pane, select a step in the Steps pane, and click **OK**. Select a workflow step that is similar to the ones for which the script template is used.
7. Click **Load Item's Workflow State**.
If the selected content item is in a workflow, the companion file is loaded in the Input Data field.
8. Click **Test Script**.
9. The test results are displayed in the Results field.
 - The value of each parameter in the script is displayed.
 - If any Idoc script errors occur, they are displayed with the script containing the errors.
10. To save the script template, click **OK**.

4.6.2.4 Changing a Script Template

To change an existing script template:

1. In [The Workflow Admin Screen](#), select **Script Templates** from the **Options** menu.
The [Workflow Scripts Screen](#) opens.
2. Select the script template you want to change.
3. Click **Edit**.
The [Add/Edit Script Screen](#) opens.
4. Click **Add**, **Edit**, or **Delete** in the Jumps pane to change the jumps.

5. Use the Field, Operator, Value fields and **Add** and **Update** buttons in the Script Clauses pane to change the conditional statements for the jumps.
6. Use the **Target Step** list to change the target step for the jump.
7. To modify the automatically generated script, click the **Custom** tab, select the **Custom Script Expression** check box, and edit the text.

Caution: If you clear the Custom Script Expression check box, the expression reverts to its original definition and modifications are lost.

8. Test the script before saving it. See [Creating a Jump](#).
9. Click **OK** to save the changes.

4.6.2.5 Deleting a Script Template

To change an existing script template:

1. In [The Workflow Admin Screen](#), select **Script Templates** from the **Options** menu.
The [Workflow Scripts Screen](#) opens.
2. Select the script template you want to delete.
3. Click **Delete**.
A confirmation screen opens.
4. Click **Yes**.

4.7 Workflow Scenarios

The following workflow scenario describe the planning process and the types of actions required to accomplish specific workflow tasks. It includes the following workflow examples:

- **Scenario 1: Criteria Workflow.** For details about the steps used to set up a criteria workflow, see [Section 4.3.2, "Setting Up a Criteria Workflow."](#)
- **Scenario 2: Tokens.** For details about creating tokens, see [Section 4.5.2.2, "Creating, Editing, or Deleting a Token."](#)
- **Scenario 3: Jump Based on Metadata.** For information about setting up a jump, see [Section 4.5.3.2, "Creating a Jump."](#)
- **Scenario 4: Time-Dependent Jump.** For information about using variables to set jumps, see [Section 4.5.3.1.3, "Jump Variables and Steps."](#)

4.7.1 Scenario 1: Criteria Workflow

Your Marketing department wants to have all marketing brochures approved by at least one of three graphic artists, the editor, and all of the marketing supervisors. The graphic artists and editor can edit the content, but the supervisors should not have editing privileges.

To set up the workflow for this example, you would:

- Define a security group called *Marketing*, and ensure that the graphic artists and the editor have Write permission, and the marketing supervisors have Read permission to the security group.

- Define a content type called *MktBrochure*.
- Define a workflow called *Marketing Brochures*, with the security group set to *Marketing* and criteria set to *Type = MktBrochure*.
- Define the first step, called *Graphic Artist*, as a Reviewer/Contributor step with approval required from at least 1 reviewer. Because the graphics department is very stable, you can assign the user logins of the three graphic artists to the step.
- Define the second step, called *Editor*, as a Reviewer/Contributor step. Assign the editor's user login to the step.
- Define the third step, called *Marketing Team*, as a Reviewer step with approval required from all reviewers. The management structure changes frequently, so set up an alias called *MktTeam* and assign it to this step.
- All marketing brochures must be checked in to the *Marketing* security group with a *Type of MktBrochure*, so it is a good idea to instruct all possible contributors of marketing brochures about how to check them in.
- For the approval process to work correctly, the *MktTeam* alias must be kept up-to-date.

4.7.2 Scenario 2: Tokens

After you created the *Marketing Brochures* workflow in Scenario 1, the Marketing department requested that all marketing brochures be returned to the original author for final review before they are released. The original author should not have editing privileges.

To set up the workflow for this example, you would:

- Create a token called *Author* and define the user as `dDocAuthor`.
- Define a fourth step in the workflow, called *Original Author*, as a Reviewer step. Assign the *Author* token to the step.

4.7.3 Scenario 3: Jump Based on Metadata

The *Marketing Brochures* workflow you created in Scenarios 1 and 3 is working smoothly, but now the Marketing department would like to automatically notify the various sales reps when a new brochure is released for one of their product lines.

To set up the workflow for this example, you would:

- Define a required custom metadata field called *Product*, and create a list of the products.
- Set up an alias for each product, and assign the appropriate sales reps to each alias. Note that you can assign each user to multiple aliases.
- Define a fifth step in the workflow, called *Notify Sales*, as a Reviewer step with approval required from zero (0) reviewers.
- Define a sub-workflow for each product that contains one Reviewer step with approval required from zero (0) reviewers. Assign the corresponding product alias to the step.
- Define an entry script in the *Notify Sales* step that jumps to the sub-workflow that matches the product.
- For the notification process to work correctly, the product list and aliases must be kept up-to-date.

4.7.4 Scenario 4: Time-Dependent Jump

The Marketing department is having trouble getting marketing brochures approved quickly. They would like to change the *Marketing Brochures* workflow to automatically move content to the next step if it hasn't been approved or rejected by the graphics department, supervisors, or original author within 7 days. The editor is allowed a little more time. They get 10 days before the content goes to the next step.

To set up the workflow for this example, you would:

- Define a script template called *AutoApprove*, with a target step that goes to the next step in the workflow if the last entry was 7 days ago.
- Add an update jump to the *Graphic Artist*, *Marketing Team*, and *Original Author* steps. Use the *AutoApprove* script template to create the jump.
- Add an update jump to the *Editor* step, using the *AutoApprove* script template. Edit the script so that the jump occurs at 10 days rather than 7 days.

4.8 Workflow Tips and Tricks

This section describes workflow tips and tricks. It covers the following topics:

- [Section 4.8.1, "Requiring Step Authentication"](#)
- [Section 4.8.2, "Setting Up Parallel Workflows"](#)
- [Section 4.8.3, "Adding Ad Hoc Step Users"](#)
- [Section 4.8.4, "Customizing Criteria Workflow E-mails"](#)
- [Section 4.8.5, "Workflow Escalation"](#)
- [Section 4.8.6, "Other Customizations"](#)
- [Section 4.8.7, "Triggering Criteria Workflows from Folders"](#)
- [Section 4.8.8, "Searching Within a Workflow Step"](#)
- [Section 4.8.9, "Suppressing Workflow Notifications"](#)

In addition to this functionality, additional customizations are available through Consulting Services. For details, see [Section 4.8.6, "Other Customizations."](#)

4.8.1 Requiring Step Authentication

It is sometimes necessary to re-authenticate a user for particular step of a workflow. For each workflow step that requires authentication before approval, do the following:

1. Add the following line to the `IntradocDir/config/config.cfg` file:


```
<workflow step name>:isRepromptLogin=true
```

 If multiple workflow steps require validation, add those steps on separate lines.
2. Restart Oracle WebCenter Content Server.
3. Set up and enable the workflow, making sure to use the step name designated in the configuration entry for the step where validation is required.

When the workflow is initiated, the users at the workflow step designated with the `isRepromptLogin` configuration variable are prompted to login in before they can approve the content at the workflow step.

In the following example, validation is required at the steps named *VIPApproval* and *CEOsignoff*. The following entries are added to the `config.cfg` file:

```
VIPApproval:isRepromptLogin=true
CEOSignoff:isRepromptLogin=true
```

Oracle WebCenter Content Server is restarted and a workflow is set up and enabled with steps named *VIPApproval* and *CEOSignoff*. Multiple users are assigned to the *VIPApproval* step, and only one user (the CEO of the company) is assigned to the *CEOSignoff* step.

Before the users at those steps can approve the workflow item, they must login again.

This functionality is available in Oracle WebCenter Content Server 7.5 and later versions.

4.8.2 Setting Up Parallel Workflows

It is sometimes desirable to have two distinct groups of users able to review content items in workflow at the same time and to have a specified number of users from each group approve the content before it proceeds in the workflow.

When using Oracle WebCenter Content Server, either all users or a specified number of users must approve the content before it continues. Usually the workflow does not differentiate between sources of approval. Consequently, all members of one group approve content while none of another group approve it, and the content would still advance through the workflow. The following code provides an example of how to add approval process discrimination.

This code allows step users to be set into groups. At each approval, the script checks for the group to which a user belongs. A user can belong to multiple groups; if the approving user is in a group, the counter for that group is incremented by one.

Extra exit conditions hold the content in the step until the extra conditions are met.

Add the following code in the **entry** portion of the step:

```
<$wfSet("set1", "0")$>
<$wfSet("set2", "0")$>
<$group1 = "user1, user2, user3,"$>
<$wfSet("group1", group1)$>
<$group2 = "user8, user9, user10,"$>
<$wfSet("group2", group2)$>
```

Add the following code in the **update** portion of the step:

```
<$if wfAction like "APPROVE"$>
<$if strIndexOf(wfGet("group1"), dUser) >=0$>
<$set1 = toInteger(wfGet("set1"))+1$>
<$wfSet("set1", set1)$>
<$endif$>
<$if strIndexOf(wfGet("group2"), dUser) >=0$>
<$set2 = toInteger(wfGet("set2"))+1$>
<$wfSet("set2", set2)$>
<$endif$>
<$endif$>
```

Add the following code in the **extra exit conditions** portion of the step (where *n* is the number of required approvers from group 1 and *r* is the number of required approvers from group 2):

```
toInteger(wfGet("set1")) >= n
toInteger(wfGet("set2")) >= r
```

By checking the approving user during each approve action, this workflow code increments the counter of the group to which the user belongs. The extra exit conditions hold the content item in the step until the minimum number of users in each group have approved it. If more than the minimum number of required approves for each group are executed, the approve actions are still logged but the content item does not proceed.

Reject actions are still absolute. A rejection from any named user still executes normal workflow reject behavior.

4.8.3 Adding Ad Hoc Step Users

You can add users to workflow steps without using metadata fields normally accessed by tokens. For example, a content item is traveling (and being edited) in workflow; each edit lists the person editing the content as the `dDocAuthor`. To send the item to the original author after the workflow cycle, a special token must be created:

```
<$wfAddUser(wfGet("originalContributor"), wfGet("type"))$>
```

Add the following code to the **entry event** of the first step in the workflow to restore the original author:

```
<$originalContributor=dDocAuthor$>  
<$wfSet("originalContributor", originalContributor)$>  
<$type="user"$>  
<$wfSet("type", type)$>
```

The event script uses `wfSet()` to put custom variables and values into the companion file at a point before the token call. The token then uses `wfGet()` to pull out those values and set the step user.

You can use this technique to obtain and store any standard or custom Idoc variable that holds valid user names or aliases. The Idoc variable can contain a comma-delimited list of user names or aliases. If user names are being stored, the `<$type$>` variable must be set to *user* (for example, `<$type="user"$>`). If alias names are being stored, the `<$type$>` variable must be set to *alias* (for example, `<$type="alias"$>`).

When placed in the entry event of a workflow step with the token set as the step user, the entry event code processes the information. It stores the user name (or alias) which is then called by the token and is set as a step user (or users, if a list was specified). Adding multiple or conditional code blocks and tokens (as shown previously) to your step entry events and step user definitions allows true ad hoc workflow routing.

4.8.4 Customizing Criteria Workflow E-mails

E-mails are triggered by criteria workflow at three points in the process:

- On entry to a step.
- On receipt of a reject reasons form.
- On execution of the `wfNotify` Idoc script function.

It is possible to customize the e-mail message, the e-mail subject, and the template used for e-mails sent during criteria workflows. This section describes the processes for customizing the e-mail aspects of criteria workflows.

This section includes the following topics

- [Section 4.8.4.1, "Customizing E-mail Templates"](#)
- [Section 4.8.4.2, "Customizing the Subject or Message Line"](#)

4.8.4.1 Customizing E-mail Templates

The two most commonly used templates used to generate e-mail messages sent to recipients involved in a workflow are *reviewer_mail.htm* and *reject_mail.htm*. These are stored in `IdcHomeDir/resources/core/templates`.

You can modify these templates like any other template. E-mail template modification provides the greatest flexibility and opportunity for customizing workflow e-mails. Although this kind of modification is relatively straightforward, it still requires careful component development. Modifying the subject and the message in the e-mail is often the most important part of the message, and thus is often the most modified.

Custom workflow e-mail templates based on the standard templates can also be created. To call custom templates, add them as the optional third parameter to the `wfNotify` function, as in these examples:

```
<$wfNotify(userName, "user", templateName)$>
<$wfNotify(aliasName, "alias", templateName)$>
```

If an alternate template is not specified, the system default template is used.

See the discussion of `wfNotify` in the *Oracle WebCenter Content Idoc Script Reference Guide* for more details.

4.8.4.2 Customizing the Subject or Message Line

You can customize criteria workflow e-mail subject and message lines for your application. The e-mail subject line appears in the e-mail; the message line appears in the e-mail body with other information about the workflow e-mail (workflow name, step, and content item).

The message line defaults to one of two messages, depending on whether the step is notification-only (that is, if it has zero required reviewers).

You can customize subject lines and message lines in two ways:

- You can modify the core string resource file according to standard component architecture.
- For simple customizations, you can declare the `wfMailSubject` (for e-mail subjects) or `wfMessage` (for message lines) Idoc Script variable in a criteria workflow step event script or stored in the companion file.

4.8.4.2.1 Modifying Strings The string definitions are as follows (variable 1 is the content item title and variable 2 is the name of the workflow step):

```
<@wwWfIsNotifyOnly=Workflow notification for content item '{1}' is in step '{2}'.@>
```

```
<@wwWfReadyForStep=Content item '{1}' is ready for workflow step '{2}'.@>
```

```
<@wwWfRejected=Content item '{1}' has been rejected.@>
```

You usually call these string definitions with the Idoc Script `<$lc()$>` localization function and you can alias them in a component resource file. See the `<@dynamichtml wf_approve_mail_subject@>` include definition in the *std_page.htm* file for an example of e-mail subject line string includes.

4.8.4.2.2 Changing Idoc Variables For simple e-mail or subject line changes, you can use Idoc Script rather than a component. You can place the `wfMailSubject` configuration variable or the `wfMessage` configuration variable in step event script. The value of these variables can also accept Idoc Script, as in this example:

```
<$wfMailSubject="My custom subject text for content with <$dDocTitle$> title"$>
```

No `eval()` function is required for the Idoc Script variables to evaluate.

If `wfMailSubject` or `wfMessage` is placed in the entry event of a workflow step, the e-mail messages triggered by content entering the step receives the customized subject or message line. These variables can also be declared before a `wfNotify()` function and the e-mail then generated by that function receives the customization.

4.8.5 Workflow Escalation

This example requires familiarity with tokens and coding.

Workflow escalation (that is, dynamically routing workflow content to different people than listed users) is a common workflow requirement. While this is easily accomplished with jumps and parsing of some criteria (for example, date, action, metadata) there is often some initial confusion or hesitation about where or to whom the content should go.

The issue is further complicated when the solution is to add a larger number of step users and to require only a subset of those users to approve the content before it can move on. This workflow still generates and sends out e-mails and appears in the workflow queue of non-approving users, users out of the office, and others who are there "just in case" some primary reviewer is not available.

4.8.5.1 Setting Up a Workflow Escalation

This solution incorporates two custom user metadata fields, a token, and workflow step entry and update event code.

1. Create a user metadata field with the following elements:
 - name: `OutOfOffice`
 - type: text
 - option list: yes
 - option list type: select list validated
 - option list values: `<blank>`, false, and true
2. Create another user metadata field with the following elements:
 - name: `OutOfOfficeBackup`
 - type: Long Text

The `OutOfOffice` field is a flag that the user sets as TRUE when they are out of the office. To set this flag, select **TRUE** from the list and click the update button to update the user profile.

The `OutOfOfficeBackup` field contains the user name(s) of those users who can fill in as proxies for the out-of-office user. This field should optimally contain a single user name, formatted as shown in the User Admin applet.

When the following workflow step event code finds that a listed user is "out of the office" it switches that user's name for the listed proxy (as designated by the value in the `OutOfOfficeBackup` field). The workflow step then restarts with only the users who had not yet approved the content and any designated proxies.

A token pulls the list of users out of the companion file and sets them as step users. Special workflow messages are sent to designated proxies while the content was sitting in the update step event.

3. Create a workflow Token

- name: DynamicStepUsers
- Token Code:

```
<$if wfGet("dsu")$>
  <$wfAddUser(wfGet("dsu"), "user")$>
<$else$>
  <$wfAddUser("sysadmin", "user")$>
<$endif$>
<$if wfGet("dsa")$>
  <$wfAddUser(wfGet("dsa"), "alias")$>
<$endif$>
```

The token pulls a value for the custom variable `dsu` and `dsa` out of the companion file. If no value is found for `dsu` then the `sysadmin` user is added as a precaution. The initial values for `dsu` and `dsa` are listed in the entry event of the step. If you want to assign users to the step(s), add the first contributor to the first step and the next step must include the first user plus the next user, user two.

4. Paste the following code into the **entry** event of your workflow step. Note that comments are included through the entry code; remove the comments before inserting into your step:

```
<$restartFlag=wfGet("restartStep")$>
```

See if the cause is a restart for new backup users. If so, suppress notifications to old users and notify only new ones

```
<$if restartFlag$>
<$if toInteger(wfGet("restartStep"))>=1$>
  <$wfSet("wfJumpEntryNotifyOff", "1")$>
  <$oooUsers=wfGet("outOfOfficeUsers")$>
  <$if strIndexOf(oooUsers, ",")>=1$>
```

Check for multiple out of office users

```
<$wfMessage=eval("The Following Users are out of the office: <$oooUsers$>
\nYou are the designated backup for one of them.\n
The content item <$dDocName$> is in the workflow step <$dwfStepName$>
awaiting your review")$>
<$else$>
  <$wfMessage=eval("The Following User is out of the office: <$oooUsers$>
\nYou are the designated backup for this user.\n
The content item <$dDocName$> is in the workflow step <$dwfStepName$>
awaiting your review")$>
<$endif$>
<$rsMakeFromString("ooou", oooUsers)$>
<$loop ooou$>
  <$userBackupName=row&"_Bkup"$>
  <$wfNotify(wfGet(userBackupName), "user")$>
<$endloop$>
<$wfSet("restartStep", "0")$>
<$endif$>
  <$else$>
<$wfSet("restartStep", "0")$>
<$endif$>
```

Set your step users here. Multiple users must be comma-delimited, user names must be in quotes, metadata field references are unquoted. This example proceeds, using user names rather than aliases. Slight code re-working is required if using aliases.

```
<$dynamicStepUsers= <LIST USER NAMES IN QUOTES HERE>$>
```

```
<$if strIndexOf(dynamicStepUsers, ",")>=1$>
```

If there are multiple users specified verify if any of the MULTIPLE users are out of the office

```
<$rsMakeFromString("multiDynamicUsers", dynamicStepUsers)$>
```

```
<$loop multiDynamicUsers$>
```

```
  <$if strEquals(getValueForSpecifiedUser(row, "uOutOfOffice"), "true")$>
```

If user is out of office, get their backup

```
  <$backup=getValueForSpecifiedUser(row, "uOutOfOfficeBackup")$>
```

Replace out-of-office user in users list with their backup

```
  <$dynamicStepUsers=strReplace(dynamicStepUsers, row, backup)$>
```

```
<$endif$>
```

```
<$endloop$>
```

```
<$else$>
```

Verify if the SINGLE user is out of the office

```
<$if
```

```
strEquals(getValueForSpecifiedUser(dynamicStepUsers, "uOutOfOffice"), "true")$>
```

If user is out of office, get their backup

```
<$dynamicStepUsers=getValueForSpecifiedUser(dynamicStepUsers, "uOutOfOfficeBackup")$>
```

```
<$endif$>
```

```
<$endif$>
```

```
<$wfSet("dsu", dynamicStepUsers)$>
```

Set the dsu variable into the companion file with listed and backup users

5. Paste the following code into the **update** event of your workflow step, removing comment lines before doing so:

```
<$remainingUsers=wfGet("wfUserQueue")$>
```

Get users who have yet to approve

```
<$rsMakeFromString("ru", remainingUsers)$>
```

```
<$loop ru$>
```

```
<$if strEquals(getValueForSpecifiedUser(row, "uOutOfOffice"), "true")$>
```

Check the remaining users to see if they are out of the office

```
<$if getBackup$>
```

Create list of users requiring backup substitutes

```
  <$getBackup=row & ", "&getBackup$>
```

```
<$else$>
```

```
  <$getBackup=row$>
```

```
<$endif$>
```

```
<$endif$>
```

```
<$endloop$>
```

```
<$if getBackup or strLength(getBackup)>0 $>
```

If a user is listed as out of office then rewrite the user list and restart the step

```

<$wfSet("outOfOfficeUsers",getBackup)$>
<$rsMakeFromString("needBkup", getBackup)$>
<$loop needBkup$>
<$bkupUser=getValueForSpecifiedUser(row,"uOutOfOfficeBackup")$>
<$newRemainingUsersList=strReplace(remainingUsers,row,bkupUser)$>
<$wfSet(row&"_Bkup",bkupUser)$>
<$endloop$>
<$wfSet("dsu",newRemainingUsersList)$>
<$getBackup=""$>

<$wfSet("wfJumpTargetStep", wfCurrentStep(0))$>
<$wfSet("restartStep","1")$>
<$endif$>

```

4.8.6 Other Customizations

Many workflow customizations are available through Consulting Services. This section briefly describes two of those customizations. Please consider engaging Oracle Consulting Services for a thorough evaluation of the impact associated with the replication of workflow examples.

The following customizations are discussed in this section:

- [Section 4.8.6.1, "Setting Approval by Non-Reviewers"](#)
- [Section 4.8.6.2, "Automatic Replication of Workflow Items"](#)

4.8.6.1 Setting Approval by Non-Reviewers

It is sometimes necessary to have a person approve content in a workflow step even if that individual is not part of the actual workflow. For example, if you want an outside opinion on a document in a particular stage in a workflow or if you want to designate a substitute reviewer because another reviewer is out of the office. The individual can approve content but they do not get normal workflow notifications and do not see the content items in their workflow queues.

Users with designated roles or who are members of designated aliases can approve content on this basis. These designated users see a **Bypass Approve** link in the workflow actions box for each item in a workflow to which they have normal security access. Performing a Bypass Approve approves the content item in the step in which it currently resides. Defined step exit conditions are still evaluated and still apply. The approval is logged in the Workflow History database table and in the WorkflowActionHistory ResultSet of the companion file.

A designated approver is not a regular workflow step approver and thus does not receive automatic workflow notifications. Access to a content item in a workflow where the approver wants to perform a Bypass Approve action must be intentional. The designated approver must access the **Active Workflows** menu, then select the workflow name and select an action.

The designated approver component aliases core resources. If other components are running or are planned, this must be taken into account. In some cases, you can combine component resources to include all required functionality or you can rename and re-reference them to keep all components working correctly (but separately).

4.8.6.1.1 Scenarios For the following scenarios, assume that User A has a role or alias that grants designated approver status and that a sample workflow named `MyWF` has two steps.

- Scenario 1: User A is listed as an approver for step 1 in MyWF but not in step 2. Therefore, no **Bypass Approve** link appears for Step 1. User A received default workflow action capabilities and notifications. The **Bypass Approve** link for step 2 appears under the **Workflow Actions** menu if User A accesses the **Content in workflow 'MyWF'** page when the content item is in step 2.
- Scenario 2: User A is not listed as an approver in MyWF. The Bypass Approve link appears in the action menu on the **Content in workflow 'MyWF'** page for all steps and for all content to which User A has at least Read permission in its Security group.
- Scenario 3: User A is not listed as an approver for Step 1 in MyWF. Step 1 requires two approvals from reviewers before it moves to step 2. The **Bypass Approve** link appears for User A. Click **Bypass Approve** to register an approval and fulfill one of two required approvals for the step to continue in the workflow.

4.8.6.2 Automatic Replication of Workflow Items

Content items are often processed (in one form or another) before they are 'released'. A released content item is indexed and can then be included in search results, archives, and in other processes and applications.

It is sometimes useful to release a content item before its completion in the workflow. For example, a content item must be in a released state to be replicated (and perhaps later used in disaster recovery). Items not released (such as items in workflows) are not used by the replicator.

It is possible to designate workflow items as released while still in workflow. Normal workflow actions, such as updating, checking out, and checking in are still available. However, these items are indexed and appear in search results, can be used in replication and archiving, and in any other processes or applications.

Important: There are several elements to consider before replicating workflow items. This section describes the process but does not go into detail; contact Consulting Services before setting up replication of workflow items.

4.8.6.2.1 Potential Conflicts There are several points to be aware of before setting up automatic replication:

- **Loss of data integrity:** A premature release of content, whether intentional or otherwise, can have unforeseen effects on business process management, content accessibility, and information integrity. Potential ramifications must be thoroughly considered before the release of items still in workflow is considered.
- **Non-capture of workflow information:** Workflows are a combination of process **and** content. While it is possible to release content and make it available for replication and other processes, it is not possible (without customization and assistance from Consulting Services) to capture and replicate workflow *state* information.

If content in a workflow on a source instance is replicated and released on a target instance without passing through a workflow on that instance, the recovery process involves manual effort to re-set the content's workflow state.

In most cases, cloning of workflow information is not necessary because recovery to a prior workflow state is required only during true disaster recovery. In all

other cases, content items replicate as normal after exiting a workflow and supersede versions or revisions replicated during workflow.

- Imported content items do not enter workflow: Content items replicated while in a workflow on a source instance do not enter a workflow on the target instance without additional customization and assistance from Consulting Services. Replicated content items are checked in to the target instance and released.
- Restoration of replicated workflow items requires manual intervention: You can capture some workflow information as metadata for use in a manual restoration of the workflow. Only a check-in action triggers a content item's entry into workflow. To restore an item back into a workflow requires that you create a revision.

To recover the content items on the target to a state as close as possible to their previous state on the source, a discrepancy between the number of revisions on the source and the target instances is intentionally and unavoidably introduced.

4.8.6.2.2 Scenarios For content item 1, **not released while in workflow**, the following is true:

- The content item moves through workflow in a non-released state.
- The content item is not a candidate for replication while in workflow.
- The content item is available only to named workflow step reviewers and administrators.
- When the content item completes the workflow, it is released, indexed, and is now a candidate for replication.

For content item 2, **released while in workflow**, the following is true:

- The content item moves through workflow and is released as specified. After an item is released, it cannot be 'unreleased'. New revisions of a content item created during workflow are not released unless specified.
- Content items released while in workflow display in search results and can be viewed by users with the appropriate security access.
- Users cannot edit, check out, check in, or update a released item that is in workflow unless they are designated users for the step in which the item is located and that step allows the attempted action.
- A content item released while in workflow is a candidate for automatic replication. The Replicator treats the item as if it is not in workflow.
- Content items completing workflow are replicated in the normal fashion and supersede any pre-existing content item versions replicated during workflow.

Contact Consulting Services for details about and the implications of the release of content items in workflow for replication or other purposes.

4.8.7 Triggering Criteria Workflows from Folders

It is sometimes necessary for documents in a particular folder to go through a criteria workflow. However, when you create a criteria workflow based on a folder, the criteria option of `folder` is not listed in the field list. The field list in criteria workflows only lists fields with a type of `text` or `long text`. Because `Folder (xCollectionID)` is an integer field, it is not an option.

Although you cannot select the folder field on the Edit Criteria form, you can define it as a criterion in Events. In the Entry Event of the first step, you can set up criteria to

check for the appropriate folder number (xCollectionID). If it does not fulfill the criteria, the item can exit from the workflow.

The following general steps detail how to set up such a workflow:

1. Start a new criteria workflow and choose the Security Group that the workflow uses.
2. In the Criteria Definition section, define global criteria to monitor all of the documents that enter the system. For example:

```
Field: ContentID
Operator: Matches
Value: *
```

To monitor only items coming in through a specific folder, set an extra metadata field that specifies a folder number.

If multiple workflows are in place, you can filter all content through this workflow and jump to sub-workflows through multiple criteria settings in the first step of this workflow.

3. Add the first step to the workflow.
4. In the **Events** tab, click **Edit** from the Entry Event.
5. On the **Jumps** tab, click **Add**.
6. Give the jump a meaningful name (for example, Folder Criteria) and click **OK**.
7. For the jump criteria, enter the following:

```
Field: Folder
Operator: Not Equals
Value: Folder ID on which the workflow is based
```

When done, click **Add**.

8. For the Target Step, select Exit to Parent Step and change both of the 0 parameters to 10 (for example, @wfExit(10,10). Documents not in the folder are forced out of the workflow.
9. Click **OK** on the Entry Event and click **OK** on the Add New Step dialog.
10. Add the necessary jumps, steps, and events for the rest of the workflow and enable it.

4.8.8 Searching Within a Workflow Step

When executing the GET_SEARCH_RESULTS service within a workflow step, you can experience data corruption because the workflow's data binder is being used by the service.

A solution for this is to temporarily set the security group value into a temporary variable. Then clear the current security group value, make the call for the search results, then reset the security group back again.

4.8.9 Suppressing Workflow Notifications

When a workflow step requires multiple approvers, a user who has approved the document can be re-notified during a timed workflow update cycle. To prevent additional notifications, use the wfSetIsNotifyingUsers workflow function. Used in a workflow step in the script section of the workflow, it sets an internal flag to

determine if workflow notifications are sent out during the current document action (check in, approve, update, and so on). The suppression is applied to both e-mail and updates to the workflow in the queue.

When used in combination with `wfIsFinishedDocConversion`, this function can suppress notification until conversion is finished. It does not prevent documents from advancing out of the auto-contributor step but it does stop updates of the workflow in queue and notification e-mails.

These notifications are not lost. If the `wfSetIsNotifyingUsers` function is not used in a future workflow event to suppress notifications (updates to workflow in queue and workflow mail) then all users participating in the current step are notified.

You can use the following additional functions in the script section:

- `wfIsFinishedDocConversion`, which returns a result indicating if the document is not in GENWWW after the current document action ends.
- `wfIsNotifyingUsers`, which returns a result indicating if the workflow is currently suppressing all workflow notification for this particular workflow event.

See the *Oracle WebCenter Content Idoc Script Reference Guide* for usage details for all of these functions.

4.9 Workflow Troubleshooting

This section provides solutions to several common workflow issues.

- [Section 4.9.1, "Workflow Item Stuck in EDIT or GENWWW Status"](#)
- [Section 4.9.2, "Workflow Item Stuck in REVIEW Status"](#)
- [Section 4.9.3, "Workflow Item Entered in Wrong Workflow"](#)

4.9.1 Workflow Item Stuck in EDIT or GENWWW Status

Symptom

A content item in a workflow is in EDIT or GENWWW status, and no reviewers were notified by e-mail that action is required.

Problem

Inbound Refinery failed to convert the file properly.

Recommendation

1. View the content item's status in Repository Manager or the Content Items for Workflow page (accessed from **Content Manager**, then **Active Workflows** then `<Workflow_Name>`). For more details on the conversion failure, display the Content Information page.
2. Determine why the conversion failed:
 - If the problem was with Inbound Refinery or a conversion add-on product:
 - a. Correct the problem so that the file converts properly.
 - b. Resubmit the file for conversion from Repository Manager or Content Information page. The content item continues through the workflow.

- If the problem was with a file in a criteria workflow and the content item is the only item in the workflow:
 - a. Save a copy of the native file.
 - b. Disable the workflow to release the content item.
 - c. Delete the released revision using Repository Manager or the Content Information page.
 - d. Correct the problem so that the file converts properly.
 - e. Check in the content item again so that it goes through the entire workflow process.
- If the problem was with a file in a criteria workflow and there are multiple content items in the workflow:
 - a. Save a copy of the native file.
 - b. Delete the "stuck" revision using Repository Manager. (You could disable the workflow, but all content items in the workflow would be released.)
 - c. Correct the problem so that the file converts properly.
 - d. Check in the content item again so that it goes through the entire workflow process
- If the problem was with a file in a basic workflow and the content item is the only item in the workflow:
 - a. Save a copy of the native file.
 - b. Cancel the workflow to delete the revision from the system.
 - c. Correct the problem so that the file converts properly.
 - d. Contribute the content item again to the Basic workflow so that it goes through the entire workflow process.
- If the problem was with a file in a basic workflow and there are multiple content items in the workflow:
 - a. Save a copy of the native file.
 - b. Delete the "stuck" revision using Repository Manager. (You could cancel the workflow, but all content items in the workflow would be deleted from the system.)
 - c. Correct the problem so that the file converts properly.
 - d. Contribute the content item again to the Basic workflow so that it goes through the entire workflow process

4.9.2 Workflow Item Stuck in REVIEW Status

Symptom

A content item in a workflow is in REVIEW status, and the minimum number of reviewers have approved it, but the revision is not moving to the next step.

Problem

The content item does not meet the exit criteria of the workflow.

Recommendation

1. Check the exit condition definition in the workflow step to see why the document does not meet the criteria.
2. Determine if the file is finished interacting with an external process. Resolve any problems with the external process to see if the file meets the exit condition.
3. If there is an error in the exit condition, external processing or both, you can check out the document and check it back in with the correct metadata to meet the exit condition.

4.9.3 Workflow Item Entered in Wrong Workflow

Symptom

A content item entered the wrong criteria workflow.

Problem

Two or more criteria workflows have the same criteria defined. The content item matched this criteria, so it entered the first matching workflow in the workflow list.

Recommendation

Redefine the criteria so that each workflow has a unique combination of the security group and metadata field value. If necessary, use jumps and sub-workflows to define additional criteria within the main workflow.

PDF Watermark

PDF Watermark is an optional component that is automatically installed with Oracle WebCenter Content Server. A watermark is a image or text superimposed on selected pages in a PDF document. When enabled, the PDF Watermark component can apply a watermark at check-in (static watermark) or when a user requests to view or download a PDF document (dynamic watermark).

PDF Watermark can also add security features to PDF files as they are downloaded for viewing. You can add password security and enable or disable the ability to print or copy the contents of the file.

This chapter provides information about managing PDF Watermark. It covers the following topics:

- [Section 5.1, "PDF Watermark Overview"](#)
- [Section 5.2, "Watermarking Scenarios"](#)
- [Section 5.3, "Managing PDF Watermark"](#)

5.1 PDF Watermark Overview

This section covers the following topics:

- [Section 5.1.1, "Static Watermarks"](#)
- [Section 5.1.2, "Dynamic Watermarks"](#)
- [Section 5.1.3, "Types of Watermark"](#)
- [Section 5.1.4.1, "Watermark Metadata Configuration"](#)
- [Section 5.1.4, "Templates"](#)
- [Section 5.1.5, "Dynamic Watermark Rules"](#)
- [Section 5.1.6, "PDF Optimization"](#)
- [Section 5.1.7, "Watermark Placement"](#)

5.1.1 Static Watermarks

A static watermark is applied during content check-in as a follow-on step to the Inbound Refinery conversion. To select a watermark for content to be converted to PDF, enter a valid **Watermark Template ID** during check in.

Only documents that Inbound Refinery converts to PDF can receive a static watermark. After a document receives a static watermark, all viewers of the document see the same watermark.

In the same way, content checked in by an automated process such as WebDAV or BatchLoader can also be given a static watermark, provided a valid Watermark Template ID is provided.

For more information about creating templates and template IDs, see [Section 5.1.4, "Templates."](#)

5.1.2 Dynamic Watermarks

Dynamic watermarks are generated as needed when a user requests to view or download a PDF document. Dynamic watermarks can contain variable information (for example, the user name or the requesting user, or the date and time of download). For this reason, different users may see the same content with different watermarks. With dynamic watermarks, only the web layout form is watermarked. The original PDF file is unchanged in its vault location.

Dynamic watermarking is rules-based. If a request for a PDF document satisfies a pre-defined rule, the template associated with that rule is used to watermark a copy of the content before the copy is returned to the requesting user. System administrators define rules and set up specific conditions for determining which requested content gets a dynamic watermark.

For more information about specifying rules for dynamic watermarks, see [Section 5.1.5, "Dynamic Watermark Rules."](#)

5.1.3 Types of Watermark

You can create the following types of watermarks:

- **Text:** You can specify your own text, include metadata values for the content item, and include special keywords, such as \$DATE\$, that provide information about the content item at the point it is watermarked. For information about specific text options, see [Section A.3.7, "Add New/Edit Text Watermark Window."](#)
- **Image:** You can include an image in any of the supported bitmap (raster) formats. For information about specific image options, see [Section A.3.8, "Add New/Edit Image Watermark Window."](#)
- **Signature:** If you enable the Electronic Signatures component, you can create a watermark from the electronic signature metadata associated with a content item. For information about specific image options, see [Section A.3.9, "Add New/Edit Signature Watermark Window."](#)

With each type of watermark, you can specify size, position, page range, and other options suited to each type of watermark. For more information about watermark placement, see [Section 5.1.7, "Watermark Placement."](#)

You can include one or more watermarks of any type in a given document. The watermarks you define are stored in a template that is checked in with the content ID and default metadata values you provide when you save the template.

5.1.4 Templates

Whether you apply a watermark statically at check-in or dynamically when the PDF file is requested, the watermark information is stored in a *template*. This template includes information about the text or image watermark itself and any rules defined for its use.

When you create and save a new template, it is checked in with the default metadata defined on the **Configuration** tab. When you modify and save an existing template,

the template is checked out of Oracle WebCenter Content Server and it is checked back in as a new revision preserving any metadata currently in place. Therefore, it is important to set any metadata defaults before you save a newly created template.

Note: Legacy schema templates are supported for watermarking, but any change to the template results in an upgrade to the new schema. Consequently, any template which is changed in Oracle WebCenter Content Server version 11gR1 may not work correctly with older versions of Oracle WebCenter Content Server.

5.1.4.1 Watermark Metadata Configuration

A template is checked into the content repository as a managed content item with the default metadata you specify and two additional metadata fields:

- **Watermark Template ID:** This field is the content ID (dDocName) for the template. You assign this value when you create a template. For static watermarks, you specify the Watermark Template ID to use when you check in the content item.
- **Watermark Template Type:** This field provides a list of supported template types. Currently, a single option is provided, the default PDFW_Template.

In addition to these fields, you can specify additional metadata values for the template. This helps ensure that default values are provided for fields that require a value. Use the **Configuration** tab on the PDF Watermark Administration screen to set the default metadata field values for the template before you save the template. You can modify the content information for an existing template as you would for any content item.

5.1.4.2 Template Security

You can add password security to access or modify the PDF files associated with a template and enable or disable the ability to print or copy the contents of the file.

A *User Password* requires the user to provide a password to open and view the PDF. An *Owner Password* restricts the ability to change the PDF file or modify the security settings within the PDF file.

These security settings set access restrictions within the associated PDF file itself using PDF security. These access restrictions are independent of access restrictions to the content item defined by Content Server.

5.1.4.3 Password Encryption

User/Owner passwords are encrypted in the PDF Watermark Template with a third-party encryption library. Encryption is performed automatically when the template is saved and decryption is performed automatically when the template is used for a watermark.

Note: Oracle does not provide an encryption library. Library `bcprov-jdk14-138.jar` is a recommended third-party encryption library that you can download from BouncyCastle.org, but you can use any other library. For information about specifying an encryption library, see [Section 5.3.1, "Specifying the Classpath for an Encryption Library."](#)

Passwords in legacy templates are not encrypted until the template is saved using the PDF Watermark Administration screen. You cannot save a template unless it has been changed. Therefore, to encrypt template passwords, edit each legacy template and make a minor change before saving.

5.1.5 Dynamic Watermark Rules

Rules are used to determine which template is applied for dynamic watermarking.

After you create a template, you can define one or more rules for the template.

Note: You can use the same template for both static and dynamic watermarking. The rules you assign to a template are used only for dynamic watermarking.

If a template has multiple rules, the rules are applied in the order listed. Order rules with the most specific tests earlier in the list, and more general ones after that. All rules must test positive for the watermark to be applied.

Within a rule, you specify one or more criteria based on the values of selected metadata fields. For example, you can test the `dDocAuthor` field for specific authors or the `dDocType` for a specific type of document. The order in which you define criteria for a rule does not matter. All criteria must be true for the associated rule to test positive.

5.1.6 PDF Optimization

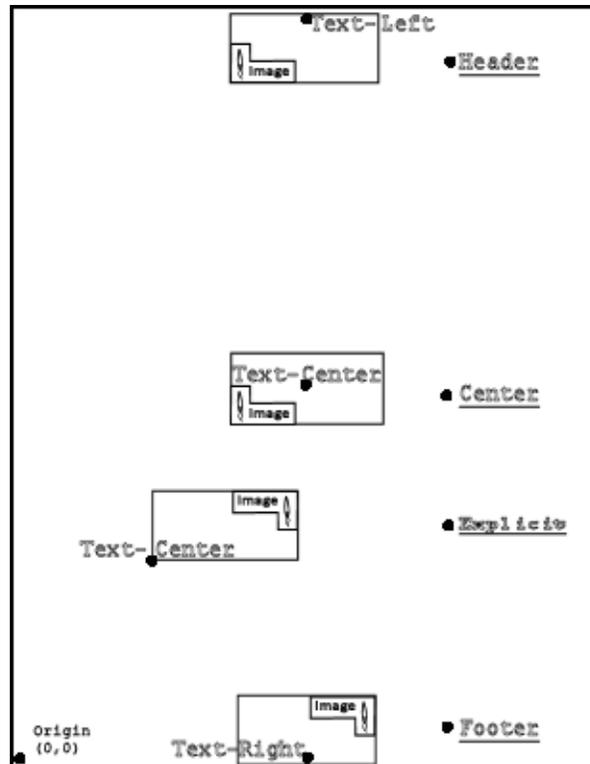
PDFs that come from the PDF Converter may have been optimized for faster Web viewing. If a static watermark is applied to that content, the optimization is lost. Post-watermarking optimization requires a third-party optimizer which is not provided with PDF Watermark. To use optimization, a distiller engine/optimizer must be installed and fully operational. The chosen optimizer must be able to execute conversions with a command-line (for example, a script file or a .bat file).

Important: A PDF optimizer is not provided with PDF Watermark. If using the Optimization feature, install a third-party distiller engine before use and make sure the optimizer is fully operational. The optimizer must be able to execute conversions on a command-line (for example, a script file or a .bat file).

5.1.7 Watermark Placement

PDF Watermark provides standard options for placing text or image watermarks at the top (header), center, or bottom (footer) of the page. You can also specify a particular location on the page with X-Y coordinates. You can specify multiple watermarks for a given document.

In the image below, the reference points for each of the positions is indicated by a point. The example image in each of the positions shows the orientation relative to the associated reference point. Example text in each of the positions shows one of the available horizontal alignment options (left, right, center). All text alignment options are available at each of the positions.



For standard placement, text and images reference a point at the top-center, middle-center, or bottom-center of the page. Images center horizontally around the associated reference point. With text, you can specify the horizontal alignment of the text with respect to this reference point (left, right, or center aligned).

For explicitly placed watermarks, the coordinates are in *points*, with each point equal to 1/72". The origin (0, 0) is the lower left corner of the page. For images, these coordinates specify the lower left corner of the image with the image extending up and to the right. For text, these coordinates specify the horizontal reference point for the alignment options, similar to the standard placement options.

5.2 Watermarking Scenarios

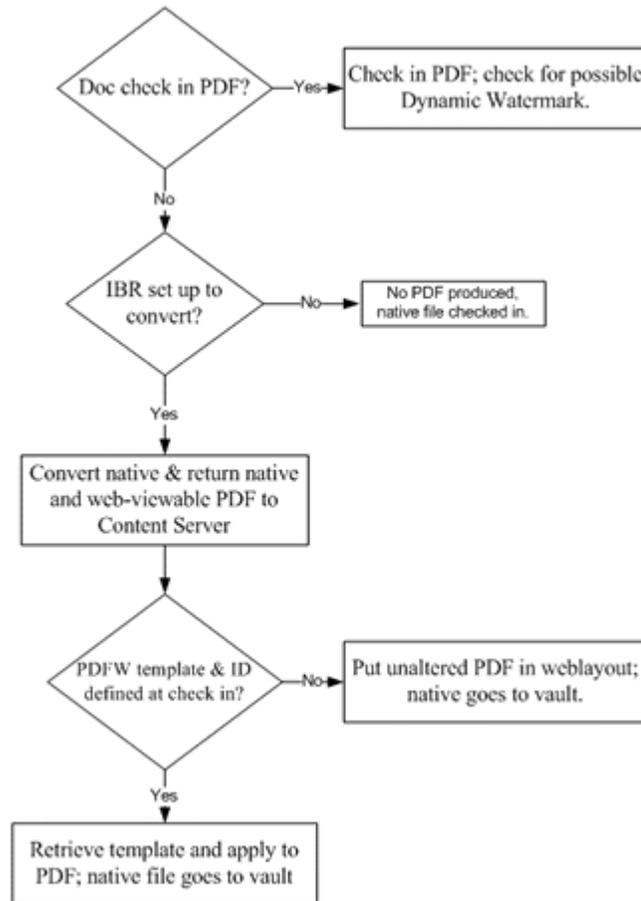
This section covers the following topics:

- [Section 5.2.1, "Static Watermarking Scenario"](#)
- [Section 5.2.2, "Dynamic Watermarking Scenario"](#)

5.2.1 Static Watermarking Scenario

Oracle WebCenter Content Server receives processed content from Inbound Refinery. Inbound Refinery must have PDF Converter installed, enabled, and configured to convert the necessary file formats into PDF. When the PDF file is presented, the watermark template selected during the content check in is applied.

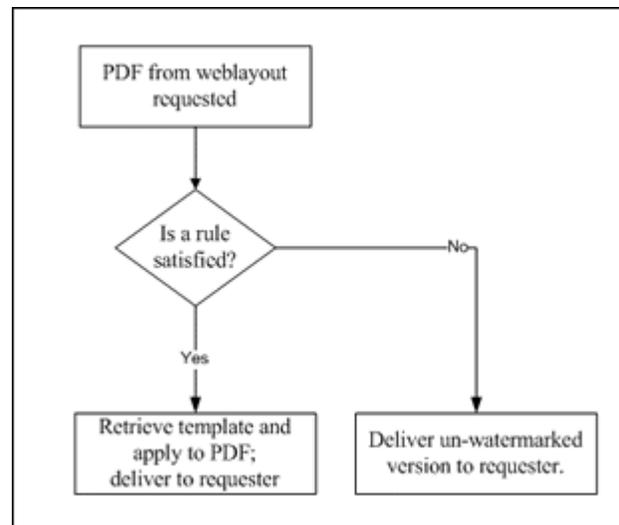
Previous versions of watermarking required the user to define several field variables. Watermark elements are now pre-defined in the template used to watermark the incoming PDF. The watermark is applied and is delivered to requesters without regard for dynamic watermarking rules. Rules-based watermarking (Dynamic) can also be applied in addition to a static watermark.



5.2.2 Dynamic Watermarking Scenario

When a Web-viewable PDF is requested by a user, a check is performed based on the defined rulesets to determine if a watermark is applied to the Web-viewable PDF delivered to the requester.

If a request for a PDF document satisfies a pre-defined rule, the template associated with that rule is used to watermark a copy of the content before the copy is returned to the requesting user.



Important: A PDF optimizer is not provided with PDF Watermark. If using the Optimization feature, install a third-party distiller engine before use and make sure the optimizer is fully operational. The optimizer must be able to execute conversions on a command-line (for example, a script file or a .bat file).

5.3 Managing PDF Watermark

This section describes tasks that are used to manage PDF Watermark.

- [Section 5.3.1, "Specifying the Classpath for an Encryption Library"](#)
- [Section 5.3.2, "Starting PDF Watermark Administration"](#)
- [Section 5.3.3, "Setting Template Metadata Defaults"](#)
- [Section 5.3.4, "Adding or Editing Templates"](#)
- [Section 5.3.5, "Creating and Editing Rules"](#)

5.3.1 Specifying the Classpath for an Encryption Library

The passwords you define in a template set corresponding passwords within the PDF file itself when the PDF file is rendered. The passwords stored in the template are encrypted using a third-party encryption library. A reference to an encryption library used with PDF Watermark must be provided for the Oracle WebCenter Content Server to encrypt passwords stored in the template.

Note: Oracle does not provide an encryption library for encrypting passwords stored in the template. This procedure assumes the use of a third-party encryption library. One such library is `bcprov-jdk14-138.jar` which is downloadable from BouncyCastle.org, but you can use any other library.

1. Download an encryption library .jar file and paste it into the following directory:
/shared/classes

2. From the Windows Start menu, choose **Programs** then **Content Server-[Instance Name]** then **Utilities** then **System Properties**.

The System Properties applet is started.

3. Open the **Paths** tab.
4. Specify the following as the classpath:
`JAVA_CLASSPATH; %SHAREDDIR/classes/bcprov-jdk14-138.jar`
5. Click **OK** to save the changes and exit the System Properties utility.

5.3.2 Starting PDF Watermark Administration

Templates, rules and configuration for PDF Watermark are managed in using the PDF Watermark Administration screen.

1. Choose **Administration** then **PDF Watermark Administration** from the Main menu.
2. Click **PDF Watermark Administration**.

The [PDF Watermark Administration Screen](#) opens.

5.3.3 Setting Template Metadata Defaults

Define any required metadata field values before creating a template. After you save (check in) the template, you can update it to modify the metadata values, if necessary, as you would any content item.

Follow these steps to define specific metadata fields for template check in:

1. Click the **Configuration** tab on the [PDF Watermark Administration Screen](#).
2. Highlight the Field Name and Value pair to define/edit.
3. Click **Edit**.
The [Edit Default Value Screen](#) opens.
4. Set the value to be applied for the Field name selected.
5. Click **Apply**.

5.3.4 Adding or Editing Templates

Before you create a template, you should first provide any default metadata you want applied to the template. For more information about default template metadata, see [Section 5.3.3, "Setting Template Metadata Defaults."](#)

To add a template, perform the following steps:

1. Select the **Templates** tab on the [PDF Watermark Administration Screen](#).
2. To edit an existing template, select the template and click **Edit**. To create a new template, click **Add**.

The [Add New/Edit Template Screen](#) opens.

3. Name your template and assign it a meaningful content ID.
Once you save (check in) the template, you cannot change the content ID.
4. To save changes and check in the template, click **OK**.

5.3.4.1 Setting Security

To provide password security and other restrictions for watermarked PDF documents, perform the following steps:

Note: These security settings set access restrictions within the associated PDF file itself using native PDF security. These access restrictions are separate and in addition to the security defined by Content Server.

1. Open the [Add New/Edit Template Screen](#) and click the Security tab.
For more information about opening the Add New/Edit Template screen, see [Section 5.3.4, "Adding or Editing Templates."](#)
2. To set passwords or other security options, you must first select an encryption bit-depth for **Security Level**. The higher the number, the stronger the encryption.

Note: This encryption level applies to the passwords defined in the PDF file itself, not the watermark template. Oracle does not provide an encryption library for encrypting passwords stored in the template. For more information about adding an encryption library, see [Section 5.3.1, "Specifying the Classpath for an Encryption Library."](#)

3. To restrict access to the PDF file associated with the template, specify a **User Password**. Users are required to specify this password to view or download the PDF.
4. To restrict the ability to change the PDF file or modify the security settings within the PDF file, specify an **Owner Password**.
This password applies to the associated PDF file itself, not the current watermark template. Access to the template is governed by Content Server's security model.
5. To prevent the user from printing any portion of the PDF file, set **Print Allow** to **No**. To permit printing at low resolution, selected **Degraded**.
6. To prevent the user from copying portions of the PDF file, set **Copy Allow** to **No**.

For more information about these settings, see [Section A.3.6, "Add New/Edit Template Screen."](#)

5.3.4.2 Add or Edit a Text Watermark

To add or edit a text watermark, perform the following steps:

1. Open the [Add New/Edit Template Screen](#) and click the Text Watermark tab.
For more information about opening the Add New/Edit Template screen, see [Section 5.3.4, "Adding or Editing Templates."](#)
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**. The [Add New/Edit Text Watermark Window](#) opens.
3. Specify the **Text** to appear in the watermark. The text can include embedded symbols that are replaced by document information, such as the page count or the document name when the watermark is rendered.
4. Select the **Location** on the page where the watermark appears.

For more information about watermark placement, see [Section 5.1.7, "Watermark Placement."](#)

5. If you select **Explicit** as the location, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.
6. Specify the **Rotation** of text from 0 to 359 degrees, rotated counter clockwise.
7. Select the horizontal **Alignment** at the specified location.

For more information about text alignment, see [Section 5.1.7, "Watermark Placement."](#)

8. Select the font, size, weight and color. Note that weight is disabled for those fonts that do not have an extended weight.
9. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
10. Specify a **Page Range**. If left blank, the page range includes the entire document.
Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page without having to specify the actual page number. For example:
1,2,4,12:24,50:LAST.
11. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.
12. Click **OK** when done.

For more information about individual settings, see [Section A.3.7, "Add New/Edit Text Watermark Window."](#)

5.3.4.3 Add or Edit an Image Watermark

Before you can an image as a watermark, check the image into the system and note the content ID. To add or edit an image watermark, perform the following steps:

1. Open the [Add New/Edit Template Screen](#) and click the Image Watermark tab.
For more information about opening the Add New/Edit Template screen, see [Section 5.3.4, "Adding or Editing Templates."](#)
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**. The [Add New/Edit Image Watermark Window](#) opens.
3. Specify the **Content ID** of the image to use.

The image can be any supported bitmap (raster) image format, such as GIF or JPG.

4. Optionally specify a **Scale Factor** to preserve or modify the size of the image when it is used as a watermark. Without specifying a scale factor, images are rendered at 72 dpi.

The Scale Factor is expressed as a percentage based on the following formula:

$$\frac{\text{<default dpi>}}{\text{<image dpi>}} * 100\%$$
 For example, to maintain the size and resolution of a 300 dpi image, you calculate the Scale Factor as follows: $72 \text{ dpi} / 300 \text{ dpi} * 100\% = 24\%$ for a Scale Factor of 24.

5. Select the **Location** on the page where the watermark appears.

For more information about watermark placement, see [Section 5.1.7, "Watermark Placement."](#)

6. If you select **Explicit** as the location, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.
7. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
8. Specify a **Page Range**. If left blank, the page range includes the entire document.
Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page without having to specify the actual page number. The following page range includes all of these options: 1,2,4,12:24,50:LAST.
9. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.
10. Click **OK** when done.

For more information about individual settings, see [Section A.3.8, "Add New/Edit Image Watermark Window."](#)

5.3.4.4 Add or Edit an Electronic Signature Watermark

To add or edit an electronic signature watermark, perform the following steps:

1. Open the [Add New/Edit Template Screen](#) and click the Signature Watermark tab.
For more information about opening the Add New/Edit Template screen, see [Section 5.3.4, "Adding or Editing Templates."](#)
2. To add a watermark, click **Add**. To edit an existing watermark, click **Edit**. The [Add New/Edit Signature Watermark Window](#) opens.
3. Specify the **Label** to appear in the watermark. The text can include embedded symbols that are replaced by document information, such as the page count or the document name when the watermark is rendered.
4. Specify the **Fields** to use in the watermark as a comma-delimited list.

Note: The fields you specify here are the standard or user-defined fields from the Electronic Signatures table.

5. Select the **Location** on the page where the watermark appears.
For more information about watermark placement, see [Section 5.1.7, "Watermark Placement."](#)
6. If you select **Explicit** as the location, specify the **X-Coordinate** and **Y-Coordinate** location for the watermark. Values are specified in points. Each point is 1/72 in. measured from the lower-left corner of the page.
7. Select the font, size, weight and color. Note that weight is disabled for those fonts that do not have an extended weight.
8. Select whether to **Layer** the watermark Over or Under the content in the PDF (including other watermarks).
9. Specify a **Page Range**. If left blank, the page range includes the entire document.
Separate specific pages with commas (1,2,4). Separate the first and last pages in a page range with a colon (12:24). Use the keyword LAST to designate the last page

without having to specify the actual page number. For example:
1,2,4,12:24,50:LAST.

10. Specify a Page Range **Modifier** to watermark **Even Pages Only** or **Odd Pages Only**.

11. Click **OK** when done.

For more information about individual settings, see [Section A.3.9, "Add New/Edit Signature Watermark Window."](#)

5.3.5 Creating and Editing Rules

Before you can define rules for applying a template, you must first create the template. For more information about creating a template, see [Section 5.3.4, "Adding or Editing Templates."](#)

Follow these steps to add or edit a rule:

1. Select the [Rules Tab](#) on the [PDF Watermark Administration Screen](#).
2. To add a new rule, click **Add**. To change an existing rule, select a rule and click **Edit**.

The [Add New/Edit Rule Screen](#) opens.

3. For a new rule, enter a **Name** that describes the way a rule is used.

After you save a rule, you cannot change the name. To change the name of a rule, you must delete the rule and create a new one.

4. Select a **Template ID** to associate with the rule.
5. To add a new criterion, click **Add**. To change an existing criterion, select the criterion and click **Edit**.

The [Add New/Edit Criteria Screen](#) opens.

6. For a new criterion, select the **Field Name**.

After you save a criterion, you cannot modify the field selection. To specify a different field name, create a new criterion.

7. Specify the **Value** for the selected field. If the field chosen is a list, select a value from the options list.

Note: Rules criteria are case-sensitive. The value you enter must match the case of the returned value. For example, if the title you enter is "foobar" and the value returned is "FooBar", it is considered a mismatch and the rule fails.

8. To save the criterion, click **OK**.
9. To save the criteria for the current rule, click **OK**.

Within a rule, the order of criteria does not matter. All criteria must be satisfied for the rule to apply.

10. To change the order of the rules assigned to the template, select a rule and use the **Move Up** and **Move Down** buttons to change the position of the rule in the list.

The order in which the rules are tested can be significant, depending on the criteria used. In general, order the rules with the most specific tests (number of criteria) high in the list, and the more general ones (fewer criteria) lower down.

11. Click OK.

Using Folders and WebDAV

Oracle WebCenter Content Server includes components that provide a hierarchical folder interface, similar to a conventional file system, for organizing and managing some or all of the content in the repository.

- **Folders:** This component (also called FrameworkFolders after the component) provides a hierarchical folder interface within the browser, similar to a conventional file system, for organizing, locating, and managing repository content and content item metadata. The Folders functionality is installed but disabled by default. Folders is a scalable, enterprise solution and is meant to be a replacement for Contribution Folders.

Note: Unless you are migrating content from Contribution Folders to the Folders interface, you should not enable both Contribution Folders and Folders. For more information about migrating Contribution Folder content, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

- **Contribution Folders:** This optional component (also called virtual folders or folders_g after the name of the component) provides a hierarchical folder interface within the browser, similar to a conventional file system, for organizing repository content. The component is installed but disabled by default. The newer, Folders component is meant to be a replacement for Contribution Folders.
- **WebDAV (Web-Based Distributed Authoring and Versioning):** Both folder components work with Content Server's built-in WebDAV functionality to allow users to remotely manage and author content using clients that support the WebDAV protocol. The WebDAV interface provides a subset of the options available through the browser interface. In general, you can create, delete, move, and copy both folders and content items, and you can modify and check in content items. To check out content items through the WebDAV interface, you must use a WebDAV client that can open the file. To perform other management tasks, such as specifying or propagating metadata values, you must use the standard browser interface.

This chapter provides information about administering folders and WebDAV interfaces. It covers the following topics:

- [Section 6.1, "Using Folders"](#)
- [Section 6.2, "Managing Folders"](#)
- [Section 6.3, "Using Contribution Folders"](#)
- [Section 6.4, "Managing Contribution Folders"](#)

- [Section 6.5, "WebDAV Interface"](#)
- [Section 6.6, "Administering WebDAV"](#)
- [Section 6.7, "WebDAV Troubleshooting"](#)

6.1 Using Folders

The Folders component (also called Framework Folders) provides a hierarchical folder interface, similar to a conventional file system, for organizing and locating some or all of the content in the repository. The Folders functionality is installed but disabled by default. This is a scalable, enterprise solution and is meant to be a replacement for Contribution Folders.

Note: Unless you are migrating content from Contribution Folders to the Folders interface, you should not enable both Contribution Folders and Folders. For more information about migrating Contribution Folder content, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

This section covers the following topics:

- [Section 6.1.1, "The Folders Interface"](#)
- [Section 6.1.2, "Folders and Files"](#)
- [Section 6.1.3, "Shortcuts and Links"](#)
- [Section 6.1.4, "Query Folders and Folder Search"](#)
- [Section 6.1.5, "Folders Retention"](#)
- [Section 6.1.6, "Personal Folder"](#)
- [Section 6.1.7, "Security and User Access"](#)
- [Section 6.1.8, "Content Item Versioning"](#)
- [Section 6.1.9, "Folder and Content Item Metadata"](#)

6.1.1 The Folders Interface

The Folders hierarchy is accessible through both the standard content management Web interface and through the WebDAV interface. With the standard interface, you access folders and content items (files) with a browser and specially designed Web pages. With the WebDAV interface, you create a network connection to Content Server and then access folders and files through Windows Explorer as you would a shared folder.

The familiar folder and file model provides a framework for organizing and accessing content stored in the repository. Functionally, folders and files are very similar to those in a conventional file system. You can copy, move, rename, and delete folders and files. You can also create shortcuts to folders or files so you can access a content item from multiple locations in the hierarchy.

You can think of the files in the Folders interface as symbolic links or pointers to content items in the repository. The operations you perform in the Folders interface, such as searching or propagating metadata, effectively operate on the associated content items.

6.1.2 Folders and Files

As with a conventional file system, Folders offers a convenient way to organize content. Users can easily view the relationship between folders and subfolders and can browse to a group of content items.

Using Folders, users can perform the following actions with the privileges defined by Content Server's standard security model:

- Browse to locate content items for check-in, check-out, and to view and change folder and item information.
- Create new folders and subfolders.
- Create new content items in a folder or add existing repository content to a folder.
- Add shortcuts to folders or content items in one or more locations. Shortcuts act as placeholders for the referenced content item.
- Move or copy folders or files to other locations.
- Rename a folder or file.
- Remove a file from the folders hierarchy. This does not affect the associated content item.
- Delete a folder or file. When you delete a folder or file, the folder or file and any shortcuts to it are removed from the folders hierarchy. Any content items associated with the files are set to *expired* in the repository.
- Create a query folder that contains content items returned by the query associated with the folder. For more information about query folders, see [Section 6.1.4, "Query Folders and Folder Search."](#)
- Create a retention query folder and assign retention rules for the content items returned by the query. For more information about query folders and retention scheduling, see [Section 6.1.5, "Folders Retention."](#)
- Assign folder security and default metadata values for content items created in the folder. You can also propagate specified metadata values to the contents of a folder or block propagation for a given folder. For more information, see [Section 6.1.9, "Folder and Content Item Metadata."](#)

The Folders interface follows several conventions familiar to users of file systems:

- Use standard Windows naming conventions when creating folders. Do not use special characters such as the forward or backward slash characters or the double quote character.
- Content Server can store multiple files of the same name as separate content items. However, in the Folders interface, file names in a given folder must be unique (in the same way that a folder in Windows cannot contain two files with the same name).

6.1.3 Shortcuts and Links

With Folders, you can reference the same folder or content item in multiple locations using shortcuts that act as placeholders for the referenced folder or file. You can create shortcuts to folders or files to help you locate and manage the target content items within the folder hierarchy.

6.1.3.1 Folders and Shortcuts

Folders and folder shortcuts are identified with different icons:

Icon	Description
	Folder: Folders can contain other folders, content items, and shortcuts to other folders and content items. Folders are identified by a standard folder icon.
	Folder Shortcut: A folder shortcut includes the contents of the associated folder in the hierarchy at the point where the shortcut is stored. Folder shortcuts are identified by a folder icon with an arrow and can reference either a folder or a query folder. Folder shortcuts are excluded from metadata propagation actions.
	Query Folder: The contents of a query folder are the repository content items returned by the query associated with the folder. Query folders are identified by a folder icon with a magnifying glass.
	Retention Query Folder: Similar to a query folder, the contents of a retention query folder are the repository content items returned by the query associated with the folder. You can additionally specify retention rules for the content items returned by the query. Retention query folders are identified by a folder icon with a magnifying glass and a clock.

6.1.3.2 Content Item Links

You can think of content items in the Folders interface as links to items in the repository. There are two types of links for content items:

Icon	Description
	File (primary link): There can be only one primary link to a content item in the Folders interface. The primary link represents the content item in the repository and is identified by a standard document icon. In most respects, working with a file (or primary link) is the same as working directly with the content item in the repository. For example, if you delete a file, the status of the associated content item in the repository is set to "expired."
	Shortcut (secondary link): There can be any number of file shortcuts in the Folders interface to an associated content item. A file shortcut is identified by a document icon with an arrow indicating that it is a reference to the actual content item. Shortcuts are excluded from metadata propagation actions. Changes you make by means of the shortcut (such as metadata changes) are made to the underlying content item. Changes you make to the shortcut itself (such as deleting the shortcut) do not affect the underlying content item.
	Query result: The contents of a query folder are the repository content items returned by the query associated with the folder. Query content items are identified by a document icon with a magnifying glass.

6.1.4 Query Folders and Folder Search

A query folder functions much like a saved search; each time you access the folder, you initiate the query associated with the folder. The contents of a query folder are the content items returned by the query. The contents of query folders can change dynamically as the contents of the repository change.

Query folders contain the actual repository content items returned by the query. That is, folders and shortcuts are not included in the contents of query folders.

With the contents of a query folder, you can copy the associated content items, view and update metadata information for individual items, or propagate metadata changes through all items in the query folder.

Folders also expands the standard search results options to include the **Create Query Folder** option to save a search query as a query folder.

To search for folders or files from within a folder, use the options in the Search menu in a given folder. You can search any or all folder metadata fields.

6.1.5 Folders Retention

With Folders, you can perform basic content retention scheduling by creating a retention query folder, assigning retention attributes to the folder, and then configuring the retention schedule. You can assign retention rules based on the age of the content item or on the number of revisions. If you have a license for Oracle WebCenter Content: Records, you can also define retention rules based on categories defined in Records.

You must be an administrator to specify retention rules or schedules. For information about specifying retention scheduling, see [Section 6.2.2.1, "Specify Retention Rules"](#). For information about specifying retention scheduling, see [Section 6.2.2.2, "Configure Retention Schedule"](#).

Considerations

The following considerations apply to retention query folders:

- Retention rules are associated with the retention query folder but are stored separately from the standard folder metadata. For this reason, you cannot search for a query folder based on the folder's retention attributes.
- Unlike standard query folders, retention query folders search only database values and cannot perform full-text searches even if full-text search is supported on your system.
- If you specify multiple retention rules for a particular retention query folder, all the rules must be satisfied for the disposition to occur. For example, if you specify the age as 1 calendar year and the number of revisions to keep as 3, only those items that are more than 1 year old and that are older than the last three revisions are deleted.
- Different queries can include the same content item in their results. In this case, the retention rules for each retention query folder are applied independently from one another. For example, if one query folder specifies the number of revisions to keep as 2 and another specifies the revisions to keep as 3, only two revisions of the item are retained.
- Folders retention is treated differently than that in Oracle WebCenter Content: Records. When using Records, if multiple delete actions are called, the retention with the longest interval is used. In Folders, the shortest interval always runs first.
- Folders retention processes items based on the values in the dCreateDate row in the Revisions table in the database.

Considerations with Oracle WebCenter Content: Records

If you use both Folders and Oracle WebCenter Content: Records on the same system, the following additional considerations apply:

- If you have Records installed, it is possible to have two retention schedules (as well as multiple rules) for the same item. If a content item has retention rules defined in both Content Server and in Oracle WebCenter Content: Records, only the retention and schedule defined by the Records system are used.
- If you have Records installed with a level of DoD Baseline or higher, retention query folder options are not available in the Content Server interface. Any existing

retention query folders retain their icon and (inactive) retention attributes, but function as a standard query folder.

If the level is then set to Standard or lower, then retention query folder options are enabled in Content Server and the rules for any existing retention query folders become active.

6.1.6 Personal Folder

In the root folder of the Folders hierarchy is a Users folder that contains a folder defined for you as an authenticated user. You can create subfolders and content items in the same way you do with other folders in the hierarchy. Your personal folder, however, is visible only to you. Every authenticated user can have a personal folder.

Folders provides menu options to quickly add folders, files, and shortcuts to your personal folder, referred to in menus as **Add to My Folder**.

To access your personal folder, click **My Content Server** in the tray area and then click **My Folders**.

6.1.7 Security and User Access

Users can create and edit folders, shortcuts to folders, and links to documents as allowed by Content Server's standard security model. Folders are assigned security attributes in the same way they are assigned to content items, including security group, account, and Access Control List attributes, if enabled.

By default, folders inherit the security settings and other default metadata defined for the parent folder. You can, however, explicitly set security and metadata values for a given folder and propagate those values to folders and content items within the folder.

6.1.8 Content Item Versioning

You can check out content items and check in new versions of those content items through the Folders interface in much the same way you do through the standard content management pages. When you view or edit the metadata information for a particular content item, you can choose menu options to check out the item and then check in a new version of that item.

Folders provides two modes for viewing content item versions:

- **Published Items (consumption mode):** The latest released revisions of documents are displayed. These are the same revisions that are returned in search result listings.
- **All Items (contribution mode):** The latest revision of each document is displayed. These can include the revisions of documents that are still in workflow or have otherwise not finished with the search indexing process.

As a user, you can switch between the two modes to see released content items only or to see content items that require work before being released. The selection you make remains in effect until you explicitly change it.

6.1.9 Folder and Content Item Metadata

Every folder has a set of metadata values that can be applied to content items added to the folder. You can configure folders to enforce metadata rules on their content items or allow any or all values to be modified. For example, a folder could be configured to enforce 'Secure' as the value for the Security Group metadata field. Then, when a

content item is added to that folder, the Security Group value automatically updates to Secure.

Folders inherit the default metadata assigned to their parent folders unless the folder is explicitly configured otherwise. Subsequent changes to a parent folder's metadata do not affect the metadata for existing subfolders unless explicitly propagated down through the hierarchy.

Folder metadata inheritance and propagation make it easy to apply metadata to content items. Whether you are an administrator managing all folders and files or a user managing your own folders and files, it is a good idea to plan your metadata strategy before you start creating folders and adding content items. Your strategy should include the following basic steps:

1. Determine whether specific folders or branches in the hierarchy have unique metadata requirements and how best to identify and manage those requirements.
2. Determine which metadata fields (if any) a user should specify when adding or checking in a content item through a particular folder.
3. Determine which metadata fields (if any) should have a default value or an enforced value for a particular folder.
4. Determine which subfolders (if any) are eligible to be changed when propagating metadata through a folder.
5. Determine whether to use profiles to manage metadata requirements. An administrator can create one or more profiles to organize, selectively display, and control access to metadata fields based on rules associated with the profile.

6.1.9.1 Default Metadata

Default metadata values are automatically applied to new content items created in or checked in to a folder. To modify the default metadata values for a folder, you must have Delete permission to the folder or be the Author and have Write permission.

If default values are not provided for all required fields, you are prompted to provide them when you create or check in the content item.

Default metadata values are also used as the default values when propagating metadata.

If you are using Oracle WebCenter Content: Desktop and the folder has the **Prompt for Metadata** option selected, you are prompted to provide metadata values for the item rather than relying on the folder's default metadata settings. For more information about Desktop, see *Oracle WebCenter User's Guide for Desktop*.

6.1.9.2 Metadata Propagation

With proper permissions, you can propagate metadata values from a folder to its subfolders and content items. To propagate metadata to the content items in a particular folder, you must have Write permission for the folder and the content items themselves. To propagate to any folders below the folder in the hierarchy, you must have Delete permission to the folders.

Content items in a folder do not necessarily have the same security settings. To propagate metadata to content items, you must also have Write permission for the content item. To restrict changes to folders only, you can optionally select the **Propagate To Folders Only** option.

When you propagate metadata, you select the metadata fields and can specify the values to propagate from the metadata available for the current folder. You can

propagate any metadata value that you can change. For example, you can propagate the Security Group or Owner values, but you cannot propagate the Content ID. You can also propagate a blank field, such as the Comment or Expiration Date fields, to clear the associated values from content items.

You can configure folders to prevent propagation by selecting **Inhibit Propagation** in the folder information for that folder. You can optionally override a folder's inhibit setting using the **Force Propagation** setting on the Propagate window.

6.1.9.3 Metadata Profiles

An administrator can create sets of metadata as one or more profiles that the administrator or other users can easily apply to folders when specifying folder defaults or when propagating metadata. For more information about using profiles, see the [Section 3.1, "Using Schemas to Customize Metadata."](#)

6.2 Managing Folders

Folders (FrameworkFolders component) provides a hierarchical folder interface, similar to a conventional file system, for organizing and locating some or all of the content in the repository.

This section covers the following topics:

- [Section 6.2.1, "Setting Configuration Variables"](#)
- [Section 6.2.2, "Working with Retention Scheduling"](#)
- [Section 6.2.3, "Migrating to the Folders Structure"](#)

6.2.1 Setting Configuration Variables

You can set configuration variables in Content Server's `config.cfg` file to modify the behavior of Folders. This section covers the following topics:

- [Section 6.2.1.1, "Folder Variables"](#)
- [Section 6.2.1.2, "Folders Migration Variables"](#)
- [Section 6.2.1.3, "Folders WebDAV Variables"](#)

6.2.1.1 Folder Variables

These variables configure optional settings in the Folders interface.

Variable	Description
AuthorDelete	If set to true, the owner/author of an item can delete the item as long as they have Write privileges, otherwise, they require Delete permission. The default value is true.

Variable	Description
DisablePersonalFolderFormat	<p>Set to true to disable personal folder naming specified by FldPersonalFolderFormat. The default is false.</p> <p>If you change or disable the name format for personal folders after personal folders are created, you must manually rename existing folders, or recreate them. For example, if the personal folder for user abc.def@oracle.com is formatted with the name abc.def and then DisablePersonalFolderFormat is set, the database retains the existing folder name, but the user interface expects it to be named abc.def@oracle.com. You must rename the folder to match the disabled formatting or delete the row from the database and recreate the folder when the user logs in.</p>
FldDefaultFilesLoadCount	Number of files to display in the folder explorer. The default is 50.
FldDefaultFoldersLoadCount	Number of folders to display in the folder explorer. The default is 50.
FldEnableInProgressIndicator	If set to true, enables the Process Indicator shown during copy, move, delete, and propagate operations. The default value is false.
FldPersonalFolderFormat	<p>Specify the regular expression used to construct the name of the personal folder from the user's name. By default, the regular expression is <code>(.+)(.+):\$1</code> (two groups of one or more characters separated by "@" and using the first group as the folder name. For example, the user name abc.def@oracle.com results in a personal folder is named abc.def. Refer to http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html for information about regular expressions.</p>
FldShowAutoPropagateOption	<p>By default, moved items retain the metadata defined for the item and do not inherit metadata values in the new location. If you set this variable to true, the Auto propagate destination's metadata to folder option is added to the Choose a Destination window for mover operations. If the user selects this option, moved items inherit the metadata defined by the enclosing folder in the same way that copied items do. The default value is false.</p>
FoldersDefaultDocType	Specify a document type to use if the document type cannot be determined when creating a content item. The default document type is Document.
FoldersIndexParentFolderValues	<p>If set to true and Oracle Text Search is in use, sub-folder searching is enabled. The default is false.</p> <p>When enabled, the system adds all paths to all documents to the search index. Documents are reindexed whenever they are added to or removed from a folder. In addition, the document is reindexed if its full path changes in any way (for example, when the parent folder is moved).</p>

6.2.1.2 Folders Migration Variables

These variables configure optional settings in the Folders Migration utility. The Folders Migration utility migrates folder content and structure from Contribution Folders (Folders_g component) to Folders (FrameworkFolders component). The utility is available the tables associated with Contribution Folders are present in the database schema. For more information about migrating content, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

Variable	Description
FldMigrateDefaultSecurityGroup	Specify the default Security Group to assign to migrated folders if one is not already associated with the folder. If not set explicitly, the default value is Public. Contribution Folders do not need and may not have a Security Group setting. Migrated folders require a security setting.
FldMigrateRootBaseName	Specify the base name for the root folder created during migration. The folder name has the form: <\$FldMigrateRootBaseName\$>_<\$date\$>_#<\$run_index\$> If not set, the base value defaults to "Migrate".
FolderMigrateExcludeList	Specify the list of folders to exclude from the migration. The list may include folder IDs and folder marks. If not set explicitly, only the TRASH folder is excluded.
ShowFolderMigrationMenu.	Set to 0 (zero) to prevent the Folder Migration option from showing in the Administration menu. If set to 1 or if not set explicitly, and migration is possible, the option is displayed.

6.2.1.3 Folders WebDAV Variables

These variables configure optional settings in the Folders WebDAV interface.

Variable	Description
OVERWRITE	Set to false to prevent a WebDAV copy from writing over items with the same name. The default value is true

6.2.2 Working with Retention Scheduling

You can specify how to dispose of content item revisions based on the age of the content item or on the number of revisions. If you have a license for Oracle WebCenter Content: Records, you can also define retention rules based on categories defined in that product. For additional retention query folder considerations, see [Section 6.1.5, "Folders Retention."](#)

To define retention scheduling for the contents of a retention query folder, you must first specify the retention rules associated with the folder and then specify the retention schedule for each of the rules used with one or more retention query folder.

This section covers the following topics:

- [Section 6.2.2.1, "Specify Retention Rules"](#)
- [Section 6.2.2.2, "Configure Retention Schedule"](#)

6.2.2.1 Specify Retention Rules

You can specify retention rules when you create a retention query folder and modify them at a later time. You can specify retention rules for retention query folders only, and only if you are an administrator. Retention query folders that do not include retention rules act like standard query folders.

Note: If you have Oracle WebCenter Content: Records installed with a level of DoD Baseline or higher, retention query folder options are not available in the Content Server interface. Any existing retention query folders retain their icon and (inactive) retention attributes, but function as a standard query folder.

The following procedure shows how to specify retention rules. For more information about creating folders and specifying queries, see the *Oracle WebCenter Content User's Guide for Content Server*.

Query folders with retention rules apply the rules on a schedule you specify. For more information about how to create a retention schedule, see [Section 6.2.2.2, "Configure Retention Schedule."](#)

1. Navigate to the folder where the retention query folder resides.
2. To change metadata values, including the retention rules, choose **Update Folder Information** from the Actions menu for the associated folder.

To change metadata values for the folder when you are viewing the contents of the folder, choose **Folder Information** from the **Edit** menu on the page.
3. Click **show advanced retention options**.
4. Choose one or more retention options. For example, to keep only the most recent 3 revisions of a content item, choose **Revisions** and specify **3**. Older revisions are expired on the retention schedule specified for Revisions.
 - a. **Revisions:** Specify how many revisions of the content items in the query folder to keep and click **Update**.
 - b. **Age:** Specify how long to keep the content items in the query folder and click **Update**.

If you have the full Oracle WebCenter Content: Records product, the units list includes fiscal units as well as calendar units.
 - c. **Category:** Assign a category to the query folder and use the retention defined for the category to determine how to dispose of the content items.

This option is available only with the full Oracle WebCenter Content: Records product.
5. Make any additional changes to the folder metadata or query and click **Save**.

6.2.2.2 Configure Retention Schedule

Query folders with assigned retention rules apply the rules on a schedule you specify. You can specify a different schedule for each type of retention rule. Content items that are included in multiple query folders can have multiple retention rules, and therefore multiple schedules, applied to them.

Note: Folders retention rules are treated differently than those in Oracle WebCenter Content: Records. When using Records, if multiple delete actions are called, the retention with the longest interval is used. In Folders, the shortest interval always runs first.

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

For additional retention query folder considerations, see [Section 6.1.5, "Folders Retention."](#)

1. From the Administration menu, choose **Folders Retention Administration** and then choose **Configure Scheduled Jobs**.

The Folder Retention Scheduled Jobs page opens.

2. Specify schedules for retention rules governed by age or revision.

Age-based rules process items based on the values in the dCreateDate row in the Revisions table in the database.

- a. **Weeks/Days:** Select a Start Time and an End Time. This schedules the retention for query folders with Weekly retention rules. To run the scheduled disposition immediately, click **Run Now**.
- b. **Calendar Months:** Select a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Monthly or Quarterly retention rules. To run the scheduled disposition immediately, click **Run Now**.
- c. **Calendar Years:** Select a month, a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Yearly retention rules. To run the scheduled disposition immediately, click **Run Now**.
- d. **Fiscal Months/Fiscal Years:** If you have the Oracle WebCenter Content: Records product, you can schedule the retention for query folders with Fiscal Month and Fiscal Year retention rules. To run the scheduled disposition immediately, click **Run Now**.
- e. **Retention Revisions:** Select a day of the month, a Start Time and an End Time. This schedules the retention for query folders with Revisions retention rules. To run the scheduled disposition immediately, click **Run Now**.

Note: If you have the Oracle WebCenter Content: Records product and use category retention rules, the categories are scheduled by their associated age or revision rules. For example, a category with a retention specified in months is governed by the value you specify here for **Calendar Months**. Likewise, to immediately apply the retention rules for all items with retention rules or categories specified in months, click the **Run Now** button associated with Calendar Months on this page.

3. Click **Update**.

6.2.3 Migrating to the Folders Structure

If you have content in an existing Contribution Folders hierarchy (folders_g component) and want to migrate the folders and files to the Folders interface, you can use the Folders Migration utility to replicate the folder hierarchy and selectively migrate folder content. For more information about the Folders Migration Utility, see the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.3 Using Contribution Folders

Contribution Folders is an optional component that, when enabled, provides a hierarchical folder interface in the form of contribution folders (also called hierarchical folders), enabling the creation of a multilevel folder structure.

Note: The newer, Folders component is a scalable, enterprise solution and is meant to be a replacement for Contribution Folders.

This section covers the following topics:

- [Section 6.3.1, "Usage and Structure"](#)
- [Section 6.3.2, "Contribution Folders Component Security"](#)
- [Section 6.3.3, "Trash Bin"](#)
- [Section 6.3.4, "Metadata Propagation and Default Values"](#)
- [Section 6.3.5, "Latest Version versus Latest Released Version"](#)
- [Section 6.3.6, "Local Contribution Folders"](#)
- [Section 6.3.7, "Contribution Folder Archiving and Searching"](#)
- [Section 6.3.8, "Optimizing Performance"](#)
- [Section 6.3.9, "Metadata Inheritance"](#)

6.3.1 Usage and Structure

There are several advantages when using folders:

- **Browsing:** Users can browse through folders to find sub-folders and content items using a simple mechanism to retrieve additional information about a folder, and to traverse the tree structure. In a folder with a large number of sub-folders, the user can easily view and browse through content items in that folder.
- **Creating folders:** Users can create new folders in any folders easily, by naming the folders. Additional information such as folder metadata and default metadata is accessible only if needed.
- **Assigning folder metadata:** Users can assign metadata to folders when creating a folder or to existing folders using the same process.
- **Assigning default metadata for items:** Users can specify metadata to be assigned to content created in or added to a folder. You can set the metadata at folder creation time or later. The steps and process are the same.
- **Assigning a Content Profile to a folder:** You can assign content profiles to a folder when you create the folder or later to determine what metadata fields are available to be set as defaults for content items added to that folder.
- **Creating new content in a folder:** Users can browse through a folder and check in a new item. If the folder specifies default metadata for new content, or a content profile, then the content check-in form reflects that.
- **Adding existing content to a folder:** Users can browse into a folder and add a link to an existing content item. If the destination folder contains items with the same name, the user is asked to rename the new link.
- **Moving or copying items:** Users can browse to a folder, select one or more sub-folders and content items, and move them or copy them into another folder.

- Deleting an item/folder: A user can browse to a folder, select one or more sub-folders and content items, and delete them. The user is prompted for confirmation of delete action. For items with multiple revisions, the user is asked whether all revisions are deleted or only the latest revision. The user should have an option to apply their answer to all selected files.
- Renaming an item/folder: A user selects a link/shortcut or sub-folder within a folder and renames it. The rename action is allowed only on single items. If the new name is same as that of an existing item or folder, the user is warned and required to change the name to be unique.

The following structure is used for Contribution Folders:

- Each Oracle WebCenter Content Server instance has a common set of contribution folders. Any change to the folders is applied systemwide.
- There is one default system-level folder, called Contribution Folders. The Trash Bin function is enabled during installation with a system-level folder called Trash created.
- The system administrator can change the name of a system-level folder, but cannot delete it or add a custom system-level folder except through changes to the database. Deleting a system-level folder disables it, but does not remove it from the system.
- Each folder in the hierarchy contains content items that have the same numeric Folder value, which is assigned automatically upon creation of the folder. Changing the value of the Folder field for a content item places it in a different folder.
- You can limit the maximum number of folders and content items in each folder so that browsing through contribution folders does not affect system performance.

The Contribution Folders component mimics the Windows file system. The use of double quotes in the name is not allowed (for example, "doublequotedfolder"). Use the standard naming conventions for Windows when creating folders.

6.3.2 Contribution Folders Component Security

The Contribution Folders component applies security at two levels:

- Content item security: The user logins and security controls in Oracle WebCenter Content Server also apply to content that is managed through contribution folders. For example, if you have Read permission for a content item, you can view the file, but you cannot check in a revision to the file.

To allow users with Read permission to access content through a contribution folder, the `GetCopyAccess` environment variable must be set. To set this variable:

1. From the Administration tray, select **Admin Server**.
 2. Click **Content Security**.
 3. Select **Allow get copy for user with read privilege**.
- Folder security: Security is also applied at the folder level:
 - Each contribution folder has an *owner*, a user who has permission to manage the folder. The owner can change a folder's metadata and delete the folder, even if they do not have Write or Delete permission to the folder's security group. However, the owner does not have additional permissions to content items in the folder.

- Users can see only the contribution folders assigned no security group or a security group for which they have at least Read permission.
- To delete a folder, a user must have Delete permission to the folder or be the owner of the folder. The user must also have permission to delete all of the content items and subfolders in that folder.
- To change a folder's default metadata, a user must have Read and Write permissions. If the environment variable `FoldersModifyWithRW=false`, a user must also have Delete permission to the folder or be the owner of the folder.

Caution: Be careful when changing the security group of a folder. If a folder is changed to a more restrictive security group, authors may no longer have permission to manage their own content items.

When creating a new folder, the metadata from the parent folder populates the fields for the new folder. The folder initially "inherits" the metadata, but can change its values without affecting the parent folder. Later changes to a parent folder's metadata do not affect the metadata for existing subfolders. To apply a parent folder's metadata to subfolders and content items, use the [Metadata Propagation and Default Values](#) feature.

6.3.3 Trash Bin

The *Trash Bin* is an optional feature that sends deleted items to a Trash folder, rather than permanently deleting the items. Items in the Trash Bin can then be permanently deleted or restored to their original location in the folder hierarchy.

Note the following considerations for the Trash Bin feature:

- Deleting a revision from the Repository Manager bypasses the Trash Bin and permanently deletes the revision.
- You can enable or disable the Trash Bin function using System Folder Configuration after installation.
- If using folders to contribute content to a Site Studio Web site, it consider disabling the Trash Bin feature. Otherwise, any deleted content items, such as those moved to Trash Bin, still appear in the tables of content (dynamic lists) on the Web site. To get rid of the content items, go into the Trash Bin in WebDAV and explicitly delete the documents from there, too.

6.3.4 Metadata Propagation and Default Values

The *metadata propagation* function enables contributors to copy specified metadata values from a folder to its subfolders and content items. Propagation is useful when moving a large number of content items to a new folder structure, or after revising the default metadata for a folder. This feature allows the application of metadata to all items in the structure.

Note the following considerations regarding metadata propagation:

- The propagation function applies each folder's metadata to all uninhibited subfolders and content items within those folders. Each uninhibited subfolder and content item inherits the metadata of the launched folder.
- When inhibiting a folder, it is not affected by metadata propagation from a higher-level folder. However, metadata propagation can still be launched *from* an inhibited folder.

- The system administrator selects which metadata fields are included in propagation. This setting applies systemwide. By default, no metadata fields are included until they are selected.
- If a folder metadata field does not have a value defined, subfolders and content items within that folder cannot inherit the blank value during propagation and any existing metadata values can remain intact for these items. The `CollectionPropagateEmptyValues` configuration variable controls if empty field values are propagated.
- When metadata propagation is launched, only folders and content items for which you have Write permission to the security group are affected.

When a file is checked in through a contribution folder, default metadata values are entered on the content check-in form. The default values are evaluated in the following order:

1. Contribution folder default values: When checking in a new content item from an Exploring page, default metadata values for that contribution folder are entered on the content check-in form.
2. User default metadata values: If any metadata defaults are not defined for the contribution folder, the user's default metadata values are applied. User default metadata values are only applicable when creating new content items using WebDAV. They are not applicable when using the Web interface.
3. System default metadata values: The system default values are applied to any fields not defined by the contribution folder or the user's default metadata. These values are defined by the system administrator. System default metadata values are only applicable when creating new content items using WebDAV. They are not applicable when using the Oracle WebCenter Content Server Web interface.
4. None: You can leave a metadata field blank if it is not a required field. If a required field is blank, an error occurs and the content item is not checked in.

6.3.5 Latest Version versus Latest Released Version

When documents are edited and checked in, the revised document is processed, indexed, then released. Before the process is complete, the revised document is considered the latest version. After the process is complete, the revised document is considered the latest released version.

Depending on the setting of the `CollectionReleasedOnly` configuration variable, users with read access to the content item see either the latest version or nothing if the item is not released. Authors, however, always see the latest version. By default, this variable is enabled and displays the latest version to all users with read access.

See the *Oracle WebCenter Content Idoc Script Reference Guide* for details about the `CollectionReleasedOnly` configuration variable.

6.3.6 Local Contribution Folders

The *local folders* function enables the mapping of a contribution folder structure to a local file system on the host system (not the user's system). Changes to the folder, its subfolders, and content items are reflected in the local directory. To allow users to access and modify files in the local directory, you can map the local folder to a shared drive and allow access using standard folder permissions.

You can use local folders to manage content, such as the files on a Web site, which contain links to other files in the same folder hierarchy. In Content Server, individual

content items are stored according to security groups and content types, not folder locations. Hyperlinks between Web pages do not work if accessed directly from Content Server. Local folders lets you place content items in a folder hierarchy to preserve the link relationships between content items.

The following outline describes how this function could be used for Web site management:

1. A Web designer creates a Web site that contains several Web pages with internal hyperlinking in a multilevel directory structure.
2. Through a WebDAV client, the designer copies the entire Web site structure to a contribution folder called *WebSite*.
3. On the Local Folders Page, the *WebSite* folder is mapped to a directory on a shared drive, *Z:\Intranet*.
4. The *\Intranet* directory is set up as a Web server virtual directory.
5. Users can access the Web site from the *Z:\Intranet* directory without logging in to Oracle WebCenter Content Server. You can update Web pages in Oracle WebCenter Content Server, and they are replicated to the local directory automatically.

Consider the following information when using local folders:

- Oracle WebCenter Content Server security does not apply to folders or content items in the local directory.
- Only content items with a status of "Released" appear in the local directory. Items that fail conversion, are still being indexed, are in a workflow, or have a future release date are not available in the local directory.
- Only the latest revision of a content item is available in the local directory.
- Modifying directories or files directly in the local file system can cause problems with the local folder mapping. All changes must be made through the Oracle WebCenter Content Server Contribution Folders interface.
- To restrict access for specific files to only users who belong to a specific security group, point local directories to */weblayout* secured directories.

6.3.7 Contribution Folder Archiving and Searching

The steps you use to export the folder hierarchy structure are different from the steps you use to archive folder content. The following considerations apply to exporting and archiving folder information: You can archive content in a separate step using Archiver.

- You can export and import the folder hierarchy structure from the Contribution Folders administration interface.
- You can import and export content items with Archiver.
- When you export the folder hierarchy, the entire structure is exported. You cannot specify a particular folder.
- The folder hierarchy is exported to a text file in HDA format, which Oracle WebCenter Content Server can import.

Caution: When you import a folder archive file, all content items are removed from the repository and replaced by the imported folder hierarchy.

If the Contribution Folders `CollectionSearchRecursiveContent` configuration variable is set to true, when users click **Search** on the interface, a **Browse** button and field are displayed in the Results Options section of the Search page. Click **Browse** to find and select a folder, including its subfolders, to be searched.

6.3.8 Optimizing Performance

This section provides guidelines for improving performance with Contribution Folders and WebDAV enabled:

- Limit the number of contribution folders, especially unused ones. The more folders used, the more RAM is required by the folder cache. If a large number of folders is needed, increase the memory available. To allocate more memory, set the `-Xmx JAVA_OPTIONS` parameter to a high enough value to accommodate the memory requirements and avoid getting errors.
- Limit the number of folders and content items in contribution folders. If the number of folders, content items or both in a contribution folder is too high, it can affect performance. When browsing through folders, each item in a folder is processed by the server, the network, and the client browser. Each item takes time and resources at each of these steps. The amount of time is dependent on many factors. A rule of thumb is that each item adds a few milliseconds to browsing response time and a few kilobytes to the size of the page displayed in the browser. Note that the number of items in a folder only affects browsing, not searching.

High numbers of folders, content items or both in a contribution folder can affect the user experience. Users can have a harder time finding things in folders that contain a large number of items.

Therefore, limit the number of folders and content items per contribution folder. The recommended maximum number for both folders and content items per folder is 1,000. Specify these limits during the Contribution Folders/WebDAV software installation or modify the limits later. For more information, see [Section 6.4.1.1, "Setting Folder and File Limits."](#)

- Perform regular database maintenance. When a system has a large number of content items and folders, Contribution Folders performance is affected by database performance. Perform periodic (for example, monthly) database maintenance to verify there is enough RAM, the indexes are optimized, and the database is not too fragmented.
- Relax security to allow users without the appropriate access privileges to see (not access) secure content or folders. The `CollectionContentSecurity` and `CollectionFolderSecurity` variables control if users can see secure content or folders on Exploring pages if they have no access privileges to the content. If these variables are set to 'false' (not the default), users with no access privileges to secure content items or folders see them on Exploring pages. However, if they try to view the content, an access-denied error is displayed. This setting speeds up browsing performance because it simplifies the queries (less filtering), but it does allow users to see some information about secure content which they cannot access.

- Limit the number of items and folders displayed on Exploring pages. Set the `CollectionDisplayResultSetSize` configuration variable to control the maximum number of items displayed on Exploring pages. If the number of items in the result set exceeds the specified number, the results are truncated and spread over multiple pages. Navigation links allow movement between pages. You can use this setting to prevent extremely large pages from being generated.
- Remove selected options from the Actions popup menu for items on Exploring pages. The following configuration variables remove certain menu options from the Actions popup menu next to the Info icons on Exploring pages:
 - `CollectionInfoEnabled`: Folder Information and Content Information options
 - `CollectionLinkEnabled`: Create Shortcut option
 - `CollectionMoveEnabled`: Move option
 - `CollectionDeleteEnabled`: Delete option

6.3.9 Metadata Inheritance

When creating a new folder or checking in new content into a folder, the metadata from the parent folder automatically populates the fields for the new folder or the new content item. The folder initially inherits the metadata, but can change its values without affecting the parent folder. Later changes to a parent folder's metadata do not affect the metadata for existing subfolders or content checked in to a folder.

There are times when items checked in to a folder should not inherit the parent folder's metadata values. For example, you can create a folder with the metadata field of `ReadOnly` set to true to prevent renaming, moving, or deleting the folder but allow content to be checked in to the folder.

If content checked in to the folder inherits the folder's metadata value of true for the `ReadOnly` field, that content cannot be deleted, even by its author. You may want to have a folder set to `ReadOnly`, but you may want content checked in to the folder to not inherit the value of true for `ReadOnly` so deletions are allowed.

You can change the value of the `ReadOnly` field to false for content checked in to the folder on the check-in page through the browser interface, but if you check in content through WebDAV, there is no way to change the value of this field at check-in time.

Follow these steps to prevent inheriting value from the parent folder. This example uses the `ReadOnly` field, but you can use any metadata field.

1. Locate the `/custom/Folders/resources` directory.
2. Copy the existing `folders_forcemeta_resource.hda` file to another name as backup.
3. Open the `folders_forcemeta_resource.hda` file in a text editor.
4. Edit the file as follows. The `ResultSet` is similar to the following:

```
@ResultSet METADATA_OVERRIDE
2
name
value
xReadOnly
0
@end
```

5. Save the file.

6. Restart Oracle WebCenter Content Server.

6.4 Managing Contribution Folders

This section discusses common tasks involved in managing contribution folders. It covers the following topics:

- [Section 6.4.1, "Configuring Contribution Folders"](#)
- [Section 6.4.2, "Managing Local Folders"](#)
- [Section 6.4.3, "Archiving Contribution Folders"](#)
- [Section 6.4.4, "URL-Mapped Folders"](#)

6.4.1 Configuring Contribution Folders

You can optimize the performance of folders in the following ways:

- [Section 6.4.1.1, "Setting Folder and File Limits"](#)
- [Section 6.4.1.2, "Enabling and Disabling System Folders"](#)
- [Section 6.4.1.3, "Disabling the Trash Bin"](#)
- [Section 6.4.1.4, "Defining System Default Metadata"](#)
- [Section 6.4.1.5, "Configuring Metadata Propagation"](#)
- [Section 6.4.1.6, "Hiding Metadata Fields Globally Except for Specific Folders"](#)

6.4.1.1 Setting Folder and File Limits

Follow these steps to modify the maximum number of folders and content items in a contribution folder:

1. Choose **Administration** then **Folder Configuration** from the Main menu.
The [Virtual Folder Administration Configuration Screen](#) opens.
2. Enter a number in the **Maximum Folders Per Virtual Folder** field. If a user attempts to define more than this number of contribution folders, an error message is displayed.
3. Enter a number in the **Maximum Content Per Virtual Folder** field. If a user attempts to check in more than this number of content items, an error message is displayed.
4. Click **Update**.

6.4.1.2 Enabling and Disabling System Folders

Follow these steps to enable a system-level hierarchical folder that was disabled:

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **System Folder Configuration**.
The [System Folder Configuration Screen](#) opens.
2. Click the gray icon next to the folder to enable it.
The folder is enabled and the folder Exploring page for the folder opens. Users can see the enabled folder.

To disable a folder, follow the same procedure. Click the green icon next to a folder to disable it.

6.4.1.3 Disabling the Trash Bin

Follow these steps to disable the Trash Bin after the initial Contribution Folders setup:

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **System Folder Configuration**.

The [System Folder Configuration Screen](#) opens.

2. Click the green dot next to **Trash** to disable the Trash Bin.

Any content deleted from folders is permanently deleted rather than being moved to the Trash Bin. **Content, after it is deleted, can no longer be restored.**

Note: Disabling the Trash Bin can be particularly useful when using Site Studio. For more information, see [Section 6.7.8, "Deleting Content From Contribution Folders for Site Studio Web Site"](#).

6.4.1.4 Defining System Default Metadata

Follow these steps to define the system default metadata to be applied on initial check-in. These defaults are applied to any content checked in through a contribution folder *only* if a value is not defined for the folder or by the user.

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Folder Configuration** then **System Default Information Field Configuration**.

The [System Default Information Field Configuration Page](#) opens.

2. Specify the default values to be applied to content upon check-in. You can use Idoc Script in any information field.
3. Click **Update**.

6.4.1.5 Configuring Metadata Propagation

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Folder Configuration** then **Information Field Inherit Configuration**.

The [Information Field Inherit Configuration Page](#) opens.

2. Select check boxes for the metadata fields to be propagated.
3. Click **Update**.

When a contributor clicks **Propagate** on a Hierarchical Folder Information page, only the selected metadata values are propagated.

To propagate the inhibit setting itself, select the check box for the Inhibit Metadata Update field on the [Information Field Inherit Configuration Page](#). However, the inhibit setting only propagates from *false* to *true* or *false* to *blank*, and not from *true* to *false* or *blank* to *false*. Any folders and content items set to *true* or *blank* are not included in the propagation process.

6.4.1.6 Hiding Metadata Fields Globally Except for Specific Folders

Use the following procedure to hide one or more metadata fields globally for all folders and for new check-ins, but allow those metadata fields to be visible for checking in content using specific WebDAV contribution folders. For more details about using rules, see [Section 3.2, "Using Profiles to Customize Content Screens."](#)

1. Choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Rules** tab.

The [Configuration Manager: Rules Tab Screen](#) opens.

2. Click **Add** to add a rule. Enter information for the rule name and description.
3. In the **General** tab, select **is Global rule with Priority** and **Use rule activation condition**.
 - a. Click **Edit** next to the **User rule activation condition** check box.
 - b. Click **Add** to add a condition.
 - c. Make sure the condition is highlighted and select the **Clause** tab.
 - d. In the Field menu, select **Folder**.
 - e. In the Operator menu, select *Not Equals*.
 - f. In the Value menu, enter the `xcollectionID` of the folder where the metadata field appears. The `xcollectionID` is located in the database Collections table under `dCollectionID`.
 - g. Click **Add** to add the clause to the Clause section.
 - h. Click **OK**.
4. Select the **Fields** tab from the Edit Rule window.
5. Click **Add** and select the field to hide.
6. Click **OK**.

The [Add/Edit Rule Field 'name' Screen](#) opens.

7. In the **Type** menu of the **Add Rule Field** window, select **Hidden**.
8. Click **OK**.
9. In the main **Edit Rule** window, click **OK**.
10. Test the configuration by adding content to a non-specified folder. The field is hidden. Try adding content to the folder specified in the rule. The field is visible. If multiple folders are required to display the fields, more conditions are required within the clause of the same rule.

6.4.2 Managing Local Folders

This section discusses the following topics in the management of local folders:

- [Section 6.4.2.1, "Specifying Local Folders"](#)
- [Section 6.4.2.2, "Rebuilding Local Folders"](#)
- [Section 6.4.2.3, "Removing Local Folders"](#)

6.4.2.1 Specifying Local Folders

Follow these steps to map a contribution folder structure to a local file system on the host system:

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Folder Configuration** then **Local Folders**.

The [Local Folders Page](#) opens.

2. Click **Browse**.

The Browsing dialog opens.

3. Click the folder to be mapped to the file system. Navigate to a higher-level folder to display its subfolders. The target folder is the open folder.
4. Click **OK**.
The target folder is entered in the Folder field.
5. Enter a directory name in the Local Directory field.
For example, *c:/my_website*.
6. Click **Add**.
If necessary, the directory is created on the file system and the specified folder structure is replicated to the specified directory.

6.4.2.2 Rebuilding Local Folders

Follow these steps to rebuild the directory structure for a folder that is mapped to a local file system:

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Folder Configuration** then **Local Folders**.
The [Local Folders Page](#) opens.
2. Click **Rebuild** for the folder/directory mapping to rebuild.
The directory (and all subdirectories and files) is deleted from the local file system, and the folder structure is re-copied to the directory.

6.4.2.3 Removing Local Folders

Follow these steps to delete a local folder mapping:

1. Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Folder Configuration** then **Local Folders**.
The [Local Folders Page](#) opens.
2. Click **Remove** for the folder/directory mapping to delete.
The directory (and all subdirectories and files) is deleted from the local file system, and the mapping is removed from the Local Folders page. You cannot delete a mapped contribution folder until the local folder mapping is removed.

6.4.3 Archiving Contribution Folders

This section discusses the following topics regarding archiving folders:

- [Section 6.4.3.1, "Exporting an Archive"](#)
- [Section 6.4.3.2, "Importing an Archive"](#)

6.4.3.1 Exporting an Archive

Note: Depending on the size of the folder hierarchy that is being exported as an archive file, the default heap size value for the JVM may not be adequate. If memory errors are issued during the export procedure, increase the heap size.

Follow these steps to export the folder hierarchy as an archive file:

1. Choose **Administration** then **Folder Configuration** from the Main menu.
The [Virtual Folder Administration Configuration Screen](#) opens.
2. Click **Export Archive**.
A dialog opens, prompting you to save the file.
3. Click **Save**.
4. Navigate to the directory to save the folder archive file.
5. Specify a new file name to easily identify the archive file (for example, *101127_CollectionArchive*).

Note: In Windows, the file type is left as **Text Document** and a .txt extension is appended to the file name (for example, *CollectionArchive.hda.txt*). To save the file with just the .hda extension, select the **All Files** file type.

6. Click **Save**.
The folder hierarchy is exported to the specified file.

6.4.3.2 Importing an Archive

Use the following procedure to import an archived folder structure:

Caution: This procedure removes all content items in the current folders and replaces them with the imported folder hierarchy. Typically, perform this procedure only on an Oracle WebCenter Content Server that has no content items in the repository.

1. Choose **Administration** then **Folder Configuration** from the Main menu.
The [Virtual Folder Administration Configuration Screen](#) opens.
2. Click **Browse** and navigate to the archive file to import.
3. Click **Open**.
The path and file name appear in the field.
4. Click **Import Archive**.
A confirmation prompt opens.
5. Click **OK**.
The archived folder is imported and re-created.

6.4.4 URL-Mapped Folders

To map a URL to a folder, select **Administration** then **Folder Configuration** from the Main menu. Select the **Web Url Mapped Folders** option. Select a folder and URL for it from the provided list. For more details about mapping Web URLs, see "Mapping URLs with WebUrlMapPlugin" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.5 WebDAV Interface

WebDAV (Web-Based Distributed Authoring and Versioning) is automatically installed and enabled with Oracle WebCenter Content Server and provides a way to remotely author and manage your Oracle content using clients that support the WebDAV protocol. For example, you can use Windows Explorer to manage folders and files or use Microsoft Office products to check in, check out, and modify content in the Oracle repository rather than using Oracle's Web browser interface. The WebDAV protocol is specified by RFC 2518.0. See the WebDAV Resources Page at <http://www.webdav.org> for more information.

WebDAV provides support for the following authoring and versioning functions:

- Version management
- Locking for overwrite protection
- Web page properties
- Collections of Web resources
- Name space management (copy/move pages on a Web server)
- Access control

When WebDAV is used with a content management system, the WebDAV client provides as an alternate user interface to the native files in the content repository. The same versioning and security controls apply, whether an author uses the Oracle Web browser interface or a WebDAV client.

In Oracle WebCenter Content Server, the WebDAV interface is based on the folder interface provided by either the Folders (FrameworkFolders) component or by the Contribution Folders (Folders_g) component. Except where noted, WebDAV functions similarly for both components.

Important: WebDAV does not support the use of non-ASCII characters in user names.

This section covers the following topics:

- [Section 6.5.1, "WebDAV Clients"](#)
- [Section 6.5.2, "WebDAV Architecture"](#)
- [Section 6.5.3, "WebDAV Folders"](#)
- [Section 6.5.4, "Multiple Concurrent Language Support"](#)

For information about using the WebDAV interface, see the *Oracle WebCenter Content User's Guide for Content Server*.

6.5.1 WebDAV Clients

A WebDAV client is any application that can send requests and receive responses using the WebDAV protocol. Typically, a WebDAV client requires no additional setup.

Although there are many applications that support the WebDAV protocol to some degree, Content Server is tested with, and supports the following:

- Microsoft Windows Explorer
- Microsoft Word 2002 (XP) through 2010

- Microsoft PowerPoint 2002 (XP) through 2010
- Microsoft Excel 2002 (XP) through 2010

You can use Windows Explorer to manage files created in a non-WebDAV client, but you cannot use the native application to check content in to and out of the repository.

Note: Do not confuse the term WebDAV client with Oracle WebDAV Client, which is a separate Oracle product that enhances the WebDAV interface.

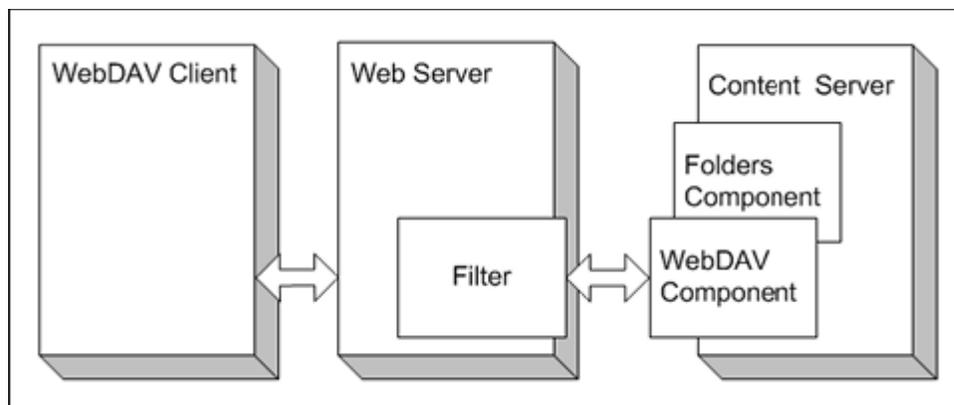
Oracle also offers Oracle WebCenter Content: Desktop, which can enhance the WebDAV client environment by more closely integrating with Windows Explorer, Microsoft Outlook, Lotus Notes, and other applications. For more information see the *Oracle WebCenter User's Guide for Desktop*.

6.5.2 WebDAV Architecture

WebDAV support is implemented through a component which handles WebDAV requests directly. A WebDAV request follows this process (as illustrated in [Figure 6-1](#)):

1. The WebDAV client makes a request to Oracle WebCenter Content Server.
2. The message is processed by the Web server through a custom filter.
3. On the Oracle WebCenter Content Server, the WebDAV component performs the following functions:
 - It recognizes the client request as WebDAV.
 - It maps the client request to the appropriate WebDAV service call.
 - It converts the client request from a WebDAV request to the appropriate request.
 - It connects to the core Oracle WebCenter Content Server and executes the request.
4. The WebDAV component converts the response into a WebDAV response and returns it to the WebDAV client.

Figure 6-1 WebDAV Process



Important: WebDAV uses several nonstandard HTTP methods, including PROPFIND, PROPPATCH, MKCOL, DELETE, COPY, MOVE, LOCK, and UNLOCK. Many third-party applications—such as firewalls, proxy servers, load balancers, and single sign-on applications, do not allow these methods by default. If your network includes any of these applications, you may have to reconfigure them to allow the WebDAV methods.

6.5.3 WebDAV Folders

You connect to WebDAV folder as you would a networked location. The credentials you use are the same as those you use for the standard browser interface for Oracle WebCenter Content Server. You can work with folders and folder content as defined by your user permissions. For example, if you have Read permission for a content item, you can view the file, but you cannot check in a revision to the file.

The WebDAV interface provides a subset of the options available through the browser interface. In general, you can create, delete, move, and copy content items and folders and modify and check in content items. To check out content items through the WebDAV interface, you must use a WebDAV client that can open the file. To perform other management tasks, such as specifying or propagating metadata values, you must use the standard browser interface.

For more information about creating a connection to a WebDAV folder and using WebDAV folders to manage content, see the *Oracle WebCenter Content User's Guide for Content Server*.

6.5.4 Multiple Concurrent Language Support

To support multiple concurrent languages, certain WebDAV properties (metadata fields) must not contain non-ASCII characters. If non-ASCII characters are used, WebDAV clients may not be able to list folders containing these characters. For example, an English desktop would have trouble displaying Japanese characters.

The specific fields that must not use non-ASCII character sets vary by WebDAV client:

Microsoft Web Folders

The following fields must not contain non-ASCII characters:

- the content name (dDocName)
- the original content name (dOriginalName)
- the content title (dDocTitle)
- the folder names

Oracle WebCenter Content Desktop

The following fields must not contain non-ASCII characters:

- the content name (dDocName)
- the original content name (dOriginalName)
- the content title (dDocTitle)
- the content type (dDocType)
- the content item author (dDocAuthor)
- the security group (dSecurityGroup)

- the folder names

6.6 Administering WebDAV

After installing WebDAV, you can perform most of the WebDAV system administration tasks from folders component Web pages. For more information about Contribution Folders, see [Section 6.4, "Managing Contribution Folders."](#) For more information about Folders, see [Section 6.2, "Managing Folders."](#)

This section covers the following topics:

- [Section 6.6.1, "WebDAV Connection Strings"](#)
- [Section 6.6.2, "Default Content Item Naming"](#)
- [Section 6.6.3, "Security and WebDAV"](#)

6.6.1 WebDAV Connection Strings

When creating a content server connection, the user must provide the WebDAV URL for that server. Please note that each defined content server connection must have its own, unique WebDAV URL. You cannot have two server connections on your computer that use the exact same WebDAV URL. The WebDAV URL typically has the following form:

```
http[s]://host-name:[port]/web-root/idcplg/webdav
```

For example:

```
http://server:7044/idc/idcplg/webdav
http://server.example.com:16200/cs/idcplg/webdav
https://server/cs/idcplg/webdav
```

With the use of a form-based login, WebDAV connection strings now require the `_dav` root before the web root. For example:

```
http://host_name:16200/_dav/cs/idcplg/webdav/
```

6.6.2 Default Content Item Naming

When users check new content in through a WebDAV folder, they cannot explicitly set metadata values such as the title for the content item. As a general rule, content items inherit any metadata defaults specified for the folder.

In the case of the content item title (`dDocTitle`), it is always set to the original file name (`dDocOriginalName`) except as noted below.

Folders Default

For Folders (FrameworkFolders component), if the folder specifies a title as part of its default metadata, the title specified by the folder is used as the document's title.

Contribution Folders Default

For Contribution Folders (Folders_g component), if the folder specifies a title as part of its default metadata, and the variable `CollectionDocTitleOverride` is set to 1, the title specified by the folder is used as the document's title.

You can modify the variable setting in the `IntradocDir/config/config.cfg` file.

6.6.3 Security and WebDAV

The following security features are included in WebDAV:

- **Access:** The user logins and security controls in the folders component and Oracle WebCenter Content Server also apply to content that is managed using WebDAV clients. For example, if you have Read permission for a content item, you can view the file, but you cannot check in a new revision to the file.
- **Login Cookie:** When a user logs in to the Oracle WebCenter Content Server through a WebDAV application, the WebDAV component sets a cookie in the client. The cookie remains set if a WebDAV request is made within the time specified by the `WebDAVMaxInactiveInterval` configuration parameter. The default is 3600 seconds, or one hour. The cookie remains set even if the WebDAV client application closes. If the cookie expires, the user must log on to the Oracle WebCenter Content Server again to perform WebDAV transactions through Microsoft Word, Excel, and PowerPoint.

The cookie includes a cryptographic key that prevents unauthorized users from generating counterfeit cookies. The `WebDAVSecretKey` parameter is used to generate the key. To prevent WebDAV login cookies from being used on other Oracle WebCenter Content Servers, change the `WebDAVSecretKey` setting to a new, unique value for each instance that is accessed through WebDAV.

- **Windows Explorer:** If a user logs in to Oracle WebCenter Content Server through Windows Explorer, the client retains the user login authentication within the shell. Even if the login cookie expires, Windows Explorer sends the user name and password to the Oracle WebCenter Content Server automatically, so the user is not prompted to log on. The only way to clear this is for the user to log out of Windows.
- **Personal Folders:** Content Server creates a personal folder for each user (`/Users/<username>/`). The Web interface prevents users from creating folders in the `/Users` directory. To prevent users from having write access to the `/Users` directory through the WebDAV interface, however, you must explicitly set permissions for the `/Users` folder. For example, you can give most users Read access to the folder, and allow only administrators to write to the folder.
- **Session timeout:** If a WebDAV client does not specify a session timeout value, the default timeout specified by the `WebDAVDefaultTimeout` setting is used. If a file remains locked (checked out) for this amount of time with no activity in the session, an "Undo Checkout" is applied to any checked out content.

6.7 WebDAV Troubleshooting

This section describes problems that can occur when using WebDAV and it offers possible solutions.

- [Section 6.7.1, "Zero-Byte Files"](#)
- [Section 6.7.2, "No Connection to WebDAV Folder"](#)
- [Section 6.7.3, "Other Connection Issues"](#)
- [Section 6.7.4, "Double-Byte Characters in File Name"](#)
- [Section 6.7.5, "Number Sign in Virtual Folder Name or File Name"](#)
- [Section 6.7.6, "ExtranetLook Component Problem"](#)
- [Section 6.7.7, "Content Item "Stuck" in Auto-Contribution Workflow Step"](#)

- [Section 6.7.8, "Deleting Content From Contribution Folders for Site Studio Web Site"](#)
- [Section 6.7.9, "WebDAV Drag and Drop Does not Work With Windows 2000"](#)
- [Section 6.7.10, "Folder Shortcuts Do Not Show Latest Changes"](#)
- [Section 6.7.11, "Profile Rule for All WebDAV Requests"](#)

Tip: See the Oracle WebCenter Content Server logs for error messages and detailed information about the operation of the WebDAV component.

6.7.1 Zero-Byte Files

When using an Office 2000 application to open a document that resides on a WebDAV server, the application displays the content as empty (0 bytes).

6.7.1.1 Cause

This problem can be caused by a combination of the temporary Internet files settings in Microsoft Internet Explorer. The WebDAV file is still present in Oracle WebCenter Content Server, but does not open properly on certain client computers with particular settings.

6.7.1.2 Solution

1. In Internet Explorer, select **Tools** then **Internet Options**.
2. On the **General** tab, click **Settings**.
3. Under "Check for newer versions of stored pages," select **Every visit to the page**.
4. Under "Temporary Internet files folder," consider increasing the amount of disk space. (The lower the amount, the sooner the empty file problem seems to occur.)
5. Click **OK** twice to save the settings and close the screen.

6.7.2 No Connection to WebDAV Folder

A client computer does not connect to WebDAV folders.

6.7.2.1 Cause

Internet Explorer is configured to use a proxy server.

6.7.2.2 Solution

Do one of the following:

- Configure the client computer to not use the proxy server instance for your HTTP server/WebDAV server. To do this in Internet Explorer, select **Tools** then **Internet Options**. Select **Connections** then **LAN Settings** then **Advanced** then **Exceptions**. Specify the IP address/host name of the WebDAV server.
- Modify the proxy server configuration to allow pass-through for WebDAV methods (WebDAV-specific HTTP/1.1 extensions) with standard GET, POST, and other HTTP/1.1 methods. See your proxy server documentation for more information.
- Windows Vista requires Service Pack 2 for WebDAV to work properly.

6.7.3 Other Connection Issues

- Some versions of Windows XP, Vista, and 7 do not connect to a WebDAV server running over HTTP and using HTTP Basic authentication. You must set a registry entry to fix this. See <http://support.microsoft.com/kb/841215> for details.
- When mapping a network drive in Windows 7, Windows remembers all failed attempts in a login session and never retries a connection after a single connection to a host has failed, even if the browser cache is cleared in Internet Explorer and you modify the WebDav URL. To work around this issue, restart Windows 7 before trying to connect to that host again through WebDAV.
- By default, Office 2010 will not open documents over WebDAV using basic authentication over a non-SSL connection. You must set a registry entry to fix this. See <http://support.microsoft.com/kb/2123563> for details.

6.7.4 Double-Byte Characters in File Name

A file with double-byte characters in the file name cannot be checked in.

6.7.4.1 Cause

If the Oracle WebCenter Content Server is running on a Western European operating system, the Microsoft WebDAV client may not be able to handle files with double-byte characters in the file name.

6.7.4.2 Solution

Either eliminate all double-byte characters from the file name, or check in the file through the Oracle WebCenter Content Server's Web browser interface.

6.7.5 Number Sign in Virtual Folder Name or File Name

Using the number sign (#) in a folder name generates errors and truncates the folder name before the number sign. Using the number sign (#) in file names generates errors.

6.7.5.1 Cause

The number sign (#) is not allowed in WebDAV folder or file names.

6.7.5.2 Solution

Eliminate the number sign (#) from the folder name. Either eliminate the number sign from the file name, or check in the file through the Oracle WebCenter Content Server's Web browser interface.

6.7.6 ExtranetLook Component Problem

The ExtranetLook component no longer works after installation of the Folder component.

6.7.6.1 Cause

The WebDAV component uses CookieLoginPlugin.dll for cookie-based login. The cookies eliminate additional login prompts when MS-Word opens a document using WebDAV. Typically, the component keeps the dll from doing forms-based logins on

Web page because most users do not want this. However, users that do want forms-based logins can get them by following the instructions below.

6.7.6.2 Solution

An additional configuration change must be made to allow forms-based login with the WebDAV component. To use the WebDAV component with the ExtranetLook component, set `WebDAVDisableOtherFilterCookies=false`.

6.7.7 Content Item "Stuck" in Auto-Contribution Workflow Step

A content item was dragged and dropped into a folder, and the content item automatically entered a workflow (as expected). However, the content item seems "stuck" in the auto-contribution step of the workflow. The only way to approve the content item is to check it out and check it back in with the **Revision Finished Editing** option selected, so that the content item moves to the first step of the workflow.

6.7.7.1 Cause

A change was made to the default workflow behavior when content items are contributed through the WebDAV interface. In Folders revision 91 and higher, a content item enters a workflow in the contribution step when contributed to a folder rather than the first step in the workflow, which used to be the default. This change supports Site Studio's preview modes, so that a content item did not advance into the workflow proper and it could be approved using the Site Studio interface. However, if not using Site Studio, this may not be the anticipated behavior.

6.7.7.2 Solution

Two configuration entries are available to address this issue:

- `AutoContributorAdvancesOnUnlock`: Enabling this configuration entry makes the content advance immediately to the first workflow step as it did in versions of the Folders component before revision 91.
- `AutoContributorAllowsReview`: This configuration entry enables users to approve a content item in a contribution step of a workflow without having to perform a check-out/check-in sequence.

6.7.8 Deleting Content From Contribution Folders for Site Studio Web Site

When documents are deleted from folders used to contribute to a Site Studio Web site, those documents still appear in dynamic lists on the Web site.

6.7.8.1 Cause

If the Trash Bin feature is enabled during the Folders component installation, a Trash Bin is created to contain any content deleted from within folders. A side-effect in Site Studio is that documents deleted from WebDAV folders still appear in Site Studio dynamic lists (such as tables of content) and queries. Explicitly delete the documents from the Trash Bin to make them disappear from all dynamic lists and queries of the Site Studio Web site.

6.7.8.2 Solution

To avoid having to delete the documents twice, see [Section 6.4.1.3, "Disabling the Trash Bin."](#) **Please note that after you disable the Trash Bin, deleted documents cannot be restored.**

6.7.9 WebDAV Drag and Drop Does not Work With Windows 2000

Attempting to drag and drop using any WebDAV client produces no file, or a file containing 0 bytes. Although the action does not successfully complete, no error message is displayed. A copy and paste of the file using the WebDAV client does work.

6.7.9.1 Cause

The problem is a known issue on some versions of Windows 2000 with Office 2000 Service Release 1 or later which have been upgraded.

6.7.9.2 Solution

The following solutions work around or resolve the drag and drop issue:

- Use copy and paste to add content in situations where the drag and drop does not work.
- Upgrade your Windows dll files as outlined in the following Microsoft knowledge base article at the following URL:
<http://support.microsoft.com/default.aspx?scid=kb;en-us;288440>

6.7.10 Folder Shortcuts Do Not Show Latest Changes

If you create a shortcut to a Web folder and use it to open the folder, the folder does not show recent changes to the folder contents.

6.7.10.1 Cause

Folder shortcuts can show cached information that is no longer current. The problem is a known issue in Microsoft Windows.

6.7.10.2 Solution

Refresh the folder display by pressing **F5** or selecting **Refresh** from the View menu.

6.7.11 Profile Rule for All WebDAV Requests

How do I create a profile rule that affects all WebDAV requests?

6.7.11.1 Solution

Check for the variable `IsWebdavRequest` in your profile rule. For example, you can use the following script for the `dOutDate` field to make sure it is set to 30 days in the future for all WebDAV check ins:

```
<$if IsWebdavRequest$>  
<$dprDerivedValue=dateCurrent(30)$>  
<$endif$>
```

Managing Content Folios

Content Folios is an optional component that is automatically installed with Oracle WebCenter Content Server. When enabled, it provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of Oracle WebCenter Content Server.

For example, you can assemble all items relevant to an upcoming brochure, such as images, logos, legal disclosures, and ad copy, and send them through a workflow process. After approval, you can download all associated content and send it for print.

This chapter contains the following topics:

- [Section 7.1, "Using Content Folios"](#)
- [Section 7.2, "Managing Content Folios"](#)

7.1 Using Content Folios

A content folio is an XML file checked in to the repository that uses elements to define a hierarchical structure of nodes, slots, and specified content items. In practice, a content folio is a logical grouping, or a framework in which to structure content. Simple folios are a flat container, while advanced folios can nest content in a hierarchy within folders. With an advanced folio, you can establish the hierarchy before, during, or after you assemble the content items.

You can add content to existing folios or lock them so changes cannot be made. You can add content items folio by searching the repository. You can add content items to an advanced folio by checking new items into the repository or by searching for existing content. An advanced folio can also contain hyperlinks to outside resources such as Web sites or shared network drives.

Content Folios adds the following functionality:

- Organize content into a simple, flat folio structure
- Organize content into an advanced hierarchical folio structure
- Create pre-structured templates for selection when creating folios
- Modify folio structure dynamically
- Lock folio structure to prevent it from being modified dynamically
- Lock content folios to prevent additions
- Unlock folios to allow additions
- Modify folios without tracking revisions
- Take a snapshot of a folio to track revisions

- Download renditions of folio content in .zip, .ppt, .pdf, or XML format
- Create multiple unstructured content baskets for use in collecting content items

Several changes are made to Oracle WebCenter Content Server during installation of Content Folios:

- Additional metadata fields: The following metadata fields are added to record the current state of a folio or template:
 - CpdIsTemplateEnabled
 - CpdIsLocked
- Additional views: The following views are added and are used on the Folio Edit page to communicate Content Folios tables to JavaScript:
 - NodPropertyView
 - LinkPropertyView
 - NodeRemovalTypeView
 - CpdTreeDisplayFunctionMapView
 - CpdPopupEditActionsView
 - ItemPropertyView
 - PneDocProfileView
- Additional Relations: The GenericUserProfileRelation is used by PneDocProfileView.
- Additional Tables: The following tables record the links that folios and content baskets have against content in the system:
 - CpdLinks
 - CpdArchiveLinks
 - CpdBasketLinks
 - CpdEditHistory

Changes made to Oracle WebCenter Content Server remain even if Folios is disabled.

7.2 Managing Content Folios

You can base the structure of a folio on a pre-defined template when you create the folio and you can optionally modify the structure of the folio when you create or edit it.

This section covers the following topics:

- [Section 7.2.1, "Creating and Editing Folio Templates"](#)
- [Section 7.2.2, "Adding Custom Viewers and Renderers"](#)

7.2.1 Creating and Editing Folio Templates

Folio templates are a predefined organization of nodes, subnodes, slots, and any content items required when creating a folio. You can select a folio template when you create an advanced folio. Folio templates are XML files checked in to and managed by Oracle WebCenter Content Server, that you can edit and revise at any time. Revisions

to a template are not applied retroactively to existing folios based on that template, but only apply to new folios created based on the template's new revision.

To create folio templates, you must have administration rights.

7.2.1.1 Creating a Folio Template

Follow these steps to create a folio template:

1. Choose **Administration** then **Folio Administration** from the Main menu. Choose **Create Folio Template**.

The [Create/Edit Folio Template Page](#) opens.

2. First save the folio template and check in the folio. Select **Save template** from the page Actions menu. Choose the profile to use with the template and click **Next**. Enter the necessary check-in information, including a descriptive title for the template. Click **Check In**.
3. Add structure or content to the template on the [Create/Edit Folio Template Page](#) and define the template properties.

The **Structure** tab of the [Create/Edit Folio Template Page](#) is divided into three sections:

- **Folio Structure Pane:** Shows the nodes, slots, and items that comprise the folio hierarchy. Right click within the folio structure area to display the following options on a contextual menu. Unless noted otherwise, the options are available for nodes, items, and slots:
 - **Insert Selected Source Item:** Inserts a selected item from the [Source Items Pane](#) in a slot. If the slot contains an item, it is replaced.
 - **Insert Item by Search:** Opens a search window to find an item to add to the folio in the selected node or slot. If the slot contains an item, it is replaced.
 - **Insert Item by Checkin:** Opens a check-in form used to add an item to be used in the selected node or slot. If the slot contains an item, it is replaced.
 - **Remove Content Item:** Removes content from a slot. It does not remove the slot. (items only)
 - **Insert hypertext:** Creates a new item in the structure that can establish a hypertext link to the specified URL.
 - **Create Node or Slot:** Creates a node or slot at the specified location.
 - **Cut, Copy, Paste:** Cuts or copies an item for later pasting if needed.
 - **Delete:** Deletes an item from the structure.
- **Element Info Pane:** When a node, slot, or item is selected in the [Folio Structure Pane](#), information about the selection is displayed and optionally modified. Modified information is written back to the XML file that is checked in. Unless noted otherwise, the following fields are available for nodes, items, and slots:
 - **Name:** Name of the object.
 - **Description:** Description of the object.
 - **Attributes (items and slots):** The uses and limitations of the object. Default attributes include the following:
 - Allow empty: The object can be left empty.

Lock content: You cannot delete items from the slot.

Removable: You can delete the object.

Allow external: You can specify an external link.

Restrict formats: Limits allowable content item formats through a comma-delimited list that maps formats to file extensions. For more information see [Section 2.3.3, "Associating File Types with Conversion Programs."](#)

Allow folio: You can specify a folio in the slot.

Content profile: The content profile used when adding an item by search or check in.

Clone item: The associated item is cloned. A cloned item is copied and checked in as a new item when a folio based on the template is created. If an item is not cloned, the original content item is associated with any folio created using the template.

- Attributes (nodes): Default attributes include the following:

Removable: You can delete the node.

Children movable: You can move items and slots within the hierarchy.

Allow item creation: You can create items within the node.

Allow node creation: You can create subnodes within the node.

Maximum items, Maximum nodes: Specifies the total number of items that you can create in the node.

Content profile: The content profile used when adding an item by search or check in.

- Content ID: (items and slots). The ID of the item.
- Create Date: (items and slots). The date a content item was created.
- Last modified: (items and slots). The last date changes were made.
- Link: (hyperlinks only): The URL of a hyperlink.

- [Source Items Pane](#): Used to collect items to be used in the folio.

4. Click **Finish** when done.

7.2.2 Adding Custom Viewers and Renderers

Oracle WebCenter Content Server ships with a default viewer that mimics the structure of the Create/Edit Folios page, and the following rendition options:

- Zip
- PDF
- XML

You can create custom viewers and renderers, but such development requires an understanding of the following:

- the structure of the folio XML
- the folio Idoc Script functions and their proper usage
- the Iterator/Renderer architecture

- the method for using a component to modify/add to the list of viewers and renderers

To add custom viewers and renderers, contact Oracle Consulting at <http://www.oracle.com/consulting/index.html>.

Using Content Tracker

Content Tracker and Content Tracker Reports are optional components automatically installed with Oracle WebCenter Content Server. They are separate modules but when enabled they provide information about system usage such as which content items are most frequently accessed and what content is most valuable to users or specific groups. Knowing the consumption patterns of an organization's content enables more effective delivery of appropriate, user-centric information.

See the *Oracle WebCenter Content Developer's Guide for Content Server* for details about customizing Content Tracker beyond what is discussed in this document.

This chapter covers the following topics:

- [Section 8.1, "Content Tracker Functionality"](#)
- [Section 8.2, "Operational Details"](#)
- [Section 8.3, "Data Tracking Functions"](#)
- [Section 8.4, "Content Tracker Reports"](#)
- [Section 8.5, "Troubleshooting"](#)

8.1 Content Tracker Functionality

Content Tracker monitors activity on an Oracle WebCenter Content Server instance and records selected details of those activities. It then generates reports that illustrate the way the system is being used. This section includes an overview about Content Tracker and Content Tracker Reports functionality.

Content Tracker incorporates several optimization functions which are controlled by configuration variables. The default values for the variables set Content Tracker to function as efficiently as possible for use in high volume production environments. See the *Oracle WebCenter Content Idoc Script Reference Guide* for more details about Content Tracker configuration variables.

This section covers the following topics:

- [Section 8.1.1, "Content Tracker and Content Tracker Reports"](#)
- [Section 8.1.2, "Data Recording, Reduction, and Reporting"](#)
- [Section 8.1.3, "Content Tracker Terminology"](#)
- [Section 8.1.4, "Installation Considerations"](#)

8.1.1 Content Tracker and Content Tracker Reports

Content Tracker monitors a system and records information collected from different sources about activities. The information is merged and written to a set of tables in the Oracle WebCenter Content Server database. Content Tracker can monitor activity based on:

- **Content item usage:** Data is obtained from Web filter log files, the Oracle WebCenter Content Server database, and other external applications such as portals and Web sites. Content item access data includes dates, times, content IDs, and current metadata.
- **Services:** Services that return content, and services that handle search requests, are tracked. By default, Content Tracker logs only the services that have content access event types but by changing the configuration, Content Tracker can monitor any service, even custom services.
- **User accesses:** Information is gathered about non-content access events, such as the collection and synthesis of user profile summaries. This data includes user names and user profile information.

After Content Tracker extracts data and populates database tables, you can use Content Tracker Reports to:

- **Generate reports:** Content Tracker Reports queries the tables and generates summary reports of activities and usage history of content items. The reports help analyze specific groups of content or users based on metadata, file extensions, or user profiles. Use the pre-defined reports, customize them, or use a compatible third-party reporting package.
- **Optimize content management practices:** You can use the reported data for content retention management. Depending on the access frequency, some items could be archived or deleted. Applications can also use the data to provide portlets with the top content for particular types of users.

8.1.2 Data Recording, Reduction, and Reporting

Content Tracker *records data* from the following sources:

- **Web server filter plug-in:** When content is requested with a static URL, the Web server filter plug-in records request details, saving the information in event log files. The event log files are used as input by the Content Tracker data reduction process.
- **Service handler filter:** Content Tracker monitors services that return content. When one of these services is called, details of the service are copied and saved in the SctAccessLog table.
- **Logging service:** Content Tracker supports a single-service call to log an event. You can call it directly with a URL, as an action in a service script, or from IdocScript.
- **Database tables:** When configured to collect and process user profile information, a data reduction process queries selected database tables to obtain information about active users during the reporting period.
- **Application API:** An interface is available to register other components and applications for tracking. This interface allows cooperating applications, such as Site Studio, to log event information in real time. The application API is designed as a code-to-code call which does not involve a service. The API is not meant for

general use. If you are building an application and are interested in using this interface, contact Consulting Services.

The *data reduction process* gathers and merges the data obtained from the data recording sources. Until this reduction process has finished, the data in the Content Tracker tables is incomplete. The reduction is run one time for each day's data gathered. You can run the reduction manually, or schedule it to run automatically, usually during an off-peak period when the system load is light.

Content Tracker Reports provide reports that answer commonly asked questions about activity and usage. Depending on how Content Tracker is configured, these reports can also indicate which searches are used most often, and which users have been most active. The reports are available directly through an interface or as an action on the Content Information page. The available categories of pre-defined report options depend on Content Tracker configuration. The reports, the underlying queries, and the output formatting can be customized.

8.1.3 Content Tracker Terminology

The following terminology is used with Content Tracker:

- **Data collection:** Gathering content access information and writing the information to event log files.
- **Data reduction:** Processing the information from data collection and merging it into a database table.
- **Data Engine Control Center:** The interface that provides access to the user-controlled functions of the Data Engine. It has the following tabs or sub-screens:
 - **Collection:** Used to enable data collection.
 - **Reduction:** Used to stop and start data reduction (merging data into database tables).
 - **Schedule:** Used to enable automatic data reduction.
 - **Snapshot:** Used to enable activity metrics. The term snapshot also denotes an information set representing the world at a particular time.
 - **Services:** Used to add, configure, and edit service calls to be logged. It is also used to define the specific event details logged for a given service.
- **Service definitions:** The ResultSet structure in the service call configuration file (SctServiceFilter.hda) that contains entries to define each service call to be logged. The service definition ResultSet is named ServiceExtraInfo.
- **Service entry:** The entry in the service definition ResultSet (ServiceExtraInfo) that defines a service call to be logged. The ServiceExtraInfo ResultSet contains one service entry for each service to be logged.
- **Field map:** A secondary ResultSet in the service call configuration file (SctServiceFilter.hda) that defines the service call data and the specific location where data is to be logged.
- **Top Content Items:** Most frequently accessed content items in the system.
- **Content Dashboard:** A screen that provides overview information about the access of a specific content item.

8.1.4 Installation Considerations

Content Tracker is supported on most hardware and networked configurations but some hardware and software combinations require special consideration, as discussed in the following sections:

- [Section 8.2.6.2, "Static URLs and WebDAV"](#)
- [Section 8.2.6.3, "Data Directory Protections"](#)
- [Section 8.2.6.4, "ExtranetLook Component"](#)
- [Section 8.2.6.1, "Tracking Limitations in Single-Box Clusters"](#)

Set the `SctUseGMT` configuration variable to true to use Greenwich Mean Time (GMT). It is set to false by default, to use local time. For more information about configuration variables see the *Oracle WebCenter Content Idoc Script Reference Guide*.

When upgrading from an earlier version of Content Tracker there is a one-time retreat (or advance, depending on location) in access times. To accommodate the biannual daylight savings time changes, discontinuities in recorded user access times are used (contingent on the use of local time and the location).

8.2 Operational Details

Depending on Content Tracker configuration, it can perform [Data Collection](#) of event information such as dynamic and static content accesses and service calls. Both types of data are recorded in a [Combined Output Table](#) (`SctAccessLog`). Service calls are inserted into the log in real time but the static URL information must first undergo the [Data Reduction](#) process (either manual or scheduled).

After activity data is collected, Content Tracker combines, analyzes and synthesizes the event information and loads the summarized activity into database tables. After reduction, this data becomes available for [Content Tracker Reports](#).

This section covers the following steps in the process and known limitations:

- [Section 8.2.1, "Data Collection"](#)
- [Section 8.2.2, "Data Reduction"](#)
- [Section 8.2.3, "Content Tracker Event Logs"](#)
- [Section 8.2.4, "Combined Output Table"](#)
- [Section 8.2.5, "Data Output"](#)
- [Section 8.2.6, "Tracking Limitations"](#)

8.2.1 Data Collection

Data collection is the initial step in any tracking function. Content Tracker data collection includes collecting information from static URL references and service call events. Data is collected using several different methods:

- [Section 8.2.1.1, "Service Handler Filter"](#)
- [Section 8.2.1.2, "Web Server Filter Plug-in"](#)
- [Section 8.2.1.3, "Logging Service"](#)

8.2.1.1 Service Handler Filter

Using the service handler filter, Content Tracker obtains information about dynamic content requests that come through the Web server, and also about other types of activity, such as calls from applications. The service request details are obtained from the DataBinder that accompanies the service call, and the information is stored in the [Combined Output Table](#) (SctAccessLog) in real time.

The SctServiceFilter.hda configuration file is used to determine which service calls are logged. It uses a ResultSet structure that includes one service definition entry for each service to be logged. When using the extended service logging function, the file also contains field maps corresponding to service definition entries.

The ServiceExtraInfo ResultSet is included in the SctServiceFilter.hda file. This ResultSet contains one or more service entries defining the services to be logged. Additional field map ResultSets are used to support the extended service logging function. Each service that has additional data values tracked must have a field map ResultSet in the SctServiceFilter.hda file to define the data fields, locations, and database destination columns for the related service.

8.2.1.2 Web Server Filter Plug-in

Managed content retrieved with a static URL does not usually invoke a service. The Content Tracker Web server filter plug-in collects the access event details (static URL references) and records them in raw [Content Tracker Event Logs](#) (sctlog files). The information in these files requires an explicit reduction (either interactive or scheduled) before it is included in the [Combined Output Table](#) with the service call data.

8.2.1.3 Logging Service

The logging service is a single-service call that can be called directly with a URL or as an action in a service script. It can also be called from IdocScript using the `executeService` function. The calling application is responsible for setting the fields to be recorded in the service DataBinder, including the descriptive fields listed in the Content Tracker service filter configuration file (SctServiceFilter.hda).

There should be no duplication or conflicts between services logged with the service handler filter and those logged with the Content Tracker logging service. If a service is named in the Content Tracker service handler filter file then such services are automatically logged so there is no need for the Content Tracker logging service to do it. However, Content Tracker does not attempt to prevent such duplication.

8.2.1.4 Enabling or Disabling Data Collection

Follow these steps to enable or disable data collection:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.

2. On the [Collection Tab](#), select (to enable collection) or clear (to disable collection) the **Enable Data Collection** check box.
3. Click **OK**.

Do not exit the applet. Wait until a confirmation message displays. If you exit before the confirmation message, the requested change(s) may not occur.

4. After the confirmation message is displayed, click **OK**.

5. Restart the Web server and Oracle WebCenter Content Server, in that order.

8.2.2 Data Reduction

During data reduction, the static URL information captured by the Web server filter plug-in is merged and written into the output table the service call data. Depending on configuration, at the time of the reduction the Content Tracker user metadata database tables are also updated with information collected from the static URL accesses and from the service call event records.

This section discusses the following topics about data reduction:

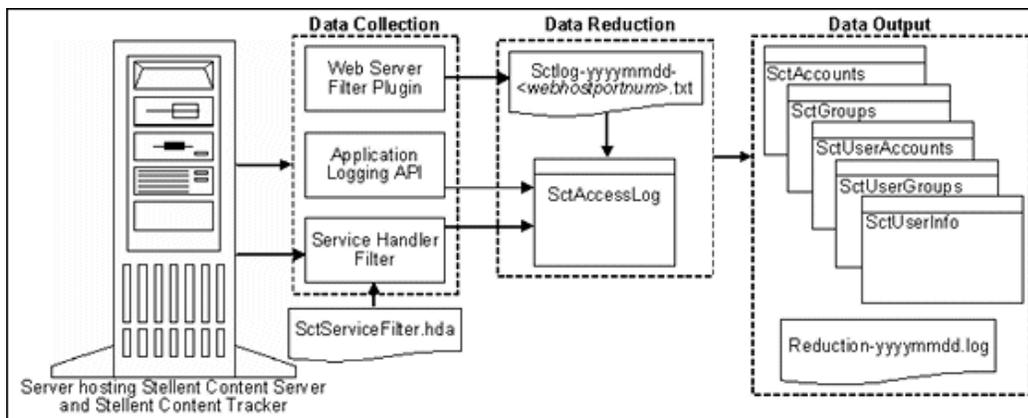
- [Section 8.2.2.1, "Standard Data Reduction Process"](#)
- [Section 8.2.2.2, "Data Reduction Process with Activity Metrics"](#)
- [Section 8.2.2.3, "Data Reduction Cycles"](#)
- [Section 8.2.2.4, "Access Modes and Data Reduction"](#)
- [Section 8.2.2.5, "Reduction Sequence for Event Logs"](#)
- [Section 8.2.2.6, "Reduction Schedules"](#)
- [Section 8.2.2.7, "Running Data Reduction Manually"](#)
- [Section 8.2.2.8, "Setting Data Reduction to Run Automatically"](#)
- [Section 8.2.2.9, "Deleting Data Files"](#)

8.2.2.1 Standard Data Reduction Process

During the data reduction process, the static URL information is extracted from the raw data files and combined with the service information stored in the SctAccessLog table. By default, Content Tracker collects and records data only for the SctAccessLog table. Although the user data output tables exist, Content Tracker does not populate them.

Depending on how Content Tracker is configured, this reduction process can:

- Combine access information for static URL content access with service details.
- Summarize information about user accounts that were active during the reporting period. This information is written to the Content Tracker's user metadata database tables.



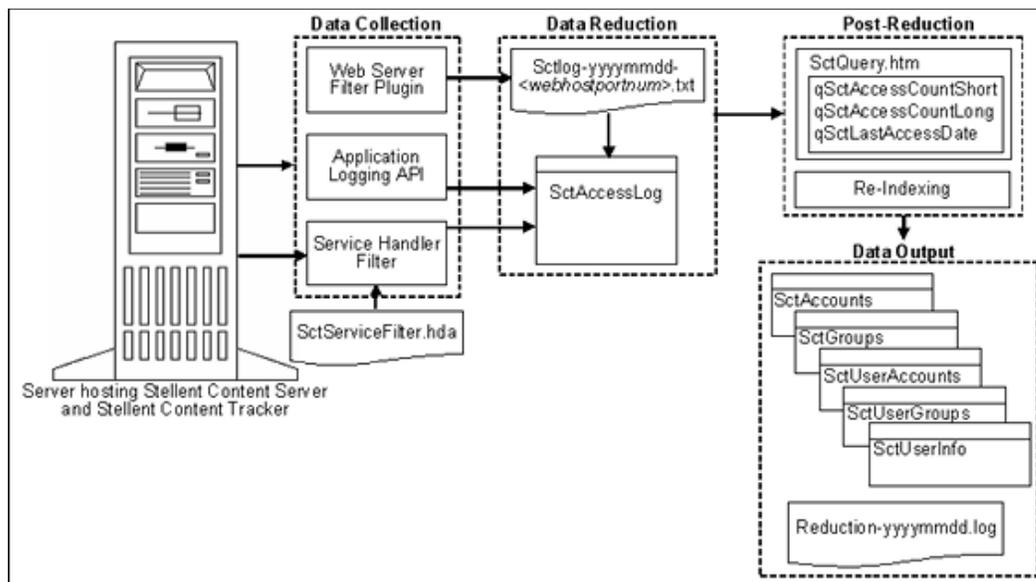
8.2.2.2 Data Reduction Process with Activity Metrics

Content Tracker provides the option to selectively generate search relevancy data and store it in custom metadata fields. You can use the snapshot function to choose which activity metrics to activate. The logged data provides content item usage information that indicates the popularity of content items.

By default, Content Tracker collects and records data only for the SctAccessLog table. Although the user data output tables exist, Content Tracker does not populate them unless the Snapshot function is activated. However, using the snapshot function affects Content Tracker's performance.

If the snapshot function and activity metrics are activated, the values in the custom metadata fields are updated following the reduction processing phase. When users access content items, the values of the applicable search relevance metadata fields change. During the later post-reduction step, Content Tracker uses SQL queries to determine which content items were accessed during the reporting period. Content Tracker updates the database table metadata fields with the new values and initiates a re-indexing cycle. However, only the content items whose access count metadata values have changed are re-indexed.

The post-reduction step is necessary to process and tabulate the activity metrics for each affected content item and to load the data into the assigned custom metadata fields. It also initiates a re-indexing cycle on the content items with changed activity metrics values to ensure that the data is part of the search index and is accessible to select and order search results.



8.2.2.3 Data Reduction Cycles

Reduced table data is moved from the primary tables to the corresponding archive tables when the associated raw data is moved from recent to archive status. The primary tables contain the output for reduction data in the new and recent cycles and the archive tables contain output for reduction data in the archive cycle.

Raw data is demoted from new to recent when the data is reduced and it is older than day. Thus, the 'new cycle' indicates that the data is for the current day or is unreduced data from previous dates. The 'recent cycle' indicates that the data is from yesterday or earlier and has been reduced.

Raw data is demoted to archive (and the corresponding rows in the SctAccessLog table are moved to the SctAccessLogArchive table) when the number of recent sets reaches a configured threshold number and a reduction process is run, either manually or through the scheduler. For more information about configuring the threshold number for recent sets, see the `SctMaxRecentCount` configuration variable information in the *Oracle WebCenter Content Idoc Script Reference Guide*. If a reduction process is never run, the raw data remains in the recent cycle indefinitely.

8.2.2.4 Access Modes and Data Reduction

The access mode used to access content items determines how those accesses are recorded in the SctAccessLog table. If content items are accessed through a service (that is, viewing the actual native file), the events are recorded in the SctAccessLog table in real time. In this case, the activity is recorded immediately and is not dependent on the reduction process.

If content items are accessed using static URLs (that is, viewing the Web location file), the Web server filter plug-in records the events in a static log file. During the data reduction process, the static log files for a specified date are gathered and the data is moved into the SctAccessLog table. In this case, if data reduction is not performed for a given date, there are no static URL records in the SctAccessLog and no evidence that these accesses ever occurred.

The difference in the way static and service accesses are processed has implications for interval counts. For example, a user might access a content item twice on Saturday, one time through the Web location file (static access) and one time through the native file (service access). The service access is recorded in the SctAccessLog table but the Web location access is not. If Sunday's data is reduced, only the service access (not the static access) is included in the summaries of the short and long access count intervals. However, if Saturday's data is also reduced, both the service and static accesses are recorded in the SctAccessLog table and included in the both intervals.

8.2.2.5 Reduction Sequence for Event Logs

Data sets are usually reduced in chronological (calendar) order to ensure that the information included in reports is current. The order in which the raw data log files are reduced determines what specific user access data is logged and counted. During reduction, the SctAccessLog and user metadata database tables are modified with data from the raw data files.

When using the snapshot function to gather search relevance information, the metadata fields associated with the activated activity metrics are also updated during data reduction. The activity metrics use custom metadata fields included in the DocMeta database table.

Content Tracker changes the activity metrics values according to the applicable data in the reduction data set. To ensure that data values are complete and current, perform data reduction on a daily basis. If the data sets are reduced out of order, re-reducing the current or most recent data set corrects the counts. However, it is always preferable to consistently reduce data in calendar order.

The following scenarios show how the reduction sequence affects the stored data.

Scenario 1:

Depending on how content items are accessed, if activity on certain days (such as Saturdays and Sundays) is never reduced, then accesses that occur on those days might never be logged or counted, see [Section 8.2.2.4, "Access Modes and Data Reduction."](#) Similarly, if a content item is accessed on Tuesday and reductions are done

for Monday and Wednesday, the Tuesday access is might not be counted toward the last access of that content item.

Scenario 2:

If there was a significant increase in accesses in the last few days, and you reduce data from two weeks earlier, the long and short access metrics for content items do not reflect the recent activity. Instead, the interval values from two weeks earlier override today's values. Reducing the current or most recent data set corrects the counts.

The reduction order does not adversely affect the Last Access date. The reduction process only changes the Last Access date if the most recent access in the reduction data set is more recent than the current Last Access value in Content Server's DocMeta database table.

If you have reduced a recent data set and a particular content item had been accessed, the Last Access field is updated with the most recent access date in the reduction data set. If you then re-reduce an older data set, the older access date for this content item does not overwrite the current value.

For more information about long and short activity metrics, see [Section A.6.1.4, "Snapshot Tab"](#) and the applicable check boxes and corresponding fields/intervals.

Scenario 3:

Reducing the data sets in an arbitrary order interferes with the demotion of "recent" data files to "archive" data files. The movement of the associated table records is based on the age, archive tables are intended to store the "oldest" data. If the data sets are reduced in random order, it is not apparent which data is the oldest.

For more information about recent and archive data files, see [Section 8.2.5.2, "User Metadata Tables,"](#) [Section 8.2.2.3, "Data Reduction Cycles,"](#) and the Cycle column on the [Section A.6.1.2, "Reduction Tab."](#)

8.2.2.6 Reduction Schedules

You can configure reduction runs to run on a scheduled basis to periodically reduce the raw data. A steady flow of raw data goes into the recent and archive repositories, and a similarly steady flow of reduced data goes from the primary tables to the archive tables.

Note that if the Content Tracker Data Engine is disabled the day before a scheduled reduction run, no data is collected. If it is enabled on the day of the scheduled reduction run, the scheduler does not run because no data is available.

Data reductions scheduled for a given day are performed on data collected during the previous day. The previous day is defined as the 24-hour period beginning and ending at midnight (system time). To conserve CPU resources, you can schedule reduction runs for early morning hours when the system load is generally the lowest.

An error can be issued if the scheduled reduction is set to run within a few minutes after midnight. If this occurs, reschedule the reduction to run later.

8.2.2.7 Running Data Reduction Manually

Follow these steps to manually reduce data:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.

2. On the [Reduction Tab](#), click (to highlight) the set of input data to reduce. Information on this screen includes the following:
 - **Cycle:** The status of the input data. Values include *new* (the input data has not been reduced), *recent* (data has been reduced but is not archived), and *archive* (data has been reduced and remains in archive cycle until deleted).
 - **Available date:** Date when the data was collected.
 - **Status:** The status of the reduction. Values include *ready* (input data is available to be reduced), *running* (data is being reduced), and *archiving* (data is being moved from *recent* to *archive* cycle).
 - **Percent Done:** the progress of the reduction cycle.
 - **Completion Date:** Date and time the reduction completed.
3. Click **Reduce Data**.

A confirmation dialog box opens.
4. Click **Yes** to reduce the data.

Note: If the current date's data is reduced, the status in the Cycle column stays as 'new' even though the data is reduced.

8.2.2.8 Setting Data Reduction to Run Automatically

Follow these steps to set data reduction to run automatically:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.
2. On the [Schedule Tab](#), select the Scheduling Enabled check box.
3. Select check boxes for the days when data reduction occurs.
4. Select the hour and minute when data reduction occurs.
5. Click **OK**.

Do not exit the applet. Wait until a confirmation message displays. If you exit before the confirmation message, the requested change(s) may not occur.
6. Click **OK** when the confirmation message is displayed.

8.2.2.9 Deleting Data Files

Follow these steps to delete data files:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.
2. On the [Reduction Tab](#), click (to highlight) the set of input data to delete.
3. Click **Delete** or **Delete Archive**.

A confirmation dialog box opens.
4. Click **OK** to delete the data.

The selected data set is deleted, and is no longer displayed in the window

8.2.3 Content Tracker Event Logs

Content Tracker supports multiple input files for different event log types and for configurations with multiple Web servers. Each Web server filter plug-in instance uses a unique tag as a filename suffix for the event logs. The unique suffix contains the Web server host name plus the server port number.

The reduction process searches for and merges multiple raw event logs named `sctLog-yyyyymmdd-<myhostmyport>.txt`. The raw event logs are processed individually.

Content Tracker may not always capture a user name for a content access event, even if the user is logged into Oracle WebCenter Content Server. In this case, the item was accessed with a static URL request and, in general, the browser does not provide a user name unless the Web server asks it to send the user's credentials. If the item is public content, the Web server does not ask the browser to send user credentials, and the user accessing the URL is unknown.

To record the user name for every document access, make sure the content is not accessible to the guest role. If the content is not public, the user's credentials are required to access the items and a user name is recorded in the raw event log entry.

Depending on Content Tracker configuration, when raw data log files in the "new" cycle are reduced, the Data Engine moves the data files into the following subdirectories:

- The default number of data sets that the recent/ directory can hold is 60 sets (dates) of input data log files. When the number of data sets is exceeded, the eldest are moved to the /archive directory.

```
<cs_root>/data/contenttracker/data/recent/yyyyymmdd/
```

- By default, Content Tracker does not archive data. Instead, the expired rows are discarded to ensure optimal performance. If appropriately configured, Content Tracker uses the archive/ directory to hold all input data log files that were moved out of the "recent" cycle.

```
<cs_root>/data/contenttracker/data/archive/yyyyymmdd/
```

When raw data files are reduced, another file (*reduction_ts-yyyyymmdd.txt*) is generated as a time stamp file.

8.2.4 Combined Output Table

The SctAccessLog table contains entries for all static and dynamic content access event records. The SctAccessLog table is organized using one line per event in the reporting period. The rows in the table are tagged according to type:

- S indicates the records logged for service calls.
- W identifies the records logged for static URL requests.

By default, Content Tracker does not log accesses to GIF, JPG, JS, CSS, CAB, and CLASS file types. Therefore, entries for these file types are not included in the combined output table after data reduction.

The Content Tracker Web server filter plug-in cannot distinguish between URLs for user content and those used by the user interface. References to UI objects, such as client.cab, can appear in the static access logs. To eliminate these false positives, use the SctIgnoreDirectories configuration variable to define a list of directory roots to be ignored by the Content Tracker filter. To log these file types, change the default setting for the SctIgnoreFileTypes configuration variable to the type

(gif,jpg,js,css). For more details about using configuration variables, see the *Oracle WebCenter Content Idoc Script Reference Guide*.

The following table describes the information collected for each record in the SctAccessLog table. By default, Content Tracker does not collect data to populate certain columns for bulky and rarely used items.

Column Name	Type / Size	Column Definition
SctDateStamp	datetime	Local date when data collected in format YYYYMMDD, depending on customer location and time of day event occurs. This may differ from date recorded for eventDate. Time set to 00:00:00 Data source: Internal
SctSequence	int / 8	Sequence unique to entry type Data source: Internal
SctEntryType	char / 1	Entry type. Values are W or S Data source: Internal
eventDate	datetime	GMT time and date when request completed. The date depends on customer location and time of day event occurs. This may differ from date recorded for SctDateStamp)
SctParentSequence	integer	Sequence of outermost Service Event in tree, if any.
c_ip	varchar / 15	IP of client
cs_username	varchar / 255	
cs_method	varchar / 10	GET
cs_uriStem	varchar / 255	Stem of URI
cs_uriQuery	varchar / [maxUrlLen]	Query portion. For example, IdcService=GET_FILE&dID=42...
cs_host	varchar / 255	Content Server server name
cs_userAgent	varchar / 255	Client User Agent Ident By default, this column contains either browser or the suffix of any string beginning with java:. This simplification ensures optimal performance for Content Tracker.
cs_cookie	varchar / [maxUrlLen]	Current cookie
cs_referer	varchar / [maxUrlLen]	URL leading to this request
sc_scs_dID	int / 8	dID Data source: from query or derived from URL (reverse lookup)
sc_scs_dUser	varchar / 50	dUser Data source: Service DataBinder dUser
sc_scs_idcService	varchar / 255	Name of IdcService. For example, GET_FILE Data source: from query or Service DataBinder IdcService
sc_scs_dDocName	varchar / 30	dDocName Data source: from query of Service DataBinder dDocName
sc_scs_callingProduct	varchar / 255	Arbitrary identifier Data source: SctServiceFilter config file or Service DataBinder sctCallingProduct

Column Name	Type / Size	Column Definition
sc_scs_eventType	varchar / 255	Arbitrary identifier Data source: SctServiceFilter config file or Service DataBinder sctEventType
sc_scs_status	varchar / 10	Service execution status Data source: Service DataBinder StatusCode
sc_scs_reference	varchar / 255	web,native,sdc_url Values indicate the rendition of the accessed file. web is a converted file (PDF), native is the original file and sdc_url is HTML. Data source: algorithmically from query parameters or ServiceFilter config file
comp_username	varchar / 50	Computed username. If a Service, obtained from UserData Service Object or HTTP_INTERNETUSER or REMOTE_USER or dUser. If a static URL, obtained from auth-user or internetuser.
comp_validRef	char / 1	Indicates if the referenced object exists and is available to the requesting user. 1 if the access was a Web reference (W), and ispromptlogin and isaccessdenied are both NULL, and the static URL exists at reduction time. Or, if the access was a service call (S) and the sc_scs_status field is NULL. NULL if the static URL did not exist at reduction time, or the user logon failed, or the logon succeeded but the user was not authorized to view the object.
sc_scs_isPrompt	char / 1	1 if true Data source: Plug-in immediateResponseEvent field "ispromptlogin"
sc_scs_isAccessDenied	char / 1	1 if true Data source: Plug-in immediateResponseEvent field isaccessdenied
sc_scs_inetUser	varchar / 50	Internet user name (if security problem) Data source: Plug-in immediateResponseEvent field internetuser
sc_scs_authUser	varchar / 50	Authorization user name (if security problem) Data source: Plug-in immediateResponseEvent field auth-user
sc_scs_inetPassword	varchar / 8	Internet password (if security problem) Data source: Plug-in immediateResponseEvent field internetpassword
sc_scs_serviceMsg	varchar / 255	Content Server service completion status Data source: Service DataBinder StatusMessage
extField_1 through extField_10	varchar / 255	General purpose columns to use with the extended service tracking function. In the field map ResultSets, the DataBinder fields are mapped to these columns.

8.2.5 Data Output

When Content Tracker is appropriately configured, the static and dynamic content access request information and all metadata fields are accessible for use in reports generated by the Content Tracker Reports component. The logged metadata includes content item and user metadata

This section covers the following topics:

- [Section 8.2.5.1, "Content Item Metadata"](#)

- [Section 8.2.5.2, "User Metadata Tables"](#)
- [Section 8.2.5.3, "Reduction Log Files"](#)

8.2.5.1 Content Item Metadata

Content Tracker uses standard Oracle WebCenter Content Server metadata tables for content item metadata. Thus Content Tracker reports reflect current content item metadata. If content item metadata changed since a content item was accessed, any generated reports reflect the changed metadata.

8.2.5.2 User Metadata Tables

Content Tracker user metadata database tables are updated with information collected about active users during the reporting time period. These tables retain data about user profiles at the time the data reduction runs. The names of the user metadata tables are formed from a root which indicates the class of information contained, and an Sct prefix to distinguish the table from native Oracle WebCenter Content Server tables.

By default, Content Tracker does not archive data so expired rows are not moved from the Primary tables to the Archive tables. Instead, the expired rows are discarded, ensuring optimal performance. Two complete sets of user metadata database tables are created:

- Primary: Named SctUserInfo, and so on, which contain the output for reduction data in the new and recent cycles.
- Archive: Named SctUserInfoArchive, and so on, which contain output for reduction data in the archive cycle.

If Content Tracker is configured to run archives, reduction data files are moved from *recent* to *archive* status and the associated table records are moved from the Primary table to the Archive table. This prevents excessive buildup of rows in the Primary tables, and ensures that queries performed against recent data complete quickly. Rows in the Archive table are not deleted. They can be moved or deleted using any SQL query tool. To delete all the rows in the Archive tables, delete the tables themselves. They are re-created during the next Oracle WebCenter Content Server restart. Reports are not run against archive data.

The following tables are created:

- The SctAccounts table contains a list of all accounts. It is organized using one line for each account.
- The SctGroups table contains a list of all user groups current at time of reduction. It is organized using one line per content item group.
- The SctUserAccounts table contains entries for all users listed in the SctUserInfo table and who are assigned accounts defined in the current instance. A separate entry exists for each user-account combination.

In multiple proxy instances, the group and account information of a user may not be determined by Content Tracker. When the current instance is a proxy, the group information for an active user defined in a different proxy is replaced by a placeholder line in SctUserGroups for that user. The line contains the user name and a hyphen (-) placeholder for the group. If at least one account is defined in the current instance, a similar entry is created in SctUserAccounts for any user who is defined in a different proxy.

- The SctUserGroups table is organized using one line for each user's group for each user active during the reporting period. It references those users who logged on

during the data collection period. If Content Tracker is running in a proxied Oracle WebCenter Content Server configuration, only groups defined in the current instance are listed. For example, a user named "joe" is defined in the master instance and has access to groups "Public" and "Plastics" in the master instance. If "joe" logs on to a proxy instance and the group "Plastics" is not defined in the proxy, only the association between "joe" and "Public" appear in SctUserGroups.

- The SctUserInfo table is organized using one line per user. It includes all users known to the current instance and additional users from a different instance who logged on to the current instance during the data collection period. In a proxied configuration, users local to one instance are usually visible from the UserAdmin application to other instances. If a user is defined locally with the same name in two instances, only the local user is visible in each of these instances.

For example, the "sysadmin" defined in the master is not the "sysadmin" appearing in the UserAdmin application for a proxy. These two different users could both log on during the same data collection period. The user from the master logs on as "sysadmin" and the proxy user logs on as "cs_2/sysadmin" (for example). The SctUserInfo file generated for this period has separate entries for "sysadmin" and "cs_2/sysadmin".

8.2.5.3 Reduction Log Files

When data reduction is run, the Content Tracker Data Engine generates a summary results log file, named *reduction-yyyymmdd.1log*. The reduction logs can be useful to help diagnose data reduction errors. For more information, see [Section 8.5, "Troubleshooting"](#).

8.2.6 Tracking Limitations

In some cases, Content Tracker has limitation in tracking data. This section provides an overview of those limitations.

- [Section 8.2.6.1, "Tracking Limitations in Single-Box Clusters"](#)
- [Section 8.2.6.2, "Static URLs and WebDAV"](#)
- [Section 8.2.6.3, "Data Directory Protections"](#)
- [Section 8.2.6.4, "ExtranetLook Component"](#)

8.2.6.1 Tracking Limitations in Single-Box Clusters

Currently, Content Tracker and Content Tracker Reports do not support multi-node clusters that are installed in a single server. This is true even though multiple network cards are installed and each cluster node has its own IP address. In this case, the Content Server instance for each cluster node can successfully bind its IntradocServerPort to its specific IP address.

Unfortunately, only one cluster node is able to bind its Incoming Provider ServerPort to its specified IP address. Consequently, all of the cluster nodes share and alternately use the same Incoming Provider ServerPort. As a result, the SctLock provider for Content Tracker can only track document accesses on one cluster node at a time.

8.2.6.2 Static URLs and WebDAV

The access counts determined by Content Tracker are generally correct, but in some circumstances the software cannot determine if the content was actually delivered to

the requesting user, or if it was, which revision of the content was delivered. The following list provides examples of when such events can occur:

- Repeated requests through WebDAV: If a user accesses a document with a WebDAV client then re-accesses the same document later, only the first WebDAV request is recorded. Access count reports for such content are usually lower than the actual number.
- Static URLs: A user saves a URL for a content file, but the content is later revised in such a way that the saved URL is no longer valid. If the user attempts to access the content with the saved URL, an error occurs. Content Tracker records this as a successful access even though content was not delivered. Access count reports for such content are usually higher than the actual number.
- Static URLs and wrong dID: If a user accesses content using a URL and the content is revised or the security group is changes before the Content Tracker data reduction operation is performed, the user is reported as seeing the latest revision. If the user accesses an original version which is then superseded by a different version, Content Tracker reports that the user got the revision, not the actual document. Access count reports for such content are usually attributed to a newer revision than actual. To minimize this effect, schedule or run data reductions on a regular basis.

This section covers the following topics:

- [Section 8.2.6.2.3, "Missed Accesses for Content Repeatedly Requested via WebDAV"](#)
- [Section 8.2.6.2.2, "False Positive for Access by Saved \(stale\) Static URL"](#)
- [Section 8.2.6.2.1, "Wrong dID Reported for Access by Saved Static URL"](#)

8.2.6.2.1 Wrong dID Reported for Access by Saved Static URL

Scenario: User accesses content via the "Web Location" (URL). The content is then revised before the Content Tracker data reduction operation is performed. The user is reported as seeing the latest revision, not the one that s/he actually saw. Access counts reported for such content tend to be attributed to a newer revision than actual. Minimize this effect by scheduling or running Content Tracker data reductions on a regular basis.

Details: This is related to False Positive for Access by Saved (stale) Static URL, described above. That is, the web server uses the entire web location, (e.g. DomainHome/ucm/cs/groups/public/documents/adacct/xyzy.doc), to locate and deliver the content, while Content Tracker uses only the ContentID portion to determine the dID and dDocName values. Moreover, Content Tracker makes this determination during data reduction, not at the time the access actually occurs. Content Tracker reports the user as having seen the revision current at the time of the reduction, not the one that was current at the time of the access.

There are some implications of this not immediately obvious, such as when the group and/or security of the revision are changed from the original. For example, if a user accesses "Public" Revision 1 of a document through a static URL, and the document is subsequently revised to Revision 2 and changed to "Secure" before the Content Tracker data reduction takes place, Tracker reports that the user saw the Secure version. This may also occur when the content file type changes. If the user accesses an original.xml version, which is then superseded by an entirely different.doc before the data reduction is performed, Tracker reports the user saw the.doc revision, not the actual.xml.

8.2.6.2.2 False Positive for Access by Saved (stale) Static URL

Scenario: User saves a "Web Location" (URL) for a content file. The content is subsequently revised in such a way that the saved URL is no longer valid. The user then attempts to access the content via the (now stale) URL, and gets a "Page Cannot be Found" error (HTTP 404). Content Tracker may record this as a successful access even though the content was not actually delivered to the user. Access counts reported for such content tend to be higher than actual.

Details: The "Web Location" of a content file is the means by which a user can access content via a "static URL". The specific file path in the URL is used in two, slightly different contexts: It is used by the web server to locate the content file in the Content Server repository, and it is also used by Content Tracker to determine the dID and dDocName of the content file during the data reduction process. The problem occurs when the content is revised in such a way that the web location for a given Content ID changes between the time the URL is saved and the time the access is attempted.

For example, if a Word document is checked in then revised to an XML equivalent, the web location for the latest revision of the content changes from:

`DomainHome/ucm/cs/groups/public/documents/adacct/xyzyz.doc`

to: `DomainHome/ucm/cs/groups/public/documents/adacct/xyzyz.xml`

where: "xyzyz" is the assigned Content ID.

The original revision is "renamed" as:

`DomainHome/ucm/cs/groups/public/documents/adacct/xyzyz~1.doc`

This means the original Web Location no longer works as a static URL. The Content ID obtained from the original URL, however, matches the latest revision. Content Tracker reports this as an access to Content ID "xyzyz", even though the web server was unable to deliver the requested file to the user.

8.2.6.2.3 Missed Accesses for Content Repeatedly Requested via WebDAV

Scenario: User accesses a document via a WebDAV client, then accesses the same document in the same manner later. Only the first WebDAV request for the document is recorded. Access counts reported for such content tend to be lower than actual.

Details: WebDAV clients typically use some form of object 'caching' to reduce the amount of network traffic. If a user requests a particular object, the client first determines if it already has a copy of the object in a local store. If it does not, the client contacts the server and negotiates a transfer. This transfer is recorded as a `COLLECTION_GET_FILE` service request.

If the client already has a copy of the object, it contacts the server to determine if the object has changed since the client local copy was obtained. If it has changed, then a new copy is transferred and the `COLLECTION_GET_FILE` service details is recorded.

If the client copy of the object is still current, then no transfer takes place, and the client presents the saved copy of the object to the user. In this case, the content access is not counted even though the user appears to get a "new" copy of the original content.

8.2.6.3 Data Directory Protections

Content Tracker's Web server filter plug-in runs in the authorization context of the user whose access request is being processed. In some cases, the owner of the request processing thread is a system account. In others, it is a requesting user or another type of non-system account used by the application.

The filter records the information in raw event logs. If the log file does not exist a new one is created using the default protection and authorization credentials of the user

who owns the event thread. If the user account has write permission to the data directory, the content access data is recorded. Otherwise, the logging request fails and the access event details are not recorded.

To ensure that Content Tracker can properly record user access requests, the data directory must be configured to accept the account authorization credentials for all users. Granting world write permission (or the equivalent) is one method. Allowing unlimited write access is recommended unless security concerns prohibit this level of unrestricted access.

8.2.6.4 ExtranetLook Component

The ExtranetLook component (if enabled) allows customizations of cookie-based login forms and pages for anonymous-type users. The component uses a built-in Web server plug-in that monitors requests and determines if a request is authenticated based on cookie settings. When a user requests access to a content item, Content Tracker must function within the authorization context of the user's account.

After collecting the access information, Content Tracker tries to record the event data in the log file. If the user's account permissions allow access to Content Tracker's data directory, then the request activity is logged. However, if the account does not have write authorization, the logging request fails and the request activity is not recorded.

8.3 Data Tracking Functions

This section describes the different data tracking functions available with Content Tracker. It covers the following topics:

- [Section 8.3.1, "Activity Snapshots"](#)
- [Section 8.3.2, "Service Calls"](#)
- [Section 8.3.3, "Web Beacon Functionality"](#)

8.3.1 Activity Snapshots

The activity snapshots feature captures user metadata that is relevant for each recorded content item access.

This section discusses the following topics:

- [Section 8.3.1.1, "Search Relevance Metrics"](#)
- [Section 8.3.1.2, "Enabling the Snapshot Function"](#)
- [Section 8.3.1.3, "Creating the Search Relevance Metadata Fields"](#)
- [Section 8.3.1.4, "Setting a Check-in Time Value for the Last Access Field"](#)
- [Section 8.3.1.5, "Populating the Last Access Field for Batch Loads and Archives"](#)
- [Section 8.3.1.6, "Linking Activity Metrics to Metadata Fields"](#)
- [Section 8.3.1.7, "Editing the Snapshot Configuration"](#)

8.3.1.1 Search Relevance Metrics

When activated, the activity metrics and corresponding metadata fields provide search relevance information about user accesses of content items. An optional automatic load function allows users to update the last access activity metric to ensure that checked-in content items are appropriately timestamped.

Content Tracker optionally fills the search relevance custom metadata fields with content item usage information that indicates the popularity of particular content items. This information includes the date of the most recent access and the number of accesses in two distinct time intervals.

Information generated from these activity metrics functions is used in various ways. For example, you can order search results according to which content items have been recently viewed or the most viewed in the last week.

If the snapshot function is activated, the values in the search relevance metadata fields are updated during a post-reduction step. During this processing step, Content Tracker uses SQL queries to determine which content items have changed activity metrics values. Content Tracker updates the applicable database tables with the new values and initiates a re-indexing cycle. However, only the content items that have changed metadata values are re-indexed.

8.3.1.2 Enabling the Snapshot Function

To use these optional features, first enable the snapshot post-processing function which activates the activity metrics choices. Then selectively enable the activity metrics and assign their preselected custom metadata fields.

Follow these steps to enable the snapshot function and activate the activity metrics:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.

2. On the [Snapshot Tab](#), select **Enable Snapshot**.

3. Click **OK**.

A confirmation dialog box opens.

4. Click **OK**.

8.3.1.3 Creating the Search Relevance Metadata Fields

Before implementing the snapshot function, decide which custom metadata fields to associate with each of the enabled activity metrics. Also, the custom metadata fields must exist and must be of the correct type. Depending on which activity metrics to be enabled, create one or more custom metadata fields using an applicable procedure.

For details about creating a custom field, see [Section 2.2.2, "Adding or Editing a Custom Field"](#). Add the following specific information for the activity metrics:

- Last Access Metric
 - Field Type: Date
 - Default Value: Optional. If not specified, the field is not populated until a content item is checked in and a data reduction run. Some applications require a default value and in those cases, enter a value in the Default Value field that ensures the Last Access field is populated with the date and time of the content check in. For details see [Section 8.3.1.4, "Setting a Check-in Time Value for the Last Access Field"](#).
 - Enable for Search Interface: Optional. Check to make the field available for searching.
- Short and Long Access Metric
 - Field Type: Integer

- Enable for Search Interface: Optional. Check to make the field available for searching.

Indexing a custom metadata field is optional, although indexing makes searches on this field more efficient. Indexing also allows users to query the accumulated search relevance statistics and generate useful data. For example, you can create a list of content items ordered by their popularity, and so on.

8.3.1.4 Setting a Check-in Time Value for the Last Access Field

The Last Access Date field is normally updated by Content Tracker when a managed object is requested by a user and a data reduction run. The field can be empty (NULL) until the next data reduction is run. Some applications require that the date and time of content check in be recorded immediately in the Last Access field.

Use any of the following methods to populate the Last Access field:

- Using the Configuration Manager: When adding the metadata field, enter an expression that populates the field with the date and time of content check in (for example, a default value of `<$dateCurrent () $>` populates the field with the current check-in date and time). After setting the value, fill the field for existing content using the Autoload option.
- Using the Autoload option: This option allows retroactive replacement of NULL values in the Last Access field with the current date and time. The only records affected are those where the Last Access metadata field is empty (NULL)
 1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.
The [Data Engine Control Center](#) opens.
 2. Click the [Snapshot Tab](#).
 3. Select one or more of the activity metric check boxes to enable them. Enter the name of the custom metadata field to be linked to the activity metric (for example, `xLastAccess`, `xShortAccess`, or `xLongAccess`).
 4. Select the **Autoload** check box.
 5. Click **OK**.

A confirmation dialog box opens and the current date and time are inserted into the applicable Last Access fields (those with NULL values) in the DocMeta database table.

Note the following considerations when using the Autoload option:

- It is primarily intended for use with applications that count check-in operations as an access activity.
- Autoload backfills the current date and time for all existing content that does not have a date value in the Last Access field. Any content checked in after the Last Access field is defined should have the field automatically populated with the check-in date and time as a default value.
- Running Autoload can affect every record in the DocMeta database table. Use this option sparingly.
- The only DocMeta records affected are those where the Last Access metadata field is empty (NULL).
- Autoload is persistent. The state of the Autoload check box is saved with all the other Snapshot settings. To prevent inadvertent use of this option,

clear the Autoload check box and re-save activity metrics field settings immediately after performing the autoload function.

- Oracle WebCenter Content Server's indexer is not automatically run after Autoload completes the update. You must decide when to rebuild the collection.
- By default, the Autoload query sets the Last Access metadata field to the current date and time. You can customize the query as needed.

8.3.1.5 Populating the Last Access Field for Batch Loads and Archives

To ensure proper retention of archived and batch loaded content, set the Last Access field date for the import/insert. Otherwise the access date for these content items is NULL, and retention based on this field fails. Also consider how the date can affect retention management. For example, an import of 1998 data is probably better tagged with that date than the date when the import was performed to accurately reflect the retention quality of the content.

The name of the Last Access field is based on the name specified when the field was created. For example, if the name Last Access is used, xLastAccess would be used in the import/insert.

See the *Oracle WebCenter Content System Administrator's Guide for Content Server* for more detailed information about using the batch loader. The following steps provide a general outline of the procedure to populate the Last Access field using Batch Loader:

1. Access the Batch Loader.
2. Create a record that establishes an appropriate Last Access date. The following is an example of an applicable file record:

```
# This is a comment
Action=insert
dDocName=Sample1
dDocType=ADACCT
xLastAccess=5/1/1998
dDocTitle=Batch Load record insert example
dDocAuthor=sysadmin
dSecurityGroup=Public
primaryFile=links.doc
dInDate=8/15/2001
<<EOD>>
```

3. Run the Batch Loader to process the file record.

8.3.1.6 Linking Activity Metrics to Metadata Fields

After the activity metrics options have been activated, they must be individually selected to enable them. Enabling the activity metrics also activates their corresponding custom metadata fields.

Follow these steps to enable the activity metrics and activate their corresponding custom metadata fields:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.

The [Data Engine Control Center](#) opens.

2. Click the [Snapshot Tab](#).

3. Select one or more of the activity metric check boxes to enable them. Enter the name of the custom metadata field to be linked to the activity metric (for example, xLastAccess, xShortAccess, or xLongAccess).
4. For the Short and Long Access Counts, enter the applicable interval amounts in days. For example, 7 days for the Short Access Count and 28 days for the Long Access Count.

The two Access Count metrics differ only in the accounting period (for example, last 30 days versus last 90 days, last week versus last year, and so on). The time intervals specified in the activity metrics are independent of each other. For example, you can set the number of days in the first interval period (Short Access) to more than those in the second interval period (Long Access).

Access counts are only tabulated for reduced dates. If data is not reduced for one or more days, the accesses on those days are not logged or counted. Do not reduce data in random order because the Access Count metrics are affected by the reduction date order.

5. Click **OK** when done.
A confirmation dialog box opens.
6. Click **OK**.

Note that the fields are case-sensitive. Make sure all field values are spelled and capitalized correctly.

Content Tracker uses the following error checks to validate each enabled activity metric field value:

- Checks the DocMeta database table to ensure that the custom metadata field actually exists.
- Ensures that the custom metadata field is of the correct type (for example, that the Last Access metadata field is of type Date, and so on).
- Checks to explicitly exclude the dID metadata field.

8.3.1.7 Editing the Snapshot Configuration

Follow these steps to modify the snapshot activity metrics settings:

1. Choose **Administration** then **Content Tracker Administration** from the Main menu. Choose **Data Engine Control Center**.
The [Data Engine Control Center](#) opens.
2. Click the [Snapshot Tab](#).
3. Make the necessary changes in the activity metrics fields.
4. Click **OK**.
A confirmation dialog box opens.
5. Click **OK**.

8.3.2 Service Calls

Content Tracker enables the logging of service calls with data values relevant to the associated services. Every service to be logged must have a service entry in the service call configuration file (SctServiceFilter.hda). In addition to the logged services, you can include the corresponding field map ResultSets in the SctServiceFilter.hda.

For details about managing service calls, see the *Oracle WebCenter Content Developer's Guide for Content Server*.

8.3.3 Web Beacon Functionality

Important: The implementation requirements for the Web beacon feature are contingent on the system configurations involved. All of the factors cannot be addressed in this documentation. Information about the access records collected and processed by Content Tracker are an indication of general user activity and not exact counts.

A Web beacon is a managed object that facilitates specialized tracking support for indirect user accesses to Web pages or other managed content. In earlier releases, Content Tracker was unable to gather data from cached pages and pages generated from cached services. When users access cached Web pages and content items, Oracle WebCenter Content Server and Content Tracker are unaware that these requests ever happened. Without using Web beacon referencing, Content Tracker does not record and count such requests.

The Web beacon involves the use of client side embedded references that are invisible references to the managed beacon objects within Oracle WebCenter Content Server. Content Tracker can record and count user access requests for managed content items that have been copied by an external entity for redistribution without obtaining content directly from Oracle WebCenter Content Server.

Two situations in particular merit the use of the Web beacon functionality: reverse proxy activity and when using Site Studio.

In a reverse proxy scenario, the reverse proxy server is positioned between the users and Oracle WebCenter Content Server. The reverse proxy server caches managed content items by making a copy of requested objects. The next time another user asks for the document, it displays its copy from the private cache. If the reverse proxy server does not have the object in its cache, it requests a copy.

Because it is delivering cached content, the reverse proxy server does not directly interact with Oracle WebCenter Content Server. Therefore, Content Tracker cannot detect these requests and does not track this type of user access activity.

A reverse proxy server is often used to improve Web performance by caching or by providing controlled Web access to applications and sites behind a firewall. Such a configuration provides load balancing by moving copies of frequently accessed content to a Web server where it is updated on a scheduled basis.

For the Web beacon feature to work, each user access includes an additional request to the managed beacon object in Oracle WebCenter Content Server. The additional request adds overhead, but the Web beacon object is very small and does not significantly interfere with the reverse proxy server's performance. Note that it is only necessary to embed the Web beacon references in objects you specifically want to track.

Another usage scenario involves Site Studio, a product that is used to create Web sites which are stored and managed in Oracle WebCenter Content Server. When Site Studio and Oracle WebCenter Content Server are located on the same server, Content Tracker is configured to automatically track the applicable user accesses. The gathered Site Studio activity data is then used in pre-defined reports, as described in [Section 8.4.1.4, "Site Studio Web Site Activity Reporting."](#)

Note: Two modes of Site Studio integration are available with Content Tracker. One type is the existing built-in integration that automatically occurs when Site Studio is installed. Use this option when you are constructing a Web site and you manage the Web pages in Oracle WebCenter Content Server.

The other form uses the Web beacon feature and Content Tracker regards Site Studio the same as any other Web site generator. Use this option when a Web site is in production mode and you no longer manage content in Oracle WebCenter Content Server.

If your Web site is intended for an external audience, you may decide to create a copy of the site and transfer it to another server. In addition to being viewed publicly, this solution also ensures that site development remains separate from the production site. In this arrangement, however, implement the Web beacon feature to ensure that Content Tracker can collect and process user activity.

For details about managing Web beacon objects, see the *Oracle WebCenter Content Developer's Guide for Content Server*.

8.4 Content Tracker Reports

Content Tracker Reports uses the captured and reduced data to generate reports that outline the usage history of particular pieces of content. Use the pre-defined reports or create custom queries for the information to be tracked. Any external commercial reporting tool can be used. For more information, see [Section 8.4.2.5, "External Report Generators."](#)

By default, Content Tracker collects and records only content access event data and excludes information gathering on non-content access events like searches and the collection and synthesis of user profile summaries. Because of this exclusion, some pre-defined report options are not displayed on the Content Tracker Report Generator main page. To make all pre-defined report options available, modify the config.cfg file to change the setting of the optimization functions, or use the Component Manager Update function.

You can derive reports from a variety of criteria, including specific users, groups of users, and any set of content that you can define with a query or a group of metadata values. Based on the variables in the system (such as number of users, amount of content, metadata count, and so on), Content Tracker Reports enables hundreds of key metrics to be included in reports. Specialized reports enable you to understand and disclose which content is most relevant to users.

This section covers the following topics:

- [Section 8.4.1, "Report Features and Considerations"](#)
- [Section 8.4.2, "Report Creation Types"](#)
- [Section 8.4.3, "Security Checks and Query Results"](#)
- [Section 8.4.4, "Using Content Tracker Reports"](#)

8.4.1 Report Features and Considerations

Consider the following issues when using report functionality:

- [Section 8.4.1.1, "Oracle and DB2 Case Sensitivity"](#)

- [Section 8.4.1.2, "Access Control Lists and Content Tracker Reports Secure Mode"](#)
- [Section 8.4.1.3, "User Authentication/Authorization and Auditing"](#)
- [Section 8.4.1.4, "Site Studio Web Site Activity Reporting"](#)

8.4.1.1 Oracle and DB2 Case Sensitivity

If Oracle database or DB2 is used as the Oracle WebCenter Content Server database, metadata values are case sensitive. You must enter values in the query report criteria with the correct capitalization or Content Tracker Reports may not return all possible matching files.

For example, if the content type in the Oracle or DB2 Oracle WebCenter Content Server database is *AdAcc* but the user enters it in the query field as *adacc*, *ADACC*, or *Adacc*, Content Tracker Reports does not return any results. In this case, and for all of the metadata fields in each of the pre-defined query reports, the entered value must match the capitalization of the metadata value.

8.4.1.2 Access Control Lists and Content Tracker Reports Secure Mode

The `SctrEnableSecurityChecks` configuration variable is set when the Content Tracker Reports component is installed and enables one of two security modes: secure and non-secure. Changing the variable provides the option to employ individual user role and account information to restrict the visibility of content item information in report results.

You can control what content items and metadata that users can see in their generated reports. Ideally, users should not see anything through Content Tracker Reports that they couldn't find through an Oracle WebCenter Content Server search. If secure mode is used, the information in any generated report is filtered based on the user's role and account privileges.

However, if Access Control Lists (ACLs) are enabled on the instance, the secure mode option in Content Tracker Reports does not work. During installation, leave the security checks preference check box blank. On an ACL-based system, the secure mode must be disabled. In this case, it is possible for users other than a system administrator to see information about content items that they would not otherwise be authorized to access and view.

Note: For more detailed information about the security checks installation preference and how it affects the report queries and report results, see [Section 8.4.3, "Security Checks and Query Results."](#)

8.4.1.3 User Authentication/Authorization and Auditing

An auditing feature is available that monitors unsuccessful attempts to access the system or permission-protected content items. Two reports are available that can help analyze attempted security breaches that include failed user logins and unsuccessful attempts to access secure content items. Information about failed access attempts is essential to safeguard system and content security and to maintain proper maintain audit trails and records.

The available auditing reports include:

- **Authorization Failures by User:** This report provides access authorization denial information that includes user names and their IP addresses. Although these users have system access privileges, their role/account memberships can restrict them from accessing particular content items (such as access to payroll content).

- **Login Failures:** This report provides login/authentication failure information that includes user names and their IP addresses. The logged data does not distinguish between external, internal, and global users because, without a successful login, it is impossible to differentiate user types.

8.4.1.4 Site Studio Web Site Activity Reporting

When using Site Studio, Content Tracker is automatically configured to track Site Studio activity. Content Tracker Reports uses the logged data to generate the pre-defined reports that summarize the Web site access results. The Site Studio-specific Web access reports are included on the Content Tracker Report Generator main page when Site Studio is installed.

The Site Studio pre-defined reports use the default Content Tracker Reports formatting and provide drill-down report capabilities. The top level reports for both are summary reports that use Site ID and Accesses as their general criteria. The drill-down reports provide the relevant statistics:

- **Web Site Content Accesses:** This report is ID-based at the top level and in later drill-down reports, the results are listed by Content ID and Relative URL. The information shows what URLs are being used to access a Web site. However, there are cases where many different URLs actually display the same page. The results of this report also provide the total number of visits to the nodes, regardless of how the user got there.
- **Web Site Accesses by URL:** This report provides summaries of the Web site relative URLs and the relevant activity sums.

8.4.2 Report Creation Types

There are three methods to produce Content Tracker Reports:

- [Section 8.4.2.1, "Pre-Defined Reports"](#)
- [Section 8.4.2.2, "Custom Reports"](#)
- [Section 8.4.2.3, "Generating Reports"](#)
- [Section 8.4.2.4, "Accessing Reports from the Information Page"](#)
- [Section 8.4.2.5, "External Report Generators"](#)

8.4.2.1 Pre-Defined Reports

Content Tracker Reports provides several pre-defined report options used to generate reports for the most commonly requested topics.

Reports produced with the Content Tracker Report Generator have the same general format and visual layout. The information in the reports is extracted from the reduced data in the SctAccessLog database table and other Oracle WebCenter Content Server database tables, if needed.

Users who request and open content items are included in the compiled results. The opened content item can be the Web location file (the absolute path to the content item), an HTML version (by using Dynamic Converter), or the actual native file. Users that open only the Content Information page are not included in the tracked data.

Information must first be accumulated by Content Tracker then undergo a data reduction cycle. Manually reducing the data immediately updates the database tables so the generated query reports also display the updated information. Otherwise, there is a one-day delay from the time a user accesses a content item until that information is included in the access history results.

When a generated query report contains an active link to a specific content item, click the link to open the corresponding Content Dashboard. The content dashboard shows the versions of content item and the access times. Click **Versions Separated** to show all version or click **All Versions Together** to combine the view of the versions.

You can generate various levels of report results for each pre-defined report. Depending on the search criteria entered on the Content Tracker Report Generator main page, the results are filtered accordingly. The top level reports are summary reports and provide very general information. Use the links on the top level reports to drill down to more specific information.

8.4.2.2 Custom Reports

In addition to the sample reports provided with Content Tracker Reports, you can create custom queries to track information. Consider the following when creating custom reports:

- When using Oracle Database and aliases to display the column names in the generated report, add the aliases to the `/shared/config/resources/upper_clmns_map.htm` file. For example, if the `Name` and `Access_Date_GMT` column headers are used, enter the following lines in the `upper_clmns_map.htm` file:

```
<tr>
<td>NAME</td>
<td>Name</td>
</tr>
<tr>
<td>ACCESS_DATE_GMT</td>
<td>Access_Date_GMT</td>
</tr>
```

- When using the extended service tracking function, be aware that the name of the service is always logged to the `sc_scs_idcService` column. When you design queries that reference the contents of the extended fields, include the service as a qualifier in the query.
- After successfully adding the custom report query to the report query file, you can use it to view the results.

8.4.2.3 Generating Reports

Follow these steps to generate a pre-defined or custom report:

1. Choose **Administration** then **Content Tracker Reports** from the Main menu.
2. Select the report type.
3. Enter any search and filtering criteria in the applicable fields.
4. Click **Submit**.

The selected report type opens.

8.4.2.4 Accessing Reports from the Information Page

You can generate the Access History Report for any content item from the Information page of that content item.

1. Search for a content item and click the associated **Info** icon.

The Content Information page opens.

2. Select **View Access History Report** from the Global Actions list.

The most current Content Access Report for the content item opens.

3. On the Content Access Report, click **Accesses**.

The most current Accesses by Day report for the content item opens.

4. On the Content Access Report, click **Users**.

The most current Accesses by User report for the content item opens.

8.4.2.5 External Report Generators

You can use commercial report generation tools to produce basic text reports or more sophisticated graphics such as bar graphs or pie charts from the data collected by Content Tracker.

This guide assumes that users have a working knowledge of the external reporting tool they are using to create custom reports. For this reason, only basic guidelines that are applicable to most commercially available reporting products are discussed here.

8.4.2.5.1 Using an External Report Generator To generate custom reports from an external reporting tool:

1. Open the external reporting tool application
2. Set up an ODBC connection (if appropriate) to the database.
3. Select the database tables to use in the report.
4. Link the selected tables based on key IDs or fields common within the files. Ideally, each selected table could be linked using the same key ID or field if it is common to each table.
5. Choose and integrate the fields from each table into the report form. In most cases, the fields can be selected, dragged, and dropped onto the form.

In this step, design the customized report. The specific fields, select display as columns on the final, basic text report that the external reporting application generates.

6. Create custom parameters, criteria or both if the external reporting application supports these options.

For example, one type of custom parameter would allow you to either have queried information hard-coded into the final report or use a prompt to obtain input directly from the end user. Additionally, creating specific sort criteria can strategically restrict and optimize the aggregate data included in the final report.

7. Specify the sorting order of the selected fields and format the final report output.
8. Preview the final report (optional).
9. Check the report into a delivery mechanism.

Generally, you can format and deliver the final report as Web-viewable pages or as a printable file. The external reporting application can also use the data results to create attractive graphics such as bar graphs or pie charts.

Additionally, you can import the saved file into other products such as Microsoft Excel or Word files.

8.4.3 Security Checks and Query Results

During the installation process for Content Tracker Reports, you can use individual user role and account information to restrict the visibility of content item information

in report results to control what content items and metadata that users see in their generated reports. Ideally, users should not see anything through Content Tracker Reports that they couldn't find through an Oracle WebCenter Content Server search.

Caution: If Access Control Lists (ACLs) are enabled on the instance, the secure mode option in Content Tracker Reports does not work. For more information, see [Section 8.4.1.2, "Access Control Lists and Content Tracker Reports Secure Mode."](#)

The `SctrEnableSecurityChecks` configuration variable is set when the Content Tracker Reports component is installed. This variable enables the use of either secure or non-secure mode. During installation, select a mode by checking or not checking the security check box. After installation, change the setting using the Component Manager.

If `SctrEnableSecurityChecks=True`, Content Tracker Reports operates in secure mode. The same security criteria (role and account qualifications) used to limit search results are also applied to the Content Tracker Reports queries and the generated reports. Two different users running the Top Content Items report could see different results. If set to false (the default), a user other than a system administrator can see information about content items that they would not be authorized to access and view.

The `contenttrackerreports_query.htm` file contains all the Content Tracker Report Generator's queries that produce the pre-defined and custom reports. To support non-secure and secure modes, this file contains two sets of queries.

Note: For localization support, the word "document" was changed to "content item" in the pre-defined report names. However, the corresponding report queries still include an abbreviation for the word document (doc). The report query names have not been changed in the `contenttrackerreports_query.htm` file.

For example, the "Top Content Items" report is a pre-defined report listed on the Content Tracker Report Generator main page. The corresponding report queries in the `contenttrackerreports_query.htm` file use the pre-existing naming conventions:

qSctrTopDocs (non-secure version)

qSctrTopDocs_SEC (secure version)

This section covers the following topics:

- [Section 8.4.3.2, "Pre-Defined Reports and Security Modes"](#)
- [Section 8.4.3.3, "Custom Reports and Security Modes"](#)
- [Section 8.4.3.4, "Changing the Security Configuration"](#)
- [Section 8.4.3.6, "Enabling or Disabling Security Checks for Report Queries"](#)
- [Section 8.4.3.7, "Customization for Report Query Security"](#)
- [Section 8.4.3.8, "Creating Secure Report Queries"](#)

8.4.3.1 Security Mode Examples

A user might have admin, contributor, guest, and sysmanager privileges (a semi-admin user) but does not have the proper role/account membership to see a

particular content item (such as the payroll report). The assigned privileges allow this user to access the Content Server Admin page, and the Content Tracker Report Generator main page. But when this user performs a standard search in Content Server, the results page would not reveal that the payroll report exists.

If the security checks preference variable is enabled, Content Tracker Reports enforces the same role/account membership checks. Then, depending on the user requesting a specific report, the role/account matching activity determines what content item usage data is included.

As demonstrated in the following examples, the report results generated for a specific user (the semi-admin user described above) are contingent upon if the preference variable is enabled or not.

- **Secure mode example:**

When the security checks preference is enabled, Content Tracker Reports is running in secure mode and checks for role/account matches. In this case, the semi-admin user is not entitled to retrieve and view confidential data. Due to the restrictions associated with this user's role/account privileges, the payroll content item remains completely invisible. The data is not included in report results and the user is unaware of its existence.

- **Non-secure mode example:**

When the security checks preference is disabled, Content Tracker Reports is running in non-secure mode and does not check for role/account matches. In this case, although the semi-admin user is not entitled to access or view the payroll report, some confidential information associated with the payroll content item can nevertheless be retrieved.

At the very least, the user can discover the payroll report's existence and view some of its metadata. The danger in this situation depends on what kind of information the metadata contains. In some cases, even knowing the content item exists could be a serious breach of security.

Note: This kind of security breach is not limited to semi-admin users. For example, a non-privileged user (that is, someone not ordinarily authorized to view a particular content item on a search results page) might gain access to the Content Tracker Report Generator main page. This could occur either by reaching the Admin page or by guessing a URL. In this case, the user would see a report containing some of the metadata describing the prohibited content item.

8.4.3.2 Pre-Defined Reports and Security Modes

Most pre-defined report queries have both secure and non-secure forms included in the contenttrackerreports_query.htm file. If the search results of a query can be affected by user role and account privileges, then secure variants of the non-secure queries are included. If the security checks variable is enabled, then the secure forms of queries take precedence and are executed instead of the corresponding non-secure queries.

It is not possible to selectively enable or disable the security checks preference variable for individual report queries. However, you can manage secure and non-secure queries by customizing the contenttrackerreports_query.htm file. you can disable security checks (account matching) for a particular query by deleting or renaming the secure form of the query.

8.4.3.3 Custom Reports and Security Modes

In addition to the pre-defined reports, you can create custom reports based on search queries tailored to specific needs. In addition to creating custom reports, selective security checks for the reports can be implemented. You can include both the non-secure and secure forms of the query in the contenttrackerreports_query.htm file.

For example, you can add a custom report with both query forms. If the non-secure query name is qMyTopTwenty, then the secure query name would be qMyTopTwenty_SEC. If the security checks preference variable is enabled, the report is generated using the secure query (qMyTopTwenty_SEC). If the security checks preference variable is not enabled, the report is generated using the non-secure query (qMyTopTwenty).

Note: The secure form of a custom query should follow the specific pattern of the existing secure queries in the contenttrackerreports_query.htm file. For more information, see [Section 8.4.3.8, "Creating Secure Report Queries."](#)

8.4.3.4 Changing the Security Configuration

Follow this procedure to manually enable or disable the SctEnableSecurityChecks setting:

1. Choose **Administration** then **Admin Server** from the Main menu.
The Content Admin Server page opens.
2. Click the name of the instance on which to change the Web beacon preference setting.
The Content Admin Server <instance_name> page opens.
3. Click **Component Manager**.
The Component Manager page opens.
4. In the Update Component configuration field, select **Content Tracker Reports** from the list.
5. Click **Update**.
The Update Component Configuration page opens.
6. In the SctWebBeaconIDList preference field, enter the applicable Web beacon object dDocNames separated by commas.
7. Click **Update**.
8. Restart Oracle WebCenter Content Server to apply the changes.

8.4.3.5 Security Mode Selection

To generate a requested report, Content Tracker Reports must select and execute the applicable non-secure or secure query.

This section covers the following topics:

- ["Query Type Selection Process"](#) on page 8-31
- ["Report Query Selection Example"](#) on page 8-32

8.4.3.5.1 Query Type Selection Process Content Tracker Reports chooses a report query based on the following process:

- When a user submits a report request, the name of that report query is fed to a dedicated Content Tracker Reports service.
- The Content Tracker Reports service enforces the security checks setting as follows:
 - **If the security checks preference is disabled:**

Content Tracker Reports is running in non-secure mode and does not perform role/account matching (user role and account privilege verification). The Content Tracker Reports service searches for the non-secure version of the query and uses it to generate the requested report. It is irrelevant if there is a secure version of the report query.

In non-secure mode, only non-secure queries are used to generate reports. As a result, all users see the same report results regardless of their individual role and account memberships.
 - **If the security checks preference is enabled:**

Content Tracker Reports is running in secure mode and performs role/account matching (user role and account privilege verification).

To begin processing:

The Content Tracker Reports service appends the "_SEC" suffix to the submitted query name and searches the contenttrackerreports_query.htm file for this variant of the requested query.

During the search:

 - * If the secure form of the query is found, then it is used to generate the requested report.

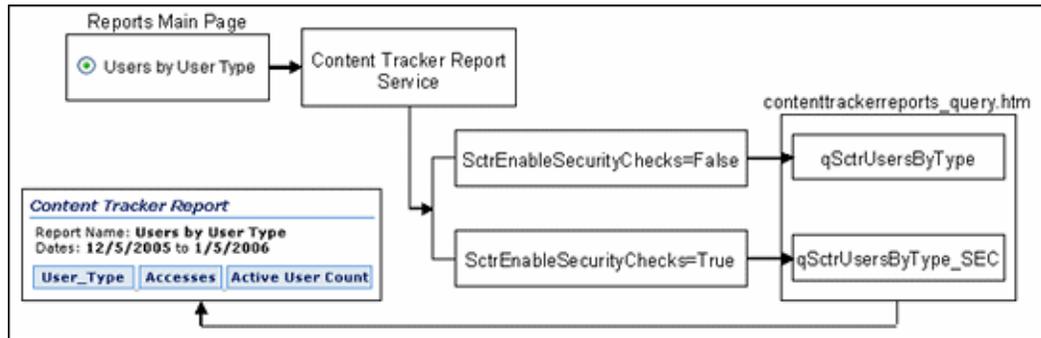
This means that the security checks to enforce role/account matching are performed and the query results are limited by the role and account privileges of the user requesting the report. Accordingly, different users may see different data results.
 - * If the secure form of the query is not found, then the non-secure variant is used.

This actually produces the same result as if the security checks preference was disabled. This means, role/account permissions are not authenticated and the content item data is not filtered. Thus the results included in reports are identical for all users. It is possible for users without proper permissions to view confidential information.

8.4.3.5.2 Report Query Selection Example When a user requests the User Type report:

1. The report query name (qSctrUsersByType) is passed to the Content Tracker Reports service.
2. The Content Tracker Reports service evaluates the request based on the security checks preference variable:
 - a. If security checks are disabled (set to false), then the service finds the qSctrUsersByType query in the contenttrackerreports_query.htm file.
 - b. If security checks are enabled (set to true), then the service adds a security suffix to the query name (qSctrUsersByType_SEC) and searches for this variant in the contenttrackerreports_query.htm file.

- Depending on the security checks status, Content Tracker Reports uses the applicable query to generate the Users by User Type report.



8.4.3.6 Enabling or Disabling Security Checks for Report Queries

Follow these steps to disable or enable security checks (account matching) for particular report queries:

- In a text editor, open the necessary file:
 - IntradocDir*/custom/ContentTrackerReports/resources/contenttrackerreports_query.htm
- Locate the secure version of the query to disable.
- Rename the query. For example, to disable the qSctrUsersByType_SEC query, you can add the suffix "_disabled" to the query name:

qSctrUsersByType_SEC_disabled

Renaming the query ensures that the Content Tracker Reports service cannot find the secure query in the contenttrackerreports_query.htm file. Instead, the non-secure version (qSctrUsersByType) is used.

Note: Renaming a secure query is a temporary disabling solution. To use the secure version of a query later, re-enable it by restoring its original name. If you delete the secure version of the query, you must re-create the entire secure version of the query to use it again.

- Save and close the contenttrackerreports_query.htm file.
- Restart the Oracle WebCenter Content Server to apply the changes.

8.4.3.7 Customization for Report Query Security

In secure mode, Content Tracker Reports always gives priority to the secure forms of queries. If a secure form of a query is found in the contenttrackerreports_query.htm file, then it is used to generate the report instead of the corresponding non-secure query.

It is not possible to selectively enable or disable the security checks preference variable for individual report queries. However, it is possible to manage secure and non-secure queries by customizing the contenttrackerreports_query.htm file.

Customizing the report query file involves:

- Selectively enabling or disabling security checks (account matching) for specific report queries.

- Creating one or more non-secure custom report queries and, depending on the security requirements of the information, selectively including the corresponding secure version.

8.4.3.8 Creating Secure Report Queries

Follow these steps to create a secure version of a non-secure report query:

1. In a text editor, open the contenttrackerreports_query.htm file:
IntradocDir/custom/ContentTrackerReports/resources/contenttrackerreports_query.htm
2. Locate the query for which to create a secure version. For consistency, add your secure query immediately following the corresponding non-secure version.
3. Design your secure SQL report query: It might be helpful to review Step 2 in the procedure for [Creating Custom Report Queries](#).
4. Adjust your query to ensure that it follows the pattern of the existing secure queries:
 - a. In the FROM clause, include the Revisions table.
 - b. In the WHERE clause, include the %SCTR_SECURITY_CLAUSE% token. This token acts as a placeholder for the WHERE clause that the Content Tracker Reports service inserts.
 - c. Complete the query following the established pattern in the existing secure queries.
5. Save and close the contenttrackerreports_query.htm file.
6. Restart the Oracle WebCenter Content Server to apply the changes.

8.4.4 Using Content Tracker Reports

This section provides information and task procedures about Content Tracker Reports functions. It covers the following topics:

- [Section 8.4.4.1, "Generating Reports"](#)
- [Section 8.4.4.2, "Accessing Drill Down Reports"](#)
- [Section 8.4.4.3, "Accessing Reports from the Information Page"](#)
- [Section 8.4.4.4, "Viewing Access Results by Revision"](#)
- [Section 8.4.4.5, "Viewing Access Results for All Versions Combined"](#)
- [Section 8.4.4.6, "Creating Custom Report Queries"](#)

8.4.4.1 Generating Reports

Follow these steps to generate a pre-defined or custom report:

1. Choose **Administration** then **Content Tracker Reports** from the Main menu.
2. Click the report type.
3. Enter any search and filtering criteria in the applicable fields.
4. Click **Submit**.

The selected report type opens.

8.4.4.2 Accessing Drill Down Reports

Follow these steps to access one or more drill down reports:

1. Generate a pre-defined or custom report. For details, see [Section 8.4.4.1, "Generating Reports."](#)
2. After generating a pre-defined report, certain line item results contain an active drill down report link. Click the link.

The selected drill-down report opens.

Note: Some reports contain multiple levels of drill down reports. For example, the Top Content Items report contains a DocName drill down report link. Click this link to generate another report that displays the applicable content access details for the selected content item. In this report, two additional drill down reports are available: one for Accesses and another for Users.

8.4.4.3 Accessing Reports from the Information Page

Follow these steps to generate an Access History Report for a content item from the Information page of that content item:

1. Search for a content item and click the associated **Info** icon.

The Content Information page opens.

2. Select **View Access History Report** from the Global Actions list.

The most current Content Access Report for the content item opens.

3. On the Content Access Report, click **Accesses**.

The most current Accesses by Day report for the content item opens.

4. On the Content Access Report, click **Users**.

The most current Accesses by User report for the content item opens.

8.4.4.4 Viewing Access Results by Revision

By default, the access results for multiple versions of a single content item are displayed individually on the Content Dashboard. Follow these steps to see the separated access results view of the Content Dashboard report:

1. Generate a content item-based query report from the Content Tracker Report Generator main page. For details, see [Section 8.4.4.1, "Generating Reports."](#) For example, select the Top Content option on the [Content Tracker Report Generator Main Page](#) to generate the applicable report.
2. Select a content item from the results report and click the content identification number listed in the DocName column.

The Content Dashboard for the selected content item opens. By default, this view shows the access results for each revision of the selected content item that was accessed.

8.4.4.5 Viewing Access Results for All Versions Combined

Follow these steps to see the combined access results view of the content dashboard report:

1. Generate a content item-based query report from the Content Tracker Report Generator main page. For details, see [Section 8.4.4.1, "Generating Reports."](#) For example, select the Top Content option on the [Content Tracker Report Generator Main Page](#) to generate the applicable report.

2. Select a content item from the results report and click the content identification number listed in the DocName column.

The Content Dashboard for the selected content item opens.

3. Click **All Versions Together**.

The resulting content dashboard view shows the combined access results for both versions.

8.4.4.6 Creating Custom Report Queries

This section provides an example that demonstrates how to create a non-secure custom report query. This particular query generates a report that lists users and their personal attributes. The data is derived from the Oracle WebCenter Content Server's Users database table.

Note: The example in this section uses a non-secure query. Any user can view the generated report results regardless of their role and account privileges. All of the reports are generated using either non-secure or secure queries. The query selection is dependent on the security mode. For more detailed information about the optional security checks preference variable, see [Section 8.4.3, "Security Checks and Query Results."](#) To create a secure report query, see [Section 8.4.3.8, "Creating Secure Report Queries."](#)

Follow these steps to create the custom users report:

1. Design the SQL report query.
2. Enter the custom report query into the query file of Content Tracker Reports:
 - a. Navigate to the *IntradocDir/custom/ContentTrackerReports/resources* directory. Open the *contenttrackerreports_query.htm* file in a text editor.
 - b. Enter the custom report name, number of columns, and the source database table.

For example, the following excerpt from the query file illustrates that the custom query report extracts the information from all columns in the Users database table.

```
<tr>
  <td>qCustomUsers</td>
  <td>
    SELECT *
    FROM Users
  </td>
</tr>
```

3. Enter a link to the custom report in the Content Tracker Report Generator main page file:
 - a. Navigate to the *IntradocDir/custom/ContentTrackerReports/templates* directory. Open the *contenttrackerreports_main_page.htm* file in a text editor.

- b. Enter the attributes to display the link on the Content Tracker Report Generator main page.

For example, the following excerpt from the main page file illustrates that the custom report link is presented as a selectable button and is listed as the Custom Users Report link on the page.

```
<h4 class=xuiSubheading>Custom Reports</h4>
<table width=80% border=0>
  <tr>
    <td> <span class="tableEntry"><input type="radio" name="radiobutton"
value="qCustomUsers">
    Custom Users Report </span></td>
  </tr>
</table>
```

4. Enter the formatting requirements in the template resource file of Content Tracker Reports.
 - a. Navigate to the *IntradocDir/custom/ContentTrackerReports/resources* directory.
 - b. In a text editor, open the *contenttrackerreports_template_resource.htm* file.
 - c. Enter the display features to use for the generated custom report and any drill-down reports.

For example, the following excerpt from the template resource file specifies that the report title is "Deanna's First Report" and that the drill-down report is based on the content items seen by user report.

```
<!-- Custom Template -->
<@dynamichtml qCustomUsers_vars@>
  <$reportWidth = "100%"$>
  <$title = "<i>Content Access Report</i>"$>
  <$reportTitle="Deanna's First Report"$>
  <$column1Width="35%"$>
  <$column0Drill="qSctrDocsSeenByUser_Drill"$>
<@end@>
```

5. Restart the Oracle WebCenter Content Server to apply the changes.

8.5 Troubleshooting

Content Tracker has two execution trace mechanisms: the Web server filter plug-in and the Java code. These are intended for diagnosing problems at customer installations and are not to be used in production.

Hanging browser: If Oracle WebCenter Content Server terminates while the Data Engine Control Center is running, the browser can also hang. To resolve the issue, close the browser window.

This section covers the following topics:

- [Section 8.5.1, "Web Server Filter Plug-in Debugging Support"](#)
- [Section 8.5.2, "Java Code Debugging Support"](#)
- [Section 8.5.3, "DataBinder Dump Facility"](#)

8.5.1 Web Server Filter Plug-in Debugging Support

The Web server filter plug-in honors `PLUGIN_DEBUG`. Enable `PLUGIN_DEBUG` on the Filter Administration page and the Content Tracker Web server filter plug-in issues execution trace information. The trace is only meaningful to someone with access to the source. Customers with a problem are expected to enable `PLUGIN_DEBUG`, run the test scenario, then send the log segments to Customer Service for evaluation. Otherwise, turn `PLUGIN_DEBUG` off.

Follow these steps to set `PLUGIN_DEBUG`:

1. Choose **Administration** then **Admin Applets** from the Main menu.
2. Click **Filter Administration**.
The Configure Web Server Filter Plug-in page opens.
3. Select `PLUGIN_DEBUG`.
4. Click **Update**.

8.5.2 Java Code Debugging Support

Use the System Audit functionality in Oracle WebCenter Content Server for debugging support. See "System Audit Information" in the *Oracle WebCenter Content System Administrator's Guide for Content Server* for more details. Add `contenttracker` to the Active Sections list. When the list is updated, the Content Tracker execution trace information appears with the other active sections.

8.5.3 DataBinder Dump Facility

When Content Tracker records a specific service in the log file, it records the contents of the service's DataBinder object in a serialized dump file. The contents of these files are useful for debugging field maps that use the extended service call tracking function. These dump files allow you to see the available LocalData fields for the recorded service.

The Content Tracker service handler filter only creates dump files for DataBinder objects if the associated services are defined in the `SctServiceFilter.hda` file.

Caution: The dump files for DataBinder objects continue to accumulate until manually deleted. Use the `SctDebugServiceBinderDumpEnabled` configuration variable only as necessary.

Set the `SctDebugServiceBinderDumpEnabled` configuration variable to true to configure the service handler filter to write out the objects into dump files. See the *Oracle WebCenter Content Idoc Script Reference Guide* for more details about Tracker configuration variables.

The files are stored in the `/ContentTracker/DEBUG_BINDERDUMP` directory. File names consist of three parts: `service_name_filter_function_serial_number.hda`

- `service_name` is the name of the logged service (such as, `GET_FORM_FILE`).
- `filter_function` is one of the following:
 - End: Filter Event on EndServiceRequestActions. Normal end-of-service event.

- EndSub: FilterEvent on EndScriptSubServiceActions. Normal end-of-service for service called as SubService.
- Error: Filter Event on ServiceRequestError. End of service where an error occurred. Can happen in addition to End.
- *serial_number* is the unique identification number assigned to the file. Content Tracker can create multiple DataBinder object dump files for a given service.

Example:

GET_SEARCH_RESULTS_End_1845170235.hda

Using Content Categorizer

Content Categorizer is an optional component that is automatically installed with Oracle WebCenter Content Server. When enabled, Content Categorizer suggests metadata values for new documents checked in to Oracle WebCenter Content Server, and for existing documents that have or do not have metadata values. These metadata values are determined according to search rules provided by the System Administrator.

The Batch Categorizer that is included with the component can search a large number of files and create a Batch Loader control file containing appropriate metadata field values. The Batch Categorizer can also be used to recategorize content checked in to the repository.

This chapter covers the following topics:

- [Section 9.1, "Content Categorizer Functionality"](#)
- [Section 9.2, "Setting Up Content Categorizer"](#)
- [Section 9.3, "Search Rules"](#)
- [Section 9.4, "Sample doc_config.htm Page"](#)
- [Section 9.5, "XSLT Transformation"](#)

9.1 Content Categorizer Functionality

For Content Categorizer to recognize structural properties, the content must go through [XML Conversion](#) (eXtensible Markup Language). The conversion method is defined in the `sccXMLConversion` configuration variable. Content Categorizer uses [Search Rules](#) to suggest metadata values for content.

This section covers the following topics:

- [Section 9.1.1, "XML Conversion"](#)
- [Section 9.1.2, "Search Rules Overview"](#)
- [Section 9.1.3, "Using Content Categorizer"](#)

9.1.1 XML Conversion

Important: There is a problem with the XSLT transformation used to post-process PDF content converted using the Flexiondoc schema. When Flexiondoc schema are used, single words are assigned to individual XML elements, making the final XML unusable. It is necessary to use SearchML for categorizing PDF content.

Regardless of which XML converter is specified, the XML intermediate files are used only by Content Categorizer, so they are discarded after use, and documents are checked in to Oracle WebCenter Content Server in their original source form. The only exception is content that is in XML format, which is not subjected to the translation process.

With each converter, the OutsideIn XML Export technology is used in combination with a custom XSLT style sheet (flexiondoc_to_scc.xsl) to produce XML in a two-stage process. In the first stage, the native document is converted to either Flexiondoc-formatted XML or SearchML-formatted XML.

In the second stage, the style sheet is used to further refine the XML so that it is searchable by Content Categorizer. Native document properties and text segments are isolated in XML elements, which are named after the corresponding document property, paragraph style, or character style (note that character styles are not supported by SearchML).

9.1.2 Search Rules Overview

Content Categorizer executes search rules depending on the type of rule defined:

- **Pattern Matching and Abstract Rules:** Content Categorizer scans a content document looking for "landmarks." A landmark can be specific text, or it can be based on structural properties of the source document, such as styles, fonts, and formatting.
- **Option List Rule:** Content Categorizer searches for keywords whose cumulative score determines which option of a list is selected. It does not look for either landmarks or specific XML tags.
- **Categorization Engine Rule:** Content Categorizer invokes a 3rd-party categorizer engine and taxonomy to categorize a content item.
- **Filetype Rule:** Content Categorizer looks for the document file type (the filename extension).

Normally, a user-entered value on the Content Check In Form prevents Content Categorizer from applying the search rules for that field. This is also true for list fields that have a default value, such as the Type field.

Important: It is important to instruct contributors to leave any fields blank that they want to have filled by search rules.

For more details about search rules, see [Section 9.3, "Search Rules."](#)

9.1.3 Using Content Categorizer

The following tasks must be done to run Content Categorizer:

- Define the XML Conversion method. For details, see [Section 9.2.1, "Setting XML Conversion Method."](#)
- Define search rules. For details, see [Section 9.3.3, "Defining Search Rules."](#)
- Optional: Define field properties, including default values for metadata fields. For more details, see [Section 9.2.2, "Defining Field Properties \(Optional\)."](#)

Important: To use the CATEGORY search rule, install, set up and register a categorizer engine before defining the CATEGORY rule for any metadata fields.

9.1.3.1 Operating Modes

Content Categorizer can operate in either Interactive mode or Batch mode. All modes require conversion of the source documents into XML intermediate form. However, the process flows of the modes are distinctly different.

- **Batch** mode is used when recategorizing large numbers of documents in the repository. The system administrator uses a standalone utility to run Content Categorizer, then either performs a live update of content metadata or uses the output file from Batch Categorizer as input to the Batch Loader. For details about the steps used during this process, see [Section 9.1.3.1.1, "Running Batch Mode."](#)
- **Interactive** mode integrates Content Categorizer with the Content Check In Form and Info Update Form. Users click **Categorize** on the form to run Content Categorizer on a single content item. Any value that is returned by Content Categorizer is a suggested value, because the contributor can edit or replace the returned value. For details about the steps taken during this process, see [Section 9.1.3.1.2, "Interactive Mode Process."](#)

9.1.3.1.1 Running Batch Mode

The `MaxQueryRows` configuration variable is used to specify the maximum number of documents that can be included in a single batch load process. As such, it affects how many documents a user sees in Batch Categorizer. The default setting for this configuration variable is 200 but can be decreased or increased as necessary. See the *Oracle WebCenter Content Idoc Script Reference Guide* for details about the variable.

The system administrator performs the following steps during the batch mode process:

1. Run the Batch Categorizer application. See the *Oracle WebCenter Content System Administrator's Guide for Content Server* for details about running applications on UNIX systems.

The [Batch Categorizer Screen](#) opens.

2. If necessary, define filters and release date information to display a list of content to be categorized. Click **Categorize**.

The [Categorize Existing Screen](#) opens.

3. Select **Live Update** or **Batch Loader**.

- The Live Update option updates the data in the repository immediately.
- The Batch Loader option is used to create a control file, which is the output of the Content Categorizer process. The file contains an entry for each source document, and contains the values for each metadata field based on the search

rules defined in Content Categorizer. You can edit this file before submitting it to the Batch Loader.

4. To run the Batch Loader utility automatically after the Content Categorizer process is complete, select the **Run Batch Loader** check box.
5. Enter the location and file name for the log file that contains error information about the Content Categorizer process.
6. Choose **Categorize All** to work with all content items or **Categorize Selected** to use only the highlighted items in the content list.
7. Choose to categorize the **Latest Revision**, which works with only the most recent revision of an item, or **All Revisions**.
8. Choose to continue or discontinue the categorization process when Batch Categorizer encounters an error.
9. Click **OK**. The Progress bar shows the progress as the batch process moves through its steps:
 - a. Content Categorizer locates the source content.
 - b. If the content is in XML format, no translation occurs, and the process continues at step d.
 - c. If the content is not in XML format, conversion into XML occurs using the selected XML conversion method: Flexiondoc or SearchML.
 - d. Content Categorizer applies the search rules to the XML and obtains values for the specified metadata fields.
 - e. If Live Update was specified, database records are updated immediately. If Batch Loader was specified, an output control file is created, and the Batch Loader utility is run, if the option to do so after processing was specified.
10. When the batch process is complete, review the error logs. Errors encountered by Batch Categorizer are displayed on the console and also recorded in the Batch Categorizer log (if specified). Errors encountered by Batch Loader are displayed on the console and also recorded in the system log.

If the optional AddCCToArchiveCheckin component is installed and enabled, all content loaded using the Batchloader utility is categorized automatically, based on predefined rule sets. For more information about defining rule sets, see [Section 9.3.3, "Defining Search Rules."](#)

9.1.3.1.2 Interactive Mode Process

The following steps occur during the check-in process:

1. A contributor opens the Content Check In Form or the Info Update Form, selects a primary file (only on Content Check In Form), and clicks **Categorize**.
2. The Content Check In Form copies the primary file to the host and calls the Content Categorizer service.
3. Content Categorizer locates the source content.
4. If the content is in XML format, no translation occurs, and the process continues at step 6.
5. If the content is not in XML format, the specified conversion method is used.
6. Content Categorizer applies the search rules to the XML and obtains suggested values for the specified metadata fields.

7. Content Categorizer inserts the suggested metadata values into the Content Check In Form or Update Info Form, and returns the form to the contributor.
8. The contributor can check in or submit the document with the suggested values, revise the metadata values, or cancel the check in or update.

If the optional AddCCToNewCheckin component is installed and enabled, when you click **Check In** on the Content Check In Form, it performs steps 2 through 6 and completes the check in process, provided the properties for dDocTitle are set to **Override Contents**.

If the properties of dDocTitle are not set to Override Contents, then an alert is displayed requesting that the required field is completed. Field properties are set using the CC Admin Applet. For more details, see [Section 9.2.2, "Defining Field Properties \(Optional\)."](#)

9.2 Setting Up Content Categorizer

Before using Content Categorizer, install and configure the necessary software. This section discusses those tasks:

- [Section 9.2.1, "Setting XML Conversion Method"](#)
- [Section 9.2.2, "Defining Field Properties \(Optional\)"](#)

9.2.1 Setting XML Conversion Method

Follow these steps to set the XML conversion method in Content Categorizer:

1. Choose **Administration** then **Content Categorizer Administration** from the Main menu.
The [Content Categorizer Administration Page](#) opens.
2. Click **Configuration**.
The [Configuration Tab](#) opens.
3. Select the **sccXMLConversion** property and click **Edit** or double-click the property.
The [Property Config Screen](#) opens.
4. From the list, select either Flexiondoc or SearchML as the XML conversion method.
5. Click **OK**.
6. Click **Apply** to save the changes.

9.2.2 Defining Field Properties (Optional)

When any rule for a field succeeds, the found value is used (in either Batch Loader operations or Live Update operations). However, depending on how the Override value is set, the found value does not override the existing value (Override is set to false).

When all rules for a field fail, no value is assigned to the field unless a default value is defined for the field and Use Default is set to true.

Follow this procedure to define field properties for the metadata fields:

1. Choose **Administration** then **Content Categorizer Administration** from the Main menu.
The [Content Categorizer Administration Page](#) opens.
2. Click the **Field Properties** tab.
3. Select a metadata field to be edited and click **Edit**, or double-click the field.
The [Field Properties Screen](#) opens.
4. Enter a default value for the field.
The default value for a list field must match a value available for that field.
5. Select the Override check box for the value returned by the categorization process to override an existing value for the field.
6. Select the Use Default check box for the field's default value to be used if all rules fail (or are not defined) when the categorization process runs.
7. Click **OK**.
8. Repeat these steps for each field to be edited.
9. Click **Save Settings** to save the changes.

9.3 Search Rules

Search rules define how Content Categorizer determines metadata values to return to the Content Check In Form or Info Update Form (for Interactive mode) or the batch file (for Batch mode).

Every search rule is defined by:

- A **rule type**, which determines the method that Content Categorizer uses to search the XML document.
- A **key**, which defines the XML element, phrase, or keyword that Content Categorizer looks for in the document, or the categorization engine/taxonomy that Content Categorizer uses to classify the document.
- A **count**, which is used to refine the search criteria.

This section covers the following topics:

- [Section 9.3.1, "Search Rule Guidelines"](#)
- [Section 9.3.2, "Search Rule Types"](#)
- [Section 9.3.3, "Defining Search Rules"](#)

9.3.1 Search Rule Guidelines

Consider the following guidelines when creating search rules:

- You can apply search rules to any custom metadata field.
- You can apply search rules to the Title, Comments, and Type standard metadata fields. You cannot define search rules for any other standard metadata fields (such as Author, Security Group, and Account).
- You can define multiple search rules for a metadata field. (For a single metadata field, however, multiple CATEGORY rules referring to different taxonomies are not supported.)

- Multiple search rules are run in the order specified, so that if a search rule does not result in a suggested value, the next rule is run. Arrange the list from most to least specific.
- You can mix search rule types within a metadata field. For example, you can define an Option List rule, a Pattern Matching rule, and an Abstract rule for the same metadata field.
- If none of the search rules specified for a metadata field can be satisfied, the field is left blank.

9.3.2 Search Rule Types

You can use the following rules to derive metadata:

- [Section 9.3.2.1, "Pattern Matching Search Rules"](#)
- [Section 9.3.2.2, "Abstract Search Rules"](#)
- [Section 9.3.2.3, "Option List Search Rule"](#)
- [Section 9.3.2.4, "Categorization Engine Search Rule"](#)
- [Section 9.3.2.5, "Filetype Search Rule"](#)

9.3.2.1 Pattern Matching Search Rules

Pattern Matching search rules look for specific text or a specific XML element and return an associated value. For example, the *Invoice #* metadata field contain the value that follows an *Invoice:* or *Invoice Number:* label in the source document, or it can contain the value that is within the `<Invoice>` tag in the XML document.

There are two general *types* of Pattern Matching rules: Tag Search and Text Search. Within each type are several sub-types.

- Tag Search searches for the full name of an XML element that matches the key. If such an element is found, the text contained in the element is returned as the result. Tag searches are case sensitive. Sub-types include the following:
 - TAG_TEXT
 - TAG_ALLTEXT
- Text Search searches for text that matches the key. If such text is found, the text near or following the key is returned as the result. Text searches are not case sensitive. Sub-types include the following:
 - TEXT_REMAINDER
 - TEXT_FULL
 - TEXT_ALLREMAINDER
 - TEXT_ALLFULL
 - TEXT_NEXT
 - TEXT_ALLNEXT

The *key* for a Pattern Matching search rule is either an XML element (for a Tag Search) or a text phrase (for a Text Search).

The *count* for a Pattern Matching search rule defines the number of tags or text phrases that must be matched before the rule returns results. For example, a count of 4 looks for the fourth occurrence of the key. If only three occurrences of the key are found in

the document, the rule fails. The default count of 1 returns the first occurrence of the key.

The following examples illustrate the use of the Pattern Matching search rules.

Example: TAG_TEXT

This rule searches for the full name of an XML element that matches the key (including case). If such an element is found, all text that belongs to the element is concatenated and returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TAG_TEXT
- **Key:** TAG_A
- **Returns:** Title: The Big Wolf

Example: TAG_ALLTEXT

This rule searches for the full name of an XML element that matches the key (including case). If such an element is found, all text that belongs to the element, and to all children of the element, is concatenated and returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TAG_ALLTEXT
- **Key:** TAG_A
- **Returns:** Title: The Big Bad Wolf

Example: TEXT_REMAINDER

This rule searches for text that matches the key (except for case). If such text is found, any text following the key that belongs to the same XML element is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_REMAINDER
- **Key:** Title:
- **Returns:** The Big Wolf

Example: TEXT_ALLREMAINDER

This rule searches for text that matches the key (except for case). If such text is found, any text following the key that belongs to the same XML element, and to all children of the element, is returned as the result.

- **Content:** TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLREMAINDER
- **Key:** Title:
- **Returns:** The Big Bad Wolf

Example: TEXT_FULL

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the same XML element, including the key text, is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_FULL
- **Key:** Title:
- **Returns:** Title: The Big Wolf

Example: TEXT_ALLFULL

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the same XML element, including the key text and any text belonging to children of the element, is returned as the result.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLFULL
- **Key:** Title:
- **Returns:** Title: The Big Bad Wolf

Example: TEXT_NEXT

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the next non-blank XML element is returned as the result. Blank elements and elements composed of non-printing characters are not selected as the return value.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_NEXT
- **Key:** Title:
- **Returns:** Subtitle: A Play

Example: TEXT_ALLNEXT

This rule searches for text that matches the key (except for case). If such text is found, any text that belongs to the next non-blank XML element, and to all children of the element, is returned as the result. Blank elements and elements composed of non-printing characters are not selected as the return value.

- **Content:** <TAG_A>Title: The Big <TAG_B>Bad</TAG_B> Wolf</TAG_A>
<TAG_C>Subtitle: A <TAG_D>Morality</TAG_D> Play</TAG_C>
- **Rule:** TEXT_ALLNEXT
- **Key:** Title:
- **Returns:** Subtitle: A Morality Play

9.3.2.2 Abstract Search Rules

Abstract search rules look for an XML element and return a descriptive sentence or paragraph from that element. For example, the *Summary* metadata field could be filled by a returned value of "Germany is a large country in size, culture, and worldwide economics. One of Germany's largest industries includes the manufacturing of world class automobiles like BMW, Mercedes, and Audi."

The Abstract rule type is useful where there is no readily identifiable or explicitly tagged block of text in the content item. Typically, these rules are used to suggest summary or topic information about the document.

There are two *types* of abstract search rules: First Paragraph and First Sentence.

- First Paragraph searches for the full name of an XML element that matches the key. The entire paragraph of the first such element that meets the size criteria (specified by the count) is returned as the result.
- First Sentence searches for the full name of an XML element that matches the key. If such an element is found, the first sentence of the element is returned as the result.

The *key* for an Abstract search rule is an XML element.

The *count* is interpreted differently for the First Paragraph and First Sentence search rules.

- For a First Paragraph search rule, the count is a size threshold measured in percent:
 1. The rule searches the document for all paragraphs that match the key.
 2. The rule calculates the average size (based on character count) of the paragraphs that match the key.
 3. The rule multiplies the average size by the count percentage (0 = 0%, 100 = 100%).
 4. The rule looks for the first paragraph larger than the resulting number.

For example, if the count is set to 75 and the average paragraph size is 100 characters, the rule returns the first paragraph larger than 75 characters that matches the key.

If the count is set to the default of 1, the rule is likely to return the first paragraph that matches the key.

- For a First Sentence search rule, the count is the number of elements that have their first sentences returned.

For example, if the count is set to 3, the rule returns the first sentence from each of the first three elements that match the key.

The following examples illustrate the use of the Abstract search rules.

Example: FIRST_PARAGRAPH

This example returns the first <Text> element that exceeds one-half the average <Text> element paragraph size. Note that the <Title> element does not match the key value, so it is ignored for both the search and for the average length calculation.

- **Content:** <Title>Poem</Title>
 <Text>Mary had</Text>
 <Text>a little Lamb</Text>

<Text>The fleece was white as snow</Text>

<Text>And everywhere that Mary went the lamb was sure to go</Text>

- **Rule:** FIRST_PARAGRAPH
- **Key:** Text
- **Count:** 50
- **Returns:** The fleece was white as snow.

Example: FIRST_SENTENCE

This example returns the first sentence of the first two <Text> elements. Note that the <Title> element does not match the key value, so it is excluded from the search.

- **Content:** x<Title>Barefoot in the Park</Title>
 - <Text>See Dick run. See Jane run. See Dick and Jane.</Text>
 - <Text>See Spot run. See Puff chase Spot.</Text>
 - <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** FIRST_SENTENCE
- **Key:** Text
- **Count:** 2
- **Returns:** See Dick run. See Spot run.

9.3.2.3 Option List Search Rule

The Option List search rule looks for keywords within the source document, applies a score for each keyword found, and returns the value that has the highest keyword score.

For example, if the keywords *margin*, *SEC filing*, or *invoice* were found in a document, the suggested value for the *Department* field would be *Accounting*, while the keywords *tolerance*, *assembly*, or *inventory* would return *Manufacturing* as the suggested value.

- The Option List search rule usually applies to metadata fields that have a list defined in the Configuration Manager.
- Option list names and values (called **categories** in Content Categorizer) appear in Content Categorizer as specified in the Configuration Manager. If a custom list field is created or changed while the CC Admin Applet is open, close and reopen the applet to see the changes.
- The current version of Oracle WebCenter Content Server automatically inserts a blank value as the default value in a custom list field. In this case, the first value (by default, a blank value) is not considered a user-entered value, and the Option List search rule is applied. To prevent the Option List search rule from overriding the first value in a custom list field, provide a default value for that list on the Configuration Manager Applet.

There is one *type* of Option List search rule, which searches for keywords (single words or phrases) that match the keywords defined in the key.

- Keywords can be single words (for example, *dog*) or multiple-word phrases (for example, *black dog*).
- Keywords can use the following defined set of operators to further refine a search:
 - \$\$AND\$\$

- \$\$OR\$\$
- \$\$AND_NOT\$\$
- \$\$NEAR\$\$
- Keywords are pre-assigned to each category (value) in the list, and each keyword has a weight assigned to it. For details, see [Section 9.3.3.2, "Defining Option List Keywords."](#)
- The number of occurrences of each keyword found in the document is multiplied by its weight, resulting in a keyword score.
- The keyword scores for each category are added, resulting in a category score.
- The category with the highest score is returned as the suggested value.
- If there is a tie between categories, the category earliest in the list is returned as the suggested value.
- Use the weights *Always* and *Never* to override the scores and count threshold.
 - An occurrence of a keyword with the *Always* weight forces the category to be returned as the suggested value, regardless of score.
 - An occurrence of a keyword with the *Never* weight disqualifies the category from being returned as the suggested value, regardless of score.
 - If two categories have keywords assigned the *Always* weight, and both keywords occur in the document, the keyword first found in the document takes precedence.

Important: Option List searches are case sensitive and must match exactly. For example, *Invoice*, *Invoices*, *invoice*, and *invoices* must be defined to retrieve all instances of this keyword.

The *key* for an Option List search rule is the Option List name, as shown on the **Option Lists** tab of the Admin Applet.

The *count* for an Option List search rule sets a minimum threshold score for the rule to return results. For example, if the count is set to 50, and the highest accumulated keyword score is 45, the rule fails.

The following examples illustrate the use of the Option List search rule.

Example 1: Option List

In this example, the score for *Dick* and *Spot* is 30 (3 occurrences x 10), and the score for *Jane* and *Puff* is 20 (2 occurrences x 10). *Dick* is returned as the suggested value because it is earlier in the list than *Spot*:

- **Content:** <Title>Barefoot in the Park</Title>
<Text>See Dick run. See Jane run. See Dick and Jane.</Text>
<Text>See Spot run. See Puff chase Spot.</Text>
<Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacter
- **Count:** 10

- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2
Jane: Jane=10, girl=5, Janie=2
Spot: Spot=10, dog=5
Puff: Puff=10, cat=5
- **Returns:** Dick

Example 2: Option List

In this example, *Spot* is returned as the suggested value because its score of 60 (3 occurrences x 20) is higher than the other categories:

- **Content:** <Title>Barefoot in the Park</Title>
<Text>See Dick run. See Jane run. See Dick and Jane.</Text>
<Text>See Spot run. See Puff chase Spot.</Text>
<Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacter
- **Count:** 10
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2
Jane: Jane=10, girl=5, Janie=2
Spot: Spot=20, dog=10
Puff: Puff=10, cat=5
- **Returns:** Spot

Example 3: Option List

In this example, the rule fails because none of the scores is above the Count threshold of 50:

- **Content:** <Title>Barefoot in the Park</Title>
<Text>See Dick run. See Jane run. See Dick and Jane.</Text>
<Text>See Spot run. See Puff chase Spot.</Text>
<Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacter
- **Count:** 50
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2
Jane: Jane=10, girl=5, Janie=2
Spot: Spot=10, dog=5
Puff: Puff=10, cat=5
- **Returns:** Fail

Example 4: Option List

In this example, *Puff* is returned as the suggested value because the keyword "Puff" has a weight of Always:

- **Content:** <Title>Barefoot in the Park</Title>
 <Text>See Dick run. See Jane run. See Dick and Jane.</Text>
 <Text>See Spot run. See Puff chase Spot.</Text>
 <Text>See Dick chase Spot and Puff.</Text>
- **Rule:** OPTION_LIST
- **Key:** MainCharacter
- **Count:** 10
- **Option List Categories, Keywords, and Weight:** Dick: Dick=10, boy=5, Richard=2
 Jane: Jane=10, girl=5, Janie=2
 Spot: Spot=10, dog=5
 Puff: Puff=Always, cat=5
- **Returns:** Puff

9.3.2.4 Categorization Engine Search Rule

The Categorization Engine search rule uses a 3rd-party categorizer engine and defined taxonomy to determine and return a value that represents a category within the specified taxonomy, for example, News/Technology/Computers.

There is one *type* of Categorization Engine search rule, which uses the categorizer engine and taxonomy specified in the Key to return a value for the field.

The *key* for a Categorization Engine search rule is the name of the categorizer engine followed by the name of the taxonomy. For example, *EngineName/TaxonomyName*. If an engine name is defined in the Key field, Content Categorizer defaults to the first engine displayed in the Categorizer Engines list. If only one engine is defined, just enter the taxonomy name in the Key field.

The *count* for a Categorization Engine search rule sets a minimum confidence level threshold for the returned results.

When a categorization engine returns a category (or set of categories) for a given query, a confidence level is also returned, which is often expressed as a percentage for each category. The Category rule always accepts the highest-confidence category, **unless** the confidence level is below the count value specified for the rule, in which case the rule fails. For example, if the count is set to 50, and the highest-confidence category returned is 45, the rule fails.

The default count of 1 would always accept the highest-confidence category returned by the categorizer engine. The actual range for the Count value depends on the categorizer engine that is being used.

9.3.2.5 Filetype Search Rule

The Filetype search rule looks at the filename extension of a document and returns a term, usually a file type description associated with the filename extension.

There is one *type* of Filetype search rule, which uses the filename extension of the primary (native) file to return a value for the field.

When the Filetype search rule is defined for a metadata field, the filename extension of the content item is matched against all values in the DocFormatsWizard table. This table is found in the file doc_config.htm, which is located in the *IntradocDir/shared/config/resources/* directory.

If a match is found, the associated value in the Description column is extracted and translated. The resulting string is returned as the suggested metadata value for the field. If the primary file path has no extension, or if the extension does not match any of the "extensions" values in the DocFormatsWizard table, the rule fails and the next rule in the list for the metadata field is executed.

The *key* for a FILETYPE search rule is not used when determining a metadata value. **Leave the Key field blank.**

The count for a FILETYPE search rule is not used when determining a metadata value. **Leave the Count field blank.**

If a FILETYPE rule is created with non-blank Key or Count fields, a warning message is displayed indicating that these fields are not supported by the rule.

The following examples illustrate the use of the Filetype Search rule.

Example 1: Filetype Search

- **Primary File:** policies.doc
- **Rule:** FILETYPE
- **Key:** blank
- **Count:** blank
- **Returns:** Microsoft Word Document

Example 2: Filetype Search

- **Primary File:** procedures.wpd
- **Rule:** FILETYPE
- **Key:** blank
- **Count:** blank
- **Returns:** Corel WordPerfect Document

9.3.3 Defining Search Rules

During startup, Content Categorizer takes a snapshot of the current metadata field configuration including field names and lengths. If the metadata field configuration changes, restart Oracle WebCenter Content Server before running the Content Categorizer Admin Applet to add or modify any search rules.

Important: Content Categorizer requires a non-empty rule set for any file type (.doc, .txt, .xml, and so on) it is called to examine. If no rules exist for a given file type, Content Categorizer throws an exception. The easiest way to protect against this is to add at least one rule to the Default rule set. The Default rule set is used for all file types which do not have a custom rule set assigned.

This section covers the following topics:

- [Section 9.3.3.1, "Creating a Search Rule"](#)
- [Section 9.3.3.2, "Defining Option List Keywords"](#)
- [Section 9.3.3.3, "Applying Rules to the Type Field"](#)

9.3.3.1 Creating a Search Rule

Follow these steps to define search rules for any metadata field:

1. Choose **Administration** then **Content Categorizer Administration** from the Main menu.

The [Content Categorizer Administration Page](#) opens.

2. Click the [Rule Sets Tab](#).

3. In the Ruleset pane, select the ruleset from the list, or click **Add** to add a new ruleset. A ruleset contains multiple rules that apply to specific documents or a particular document type. If a specific ruleset is not defined for a given document or document type, the default ruleset is used.

If adding a ruleset, a dialog screen opens where you can enter the name for the ruleset.

4. Select a metadata field from the **Field** list.

5. Click **Add**.

The [Add/Edit Rule for Field Screen](#) opens.

6. Select the rule type from the **Rule** list.

7. Enter the search rule key in the **Key** field. For more information about types and sub-types, see [Section 9.3.2, "Search Rule Types."](#)

If CATEGORY is used, enter the categorization engine name (if there are multiple items in list of Categorizer Engines), followed by slash (/), followed by taxonomy name. For example: *EngineName/TaxonomyName*

For an OPTION_LIST search rule, keywords for the list must be defined on the **Option List** tab. For more information, see [Section 9.3.3.2, "Defining Option List Keywords."](#)

8. Enter the count in the **Count** field. For TAG and TEXT types, this is the number of tags or text phrases that must be matched before the rule returns results. For example, a count of 4 looks for the fourth occurrence of the key.

If only three occurrences of the key are found in the document, the rule fails. The default count of 1 returns the first occurrence of the key.

For FIRST_PARAGRAPH, this is the size threshold measured in percent. The first paragraph matching the key that is larger than the count percentage multiplied by the average paragraph size is returned. For example, if the count is set to 75 and the average paragraph size is 100 characters, the rule returns the first paragraph larger than 75 characters that matches the key. If the count is set to the default of 1, the rule is likely to return the first paragraph that matches the key.

For FIRST_SENTENCE, this is the number of elements that have their first sentences returned. For example, if the count is set to 3, the rule returns the first sentence from each of the first three elements that match the key.

For CATEGORY, this is the minimum confidence level threshold for the rule to return results. For example, if the count is set to 50, and the highest-confidence category has a confidence level of 45, the rule fails.

9. Click **OK** when done.
10. Add search rules to each metadata field as necessary.
 - To delete a rule, select the rule in the **Rules List** and click **Delete**.
 - To edit a rule, select the rule in the **Rules List** and click **Edit**.
 - To adjust the order of the rules, select the rule in the **Rules List** and click **Move Up** or **Move Down**. Rules are applied in the order listed. If the first rule succeeds, no other rules are applied. If the first rule fails, then the next rule is applied, and so forth.

Important: If a CATEGORY rule is added, edited, or deleted, a dialog prompts you to apply the changes and build, rebuild, or check for orphaned query trees for this rule on the **Query Trees** tab.

11. Click **Apply** to save the changes, or click **OK** to save the changes and close the [Content Categorizer Administration Page](#).

9.3.3.2 Defining Option List Keywords

To define the keywords and weights for a list:

1. Choose **Administration** then **Content Categorizer Administration** from the Main menu.
The [Content Categorizer Administration Page](#) opens.
2. Click the [Option Lists Tab](#).
3. Select a list from the **Option List**. The list includes the Type (\$DocType) list, plus lists of all custom metadata fields that have a list defined in the Configuration Manager.

Caution: When a list metadata field is deleted from the Configuration Manager, the field is removed from the **Rule Sets** tab, but it still appears in the Option List list on the **Option Lists** tab. Be careful not to select an obsolete list.

4. Select a value from the Category list. Only the pre-defined values for the list are included.
5. Enter a keyword or phrase in the Keyword field. Option List searches are case sensitive and must match exactly.
 - Keywords can be single words or multiple-word phrases.
 - Keywords can include Boolean-type expressions, where the following set of binary operators are valid: \$\$AND\$\$, \$\$OR\$\$, \$\$AND_NOT\$\$, \$\$NEAR\$\$
6. Select a weight for the keyword.
 - **Always:** If the keyword is found, the selected category is returned as the suggested value, regardless of the score.
 - **Weight:** This number multiplied by the number of occurrences of the keyword is the category's score. The category with the highest score is returned as the suggested value for the list field.

- Never: If the keyword is found, the selected category is not returned as the suggested value, regardless of the score.
7. Click **Add**.
 8. Enter keywords for each category in the selected list.
 - To delete a keyword, select the keyword in the Keywords list and click **Delete**.
 - To edit a keyword, select the keyword in the Keywords list, click **Edit**, edit the keyword, the weight or both, and click **Update**.
 9. Click **Apply** to save the changes, or click **OK** to save the changes and close the screen.

9.3.3.3 Applying Rules to the Type Field

You can configure the configuration file so Content Categorizer ignores the **Type** default value and applies search rules to the **Type** field.

This procedure applies only to the **Type** (dDocType) field. You cannot apply search rules to the other standard list fields (Security Group, Author, and Account).

To apply search rules to the Type field:

1. Open the config.cfg file located in the *IntradocDir/config/* directory in a text-only editor such as WordPad.
2. Add the following line to the file:


```
ForceDocTypeChoice=true
```
3. Save and close the file.
4. Stop and restart Oracle WebCenter Content Server.

9.4 Sample doc_config.htm Page

The following is a sample doc_config.htm page.

```
<@table DocFormatsWizard@>
```

dFormat	Extensions	dConversion	dDescription
application/ corel-wordperfect, application/wordperfect	wpd	WordPerfect	apWordPerfectDesc
application/ vnd.framemaker	fm	FrameMaker	apFramemakerDesc
application/ vnd.framebook	bk, book	FrameMaker	apFrameMakerDesc
application/vnd.mif	mif	FrameMaker	apFrameMakerInterchangeDesc
application/lotus-1-2-3	123, wk3, wk4	123	apLotus123Desc
application/lotus-freelance	prz	Freelance	apLotusFreelanceDesc
application/lotus-wordpro	lwp	WordPro	apLotusWordProDesc
application/msword, application/ms-word	doc, dot	Word	apMicrosoftWordDesc

dFormat	Extensions	dConversion	dDescription
application/vnd.ms-excel, application/ms-excel	xls	Excel	apMicrosoftExcelDesc
application/ vnd.ms-powerpoint, application/ms-powerpoint	ppt	PowerPoint	apMicrosoftPowerPointDesc
application/vnd.ms-project, application/ms-project	mpp	MSPProject	apMicrosoftProjectDesc
application/ms-publisher	pub	MSPub	apMicrosoftPublisherDesc
application/write	wri	Word	apMicrosoftWriteDesc
application/rtf	rtf	Word	apRtfDesc
application/vnd.visio	vsd	Visio	apVisioDesc
application/vnd.illustrator	ai	Illustrator	apIllustratorDesc
application/vnd.photoshop	psd	PhotoShop	apPhotoshopDesc
application/vnd.pagemaker	p65	PageMaker	apPageMakerDesc
image/gif	drw, igx, flo, abc, igt	iGrafx	apiGrafxDesc
text/postscript	ps	Distiller	apDistillerDesc
application/hangul	hwp	Hangul97	apHangul97Desc
application/ichitaro	jtd, jtt	Ichitaro	apIchitaroDesc
image/graphic	gif, jpeg, jpg, png, bmp, tiff, tif	ImageThumbnail	apThumbnailsDesc
image/application	txt, eml, msg	NativeThumbnail	apNativeThumbnailsDesc

```
<@end@>
<@table PdfConversions@>
```

dFormat	Extensions	dConversion	dDescription
application/pdf	pdf	PDFOptimization	apPdfOptimization
application/pdf	pdf	ImageThumbnail	apPdfThumbnailsDesc

```
<@end@>
```

9.5 XSLT Transformation

Oracle WebCenter Content Server uses a two-step process for categorizing content. The first step translates content into an XML format, the second step transforms the XML file into another XML file useful to Content Categorizer. The process is transparent in that the original content is not modified, and both the translated and transformed XML files are discarded after use.

This section covers the following topics:

- [Section 9.5.1, "Translation"](#)
- [Section 9.5.2, "Transformation Using XSLT Style Sheets"](#)
- [Section 9.5.3, "SearchML Transformation"](#)

- [Section 9.5.4, "Flexiondoc Transformation"](#)

9.5.1 Translation

The translation step uses the OutsideIn XML Export filters to output the XML in either SearchML or Flexiondoc XML format, depending on the type of content being translated and if the format is available for the platform being used. This translation process enables Categorizer to support a large number of different source document formats.

The transformation step uses eXtensible Style Sheet Language Transformations (XSLT) to transform the initial XML output into an XML equivalent that Content Categorizer can easily search and analyze based on search rules defined by the user.

An overview of the transformation process can be useful to anyone interested in the categorization process, and serve as a starting point for users who would like to define their own XSLT style sheets to accommodate their specific document processing needs.

Translation Using OutsideIn XML Export Filters

A run-time version of the OutsideIn XML Export product is integrated and installed with Oracle WebCenter Content Server, and it filters content checked in for categorization. The Export filters convert content to XML for transformation using Categorizer's XSLT style sheets. The transformation is necessary because the Export XML schemas, Flexiondoc and SearchML, are not in a form easily searched by Content Categorizer rules.

9.5.2 Transformation Using XSLT Style Sheets

Two style sheets are included with Content Categorizer and applied based on the initial translation format provided by the OutsideIn XML Export filter. The style sheets are located in the following directory.

`/<IntradocDir>/data/contentcategorizer/stylesheets/`

For content items output in SearchML, *searchml_to_scc.xml* is applied. For content items output in Flexiondoc, *flexiondoc_to_scc.xml* is applied. SearchML and Flexiondoc both reproduce style designations found in the source content, but they do so differently, in ways not detectable by Content Categorizer rules. The appropriate steeliest can recognize the necessary style information in each format and use that information as the basis for transforming the final output tags into an XML document useful to Content Categorizer.

The similarity between SearchML and Flexiondoc depends on the degree to which internal styles or metadata are used in the content. When working with content using named styles, such as Microsoft Word, the resultant output is similar. When working with content in formats such a PDF or text, results come out with more generic tagging.

Important: There is a problem with the XSLT transformation used to post-process PDF content that is output in Flexiondoc format. When Flexiondoc is used, single words are assigned to individual XML elements, making the final XML unsuitable for most Categorizer search rules. It is recommended to use SearchML for categorizing PDF content.

9.5.3 SearchML Transformation

When the OutsideIn XML Export filter translates content into SearchML XML format, it identifies the properties of the content item, such as title, subject, and author, and tags them as a <doc_property> element. It distinguishes the properties by a `type` attribute. It also identifies document text and tags it as a <p> element. It distinguishes styles within text by an `s` attribute.

9.5.4 Flexiondoc Transformation

When the OutsideIn XML Export filter translates content into Flexiondoc XML format, it identifies the properties of the content item, such as title, subject, and author, and tags them as a <doc_property> element, just like SearchML. However, it distinguishes the properties by a `name` attribute, instead of `type`.

Where Flexiondoc differs from SearchML is in how it identifies styles. Paragraph styles are tagged with <tx.p> tags, and character styles are tagged with <tx.r> tags, but each have an attribute based on a unique style `id`, in addition to a `name` attribute.

All styles are defined in child elements of the <style_tables> element of the Flexiondoc XML file, and given an `id` attribute, which is called when referencing the style, and which the template file uses to define a style key with a `name` attribute.

User Interface

This appendix provides information about the user interface screens for administration applications including window and menu elements and options.

- Section A.1, "Content Repository Interface"
- Section A.2, "Workflows User Interface"
- Section A.3, "PDF Watermark Interface"
- Section A.4, "Contribution Folders Interface"
- Section A.5, "Create/Edit Folio Template Page"
- Section A.6, "Content Tracker Interface"
- Section A.7, "Content Categorizer Interface"
- Section A.8, "Web Layout Editor Interface"

A.1 Content Repository Interface

This section provides information about the interfaces used with the repository and contains the following topics:

- Section A.1.1, "Using a Supported Web Browser"
- Section A.1.2, "Configuration Manager Page"
- Section A.1.3, "Content Type Interface Screens"
- Section A.1.4, "Native File Format Interface Screens"
- Section A.1.5, "Configure Thumbnail Options Screen"
- Section A.1.6, "Custom Fields Interface Screens"
- Section A.1.7, "Electronic Signatures Configuration Screen"
- Section A.1.8, "Repository Manager Interface Screens"
- Section A.1.9, "Content Interface Screens"
- Section A.1.10, "Revision Interface Screens"
- Section A.1.11, "Workflow Revision Interface Screens"
- Section A.1.12, "Subscription Interface Screens"
- Section A.1.13, "Managed Links Administration Page"
- Section A.1.14, "Schema Interface Screens"
- Section A.1.15, "Content Profile Interface Screens"

- [Section A.1.16, "Content Profile Rules Interface Screens"](#)

A.1.1 Using a Supported Web Browser

Consumers and contributors access Oracle WebCenter Content Server from a standard Web browser. The computer you use to access the content server is a *client computer*. You can access Oracle WebCenter Content Server on a supported client computer from the following supported Web browsers:

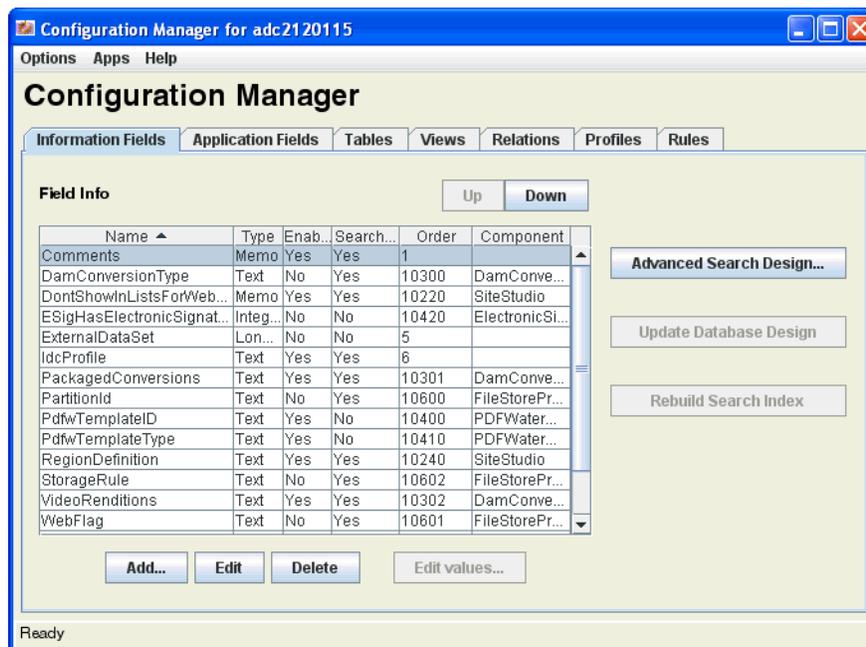
Table A-1 Supported Web Browsers

Browser	Versions
Internet Explorer	7, 8
Firefox	3.5+
Safari	4.x
Google Chrome	10.0 or higher

Note: If you are using Firefox, set Firefox to open links in a new window instead of a new tab. In some cases, help screens opened in a new tab are not viewable until the applet that launched the help closes. Opening the help in a separate window makes it viewable while the applet that launched the help runs.

A.1.2 Configuration Manager Page

This screen is an administration application used to manage content types, file formats, and custom metadata fields.



To access this page, log on as an administrator or subadministrator, and choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager**.

Note: Only administrators can work with Configuration Manager. Subadministrators do not have access to this application.

Element	Description
Options menu	Opens additional administrative applications to manage information fields and file format.
Apps menu	Provides options for other administration applications which open in the same mode (applet or standalone) as the current application.
Information Fields	Opens the Configuration Manager: Information Field Tab Screen .
Application Fields	Opens the Configuration Manager: Application Fields Tab Screen .
Tables	Opens the Configuration Manager: Tables Tab Screen .
Views	Opens the Configuration Manager: Views Tab Screen .
Relations	Opens the Configuration Manager: Relations Tab .
Profiles	Opens the Configuration Manager: Profiles Tab Screen .
Rules	Opens the Configuration Manager: Rules Tab Screen .

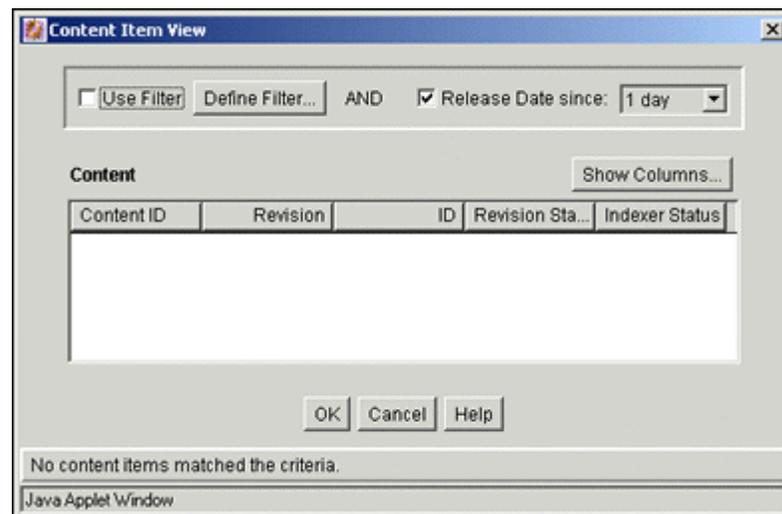
Multi-Use Screens

The following screens are used in many administration applications for a variety of detailed purposes:

- [Section A.1.2.1, "Content Item View Screen"](#)
- [Section A.1.2.2, "User View Screen"](#)
- [Section A.1.2.3, "Define Filter Screen"](#)
- [Section A.1.2.4, "Show Columns Screen"](#)

A.1.2.1 Content Item View Screen

This screen is used to select content for previewing.

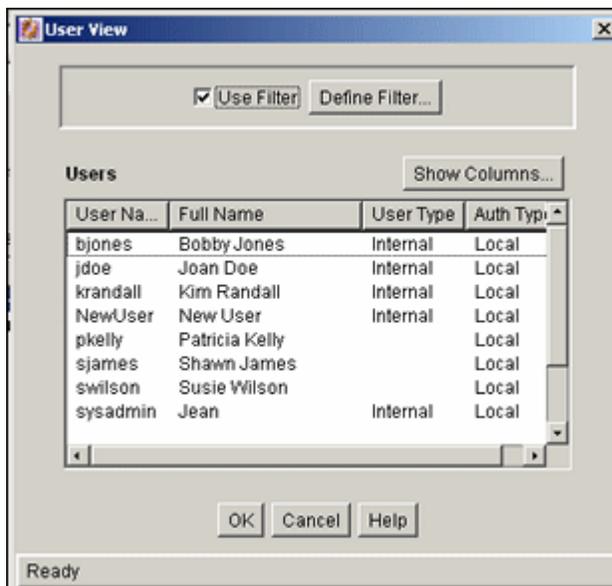


You can access this screen from different locations in the user interface.

Element	Description
Use Filter	Narrows the list of content items included in the Content pane. If selected, enables filtering based on selected fields, defined filter fields or release date, if specified.
Define Filter	Opens the Define Filter Screen .
Release Date since and date list	If selected, enables filtering based on release date since the specified elapsed time period of 1 day, 1 week, or 4 weeks.
Show Columns	Opens the Show Columns Screen .
Content pane	Displays the values of the selected display columns for each content item included in the Content items list.

A.1.2.2 User View Screen

This screen is used to select users to include when previewing profile scenarios.



You can access this screen from different locations in the user interface.

Element	Description
Use Filter	Narrows the list of users.
Define Filter	Opens the Define Filter Screen .
Show Columns	Opens the Show Columns Screen .
Users pane	Displays the values of the selected display columns for each user included in the Users list.

A.1.2.3 Define Filter Screen

This screen is used to narrow the list of revisions, users, and so forth that are displayed on several administration application screens. The items displayed are filtered based on the criteria entered. You can use the following wildcards in these fields:

- percent (%) for one or more characters

- underscore (_) for a single character

The 'Define Filter' dialog box contains the following fields and options:

- Content ID
- Title
- Author
- Type
- Security Group
- Account
- Checked out: Yes
- Checked out by
- Revision Status: Done
- Indexer Status: New
- Conversion Status: Converted
- Indexer Cycle: Idle
- Workflow State: -
- Revision Rank >=
- Revision Rank <
- Publish Type: None
- Publish Status: Content
- Latest Revision
- Check In Date >=
- Check In Date <
- Indexed Date >=
- Indexed Date <
- Release Date >=
- Release Date <
- Expiration Date >=
- Expiration Date <
- Comments

Legend: % = Match Many, _ = Match One

Buttons: OK, Cancel, Help

Java Applet Window

To access this screen, click **Define Filter** on the screen. Select one or more check boxes to activate the filter fields.

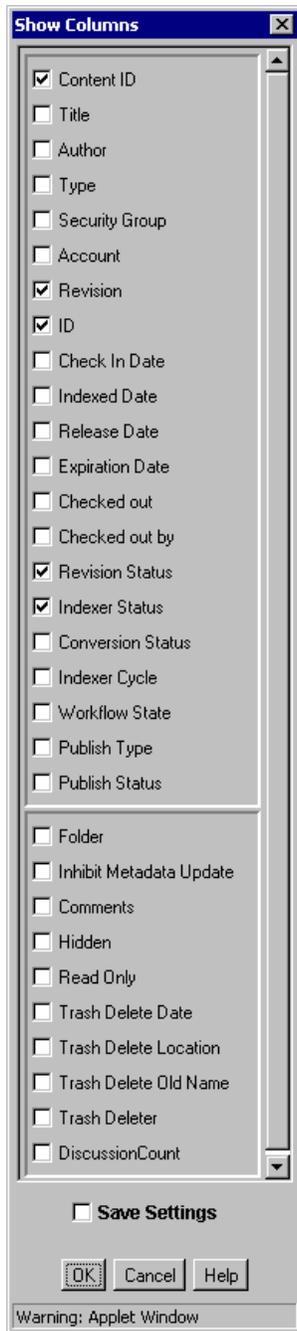
Field	Description
check boxes	If selected, the associated filter expression is applied.
Content ID	Unique Content ID of the content item.
Title	Title of the revision.
Author	User who checked in the revision.
Type	Content type of the revision.

Field	Description
Security Group	Security group assigned to the revision.
Account	Account assigned to the revision. This field is displayed only if accounts are enabled.
Checked out	Specifies if the revision is checked out.
Checked out by	User who has the revision checked out.
Revision Status	<p>Status of the revision:</p> <ul style="list-style-type: none"> ■ Done: Waiting to be released on its specified Release Date. ■ Edit: At the initial contribution step of a workflow. ■ GenWWW: Being converted to Web-viewable format, being indexed, or has failed conversion or indexing. ■ Review: In a workflow and is being reviewed. ■ Pending: In a Basic workflow and awaiting approval of all revisions in the workflow. ■ Released: Available. ■ Expired: No longer available for searching or viewing. The revision was not deleted, but only by an administrator can access it unless Notification of Expiration is used. ■ Deleted: Deleted and waiting to be completely removed from the system during the next indexing cycle.
Indexer Status	<p>Indexing status of the revision:</p> <ul style="list-style-type: none"> ■ New: Checked in but is not indexed. ■ Current: The latest revision. ■ Old: Not the latest revision. ■ Workflow: In a workflow. ■ Processing: Being prepared for indexing. ■ Update: Revision metadata is updated but the revision is not indexed. ■ Indexing: Being indexed. <p>Only one revision of any content item can be in Current, Indexing, or Update status at a time.</p>
Conversion Status	<p>Conversion status of the revision:</p> <ul style="list-style-type: none"> ■ Converted: Converted successfully and the Web-viewable file is available. ■ Processing: Being converted by Inbound Refinery. ■ Failed: Deleted, locked, or corrupted, or a search engine error occurred. ■ MetaData Only: Full-text indexing was bypassed and only the revision's metadata was indexed. ■ Refinery PassThru: Inbound Refinery failed to convert the revision and passed the native file through to the Web. ■ Incomplete Conversion: An error occurred in the conversion after a valid Web-viewable file was produced and the file was full-text indexed.

Field	Description
Indexer Cycle	State of the revision in an Indexer cycle: <ul style="list-style-type: none"> ■ Idle: Not yet in an Indexer cycle. ■ Loading for Active: Being loaded for an update cycle. ■ Indexed for Active: Being indexed during an update cycle. ■ Loading for Rebuild: Being loaded for a rebuild cycle. ■ Indexed for Rebuild: Being indexed during a rebuild cycle. ■ Rebuilt: Processed by an rebuild cycle. ■ Updated: Processed by an update cycle.
Workflow State	Workflow state of a revision: <ul style="list-style-type: none"> ■ Reviewer/Contributor: In a step where assigned users can edit or review the revision. ■ Contributor: In a step where users can only edit the revision. ■ Reviewer: In a step where users can only review the revision. ■ Pending: In a basic workflow and has completed all the steps, but to complete and exit the workflow, all content items in the basic workflow must complete all the steps.
Revision Rank >= and <	Specifies revision greater than/equal to a specific number or less than a specific number.
Publish Type	Content type for a revision used with Content Publisher.
Publish Status	Publishing status of a revision used with Content Publisher: <ul style="list-style-type: none"> ■ Content: Not staged, published, or in a workflow ■ Published: Published through Content Publisher. ■ Staging: In the staging process in Content Publisher. ■ Workflow: In a workflow.
Latest Revision	Display only latest revision of file.
Specified date	Specifies content that is greater than/equal to a specific date or earlier than a specific date: <ul style="list-style-type: none"> ■ Check In Date: Date the revision was checked in. ■ Indexed Date: Date the revision was last indexed. ■ Release Date: Date the revision was last released. ■ Expiration Date: Expiration date of the revision
Custom fields	Any custom metadata fields are also available as filter fields.

A.1.2.4 Show Columns Screen

This screen is used to select the columns displayed on some administration screens.



To access this screen, click **Show Columns** on the screen.

Element	Description
check boxes	If selected, the field is displayed. See Section A.1.2.3, "Define Filter Screen" for field descriptions.
Save Settings	If selected, the column settings are applied every time the Content tab of the Repository Manager or Content Item Subscribed screen is displayed. If unselected, the column settings apply only until the Content tab of the Repository Manager or Content Item Subscribed screen closes.

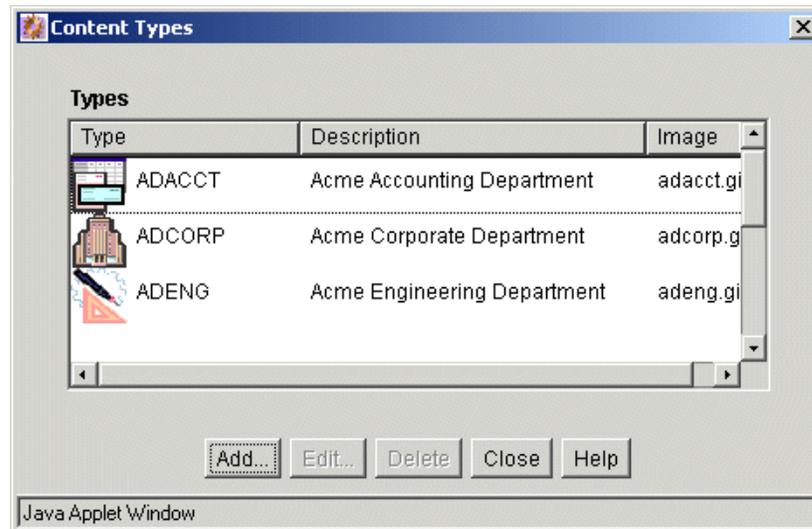
A.1.3 Content Type Interface Screens

The following screens are used when working with Content Types:

- [Section A.1.3.1, "Content Types Screen"](#)
- [Section A.1.3.2, "Add/Edit Content Type Screen"](#)

A.1.3.1 Content Types Screen

This screen is used to add, edit, and delete content types. It is also used to view the name, description, and associated GIF for existing content types and to manage the corresponding images.



To access this screen, choose **Options** then **Content Types** from the Page menu of the [Configuration Manager Page](#).

Element	Description
Type	Name of each content type and the GIF image associated with that type.
Description	Description of each content type.
Image	File name for the GIF image associated with each content type.
Add	Opens the Add/Edit Content Type Screen .
Edit	Opens the Add/Edit Content Type Screen .
Delete	Enables deletion of the selected content type. You cannot delete a content type if content exists using that type.

A.1.3.2 Add/Edit Content Type Screen

This screen is used to add or edit a content type.

To access this screen, click **Add** or **Edit** on the [Content Types Screen](#).

Element	Description
Name	Name of the content type. 30 characters maximum.
Description	Description for the content type. 80 characters maximum.
GIF list	Image that represents the content type on pages.

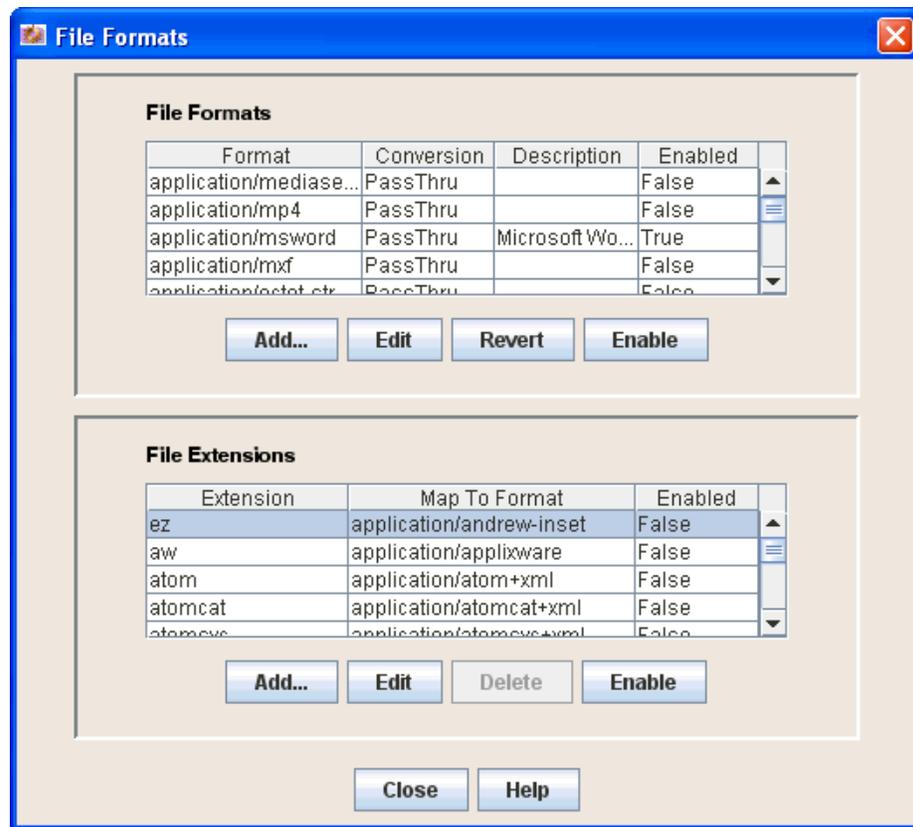
A.1.4 Native File Format Interface Screens

This section covers these screens:

- [Section A.1.4.1, "File Formats Screen"](#)
- [Section A.1.4.2, "Add/Edit File Format Screen"](#)
- [Section A.1.4.3, "Add/Edit File Extension Screen"](#)

A.1.4.1 File Formats Screen

This screen is used to set the file formats and file extensions for file conversions.



To access this option, choose **File Formats** from the Options menu on the [Configuration Manager Page](#).

File Formats pane

Element	Description
Format	Usually the MIME (Multipurpose Internet Mail Extensions) type.
Conversion	Method to use to convert the file.
Description	Description for the file format.
Enabled	Displays if the format is enabled in the interface.
Add or Edit	Opens the Add/Edit File Format Screen .
Delete	Enables deletion of the selected file format.
Enable/Disable	Enables or disables the selected file format in the interface.

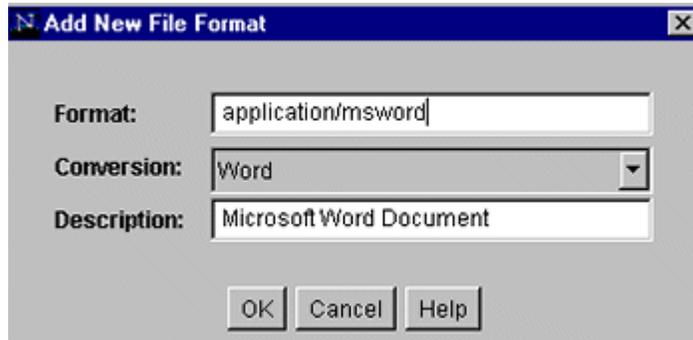
File Extensions pane

Element	Description
Extension	File extensions mapped to file formats.
Map to Format	File format to be referenced to convert files with that extension.
Enabled	Displays if the format is enabled in the interface.
Add or Edit	Opens the Add/Edit File Extension Screen .
Delete	Enables deletion of the selected file extension.

Element	Description
Enable/Disable	Enables or disables the selected file format in the interface.

A.1.4.2 Add/Edit File Format Screen

This screen is used to set conversion methods for specific file formats.

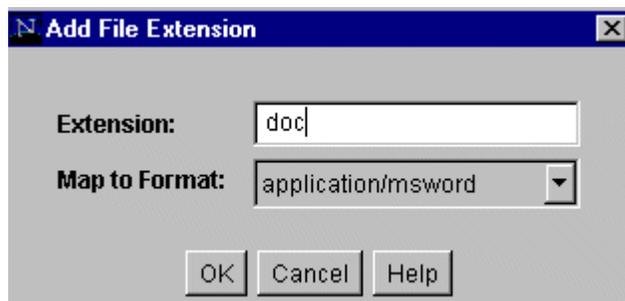


To access this screen, click **Add** or **Edit** in the File Formats pane on the [File Formats Screen](#).

Element	Description
Format	Usually the MIME (Multipurpose Internet Mail Extensions) type.
Conversion	Method to use to convert the file. To not convert this file type, choose Passthru . To use a custom conversion method, choose Custom .
Description	Description for the file format.

A.1.4.3 Add/Edit File Extension Screen

This screen is used to map file extensions to specific file formats.



To access this screen, click **Add** or **Edit** in the File Extensions pane on the [File Formats Screen](#).

Element	Description
Extension	File extension of files to be converted.
Map to Format	File format to be referenced to convert files with that extension.

A.1.5 Configure Thumbnail Options Screen

A thumbnail is a small representative image of the associated content item. Use this screen to enable and configure automatic thumbnail generation. To access this screen, choose **Configure Thumbnail Options** from the Administration tray.

Content Server provides a basic set of thumbnail creation options. Oracle WebCenter Content: Inbound Refinery provides a more extensive set of options for file conversion and thumbnail generation. For more information, see *Oracle WebCenter Content Administrator's Guide for Conversion*.

Element	Description
Enable this server to create thumbnail images	Select to enable thumbnail creation. When enabled, thumbnail images are generated automatically at check in for file types supported by Outside In Image Export and enabled on the File Formats Screen . If the content item has a format which is not supported or which is explicitly excluded, a thumbnail image is not generated and the icon associated with the Document Type (dDocType) is used. If Inbound Refinery is enabled and set up to handle thumbnails, the options you set on this window are not used.
This server will not create thumbnail images for these formats	Specify a comma-separated list of file formats for which you do not want to generate thumbnails. If you select a format from the list of enabled formats, it is added to the comma-separated list. The list of formats is taken from the enabled formats on the File Formats Screen .

Element	Description
Path to fonts	<p>Specify the directory that contains the font information used to render characters in the thumbnail. Only TrueType fonts (*.ttf or *.ttc files) are currently supported. In most cases, the fonts provided by the Java environment (<java.home>/lib/fonts/) are adequate.</p> <p>A more extensive selection of TrueType fonts, particularly those with non-western European characters, may be provided by the hosting system. For example, on Linux fonts are located in the /usr/lib/X11/fonts/TTF folder. On Windows, fonts are located in the C:\WINDOWS\Fonts folder.</p>
Timeout for thumbnail process in seconds	Specify the amount of time in seconds to wait for the thumbnail process to complete. If the thumbnail process does not complete in this time, the process is ended. The default setting is 120 seconds.
UNIX Rendering Options	<p>For Linux and Solaris SPARC systems, specify rendering options for systems running on UNIX. All other platforms use the internal graphics rendering.</p> <p>Use native operating system's native graphics subsystem: Specify that fonts and graphics are rendered using the operating system's native graphics subsystem (X11 on UNIX platforms).</p> <p>This option works only when at least one of the appropriate output solutions is present. For example, if the UNIX \$DISPLAY variable does not point to a valid X Server, but the OSGD and/or WV_GD modules required for internal graphics rendering exist, internal graphics rendering is used.</p> <p>Use internal graphics rendering: Specify that Outside In Image Export will attempt to use its internal graphics code to render fonts and graphics. This is the default option.</p>
Page Number of Native Vault File to Use to Create Thumbnail Image	For multi-page files, specify the number of the page to use to render the thumbnail. The default page number is 1.
Use quick sizing	Select for the fastest conversion of color graphics with a somewhat lower quality image.
Use smooth sizing	Select for a more accurate representation of the original graphic which will slow down the conversion speed slightly. This is the default setting.
Smooth sizing for grayscale graphics	Select this option to use smooth sizing for grayscale graphics and quick sizing for any color graphics.
Produce jpg thumbnails radio button	Select to create all thumbnails as JPG files. This is the default thumbnail file type setting.
Produce gif thumbnails radio button	Select to create all thumbnails as GIF files.
Produce png thumbnails radio button	Select to create all thumbnails as PNG files.
Update	Saves changes to settings.
Reset	Reverts to the last saved settings.

A.1.6 Custom Fields Interface Screens

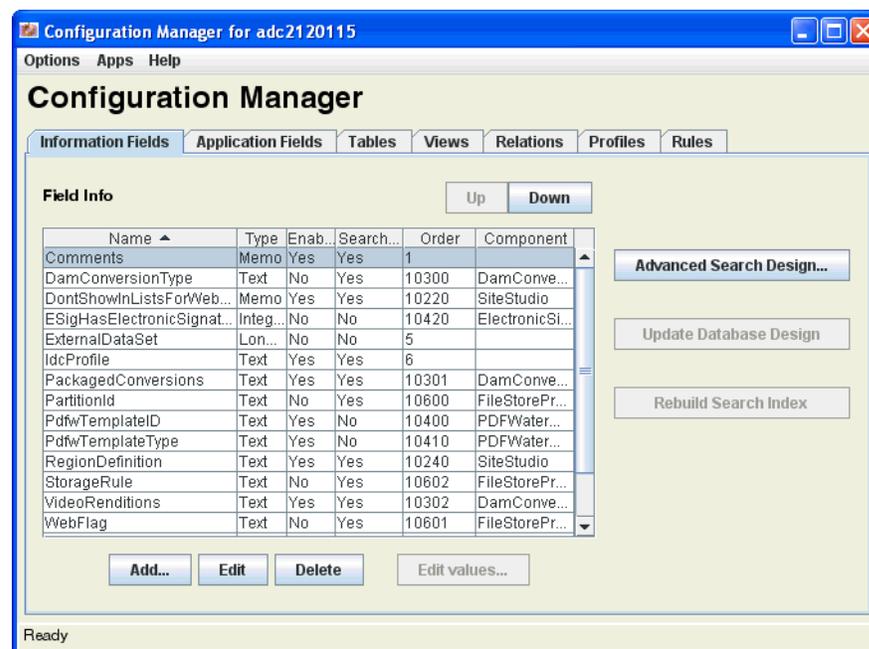
The following screens are used to add metadata fields and application fields:

Note: For information about custom fields for Electronic Signatures, see the *Oracle WebCenter Content User's Guide for Content Server*.

- Section A.1.6.1, "Configuration Manager: Information Field Tab Screen"
- Section A.1.6.2, "Add Metadata Field Name Screen"
- Section A.1.6.3, "Add/Edit Metadata Field Screen"
- Section A.1.6.4, "Configure Option List Screen"
- Section A.1.6.5, "Option List Storage Screen"
- Section A.1.6.6, "Edit View Values Screen"
- Section A.1.6.7, "Option List Screen"
- Section A.1.6.8, "Edit Tree Definition Screen"
- Section A.1.6.9, "Select Root Node for the Tree"
- Section A.1.6.10, "Advanced Search Design Screen"
- Section A.1.6.11, "Advanced Options for Field Screen"
- Section A.1.6.12, "Update Database Design Screen"
- Section A.1.6.13, "Configuration Manager: Application Fields Tab Screen"
- Section A.1.6.14, "Add/Edit Application Field Screen"

A.1.6.1 Configuration Manager: Information Field Tab Screen

This screen is used to add, edit, and delete custom metadata fields.



To access this screen, click **Information Fields** on the [Configuration Manager Page](#).

Element	Description
Name	Names of custom metadata fields.
Type	Type for each field. Values include: <ul style="list-style-type: none"> ■ Text ■ Long Text ■ Date ■ Memo ■ Integer
Enabled	Indicates if the field is displayed on Oracle WebCenter Content Server pages.
Searchable	Indicates if the field is indexed and available for searches.
Order	Indicates the place the field occupies in the sort order.
Up and Down	Rearranges the order of fields for sorting. To use, highlight a field and click the appropriate button. The field's position in the sort order is changed accordingly.
Advanced Search Design	Saves changes to the database tables. This button is active when an update is required.
Update Database Design	Saves changes to the database tables. This button is active when an update is required.
Rebuild Search Index	Rebuilds the search index. This button is active when a rebuild is required.
Add or Edit	Opens the Add Metadata Field Name Screen .
Delete	Enables deletion of the selected custom metadata field.
Edit Values	Displays a parent/child structure if a field is associated with a schema relationship. This option is active after the field is added and the database design is updated.

A.1.6.2 Add Metadata Field Name Screen

This dialog is used to define the name of a new custom metadata field.



To access this dialog, click **Add** on the [Configuration Manager: Information Field Tab Screen](#).

When adding a custom metadata field, the system automatically prefixes the name with an x to ensure that it is unique and does not conflict with any reserved names. Similarly, when a custom user information (metadata) field is defined, the system automatically prefixes the name with a u to ensure that it is also unique and does not conflict with any reserved names.

Element	Description
Field Name	Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). Do not use special characters.

A.1.6.3 Add/Edit Metadata Field Screen

This screen is used to define a custom metadata field.

The screenshot shows a dialog box titled "Edit Metadata Field 'InfoField1'". It contains the following fields and options:

- Field Caption:** InfoField1
- Field Type:** Text (dropdown menu)
- Decimal Scale:** 1 (dropdown menu)
- Field Order:** 50052
- Default Value:** (text field) with a "Select" button to the right.
- Require Value:** Required
- Placeholder:** Enabled
- Enable on User Interface:** Enabled
- Enable for Search Index:** Indexed
- Enable Option List:** Option List

Buttons at the bottom include "OK", "Cancel", "Help", and a "Configure..." button.

To access this screen, do one of the following:

- Enter a field name and click **OK** on the [Add Metadata Field Name Screen](#).
- Select a field and click **Edit** on the [Configuration Manager: Information Field Tab Screen](#).

Element	Description
Field Caption	Display label shown on Oracle WebCenter Content Server pages.
Field Type	Type for each field. Values include: <ul style="list-style-type: none"> ■ Text ■ Long Text ■ Date ■ Memo ■ Integer ■ Decimal
Decimal Scale	Specifies the supported number of digits to the right of the decimal. This field is supported for fields with a Field Type of Decimal only.
Field Order	Sequence in which the field is displayed on pages. Starting at 2, the number automatically increments as new fields are added.
Default Value	Default value for the field.
Require Value	If selected, prevents files from being checked in if the field does not contain a value.
Placeholder	If selected, makes this a field which is not stored or indexed. Placeholders are often used for the parent level of a dependent choice list.
Enable on User Interface	If selected, the field is displayed on pages.
Enable for Search Index	If selected, the field is indexed and can be used as search criteria.
Enable Option List	If selected, creates a user-selectable list on pages.

A.1.6.4 Configure Option List Screen

This screen is used to specify the type of list, the values for the list and any dependencies associated with the list.

To access this screen, click **Enable Option List** then click **Configure** on the [Add Metadata Field Name Screen](#) or the [Add/Edit Metadata Field Screen](#).

Element	Description
Option List Type	<ul style="list-style-type: none"> ■ Select List Validated ■ Select List Not Validated ■ Edit and Select List ■ Edit and Multiselect List ■ Multiselect List
Advanced	Opens the Option List Storage Screen .
Use option list	Creates a new list. The name of the new list is inserted into the field.
Edit	Opens the Option List Screen .
Use view	Used to choose values in a view instead of a created list.
Edit Values	Opens the Edit View Values Screen or the Option List Screen , depending on the type of view selected.
Use tree	Used to choose values in a tree, not a list or a view.
Edit Definition	Opens the Option List Screen .
Dependent field	If selected, enables a dependency to make the metadata field subordinate to another metadata field. Available when using a view.
Depends on field	Used to enter a field name or choose from a list of metadata to use to set dependencies.
Relationship	Lists previously defined view relationships. If none are defined, an appropriate message is displayed.

A.1.6.5 Option List Storage Screen

This screen is used to specify how the list is displayed and stored.

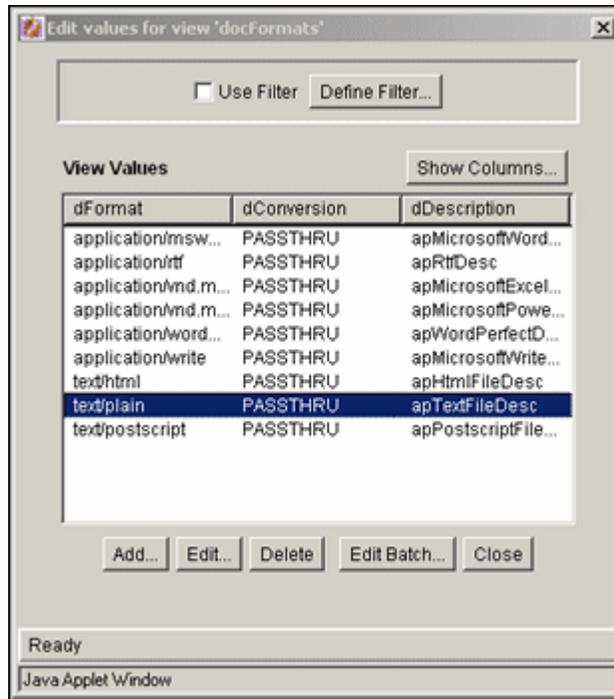


To access this screen, click **Advanced** next to the list on the [Configure Option List Screen](#).

Element	Description
Store option list keys	Permanently stores option list keys or localized option list text.
Store localized option list text	Stores localized versions of the list or localized list text.
Pad ends of storage string with separator	Active only if a Multiselect option is chosen on the Configure Option List Screen . Pads the length of the separator that stores multiselect values.
Multiselect Storage Separator	Active only if a Multiselect option is chosen on the Configure Option List Screen . Changes the separator that stores multiselect values.
Multiselect Display Separator	Active only if a Multiselect option is chosen on the Configure Option List Screen . Change the separator that displays multiselect values.

A.1.6.6 Edit View Values Screen

This screen is used to edit the values defined in a view.

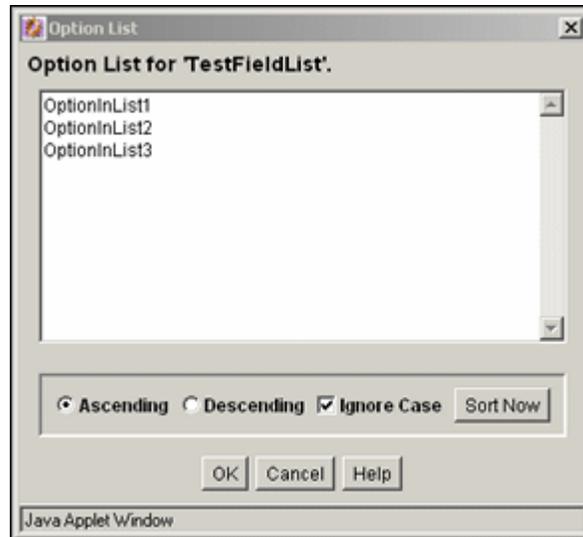


To access this screen, click **Edit Value** next to **Use View** on the [Add/Edit Metadata Field Screen](#). The columns depend on the type of view selected.

Element	Description
Use Filter	If selected, applies the filter defined by the Define Filter Screen .
Define Filter	Opens the Define Filter Screen
Show Columns	Limits the number of columns to show in the view.
Add or Edit	Opens the Add/Edit Value Screen .
Delete	Enables deletion of a value from the table.
Edit Batch	Opens the Edit Values: Edit Batch screen.

A.1.6.7 Option List Screen

This screen is used to create a list for a custom field.

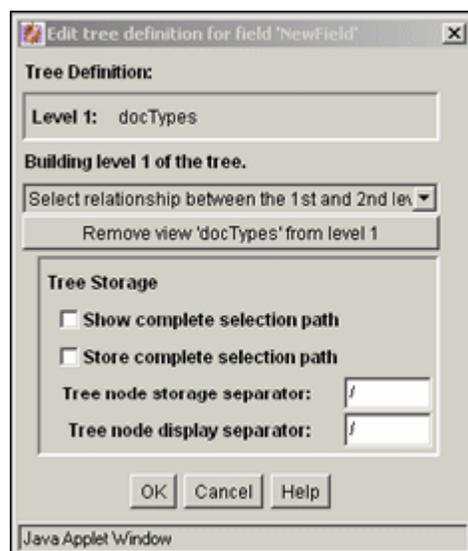


To access this screen, click **Edit** next to **Use Option List** on the [Configure Option List Screen](#).

Element	Description
Option list pane	Used to enter the values available for the custom metadata field. Each value must be on a separate line, with a carriage return between values.
Ascending or Descending	Sorts the list in alphanumeric order or reverse alphanumeric order, with capital letters preceding lower-case letters. For example, an Ascending list with Ignore Case disabled lists <i>ABCDF</i> before <i>abcde</i> .
Ignore Case	Ignores uppercase or lowercase when sorting items.
Sort Now	Sorts the list in the manner specified.

A.1.6.8 Edit Tree Definition Screen

This screen is used to define how a tree used in a list is stored and displayed.

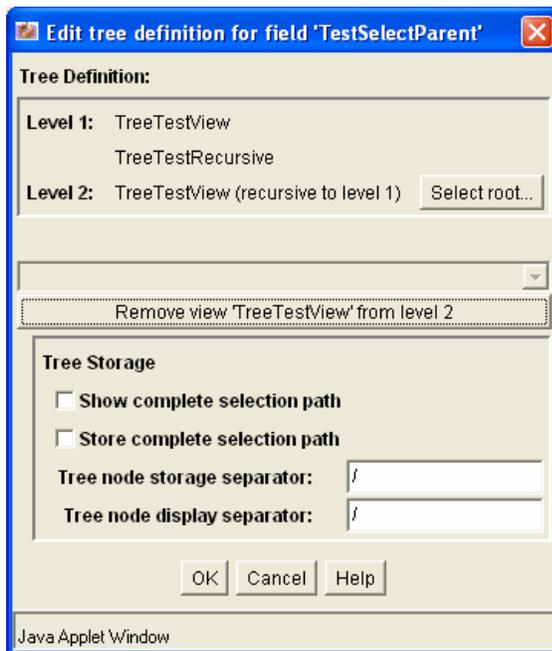


To access this screen, click **Edit Definition** next to **Use Tree** on the [Configure Option List Screen](#).

Element	Description
Select relationship menu	Used to select a relationship between levels of the list.
Remove view	If selected, removes the selected view.
Show complete selection path	If selected, displays the complete path when the option is selected.
Store complete selection path	If selected, saves the complete path when the option is selected.
Tree node storage separator	Used to store a different operator between values.
Tree node display separator	Used to change the separator between values.

A.1.6.9 Select Root Node for the Tree

This screen allows selection of parent values when browsing for a child in a dependent choice list (DCL) schema. You can choose a row in a table that is the root of the tree.

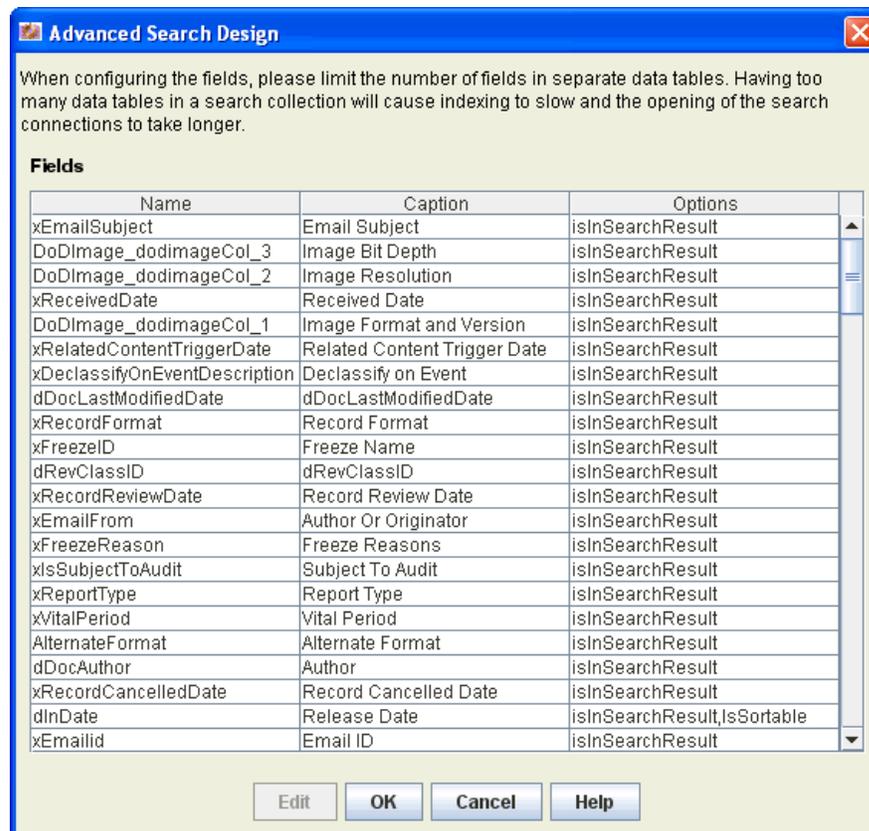


This screen opens at different locations in the user interface.

Element	Description
Tree Definition pane	Displays the tree schema hierarchy.
Select Root	Opens a popup dialog to select parent values for a child value.
Other screen elements	For descriptions of the other screen elements see Section A.1.6.8, "Edit Tree Definition Screen."

A.1.6.10 Advanced Search Design Screen

Use this screen to select and edit fields for which you can modify the search optimization and sort options.



To access this screen, click **Advanced Search Design** on the [Configuration Manager: Information Field Tab Screen](#).

Element	Description
Name	Displays the internal name of the field.
Caption	Displays the display name of the field.
Options	Displays the current set of search options for the field.
Edit	Opens the Advanced Options for Field Screen to specify search options for the selected field.

A.1.6.11 Advanced Options for Field Screen

Use this screen to configure optimization and sort options for searchable fields. WebCenter Content uses the SDATA section feature in Oracle Text 11g to index important text, date, and integer fields and define them as Optimized Fields. The SDATA section is a separate XML structure managed by the Oracle Text engine that allows the engine to respond rapidly to requests involving data and integer ranges. The Content Server system can have up to 32 Optimized Fields, which includes data, integer, standard Content Server fields like dInDate, dOutDate, and fields selected to be optimized. All Optimized Fields are SDATA fields, which by default include dDocName and dDocTitle.

Note: Specify only text, date, and integer fields as optimized fields. Memo, fields, for example cannot be optimized for search.

Any changes made on this screen require you to rebuild the search index.

Caution: Depending on the size of the search index and available system resources, the search index rebuild process can take several days. If rebuilding is necessary, rebuild at times of non-peak system usage.

To access this screen, add or delete a custom metadata field and click **Advanced Search Design** on the [Configuration Manager: Information Field Tab Screen](#).

Element	Description
Is returned in the search results	This value is specified on the Add/Edit Metadata Field Screen and cannot be modified here.
Is optimized	Selects the field for optimization. By default, the dDocName (Content ID) and dDocTitle (Title) fields are optimized.
Is sortable	Selects the field for sorting on the search results page. You must first select Is optimized to select this option. Sortable fields on the search results page become a link in column header. An arrow icon next to the field name indicates ascending or descending order. By default, dInDate (Release Date) and dDocTitle (Title) are sortable.
Is a filter category	Selects the field to show in the set of Filter by Category options listed at the top of the search results page.

A.1.6.12 Update Database Design Screen

This screen is used to add or delete metadata fields in the Oracle WebCenter Content Server database. The following table lists the events after which a database update or search index rebuild is required depending on the search engine.

Event	Action Required
Add metadata field	Update database
Edit metadata field	Update database*
Delete metadata field	Update database
Enable or disable Enable for Search Index for metadata field	Rebuild search index
Add metadata field with Enable for Search Index selected	Rebuild search index

Changes to the Require Value, Option List Default Value, Option List Key, and Option List values do not require a database update.

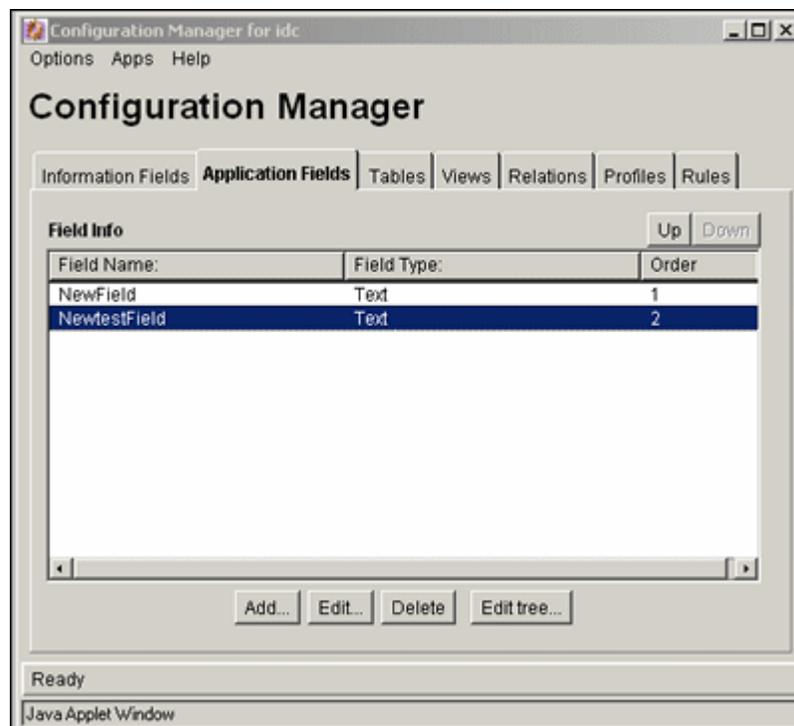


To access this screen, add or delete a custom metadata field and click **Update Database Design** on the [Configuration Manager: Information Field Tab Screen](#).

Element	Description
Info field(s) that will be added	Lists the metadata fields added since the last time the database was updated.
Info field(s) to delete check boxes	Lists the metadata fields that were deleted since the last time the database was updated. If selected, the field is deleted from the database. If unselected, the field remains hidden on the Configuration Manager screen and check-in and search pages, but it still exists in the database.

A.1.6.13 Configuration Manager: Application Fields Tab Screen

This screen is used to add, edit, and delete custom fields used on Oracle WebCenter Content Server forms.



To access this screen, click **Application Fields** on the [Configuration Manager Page](#).

Element	Description
Field Name	The names of custom application fields.
Field Type	The type for each field.
Order	The place the field occupies in the sort order.
Up or Down	Rearrange the order of fields for sorting. To use, highlight a field and click the appropriate button. The field's position in the sort order is changed accordingly.
Add or Edit	Opens the Add/Edit Metadata Field Screen .
Delete	Deletes the selected custom metadata field.

Element	Description
Edit Tree	Displays a parent/child structure if a field is associated with a schema relationship. This option is active after the field is added and the database design is updated.

A.1.6.14 Add/Edit Application Field Screen

This screen is used to add the necessary information for a custom application field.

To access this screen, click **Add** or highlight a field and click **Edit** on the [Configuration Manager: Application Fields Tab Screen](#).

Element	Description
Field Name	Name of the field. Duplicate names are not allowed. Maximum field length is 29 characters. Do not use special characters.
Field Type	Type for each field. Values include: <ul style="list-style-type: none"> ▪ Text ▪ Long Text ▪ Date ▪ Memo ▪ Integer
Field Caption	Display label shown on pages.
Enable Option List	Creates a user-selectable list on pages.
Placeholder	If selected, makes this a field which is not stored or indexed. Placeholders are often used for the parent level of a dependent choice list.
View Only	If selected, makes this a field used only in a schema view.

A.1.7 Electronic Signatures Configuration Screen

Use the Electronic Signatures Configuration screen to define additional metadata fields that are stored as part of the metadata for the electronic signature. Electronic signature information is stored and managed in a separate ElectronicSignatures table in the database.

Note: Plan your custom fields carefully before you use them. After you create a field (click **Save Changes**), you cannot change the field name, the data type, or the required status. If you delete a field, you delete any data previously stored in that field.

Electronic Signatures Configuration

Custom Signature Fields

<input type="checkbox"/>	Name	Display Label	Data Type	Choice List	Checkbox	Required
<input type="checkbox"/>	Approval	Approval level	Text	<input checked="" type="checkbox"/> AD1,AD2,AD3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Disclaimer	I have read and understand		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Element	Description
Add Field icon	Add a row to the table to define a new custom field.
Delete Field icon	Delete selected fields from the database. Fields are deleted permanently when you click Save Changes . When you delete a field, you delete any data previously stored in that field.
Move Field Up icon	Move the selected field up one position in the table order. The order of fields in the table determines the order of fields presented on the Sign Content Item page.
Move Field Down icon	Move the selected field down one position in the table order. The order of fields in the table determines the order of fields presented on the Sign Content Item page.
Select/Deselect Items	Select one or more items to move or delete. Click one time to select and individual item. Click again to deselect an item. Click the check box at the top of the column to select/deselect all field rows in the table at one time.
Name	Specify the internal identifier of the field. Maximum field name length is 29 characters. Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. The name must begin with a letter.
Display Label	Specify the name displayed to users. For check box fields, Display Label contains the text to display next to the check box.
Data Type	Select a data type from the list of supported types. When users enter a value in the field, it is validated against the selected data type: <ul style="list-style-type: none"> ■ Text: 30 characters. ■ Long Text: 200 characters. ■ Memo: 2000 characters. ■ Date: Date format (such as <i>dd/mm/yyyy</i> or <i>dd/mm/yy</i> for the English-US locale). ■ Integer: -2^{31} to 2^{31} (-2 billion to +2 billion). By definition, an integer is a natural number, so decimal values and commas are not permitted.

Element	Description
Use Choice List	Select the check box to specify a list of values from which the user can choose. Choice lists are available only for text and integer data types.
Choice List	Specify a list of values from which the user can choose. Separate values with a comma. The values you specify must conform to the data type guidelines listed above. Values are presented in the order listed. The first value in the list is the default value for the field. To provide no default value, enter a space followed by a comma as the first value in the choice list.
Checkbox	Select the check box to specify that the custom field is itself a check box. A check box field is automatically designated a required field. The user must select the check box to complete the electronic signature. The Display Label field contains acknowledgement text to display next to the check box.
Required	Specify that the user must supply a value in the associated field to complete the electronic signature.
Save Changes	Permanently save any changes made since the last save operation. After you create and save a field, you cannot change the field name, the data type, or the required status. If you delete a field, you delete any data previously stored in that field.
Reset	Discard any changes made since the last save operation.

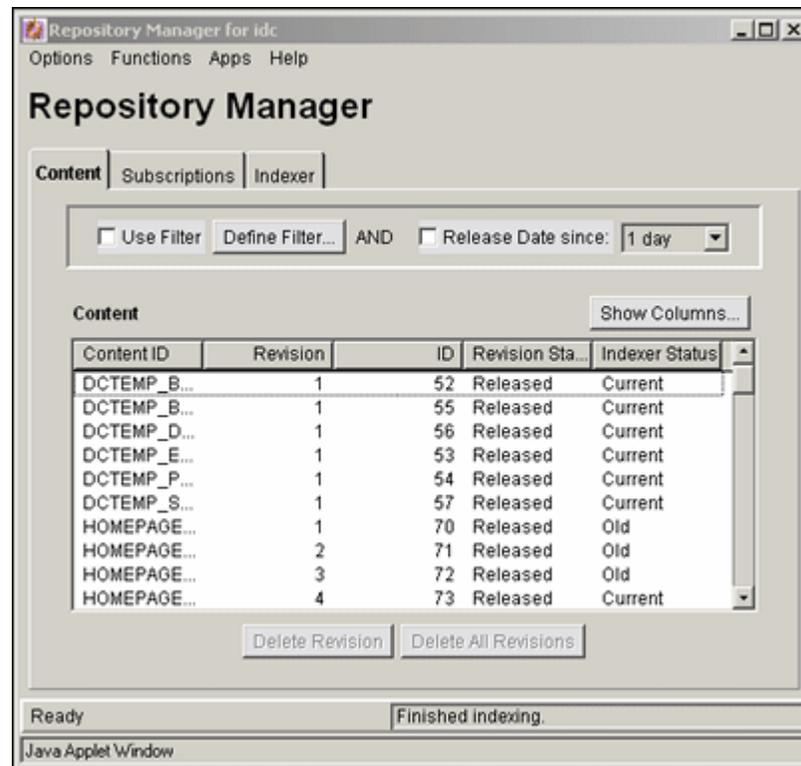
A.1.8 Repository Manager Interface Screens

The following screens are used to access the Repository Manager:

- [Section A.1.8.1, "Repository Manager Main Screen"](#)
- [Section A.1.8.2, "Repository Manager: Content Tab Screen"](#)

A.1.8.1 Repository Manager Main Screen

This screen shows the options and tabs available with the Repository Manager.

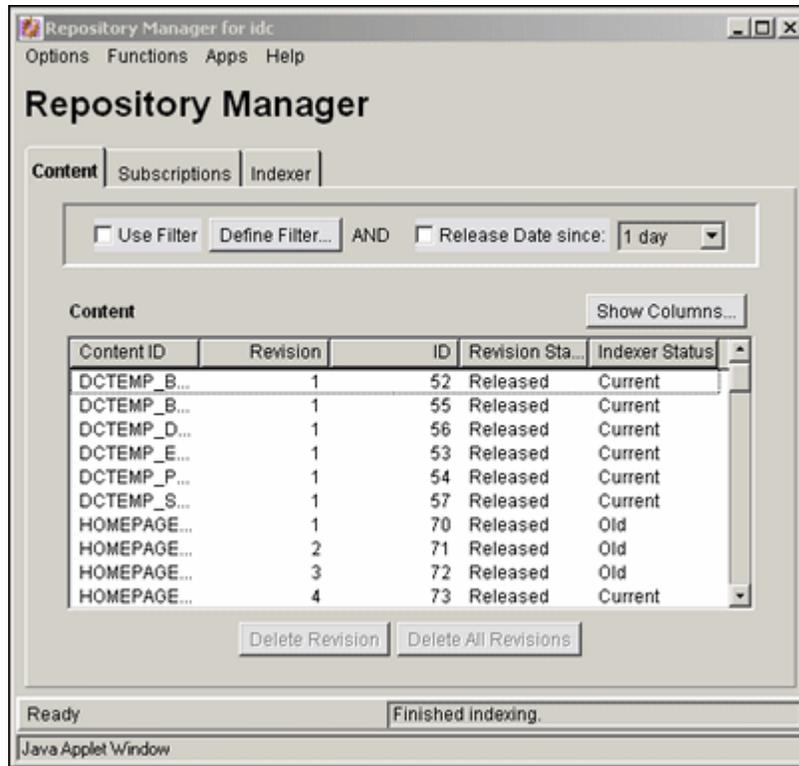


To access this screen, choose **Administration** then **Admin Applets** from the Main menu. Click **Repository Manager**. You can also start Repository Manager in standalone mode.

Element	Description
Options menu	Displays options to start tracing or to exit the Repository Manager.
Functions menu	Displays options to update content, check out content, reject content, and perform other content related actions. All options are also available from a shortcut menu, accessed when you right-click a revision in the Content list.
Apps menu	Displays other administration applications. The other applications open in the same mode (applet or standalone) as the current application.
Content	Opens the Repository Manager: Content Tab Screen .
Subscriptions	Opens the Repository Manager: Subscriptions Tab Screen .
Indexer	See the <i>Oracle WebCenter Content System Administrator's Guide for Content Server</i> for details about indexing functions.

A.1.8.2 Repository Manager: Content Tab Screen

This screen is used to display content item revisions.



To access this screen, click **Content** on the [Repository Manager Main Screen](#).

Element	Description
Use Filter	If selected, applies the filter defined by the Define Filter Screen .
Define Filter	Opens the Define Filter Screen
Release Date since	If selected, narrows the Content list as defined by the Release Date list.
Show Columns	Opens the Show Columns Screen .
Content list	Shows the revisions in the repository that match the filter settings.
Add New	Opens the Add New Content Item Screen . Only available in the standalone Repository Manager application.
Add Revision	Opens the Add New Revision Screen . Only available in the standalone Repository Manager application.
Delete Revision	Opens the Delete Revision Screen .
Delete All Revisions	Opens the Delete All Revisions Screen .

A.1.9 Content Interface Screens

The following screens are used to manage content:

- [Section A.1.9.1, "Information Screen"](#)
- [Section A.1.9.2, "Add New Content Item Screen"](#)
- [Section A.1.9.3, "Update Content Info Screen"](#)

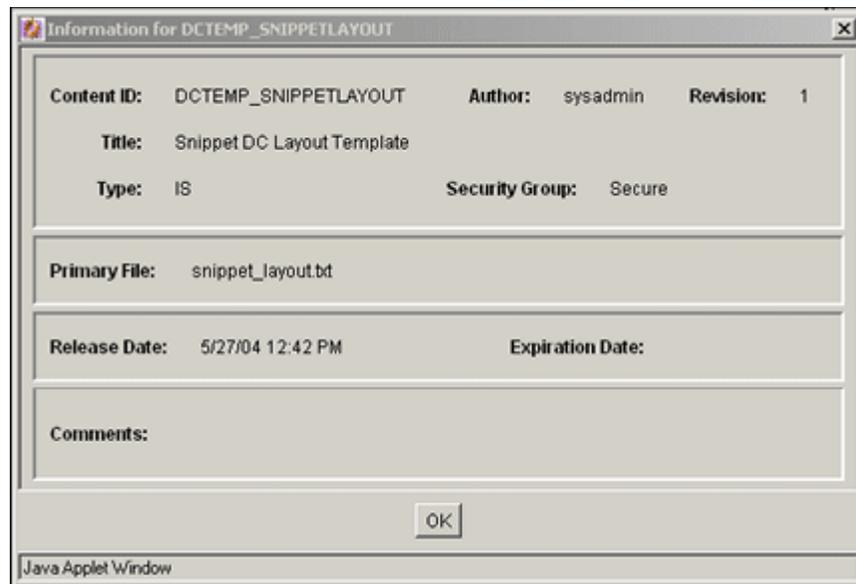
A.1.9.1 Information Screen

This screen is used to view the metadata for a revision.

To access this screen, do one of the following:

- Select a revision on the [Repository Manager: Content Tab Screen](#) then choose **Functions** then **Info**.
- Right-click a revision on the [Repository Manager: Content Tab Screen](#) and choose **Info**.

Standard metadata fields and custom metadata fields are displayed.



A.1.9.2 Add New Content Item Screen

This screen is used to check a new content item into the system without using an Oracle WebCenter Content Server check-in page.

To access this screen, click **Add New** on the standalone [Repository Manager: Content Tab Screen](#). Standard metadata fields and custom metadata fields are displayed.

A.1.9.3 Update Content Info Screen

This screen is used to change the metadata of an existing revision. To access this screen, do one of the following:

- Select a revision on the [Repository Manager: Content Tab Screen](#) and choose **Functions** then **Update** from the Page menu.
- Right-click a revision on the [Repository Manager: Content Tab Screen](#) and choose **Update** from the menu.

Standard metadata fields and custom metadata fields are displayed.

A.1.10 Revision Interface Screens

The following screens are used when working with revisions:

- Section A.1.10.1, "Add New Revision Screen"
- Section A.1.10.2, "Check Out Item Screen"
- Section A.1.10.3, "Undo Check Out Screen"
- Section A.1.10.4, "Resubmit Revision Screen"
- Section A.1.10.5, "Delete Revision Screen"
- Section A.1.10.6, "Delete All Revisions Screen"

A.1.10.1 Add New Revision Screen

This screen is used to check in a revision of an existing content item.

The screenshot shows a dialog box titled "Add New Revision for DCTEMP_PPOINT". The fields are as follows:

- Content ID: DCTEMP_PPOINT
- Author: sysadmin
- Revision: 2
- Title: PowerPoint DC Template
- Type: IS (dropdown menu)
- Security Group: Secure (dropdown menu)
- Primary File: (empty text box with Browse... button)
- Alternate File: (empty text box with Browse... button)
- Release Date: 7/13/06 10:27 AM
- Expiration Date: (empty text box)
- Comments: (empty text area)

At the bottom of the dialog are three buttons: OK, Cancel, and Help.

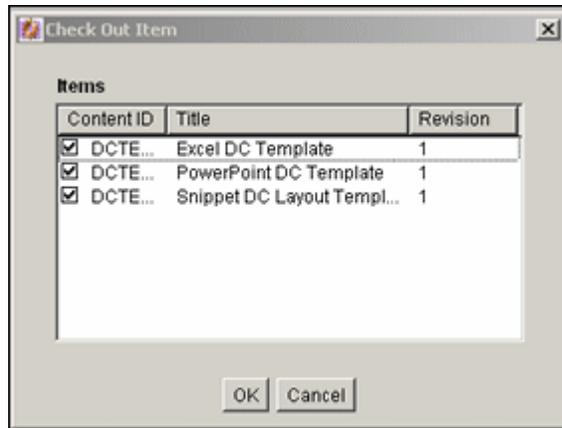
To access this screen, do one of the following on the standalone [Repository Manager Main Screen](#):

- Select a revision then click **Add Revision**.
- Select a revision and choose **Functions** then **Add Revision** from the Page menu.
- Right-click a revision and choose **Add Revision** from the menu.

Standard metadata fields and custom metadata fields are displayed.

A.1.10.2 Check Out Item Screen

This screen is used to check out revisions.



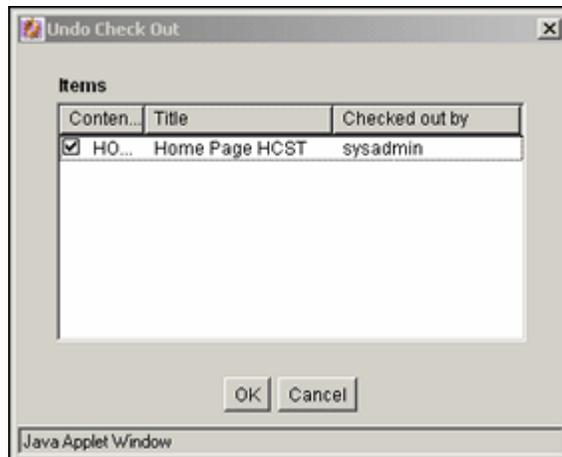
To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#) and do one of the following:

- Choose **Functions** then **Check Out** from the Page menu.
- Right-click and choose **Check Out** from the menu.

Element	Description
check boxes	If selected, the revision is checked out.

A.1.10.3 Undo Check Out Screen

This screen is used to undo a checkout.



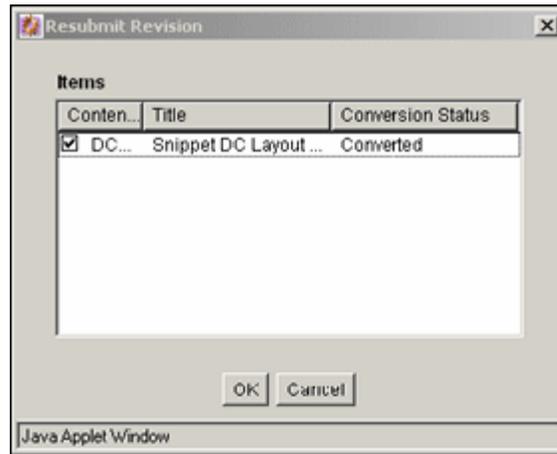
To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#), and do one of the following:

- Choose **Functions** then **Undo Check Out** from the Page menu.
- Right-click and choose **Undo Check Out** from the menu.

Element	Description
check boxes	If selected, the checkout is reversed for the revision.

A.1.10.4 Resubmit Revision Screen

This screen is used to submit a file to Inbound Refinery for conversion.



To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#) and do one of the following:

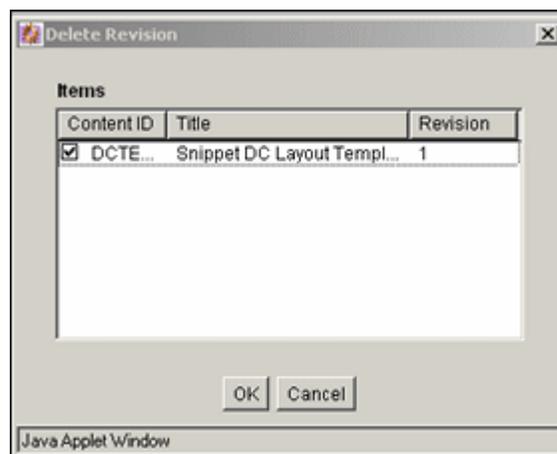
- Choose **Functions** then **Resubmit** from the Page menu.
- Right-click and choose **Resubmit** from the menu.

Note: You cannot resubmit files in the Inbound Refinery queue.

Element	Description
check boxes	If selected, the revision is resubmitted to Inbound Refinery.

A.1.10.5 Delete Revision Screen

This screen is used to delete individual revisions.



To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#) and do one of the following:

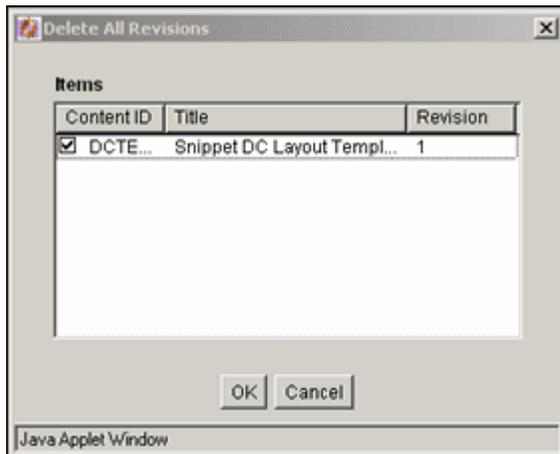
- Click **Delete Revision**.
- Choose **Functions** then **Delete Revision** from the Page menu.

- Right-click then choose **Delete Revision** from the menu.

Element	Description
check boxes	If selected, the revision is deleted.

A.1.10.6 Delete All Revisions Screen

This screen is used to delete all revisions of selected content items.



To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#) and do one of the following:

- Click **Delete All Revisions**.
- Choose **Functions** then **Delete All Revisions** from the Page menu.
- Right-click then select **Delete All Revisions** from the menu.

Element	Description
check boxes	If selected, all revisions of the content item are deleted.

A.1.11 Workflow Revision Interface Screens

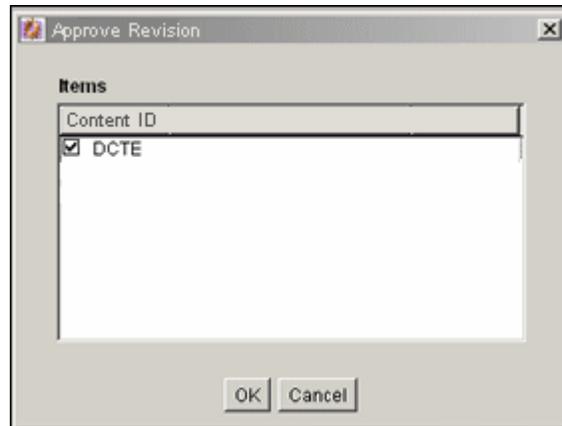
The following screens are used when handling workflows:

- [Section A.1.11.1, "Approve Revision Screen"](#)
- [Section A.1.11.2, "Reject Revision Screen"](#)

A.1.11.1 Approve Revision Screen

This screen is used to approve revisions in a workflow.

Note: Only revisions in a workflow are displayed on this screen.



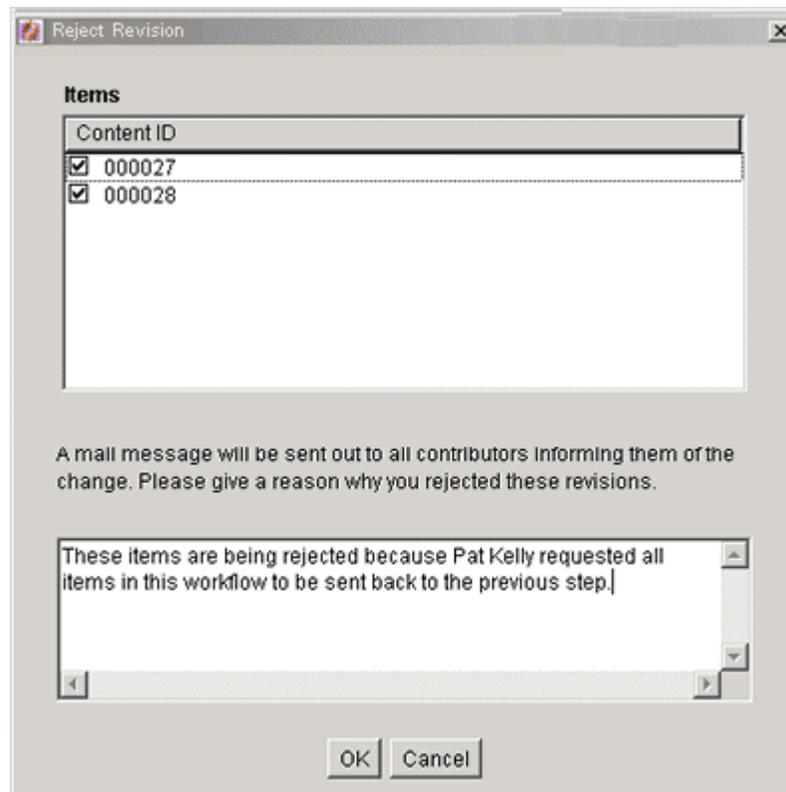
To access this screen, select one or more revisions in a workflow on the [Repository Manager: Content Tab Screen](#) and do one of the following:

- Choose **Functions** then **Approve** from the Page menu.
- Right-click and select **Approve** from the menu.

Element	Description
check boxes	If selected, the revision is approved.

A.1.11.2 Reject Revision Screen

This screen is used to reject revisions in a workflow. Only the revisions in a workflow are displayed on this screen.



To access this screen, select one or more revisions on the [Repository Manager: Content Tab Screen](#) and do one of the following:

- Choose **Functions** then **Reject** from the Page menu.
- Right-click and select **Reject** from the menu.

Element	Description
check boxes	If selected, the revision is rejected.
Rejection message	Message to be sent for all rejected revisions.

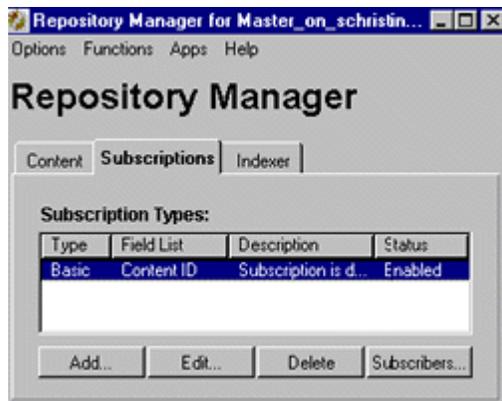
A.1.12 Subscription Interface Screens

The following screens are used when managing subscriptions:

- [Section A.1.12.1, "Repository Manager: Subscriptions Tab Screen"](#)
- [Section A.1.12.2, "Add/Edit Subscription Type Screen"](#)
- [Section A.1.12.3, "Fields Screen"](#)
- [Section A.1.12.4, "Users Subscribed Screen"](#)
- [Section A.1.12.5, "Define Subscription Filter Screen"](#)
- [Section A.1.12.6, "Content Item Subscribed Screen"](#)
- [Section A.1.12.7, "Add Subscription Screen"](#)
- [Section A.1.12.8, "Select User Screen"](#)
- [Section A.1.12.9, "Select Alias Screen"](#)
- [Section A.1.12.10, "Subscribers Screen"](#)

A.1.12.1 Repository Manager: Subscriptions Tab Screen

This screen is used to create and edit Criteria subscriptions.



To access this screen, click **Subscriptions** on the [Repository Manager Main Screen](#).

Element	Description
Type	Name of the subscription.
Field List	Active criteria fields assigned to the subscription.
Description	Description of the subscription.

Element	Description
Status	Status, either enabled or disabled, for the subscription.
Add or Edit	Opens the Add/Edit Subscription Type Screen .
Delete	Removes the subscription from the list.
Subscribers	Opens the Users Subscribed Screen .

A.1.12.2 Add/Edit Subscription Type Screen

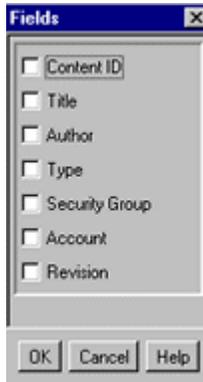
This screen is used to add or edit a subscription.

To access this screen, click **Add** or **Edit** on the [Repository Manager: Subscriptions Tab Screen](#).

Element	Definition
Subscription Type	Name given to the subscription.
Description	Description of the subscription.
Notifications	If selected, e-mail messages are sent to subscribers when content meeting the subscription criteria is checked in or updated.
Criteria Fields pane	The metadata fields used to define the subscription.
Fields	Opens the Fields Screen .

A.1.12.3 Fields Screen

This screen is used to define the metadata fields for a subscription.

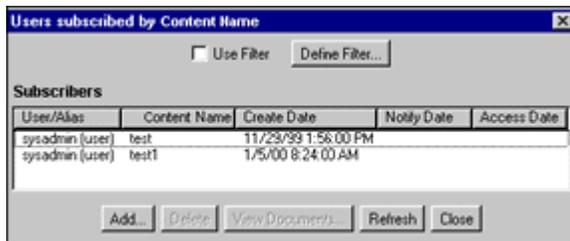


To access this screen, click **Fields** on the [Add/Edit Subscription Type Screen](#).

Element	Definition
check boxes	If selected, the field is included in the subscription criteria.

A.1.12.4 Users Subscribed Screen

This screen is used to view, add, and delete specific users and aliases for a subscription and to view the content items that meet the subscription criteria.



To access this screen, select a subscription and click **Subscribers** on the [Repository Manager: Subscriptions Tab Screen](#).

Element	Description
Use Filter	If selected, filters the list as defined by the Define Subscription Filter Screen .
Define Filter	Opens the Define Subscription Filter Screen .
Subscribers information	Subscribed users and aliases that match the filter settings. Information includes the name of the subscribed content, the date the user was added to the subscription, the last date the user was notified about a revision to the subscribed content, and the last date the user accessed the file defined by the subscription criteria. Note that the access date is not recorded for an alias.
Add	Opens the Add Subscription Screen .
Delete	Deletes the user or alias from the subscription.
View Content Items	Opens the Content Item Subscribed Screen .
Refresh	Refreshes the screen with the most current data.

A.1.12.5 Define Subscription Filter Screen

This screen is used to narrow the list of users and aliases displayed on the Users Subscribed screen.

To access this screen, click **Define Filter** on the [Users Subscribed Screen](#). The [Users Subscribed Screen](#) is filtered based on the criteria entered. You can use the following wildcards in these fields:

- When using MS Access, or MSDE:
 - asterisk (*) for one or more characters
 - question mark (?) for a single character
- With other databases:
 - percent (%) for one or more characters
 - underscore (_) for a single character

Element	Description
Alias Type	If User is selected, only users are shown. If Alias is selected, only aliases are shown.
User/Alias	Specific user or alias name.
Creation Date	Date the user or alias was added to the subscription (regardless of enabled/disabled status).
Last Notification Date	Last date the user was notified about a revision to the subscribed content.
Last User Access Date	Last date the user accessed the file defined by the subscription.

A.1.12.6 Content Item Subscribed Screen

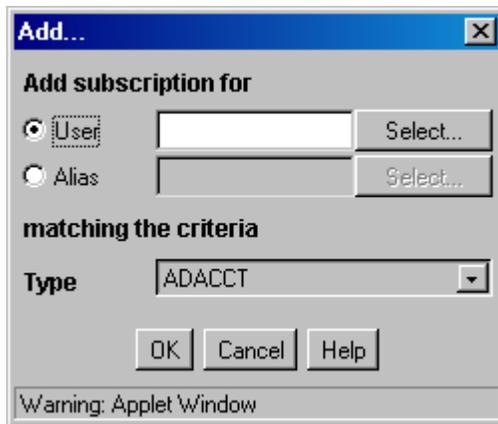
This screen is used to view content items that match the criteria for a subscription.

To access this screen, click **View Content Items** on the [Users Subscribed Screen](#).

Element	Description
Use Filter	If selected, applies the filter defined by the Define Filter Screen .
Define Filter	Opens the Define Filter Screen
Release Date since	If selected, narrows the Content list as defined by the Release Date list.
Show Columns	Opens the Show Columns Screen .
Content list	Shows the subscribed revisions matching the filter settings with a maximum of 50 revisions per page. Double-click a revision to open the Information Screen for that revision. For more details, see Section A.1.2.3, "Define Filter Screen."

A.1.12.7 Add Subscription Screen

This screen is used to add a specific subscription for a user or alias.

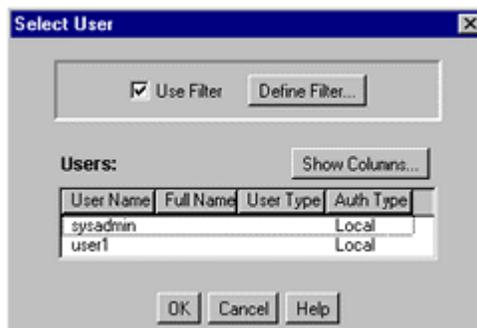


To access this screen, click **Add** on the [Users Subscribed Screen](#).

Element	Description
User or Alias	User or alias to be added to the subscription. Click Select to open the Select User Screen or Select Alias Screen .
Criteria fields	Metadata values subscribed to the selected user or alias. All criteria fields specified for the subscription are displayed.

A.1.12.8 Select User Screen

This screen is used to select a user to assign to a subscription.

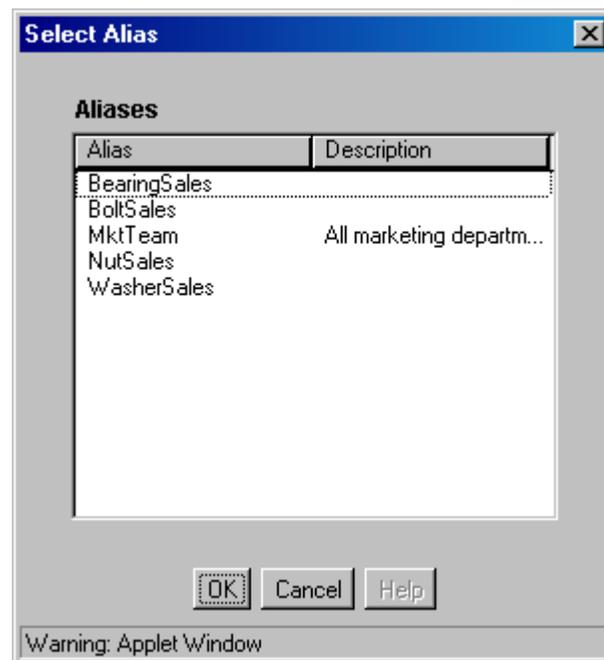


To access this screen, select the **User** option and click **Select** on the [Add Subscription Screen](#).

Element	Description
Use Filter	If selected, narrows the users list as defined by the Define Filter Screen .
Define Filter	Opens the Define Filter Screen .
Show Columns	Opens the Show Columns Screen .
Users list	Users matching the filter settings.

A.1.12.9 Select Alias Screen

This screen is used to select an alias to assign to a subscription.

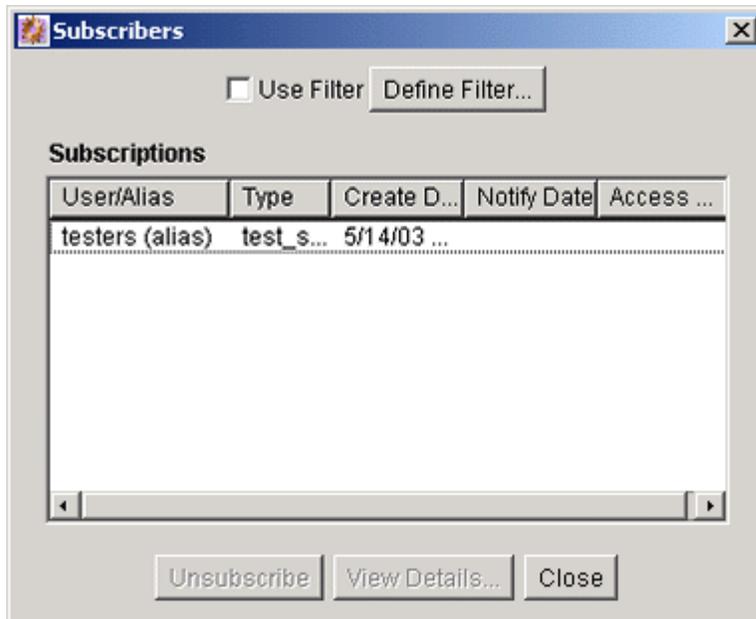


To access this screen, select the **Alias** option and click **Select** on the [Add Subscription Screen](#).

Element	Description
Alias	The available aliases.
Description	Description of the alias.

A.1.12.10 Subscribers Screen

This screen is used to view and unsubscribe users from subscriptions to a specific revision.



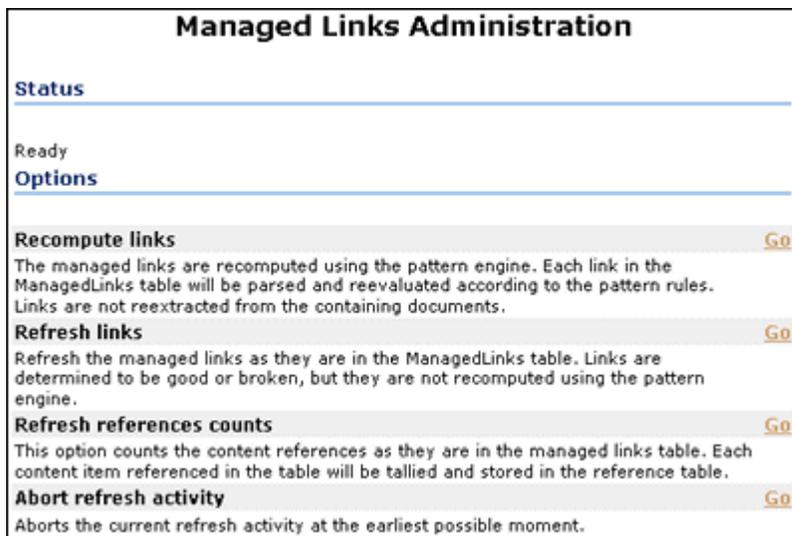
To access this screen, select a revision on the [Repository Manager: Content Tab Screen](#) and do one of the following:

- Select **Functions** then **Subscribers** from the Page menu.
- Right-click and select **Subscribers** from the menu.

See the [Users Subscribed Screen](#) for a description of the fields on this screen.

A.1.13 Managed Links Administration Page

Use the Managed Links Administration Page to update the ManagedLinks and LinkReferenceCount tables.



To access this screen, choose **Administration** then **Managed Links Administration** from the Main menu. Click **Go** next to any option to perform the action.

Element	Description
Status	An indication of activity. If idle, the status is 'Ready'. Otherwise, an indication of the type of refresh being performed, how many links have been processed, and how many errors have been encountered is displayed. Refreshing the page (for example, by pressing F5), refreshes the status message.
Recompute links	Resubmits links to the patterns engine. Use this option if the pattern rules have changed.
Refresh links option	Checks each link in the ManagedLinks table and attempts to determine if the link is valid. Site Studio links are sent to the Site Studio decode method to determine what nodes and content items are used by the link. Use this option if substantial changes were made to Site Studio node/section properties.
Refresh references counts option	Flushes the LinkReferenceCount table and queries the ManagedLinks table for the content item references
Abort refresh activity option	Aborts the current refresh activity.

A.1.14 Schema Interface Screens

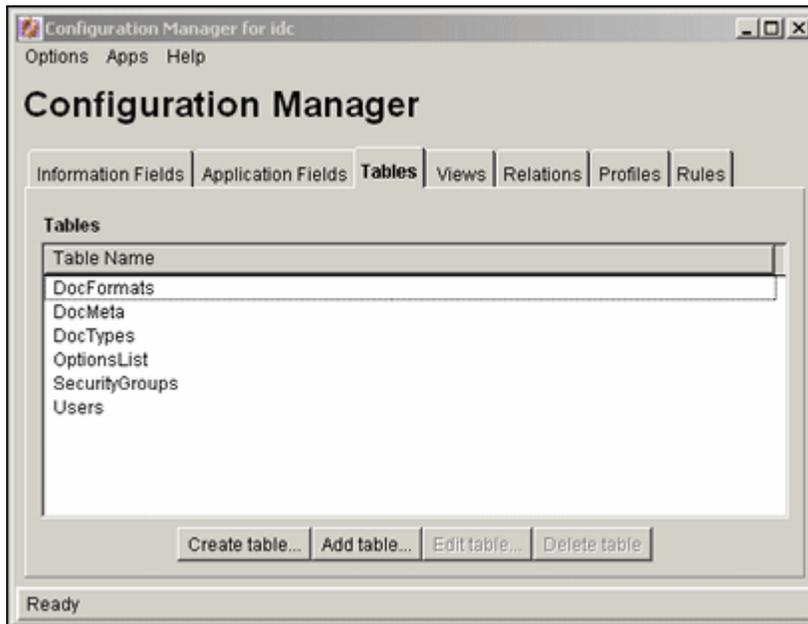
The following screens are used to create a schema:

- [Section A.1.14.1, "Configuration Manager: Tables Tab Screen"](#)
- [Section A.1.14.2, "Select Table Screen"](#)
- [Section A.1.14.3, "Create/Edit Table 'name' Screen"](#)
- [Section A.1.14.4, "Add/Edit Column Screen"](#)
- [Section A.1.14.5, "Configuration Manager: Views Tab Screen"](#)
- [Section A.1.14.6, "Add View Screen: Select Table Screen"](#)
- [Section A.1.14.7, "Add View Screen: Select Columns Screen"](#)
- [Section A.1.14.8, "Add/Edit View Screen"](#)
- [Section A.1.14.9, "Edit Values For Views Screen"](#)
- [Section A.1.14.10, "Add/Edit Value Screen"](#)
- [Section A.1.14.11, "Edit Values: Edit Batch"](#)
- [Section A.1.14.12, "Configuration Manager: Relations Tab"](#)
- [Section A.1.14.13, "Add/Edit Relationship Screen"](#)
- [Section A.1.14.14, "Edit Tree Screen"](#)

A.1.14.1 Configuration Manager: Tables Tab Screen

Important: You can use core Oracle WebCenter Content Server system tables such as Revisions, Alias, Documents, and Users, but you cannot edit the tables themselves.

This screen is used to create or edit tables and columns used in schemas. If existing tables are not used when establishing views and relationships, an external tool must be used to generate records and populate the tables created using the **Tables** tab.

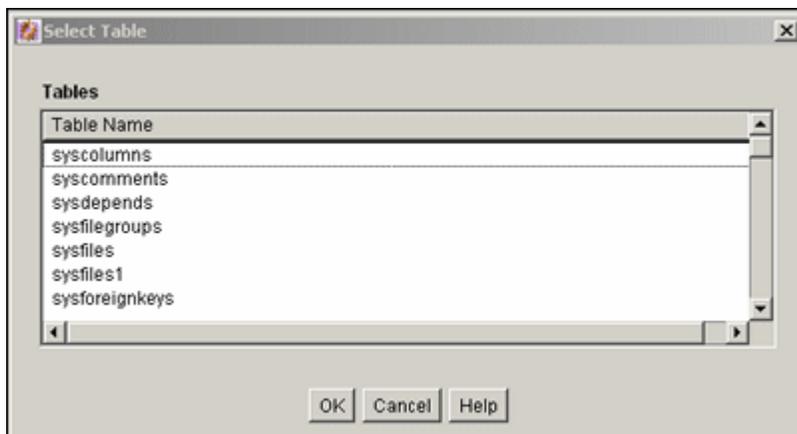


To access this screen, click **Tables** on the [Configuration Manager Page](#).

Element	Description
Table Name	Lists the existing tables.
Create table	Opens the Create/Edit Table 'name' Screen .
Add table	Opens the Select Table Screen .
Edit table	Opens the Create/Edit Table 'name' Screen .
Delete table	Enables deletion of the selected table.

A.1.14.2 Select Table Screen

This screen is used to indicate which tables are used in the schema.



To access this screen, click **AddTable** on the [Configuration Manager: Tables Tab Screen](#) or **Add table** on the [Add View Screen: Select Table Screen](#).

Element	Description
Table Name list	Lists the existing database tables from the list.

A.1.14.3 Create/Edit Table 'name' Screen

This screen is used to specify the columns for tables to be used in a schema.

Important: You can use Core Oracle WebCenter Content Server system tables such as Revisions, Alias, Documents, and Users but you cannot edit the tables themselves.

To access this screen, click **Create Table** or **Edit Table** on the [Configuration Manager: Tables Tab Screen](#) or click **Create Table** on the [Add View Screen: Select Table Screen](#).

Element	Description
Table Name	Name of the table to be created or edited.
Table Description	Description of the table to be created or edited.
Columns	Columns and their properties included in this table.
Add or Edit	Opens the Add/Edit Column Screen .
Delete	Enables deletion of the selected column.
Add Recommended	Adds standard columns to the table such as schPrimaryKey, schCreateTimestamp, and so on.
Row Creation and Row Modification Timestamp Column	Field indicating the time when a row in the table is created or modified. This column must be added to ensure the table replication functions properly.

Element	Description
Synchronize definition	Loads the definition of the table from the database and synchronizes it with the one currently in view. Useful when two people are manipulating the table simultaneously and a warning is issued, indicating that the copy of the table is outdated. Synchronizing the definition updates the table.

A.1.14.4 Add/Edit Column Screen

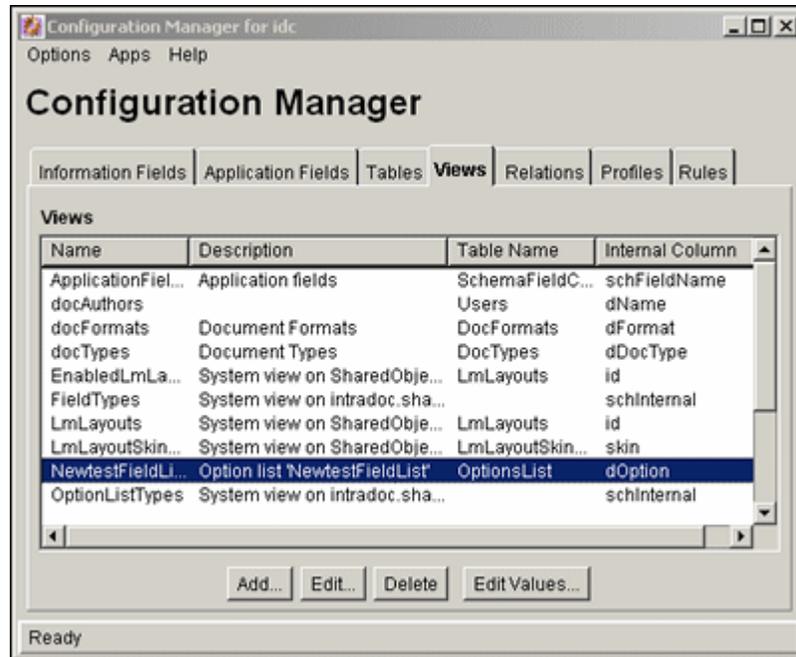
This screen is used to select the column to be the primary key in the schema.

To access this screen, select a column from the [Create/Edit Table 'name' Screen](#) and click **Edit** or click **Add** to create a column.

Element	Description
Column Name	Name of the column to be created or edited. To avoid potential conflicts with Oracle WebCenter Content Server database tables, always add a prefix to column names such as schColumnOne.
Column Type	Column type. Default: varchar.
Column Length	Length of the value to store in the column.
Primary Key	If selected, the column is designated as a primary key for the table.

A.1.14.5 Configuration Manager: Views Tab Screen

This screen is used to create the views used with the schemas.

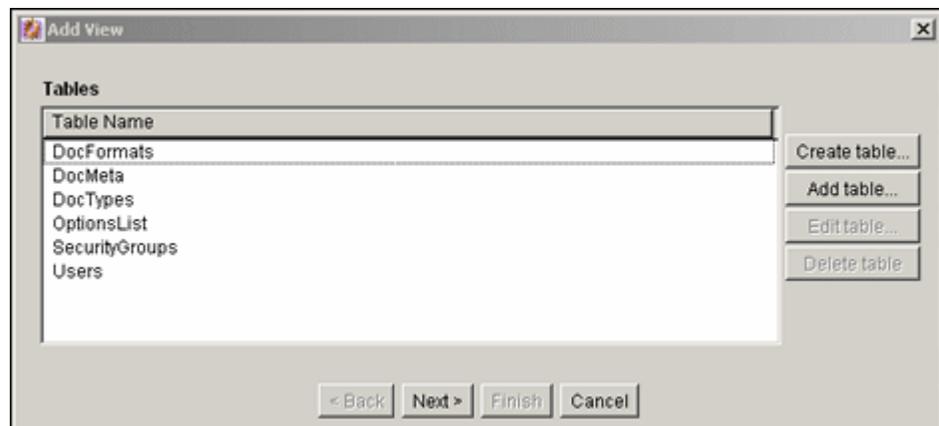


To access this screen, click **Views** on the [Configuration Manager Page](#).

Element	Description
Views	Lists the existing views and related information.
Add	Opens the Add View Screen: Select Table Screen .
Edit	Opens the Add/Edit View Screen .
Delete	Enables deletion of the selected view.
Edit Values	Opens a screen such as the Add/Edit Value Screen or the Option List Screen used to add or change values in the table associated with the view. The screen depends on the type of table used for the view.

A.1.14.6 Add View Screen: Select Table Screen

This screen is used to create a view for a schema.

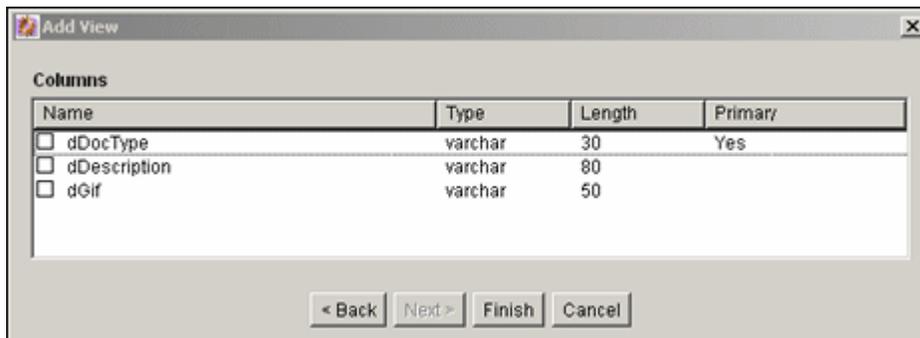


To access this screen, click **Add** on the [Add View Screen: Select Table Screen](#).

Element	Description
Table Name	Lists the tables created that do not have a view.
Create table	Opens the Create/Edit Table 'name' Screen .
Add table	Opens the Select Table Screen .
Edit table	Opens the Create/Edit Table 'name' Screen .
Delete table	Enables deletion of the selected table in this schema.

A.1.14.7 Add View Screen: Select Columns Screen

This screen is used to choose the columns for the schema view.



To access this screen, select a table from the [Add View Screen: Select Table Screen](#) and click Next.

Element	Description
Name list	Names of the existing table columns that you can include in the view and publish to a schema.

A.1.14.8 Add/Edit View Screen

The Add View screen has four main tabs used when adding views.

Add/Edit View Screen: Info Tab

This screen is used to name the new view for the schema.

This screen opens after you choose the columns to use for the view on the [Add View Screen: Select Columns Screen](#) page and click **Finish** or if a view is selected to edit on the [Configuration Manager: Views Tab Screen](#).

Element	Description
View Name	Name of the view to be created or edited.
View Description	Description of the view to be created.
Table Name	The table associated with this view. Click Change Columns to open a screen to select a column.
Internal Column list	Column name in the view being created (used internally).
Visible Column list	Column name displayed to system users.
Default Display Expression	Indicates how the name in the list is displayed. Specify either text or an Idoc Script expression. To prevent the value set for this field being displayed on the Content Information page rather than the actual value assigned to that field, clear this field when creating the view.

Select Columns

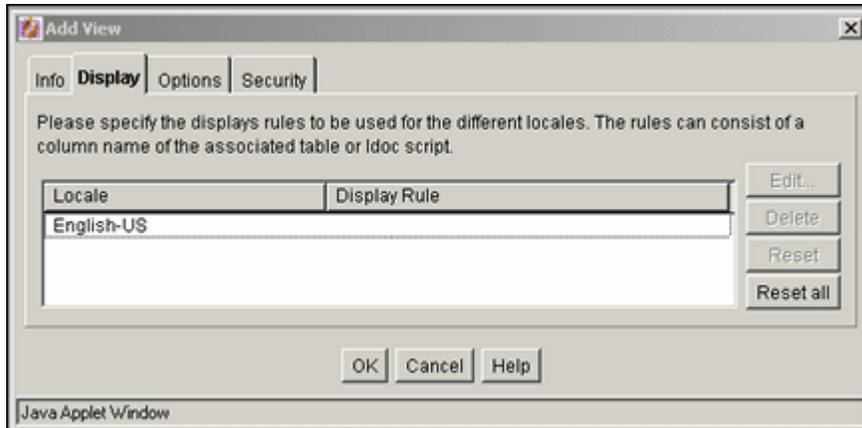
This screen is used to change the list of columns to be used in the schema view.

Name	Type	Le...	Primary
<input checked="" type="checkbox"/> dKey	var...	50	Yes
<input checked="" type="checkbox"/> dOption	var...	50	
<input checked="" type="checkbox"/> dOrder	int	19	Yes

To access this screen, click **Change Columns** on the **Info** tab of the [Add/Edit View Screen](#).

Add/Edit View Screen: Display Tab

This screen is used to specify rules for the display of the schema data.



To access this screen, click **Edit** on the [Configuration Manager: Views Tab Screen](#) or click **Add** on the [Configuration Manager: Views Tab Screen](#) and follow the steps needed to create a view. Click the **Display** tab to open this screen.

Element	Description
Locale/Display Rule list	Lists the defined display rules for the locales.
Edit	Opens the Edit Display Rule screen for the selected rule.
Delete	Enables deletion of the selected locale/display rule.
Reset	Resets the display rule for the selected locale.
Reset all	Resets all of the display rules for their respective locales.

Display Tab: Edit Display Rule

This screen is used to alter the display rules for the schema.



To access this screen, click **Edit** on the **Display** tab.

Add/Edit View Screen: Options Tab

This screen is used to establish the sort order and criteria for the data in the schema.

To access this screen, click **Edit** on the [Configuration Manager: Views Tab Screen](#) or click **Add** on the [Configuration Manager: Views Tab Screen](#) and follow the steps needed to create a view. Click the **Options** tab to open this screen.

Element	Description
Column list	Columns selected using the Add View Screen: Select Columns Screen .
Edit criteria fields	Criteria used to narrow the table values for the view.
Sort by	Selects the database used for sorting. Options include client, server, or database.
Sort Field lists	Lists the columns to be used in sorting.
Sort Order	Sorts either in ascending or descending order.

Add/Edit View Screen: Security Tab

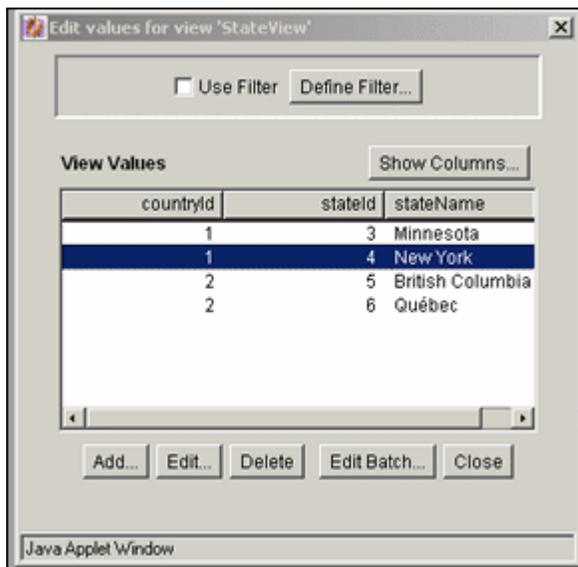
This screen is used to establish the security rules to use for the schema.

To access this screen, click **Edit** on the [Configuration Manager: Views Tab Screen](#) or click **Add** on the [Configuration Manager: Views Tab Screen](#) and follow the steps needed to create a view. Click the **Security** tab to display this screen.

Element	Description
Publish view data	Makes the view visible to other users.
No security	Disables standard filter security for the schema.
Use standard document security	Provides a minimal level of security for the schema and the documents in the schema.
Use custom security implementator	Enables alteration of the security filter.

A.1.14.9 Edit Values For Views Screen

This screen is used to select values assigned to the view for editing. The type of information displayed on this screen is dependent on the type of list chosen to use for the view.



To access this screen, click **Edit Values** on the [Configuration Manager: Views Tab Screen](#). This screen is identical to the [Edit View Values Screen](#), which you can access through the Configuration Manager.

Element	Description
Use Filter	If selected, applies the filter defined by the Define Filter Screen .
Define Filter	Opens the Define Filter Screen
Show Columns	Limits the number of columns to show in the view.
Add or Edit	Opens the Add/Edit Value Screen .
Delete	Enables deletion of a value from the table.
Edit Batch	Opens the Edit Values: Edit Batch screen.

A.1.14.10 Add/Edit Value Screen

This screen is used to change the values in the view or to add a new column to the table associated with the new metadata field.

To access this screen, highlight a value assigned to the view on the [Edit Values For Views Screen](#) and click **Edit**.

A.1.14.11 Edit Values: Edit Batch

This screen is used to alter large amounts of information in a line editor, compared to the single line edits made with the [Edit Values For Views Screen](#), the [Add/Edit Value Screen](#), or the [Edit View Values Screen](#).

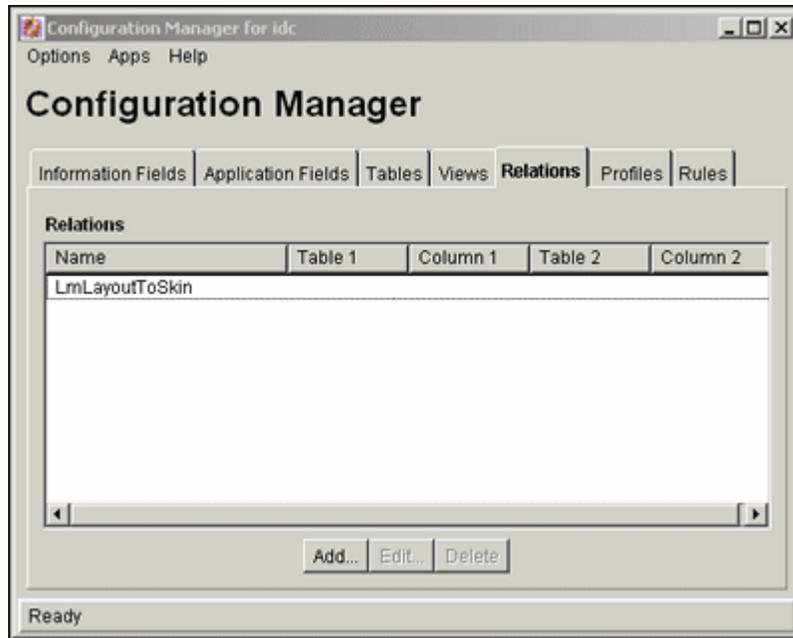
countryId	stateId	stateName
1	3	Minnesota
1	4	New Mexico
2	5	British Columbia
2	6	Québec
1	7	Illinois
1	8	Iowa
4	9	England
1	10	Wisconsin
3	11	Mexico City

To access this screen, click **Edit Batch** on the [Edit Values For Views Screen](#).

The existing columns in the table are displayed. Add values to the table by entering the data in the appropriate columns, separated by a pipe (|) symbol. Each row in the table should begin on a new line.

A.1.14.12 Configuration Manager: Relations Tab

This screen lists the relationship between schema views and schema tables.



To access this screen, click the **Relations** tab on the [Configuration Manager Page](#).

Element	Description
Relations list	Lists the existing relationships between specific tables and columns.
Add or Edit	Opens the Add/Edit Relationship Screen .
Delete	Enables deletion of the selected relationship.

A.1.14.13 Add/Edit Relationship Screen

This screen is used to add or alter a schema relationship between a table and a view.



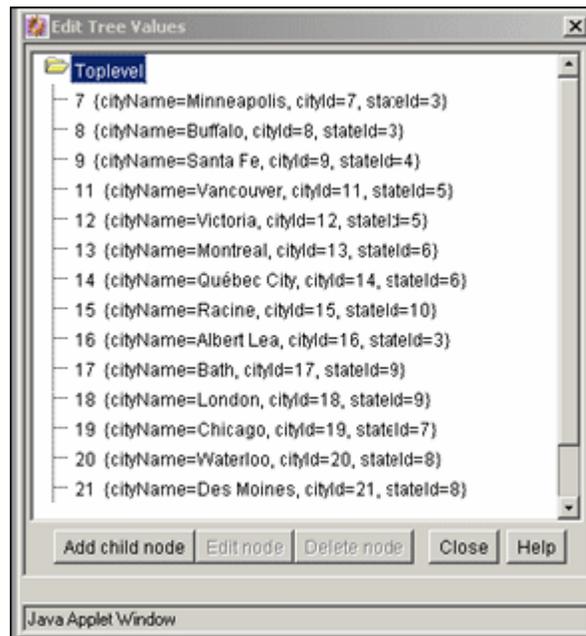
To access this screen, click **Add** or **Edit** on the [Configuration Manager: Relations Tab](#).

Element	Description
Relationship Name	Name of relationship being created or edited.
Relationship Description	Brief description of relationship.
Parent Info list and field	Table that determines choices in dependent choice list and the column in the parent table.

Element	Description
Child Info list and field	Table that is dependent on the choice from the parent table and the column in the child table.

A.1.14.14 Edit Tree Screen

This screen provides a hierarchical view of the values in a list or table.



To access this screen, highlight a field associated with a table and click **Edit Tree** on the [Configuration Manager: Information Field Tab Screen](#). If a list created with the [Option List Screen](#) is used, that list opens, not the hierarchical view of a tree.

Element	Description
Add Child Node	Active when a parent node is selected. Opens the Add Node screen, which has the same functionality as the Add/Edit Value Screen . See that screen for details on use.
Edit Child Node	Active when a node is selected. Opens the Edit Node screen, which has the same functionality as the Add/Edit Value Screen . See that screen for details on use.
Delete node	Deletes a node from the table. If a parent is deleted, children are also deleted.

A.1.15 Content Profile Interface Screens

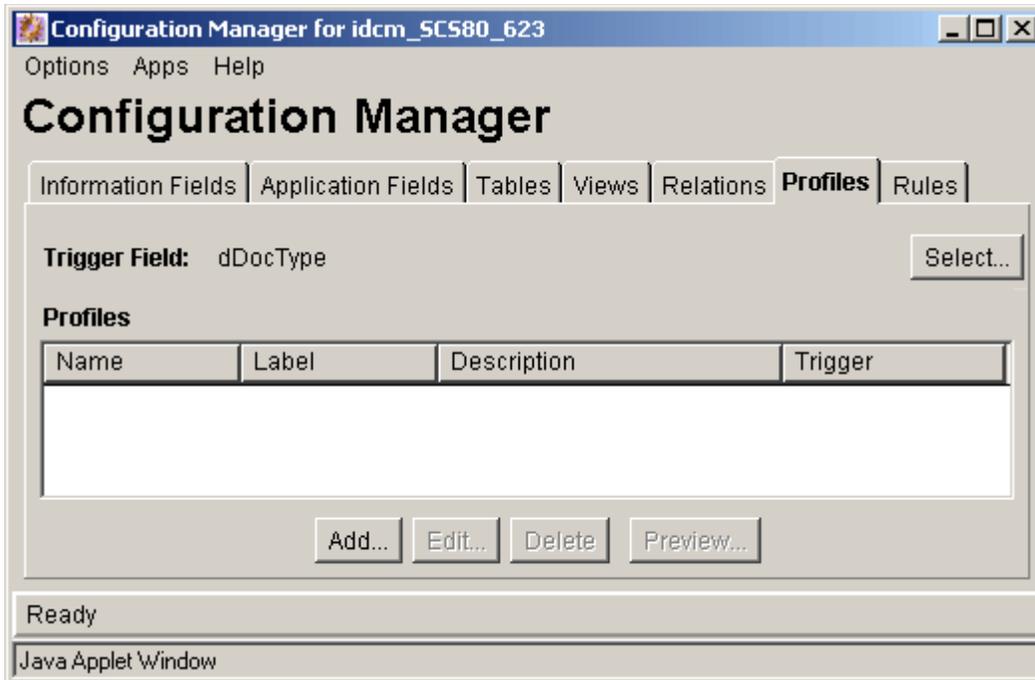
The following screens are used in the creation of a content profile:

- [Section A.1.15.1, "Configuration Manager: Profiles Tab Screen"](#)
- [Section A.1.15.2, "Edit Trigger Field Screen"](#)
- [Section A.1.15.3, "Add Profile Screen"](#)
- [Section A.1.15.4, "Add/Edit Profile Screen"](#)
- [Section A.1.15.5, "Profile Links Screen"](#)

- [Section A.1.15.6, "Check In/Search Link Screen: Conditions Tab, Custom Tab"](#)
- [Section A.1.15.7, "Check In/Search Link: Add Condition Screen"](#)
- [Section A.1.15.8, "Add Rule in Profile Screen"](#)
- [Section A.1.15.9, "Preview Profile Screen"](#)
- [Section A.1.15.10, "Preview Results Screen"](#)

A.1.15.1 Configuration Manager: Profiles Tab Screen

This screen is used to create, edit, delete, and preview profiles.



To access this screen, choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then the **Profiles** tab.

Element	Description
Profiles	Lists the names of existing profiles and other information such as label, description, and the trigger (list values used to identify checked-in documents). Click Select to open the Edit Trigger Field Screen .
Add or Edit	Opens the Add Profile Screen .
Delete	Enables deletion of the selected profile.
Preview	Opens the Preview Profile Screen .

A.1.15.2 Edit Trigger Field Screen

This screen is used to select or change the trigger field.

Caution: When a trigger field is changed, profiles can become invalid. It is the responsibility of the system administrator to resolve the situation. The user interface provides hints about invalid profiles.

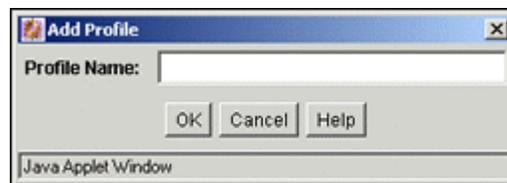


To access this screen, click **Select** on the [Configuration Manager: Profiles Tab Screen](#).

Element	Description
Field Name	List metadata fields defined as lists. If <i>none specified</i> is used, profiles are disabled.

A.1.15.3 Add Profile Screen

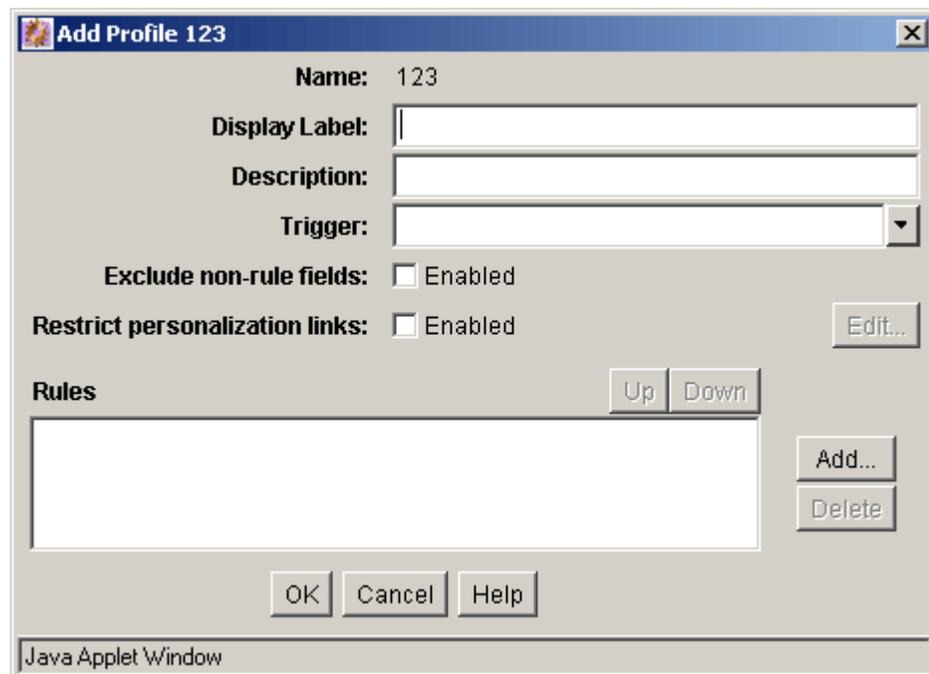
This screen is used to create and name a new profile.



To access this screen, click **Add** on the [Configuration Manager: Profiles Tab Screen](#).

A.1.15.4 Add/Edit Profile Screen

This screen is used to define or edit a profile.

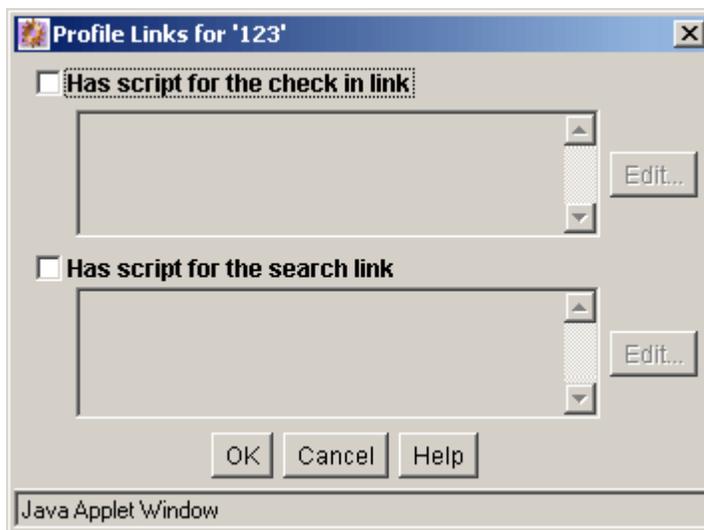


This screen opens when you click **OK** on the [Add Profile Screen](#) or when you select a profile on the [Configuration Manager: Profiles Tab Screen](#) and click **Edit**.

Element	Description
Name	Name assigned to the profile using the Add Profile Screen .
Display Label	Name displayed in the My Check in and My Search profile links.
Description	Description of the profile.
Trigger list	List values associated with the profile trigger.
Exclude non-rule fields	If selected, excludes all metadata fields not belonging to the rules in the profile. If unselected, all metadata fields belonging to all rules are included.
Restrict personalization links	If selected, suppresses check-in or search links to a particular user or group of users. Click Edit to open the Profile Links Screen to edit how links are displayed.
Rules pane	Lists the rules included with the profile.
Up/Down	Adjusts the placement order of the rules in the list. The position of each rule in the list is relevant to its priority in the evaluation process.
Add	Opens the Add Rule in Profile Screen .
Delete	Enables deletion of the selected rule and removal of it from this profile.

A.1.15.5 Profile Links Screen

This screen is used to suppress the display of any or all check-in or search links to a particular user or group of user by adding Idoc Script code that must evaluate to true before the link is displayed in the browser.



To access this screen, select **Restrict personalization links** on the [Add/Edit Profile Screen](#) and click **Edit**.

Element	Description
Has script for the check in link or search link	If selected, the associated Idoc Script must evaluate to true before allowing the display of a link on the Content Check In Form or the Advanced Search Form. If unselected, disables any associated Idoc Script.
Edit	Opens the Check In/Search Link screen.

A.1.15.6 Check In/Search Link Screen: Conditions Tab, Custom Tab

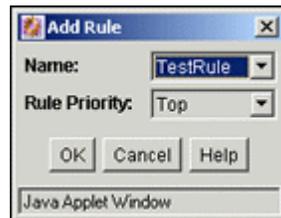
This screen is used to add the conditions that determine if links are displayed on the check-in or search pages. For details about using the **Conditions** tab and the **Custom** tab, see [Section A.1.16.4, "Edit Activation Condition Screen."](#)

A.1.15.7 Check In/Search Link: Add Condition Screen

This screen is used to provide the name of the new condition. To access this screen, click **Add** on the [Check In/Search Link Screen: Conditions Tab, Custom Tab](#). For details, see [Section A.1.16.4, "Edit Activation Condition Screen."](#)

A.1.15.8 Add Rule in Profile Screen

This screen is used to include one or more rules in a profile.



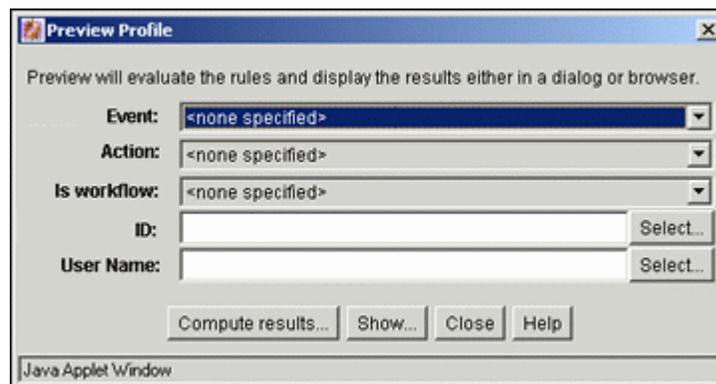
To access this screen, click **Add** on the [Add/Edit Profile Screen](#).

Element	Description
Name	The names of available rules that you can add.
Rule Priority	Adjusts the general placement order of the rules in the list on the Add/Edit Profile Screen . Options include Top, Middle, or Bottom.

A.1.15.9 Preview Profile Screen

Use this screen to simulate and review rules and the trigger field in a profile.

To display the evaluation results in either a dialog or browser window click **Compute results** or **Show**.

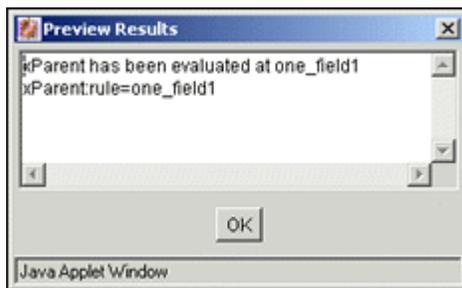


To access this screen, click **Preview** on the [Configuration Manager: Profiles Tab Screen](#).

Element	Description
Event	Specifies when an event is included in the profile evaluation. Options include: <ul style="list-style-type: none"> ■ none specified ■ On Request ■ On Submit ■ On Import
Action	Specifies when an action is included in the evaluation. Options include: <ul style="list-style-type: none"> ■ none specified ■ Check in new ■ Check in selected ■ Content Information ■ Content update ■ Search
Is workflow	Specifies when a workflow state is considered in the evaluation. <ul style="list-style-type: none"> ■ None specified: The document is or is not in a workflow, but its workflow state is not specified. ■ Yes: The document is in a workflow. ■ No: The document is not in a workflow.
Content ID	Content ID of the selected document to use in the evaluation. The value is based on the selected filter criteria. Click Select to open the Content Item View Screen to select other content.
User Name	Name used in the evaluation. The value is based on the selected filter criteria. This field is only used with Compute results and is not used with Show . Click Select to open the User View Screen .
Compute Results	Opens the Preview Results Screen .
Show	Launches a browser window showing a duplicate of the page that the end user sees. It is necessary to select On Request as the Event field value, select an Action value, and leave the User Name field blank.

A.1.15.10 Preview Results Screen

This screen is used to compute and review the selections made on the Preview Profile screen. It shows the coded rule statements (script strings) that result from the preliminary evaluation and reflects any field value changes made to facilitate previewing various profile scenarios.



To access this screen, click **Compute results** on the [Preview Profile Screen](#).

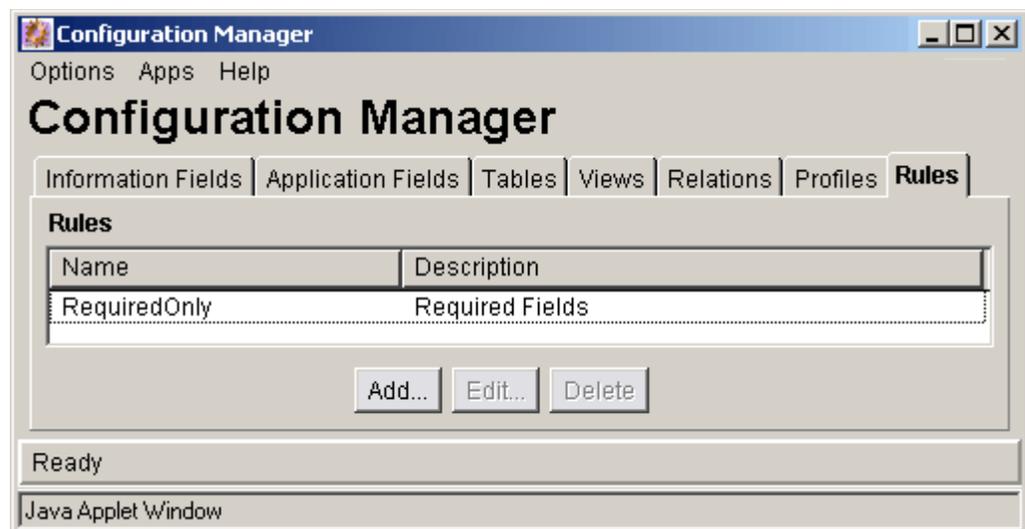
A.1.16 Content Profile Rules Interface Screens

The following screens are used to create profile rules:

- [Section A.1.16.1, "Configuration Manager: Rules Tab Screen"](#)
- [Section A.1.16.2, "Add/Edit Rule Screen"](#)
- [Section A.1.16.3, "Edit Group Header Screen"](#)
- [Section A.1.16.4, "Edit Activation Condition Screen"](#)
- [Section A.1.16.5, "Add Rule Field Screen"](#)
- [Section A.1.16.6, "Add/Edit Rule Field 'name' Screen"](#)
- [Section A.1.16.7, "Edit Default/Derived Value Screens"](#)
- [Section A.1.16.8, "Edit Default/Derived Value: Select Field Screen"](#)
- [Section A.1.16.9, "Edit Derived Value: Conditions Tab"](#)
- [Section A.1.16.10, "Edit Restricted List Screen"](#)

A.1.16.1 Configuration Manager: Rules Tab Screen

This screen is used to create, define, edit, and delete content profile rules.



To access this screen, choose **Administration** then **Admin Applets** from the Main menu. Click **Configuration Manager** then click the **Rules** tab.

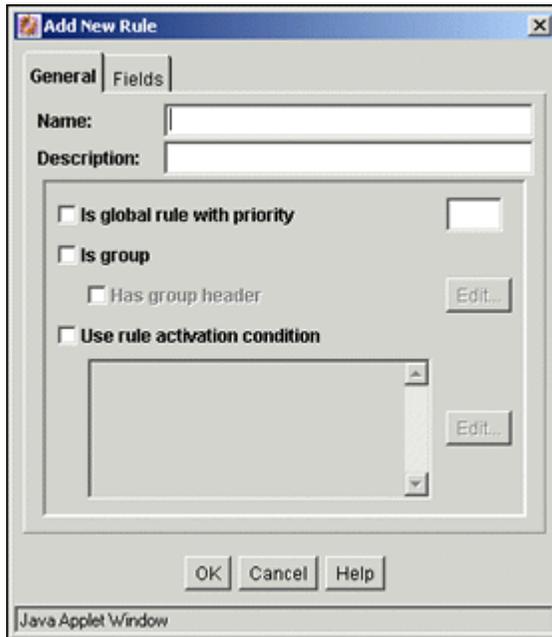
Element	Description
Name	Names of the existing rules.
Description	Description of each rule.
Add/Edit	Opens the Add/Edit Rule Screen where the rule is configured.
Delete	Enables deletion of the selected rule.

A.1.16.2 Add/Edit Rule Screen

This screen has two tabs used to specify rule information and fields for profiles.

Add/Edit Rule Screen: General Tab

This screen is used to specify global rules, define rule groups with optional headers, and define activation conditions.

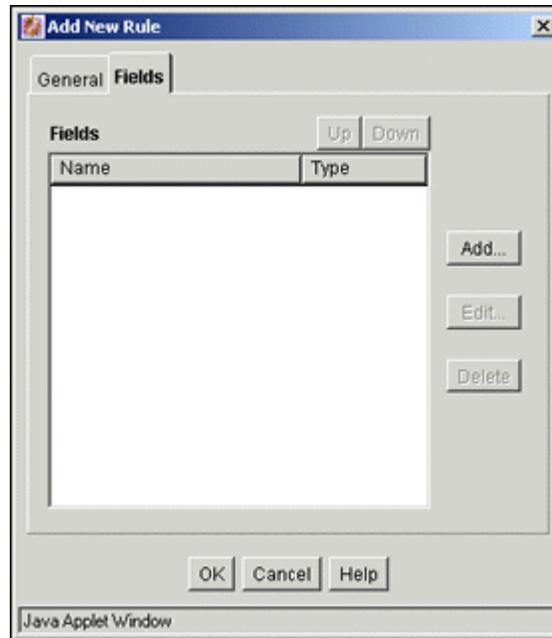


To access this screen, click **Add** or **Edit** on the [Configuration Manager: Rules Tab Screen](#).

Element	Description
Name	Name of the rule being defined or edited.
Description	Description of the rule.
Is global rule with priority and priority field	If selected, enables this as a global rule. The priority field determines the order in which the rule is evaluated. A lower priority rule is executed before higher priority rules, allowing higher priority rules to override the changes made by lower priority rules.
Is group	If selected, groups metadata fields. If unselected, disables field grouping for the rule.
Has group header	If selected, enables the addition of a label to a group of fields belonging to the rule. Click Edit to open the Edit Group Header Screen to specify header formatting.
Use rule activation condition	<p>If selected, enables a profile to change based on rules that are applied or suppressed if specific conditions are met. Sets an activation condition for the rule being defined or edited.</p> <p>The Activation Condition text pane becomes active and displays the computed Idoc Script for each activation condition for the rule. The script statements are automatically generated after the condition is added and its properties are defined. Customized text is also displayed.</p> <p>Click Edit to open the Edit Activation Condition Screen to add or alter conditions.</p>

Add/Edit Rule Screen: Fields Tab

This screen is used to select and add specific metadata fields for use in the rule.



Each metadata field is assigned specific attributes such as the general position within the list of fields in the rule and a display type. For more information about assigning attributes to metadata fields in rules, see [Section A.1.16.5, "Add Rule Field Screen"](#) and [Section A.1.16.6, "Add/Edit Rule Field 'name' Screen."](#)

To access this screen, click **Add** or **Edit** on the [Configuration Manager: Rules Tab Screen](#) and click the **Fields** tab.

Element	Description
Up or Down	Adjusts the placement order of the metadata fields in the list. The position of each metadata field in the list is relevant to its priority in the evaluation process.
Name	The metadata fields belonging to the rule.
Type	The kind of display attribute assigned to each metadata field.
Add	Opens the Add Rule Field Screen .
Edit	Opens the Add/Edit Rule Field 'name' Screen .
Delete	Enables deletion of the selected field and removal of it from this rule.

A.1.16.3 Edit Group Header Screen

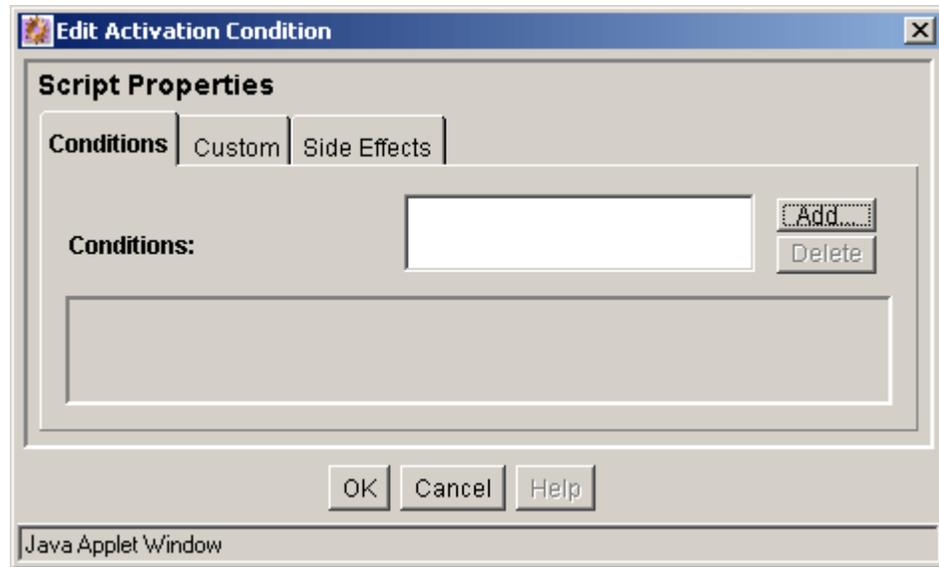
This screen is used to add or edit a header for a group of metadata fields.

To access this screen, select **Is group** and **Has group header** and click the corresponding **Edit** button on the [Add/Edit Rule Screen](#), General tab.

Element	Description
Hide Group by default	If selected, only the group header with a Show link appears when the page loads. If unselected, fields are displayed on pages with a Hide link, you can click to hide the metadata fields.
Start and End Include	Specifies include files that determine layout. Options can be: <ul style="list-style-type: none"> ▪ Standard separator ▪ Start/End HTML table ▪ Display Nothing (default)
Header text pane	Text for the header.

A.1.16.4 Edit Activation Condition Screen

This screen is used to define specific conditions for a rule.



To access this screen, select **Use rule activation condition** and click **Edit** on the [Add/Edit Rule Screen](#).

The **Conditions** tab and **Custom** tab are mutually exclusive. If the **Conditions** tab is used to define rule conditions, the **Custom** tab is disabled.

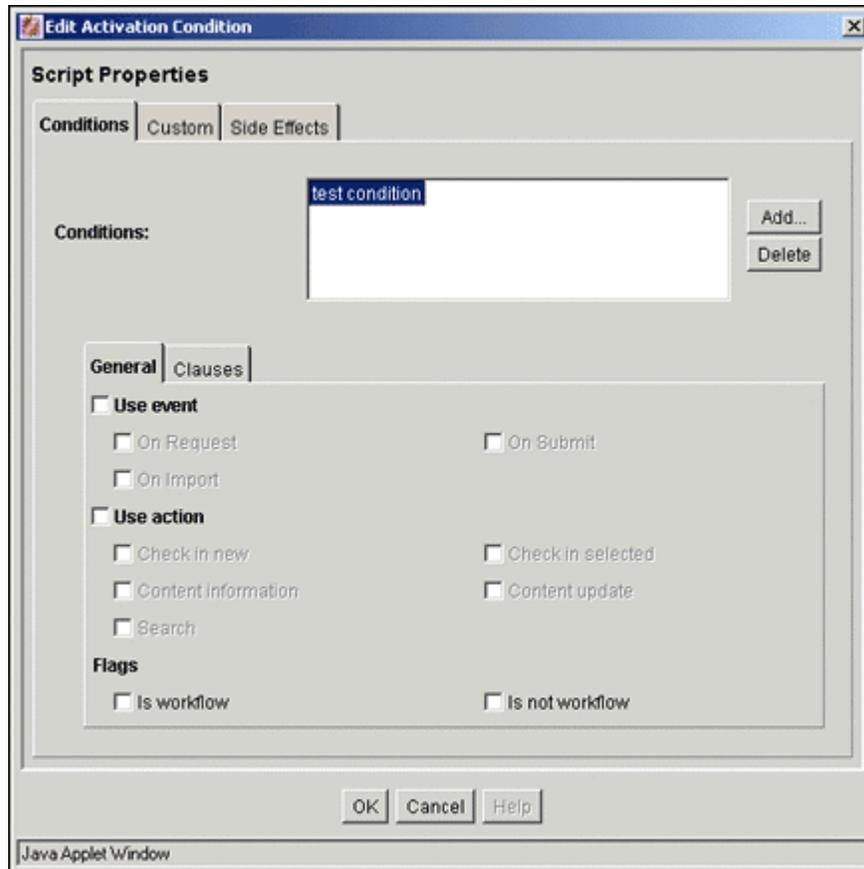
Element	Description
Conditions pane	Activation conditions created for the rule.
Add	Opens a dialog used to enter a condition name.
Delete	Enables deletion of the selected activation condition and removal of it from the rule.

Edit Activation Condition: Conditions Tab

This screen is used to add activation conditions and define them using the General and Clauses panes which are displayed after adding the first condition.

Edit Activation Condition: Conditions Tab: General Pane

This pane is used to specify the event, action, or state that triggers the activation condition of the rule.

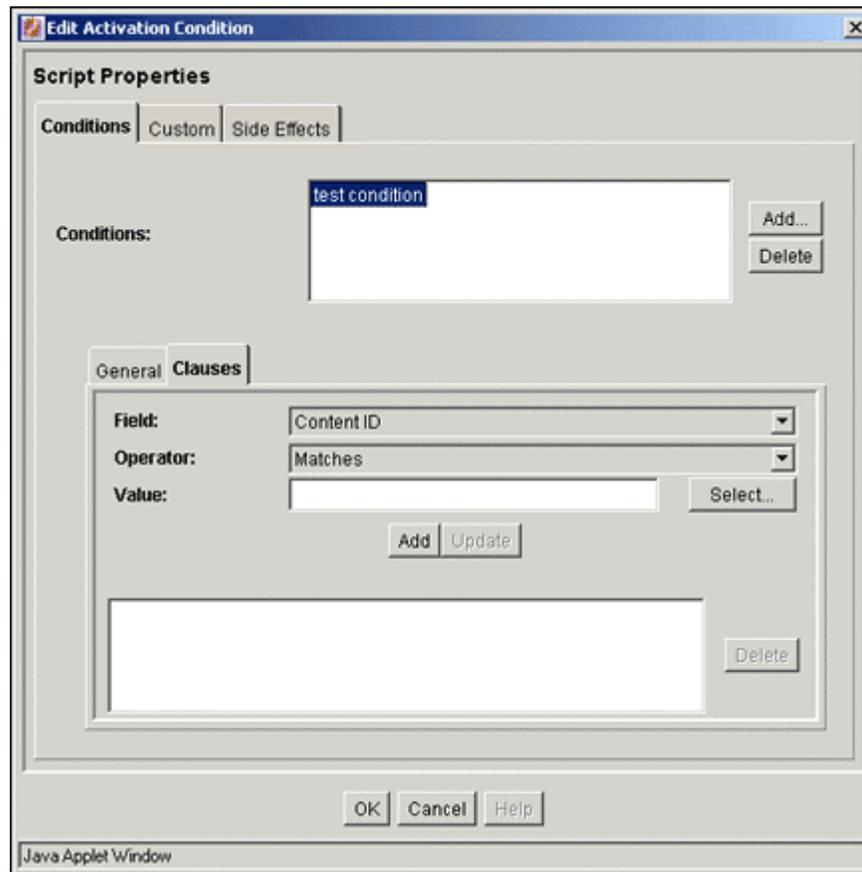


The General and Clauses panes open when you click **Add** and specify an activation condition.

check box	Description
Use event	<p>If selected, enables a profile, rule or both to perform differently using activation conditions based on events as determined by the system. Depending on the event, some profile rules are activated while others are not. Events include:</p> <ul style="list-style-type: none"> ■ On Request ■ On Import ■ On Submit
Use action	<p>If selected, enables a profile, rule or both to perform differently using activation conditions based on a user action detected by the system. Check boxes for these events are enabled when the Use Action check box is selected:</p> <ul style="list-style-type: none"> ■ Check In New ■ Content Information ■ Search ■ Check In Selected ■ Content Update
Is/Is Not in Workflow	<p>If selected, enables a rule to perform differently based on the workflow state of a document. Depending on the state, some profile rules are activated while others are not.</p>

Edit Activation Condition: Conditions Tab: Clauses Pane

This section is used to generate custom Idoc Script clauses for the activation condition of the rule.



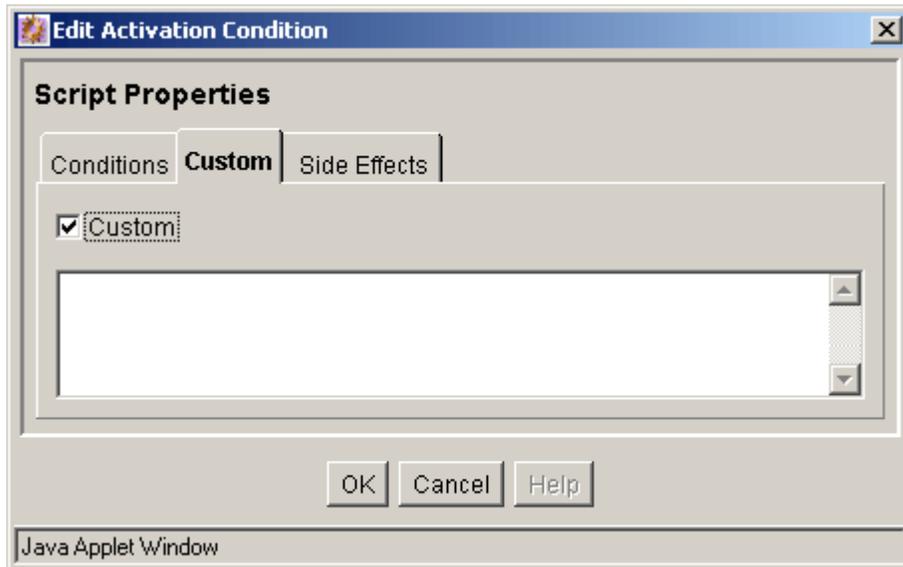
The **General** and **Clauses** tabs open after adding an activation condition. The **Clauses** tab is essentially an Idoc Script wizard. It is primarily used to automate the process of creating Idoc Script statements.

Element	Description
Field	A list of metadata options.
Operator	The method used for searching the metadata fields. Operators include: <ul style="list-style-type: none"> Matches Contains Word Begins With Is Date Before (date operator) Is Date After (date operator)
Value	Depending on the selected field, the value can be an editable field to enter data, a list of options, or an editable field which activates the Select button. If the field value is Content ID, click Select to open the Custom pane. If the field is author, a selection screen of users opens.
Add	Adds the completed clause (Field + Operator + Value) to the Clause pane.
Update	Used to edit the completed clause without deleting and redefining the clause. Highlight the clause in the Clause pane, edit the Value field, and click Update . The revised clause appears in the Clause pane.

Element	Description
Clause pane	Lists the existing clauses for the activation condition.
Delete	Enables deletion of the selected clause.

Edit Activation Condition: Custom Tab

The **Custom** tab and **Conditions** tab are mutually exclusive. If the **Custom** tab is used to define rule conditions, the **Conditions** tab is disabled for the current rule.

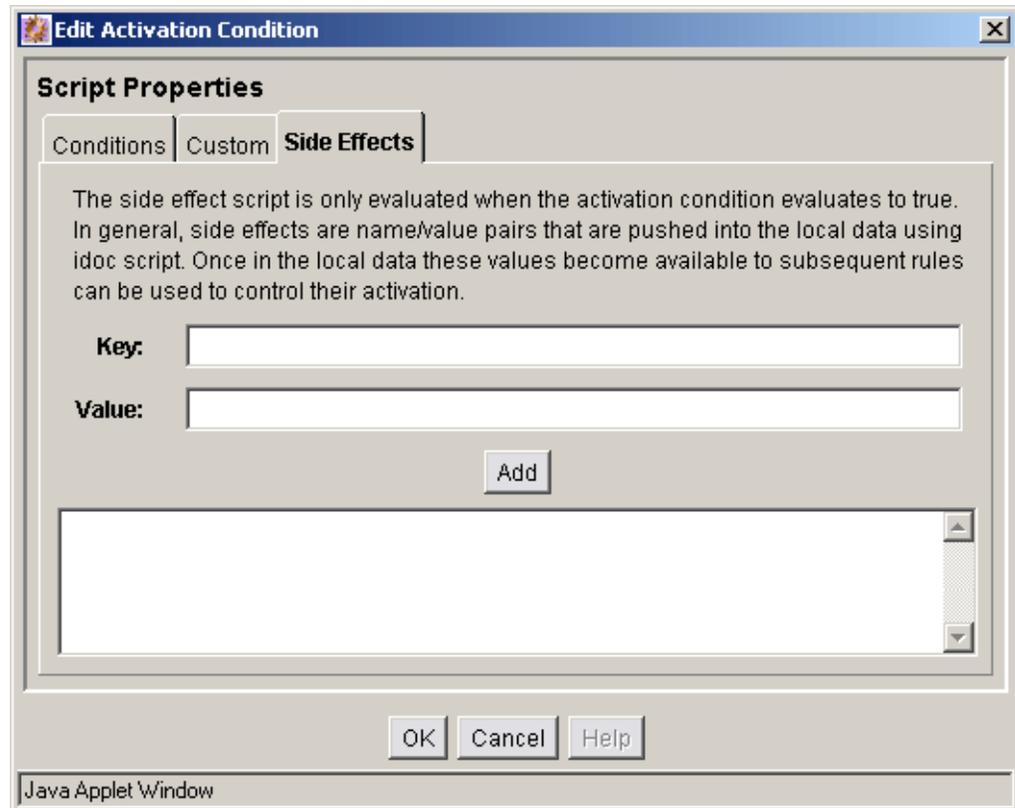


You can access this screen from various points in the user interface.

To use this screen, select **Custom**. The text pane is then enabled where you can enter custom text. The information entered is displayed in the text pane on the [Add/Edit Rule Screen](#).

Edit Activation Condition: Side Effects Tab

This screen is used to define specific side effects of conditions.

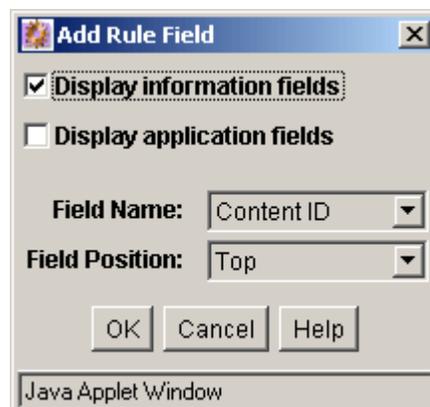


To access this screen, click **Side Effects** on the [Edit Activation Condition Screen](#).

Element	Description
Key	Name used as the Idoc Script variable.
Value	Literal string equating to the Idoc Script variable.
Add	Converts the key and value to Idoc Script and displays it in the Idoc Script pane.

A.1.16.5 Add Rule Field Screen

This screen is used to include one or more metadata fields in the rule.



To access this screen, click **Add** on the [Add Rule in Profile Screen](#), Fields Tab.

Element	Description
Display information fields	If selected (default), lists metadata fields in the Field name list so they are available for display on the standard check-in and search pages.
Display application fields	If selected, lists custom application fields in the Field name list, making them available for display on the standard check-in and search pages. Important: If a rules displays an application field, the field behavior (as defined for the application that normally uses the field) changes.
Field Name	Opens a list of metadata fields that you can add to the rule.
Field Position	Adjusts the placement order of the metadata fields in the list. The position of each metadata field in the list is relevant to its priority in the evaluation process.

A.1.16.6 Add/Edit Rule Field 'name' Screen

This screen is used to add and define the required and optional attributes to the metadata fields belonging to a rule.

This screen opens after adding a metadata field using the [Add Rule Field Screen](#). When editing an existing metadata field (selected from the list on the [Add/Edit Rule Screen](#), Field Tab), this screen opens when you click **Edit**.

Element	Description
Type	List of attribute for the metadata field which determines how the metadata field is displayed on the check-in and search pages. Values include: <ul style="list-style-type: none"> ■ Edit ■ Label ■ Hidden ■ Excluded ■ Required.
Required Message	If Type List is set to Required, a message is also required.
Use custom label	Changes the label displayed in the interface for the field.
Use custom include	Used to reposition standard fields. If selected, allows the use of the include file. Provided files are: <ul style="list-style-type: none"> ■ Standard Separator ■ Display Nothing
Exclude field from the group count	If selected, prevents the field from being counted as part of the group. If unselected (default), the field is included when counting the number of fields in a group.
Use default value and pane	Allows display of a default value on the Content Check In Form or Search page. If selected, the Edit button is enabled and the field can use default values. The pane displays the computed Idoc Script for the default value, which is automatically generated after the default value attribute is added and its properties are defined.
Is derived field and pane	Allows the field to be set to a specified value on update or check-in. Derived values are computed for On Submit and On Import events. If selected, the Edit button is enabled and the field can use derived values. The pane displays the computed Idoc Script for the derived value, which is automatically generated after the default value attribute is added and its properties are defined.
Has restricted list and pane	Allows the list metadata field to be restricted to either a specific list of values or to a filtered list of values. If selected, the Edit button is enabled and the metadata field can use a restricted list. The pane displays the computed Idoc Script for the restrict list field, which is automatically generated after the default value attribute is added and its properties are defined.

Note: The standard include file options listed in the Start Include and End Include lists are defined in the DpDisplayIncludes table of the std_resources.htm file. To add additional include options, a custom component must be written defining the new includes and merging them into the DpDisplayIncludes table.

A.1.16.7 Edit Default/Derived Value Screens

This screen is used to add and define default value field attributes. For details about using the **Conditions** and **Custom** tab, see [Section A.1.16.4, "Edit Activation Condition Screen."](#)

To access this screen, select **Use default value** and click the corresponding **Edit** button on the [Add/Edit Rule Field 'name' Screen](#).

A.1.16.8 Edit Default/Derived Value: Select Field Screen

This screen is used to select a default metadata value to include when the completed default value clause (Field + Operator + Value) is processed. Schema values can also be used to create the default value field attribute if the metadata field is associated with a schema view.



To access this screen, click **Compute** on the [Edit Default/Derived Value Screens](#).

Element	Description
Field Name	Opens a list of metadata options.
Column	Opens a list of table columns. A column is shown only if the metadata field is associated with a schema view.

A.1.16.9 Edit Derived Value: Conditions Tab

This screen is used to add and define derived value field attributes. For details about using the **Conditions** or **Custom** tab, see [Section A.1.16.4, "Edit Activation Condition Screen."](#)

A.1.16.10 Edit Restricted List Screen

This screen is used to allow the list metadata field (on presentation) to be restricted to either a specific list of values or to a filtered list of values resulting from the evaluation process of one or more regular expressions. This choice determines how the system interprets the values entered in the text pane.



To access this screen, select **Has restricted list** and click the corresponding **Edit** button on the [Add/Edit Rule Field 'name' Screen](#).

Element	Description
Restricted value text pane	Allows entry of specific items to be included in the modified list. If the metadata field for this restricted list was defined as a list, the displayed results in the user interface includes the values entered in this pane if they are also in the master list.
Allow Java Regular Expressions	<p>If selected, enables display of a filtered list of values based on the evaluation of one or more regular expressions. Using wildcards and other special characters in the expression displays a subset of all values in the metadata field's usual list that match the evaluated regular expression.</p> <p>If unselected, enables display of a specific set of actual values specified in the text pane if each value is in the master list. This selection overrides the metadata field's master list and sets the list to a specified set of values. The values are not evaluated, so whatever is entered into the text pane is displayed.</p>

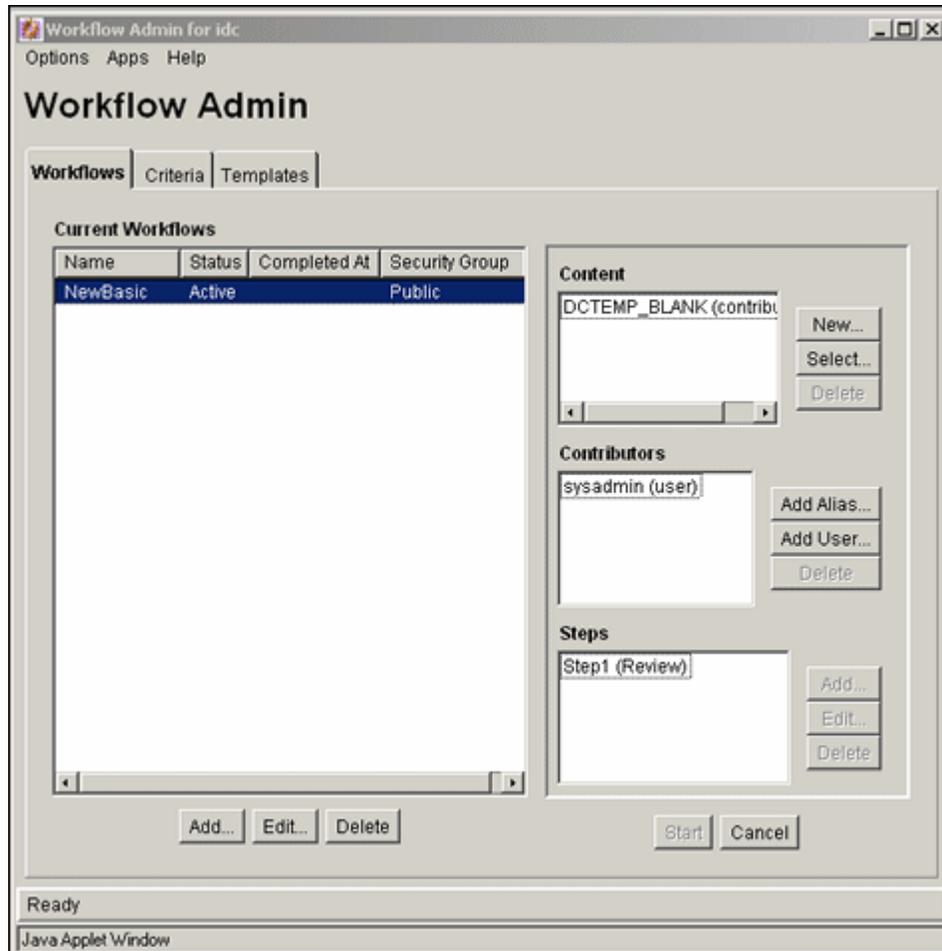
A.2 Workflows User Interface

This section contains information about the interface screens used with workflows. It covers the following topics:

- [Section A.2.1, "The Workflow Admin Screen"](#)
- [Section A.2.2, "The Criteria Workflow User Interface"](#)
- [Section A.2.3, "The Basic Workflow User Interface"](#)
- [Section A.2.4, "Tokens User Interface"](#)
- [Section A.2.5, "The Jump User Interface"](#)
- [Section A.2.6, "Workflow Template Interface Screens"](#)
- [Section A.2.7, "Workflow Scripts User Interface"](#)

A.2.1 The Workflow Admin Screen

This screen is used to manage workflows.



To access this screen, choose **Administration** then **Admin Applets** from the Main menu. Click **Workflow Administration**.

Element	Description
Page Menus	The Options menu is used to access screens to create tokens, templates, and other workflow functionality. The Apps menu accesses other applications, which open in the same mode (applet or standalone) as the current application.
Tabs	The tabs are used to add, edit, or delete the item noted on the tab (Basic workflows, Criteria workflows, or templates).

A.2.2 The Criteria Workflow User Interface

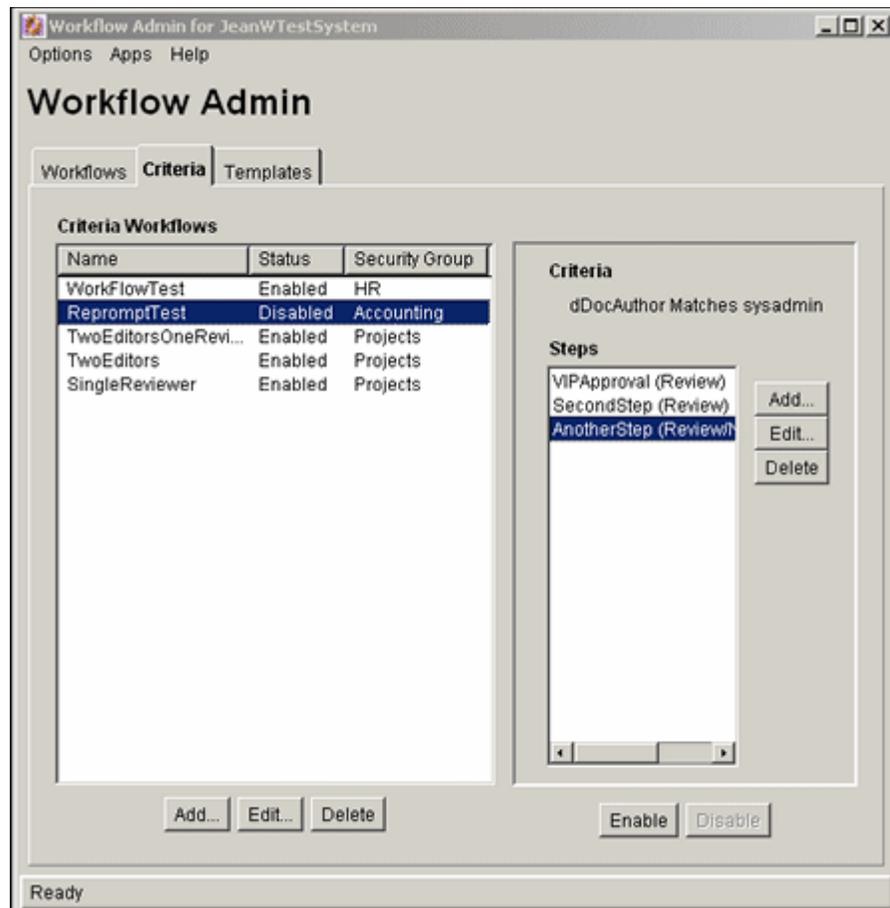
The following screens are used in the creation of criteria workflows:

- [Section A.2.2.1, "Criteria Tab"](#)
- [Section A.2.2.2, "New/Edit Criteria Workflow Screen"](#)
- [Section A.2.2.3, "Add New/Edit Step Screen"](#)
- [Section A.2.2.4, "Add Alias to Step Screen"](#)
- [Section A.2.2.5, "Add User to Step"](#)
- [Section A.2.2.6, "Add Token to Step"](#)

- [Section A.2.2.7, "Edit Additional Exit Condition Screen"](#)

A.2.2.1 Criteria Tab

This screen is used manage all aspects of Criteria workflows and sub-workflows.



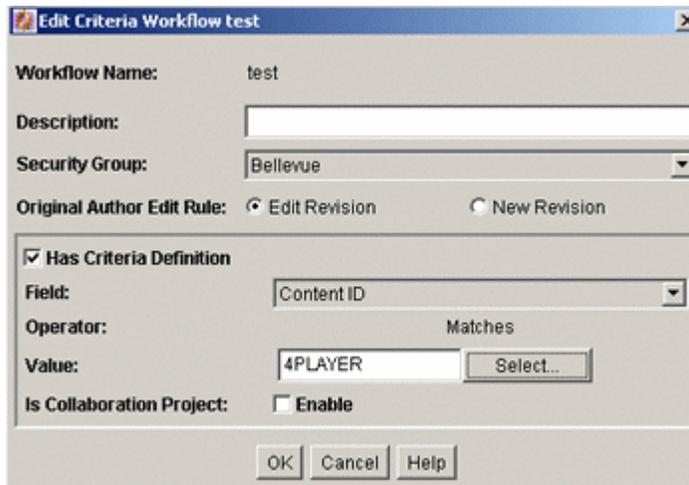
To access this screen, click the **Criteria** tab on the [The Workflow Admin Screen](#).

Element	Description
Criteria Workflow pane	<p>Columns:</p> <ul style="list-style-type: none"> ■ Name: Workflow names. ■ Status: Enabled or disabled. ■ Security Group: Security group that causes the content to enter the workflow. <p>Buttons:</p> <ul style="list-style-type: none"> ■ Add or Edit: Opens the New/Edit Criteria Workflow Screen where criteria for the workflow is specified. ■ Delete: Deletes a selected workflow.

Element	Description
Criteria Step pane	<ul style="list-style-type: none"> Criteria field (top of pane): Shows the criteria defined for the selected workflow. Step list: All steps and step types included in the selected workflow. <p>Buttons:</p> <ul style="list-style-type: none"> Add or Edit: Opens the Add New/Edit Step Screen where steps for the workflow are specified. Delete: Deletes a selected step. Enable: Enables the selected workflow. Disable: Disables the workflow. If items are in a workflow, all revisions are released to the system.

A.2.2.2 New/Edit Criteria Workflow Screen

This screen is used to add or edit a Criteria workflow or sub-workflow.



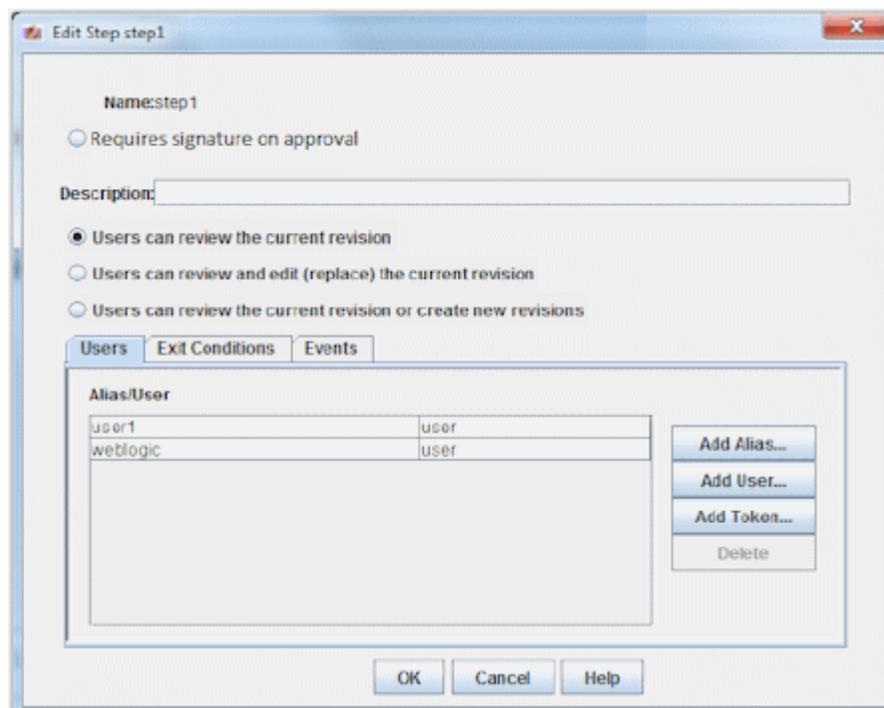
To access this screen, click **Add** or **Edit** in the Criteria Workflow pane of the [Criteria Tab](#).

Element	Description
Workflow Name	Name for the workflow.
Description	Description of the workflow.
Security Group	Security group the revision must be in to enter the workflow.
Use Template	If selected, uses a workflow template and displays a list. Only displayed if at least one workflow template exists.
Original Author Edit Rule	If Edit Revision is selected, keeps the content in the workflow at the existing revision when the original author edits it. If New Revision is selected, the original author can create a new revision of the content after editing the item during workflow.
Has Criteria Definition	If selected, a criteria definition is created. If unselected, a sub-workflow is created.
Field	Field evaluated when each content item is checked in. Options are Content ID, Author, Type, Comment, Account (if accounts are enabled), and any custom metadata fields.

Element	Description
Operator	Defaults to Matches.
Value	Value for the field. Use the asterisk (*) as a wildcard to match one or more characters or the question mark (?) to match one character. click Select to display a list of existing items to use.

A.2.2.3 Add New/Edit Step Screen

This screen is used to add or edit a Criteria workflow step.



To access this screen, select a workflow in the left pane and click **Add** or **Edit** in the right pane of the [Criteria Tab](#).

Element	Description
Name	Name for the step.
Requires signature on approval	If selected, the user must provide credentials for an electronic signature to approve the revision. The standard Approve action is replaced by the Sign and Approve action in the list of step options. This option is only available if you enabled the Electronic Signatures component.
Description	Description for the step.
User check boxes	Selections determine the actions users can take on an item in the workflow.

Users Tab Fields

Element	Description
Alias/User list	Lists the users, aliases, and tokens assigned to the step.

Element	Description
Add Alias, Add User, Add Token	Opens the appropriate screen where you can select an alias, user or a token.
Delete	Deletes the highlighted item.

Exit Conditions Tab Fields

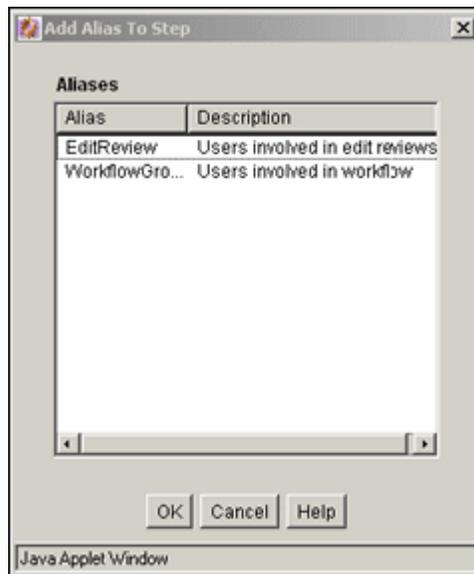
Element	Description
Reviewers and field	Determines how many users must approve the revision before the workflow passes to the next step.
Use Additional Exit Condition	Lists additional conditions to be met before the workflow passes to the next step.
Edit	Opens the Edit Additional Exit Condition Screen .

Events Tab Fields

See [Section A.2.5.1, "Add New/Edit Step Screen: Events Tab"](#)

A.2.2.4 Add Alias to Step Screen

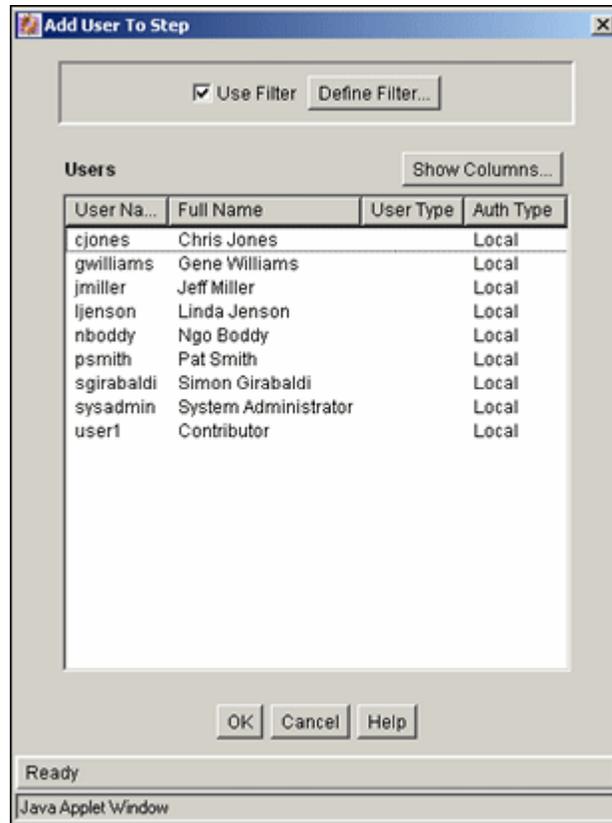
This screen is used to assign aliases to a Criteria workflow step.



To access this screen, click **Add Alias** on the **Users** tab of the [Add New/Edit Step Screen](#). Select an alias from the list and click **OK**.

A.2.2.5 Add User to Step

This screen is used to assign users to a Criteria workflow step.



To access this screen, click **Add User** on the **Users** tab of the [Add New/Edit Step Screen](#). See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns Screen"](#) for details about filtering information. To add a user, select the user name and click **OK**.

A.2.2.6 Add Token to Step

This screen is used to assign workflow tokens to a Criteria workflow step.



To access this screen, click **Add Token** on the **Users** tab of the [Add New/Edit Step Screen](#). This screen is only accessible if tokens are added to the system.

A.2.2.7 Edit Additional Exit Condition Screen

This screen is used to define exit conditions for a Criteria workflow step.

To access this screen, click **Edit** on the **Exit Conditions** tab of the [Add New/Edit Step Screen](#).

Element	Description
Field	The workflow condition or metadata field to be evaluated.
Operator	Operator (such as 'Matches') to use with the field.
Value	Value for the field. Use an asterisk (*) as a wildcard to match one or more characters or a question mark (?) to match a single character. Click Select to open a list of existing items to use for a value in the field. This button appears only when certain metadata fields are selected.
Add	Adds the conditional statement defined by the Field, Operator, and Value fields to the exit condition clause.
Update	Changes the selected conditional statement to the statement defined by the Field, Operator, and Value fields.
Condition Clause pane	Lists the conditional statements that were added to the exit condition. You can append multiple clauses as <i>AND</i> statements.
Delete	Deletes the selected conditional statement.
Custom Condition Expression	<p>If selected, enables display and edit of the Idoc Script generated from the condition clauses. Additional conditions must be Idoc Script statements that evaluate to true or false. The code must not be enclosed in Idoc Script tags <\$ \$>.</p> <p>If unselected, the expression reverts to its original definition. All modifications are lost.</p>

A.2.3 The Basic Workflow User Interface

The following screens are used in the creation of Basic workflows:

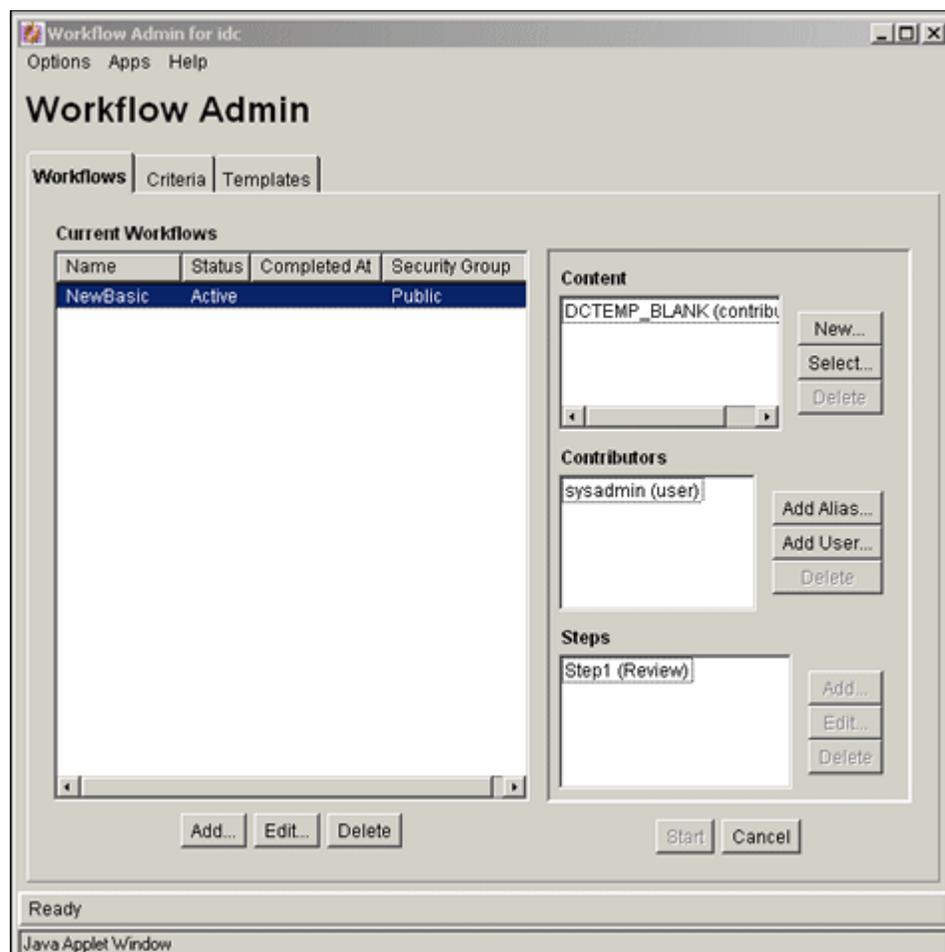
- [Section A.2.3.1, "Workflow Admin: Workflows Tab"](#)

- Section A.2.3.2, "Add New/Edit Workflow Screen"
- Section A.2.3.3, "Add Content to Workflow (New Content) Screen"
- Section A.2.3.4, "Add Content to Workflow (Existing Content) Screen"
- Section A.2.3.5, "Add Alias to Workflow Screen"
- Section A.2.3.6, "Add New/Edit Step Screen"
- Section A.2.3.7, "Add Alias to Step Screen"
- Section A.2.3.8, "Add User: Basic Workflow"
- Section A.2.3.9, "Add Token: Basic Workflow"
- Section A.2.3.10, "Edit Additional Exit Condition Screen"
- Section A.2.3.11, "Start Workflow Screen"

Many of the screens used in the creation of the Criteria workflow are the same screens used in Basic workflows. They are repeated here for completeness.

A.2.3.1 Workflow Admin: Workflows Tab

This screen is used to add, edit, start, cancel, and delete Basic workflows.



To access this screen, click the **Workflows** tab on the [The Workflow Admin Screen](#).

Element	Description
Current Workflow pane	<p>Columns:</p> <ul style="list-style-type: none"> Name: Workflow names. Status: Enabled or disabled. Completed At: When content in a finished workflow was released to the system. Security Group: Security group that causes the content to enter the workflow. <p>Buttons:</p> <ul style="list-style-type: none"> Add or Edit: Opens the Add New/Edit Workflow Screen where criteria for the workflow is specified. Delete: Deletes a selected workflow.
Content pane	<p>Lists the content items included in the selected workflow.</p> <p>Buttons:</p> <ul style="list-style-type: none"> New: Used to add new content to the workflow. Select: Used to select existing content for the workflow. Delete: Deletes the selected item.
Contributors pane	<p>Lists the users, aliases, and tokens assigned to the initial contribution step of the selected workflow.</p> <p>Buttons:</p> <ul style="list-style-type: none"> Add Alias or User: Used to add people to the workflow. Delete: Deletes the selected user from the step.
Steps pane	<p>Lists the steps and step types included in the selected workflow.</p> <p>Buttons:</p> <ul style="list-style-type: none"> Add or Edit: Used to add or edit a step. Delete: Deletes the selected step.
Screen Buttons	<ul style="list-style-type: none"> Start: Opens the Start Workflow Screen where you can compose an e-mail message. Cancel: Cancels the selected workflow. If content is still in the workflow, revisions in the workflow are deleted. Edits are lost unless they were saved on a local drive.

A.2.3.2 Add New/Edit Workflow Screen

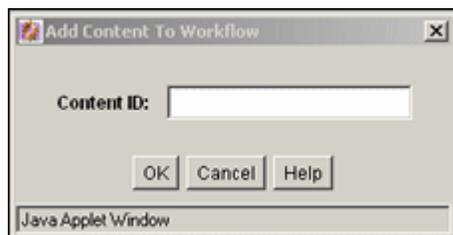
This screen is used to add or edit a Basic workflow.

To access this screen, click **Add** or **Edit** in the Current Workflows pane of the [Workflow Admin: Workflows Tab](#).

Element	Description
Workflow Name	Name for the workflow.
Description	Description of the workflow.
Security Group	Security group for the content items.
Original Author Edit Rule/New Revision	If selected, permits the original author to create a revision of the content when the author edits the content item.
Use Template	If selected, uses a template and displays a list of templates for use. This box is displayed only if a template exists.

A.2.3.3 Add Content to Workflow (New Content) Screen

This screen is used to specify a new content item for a Basic workflow.

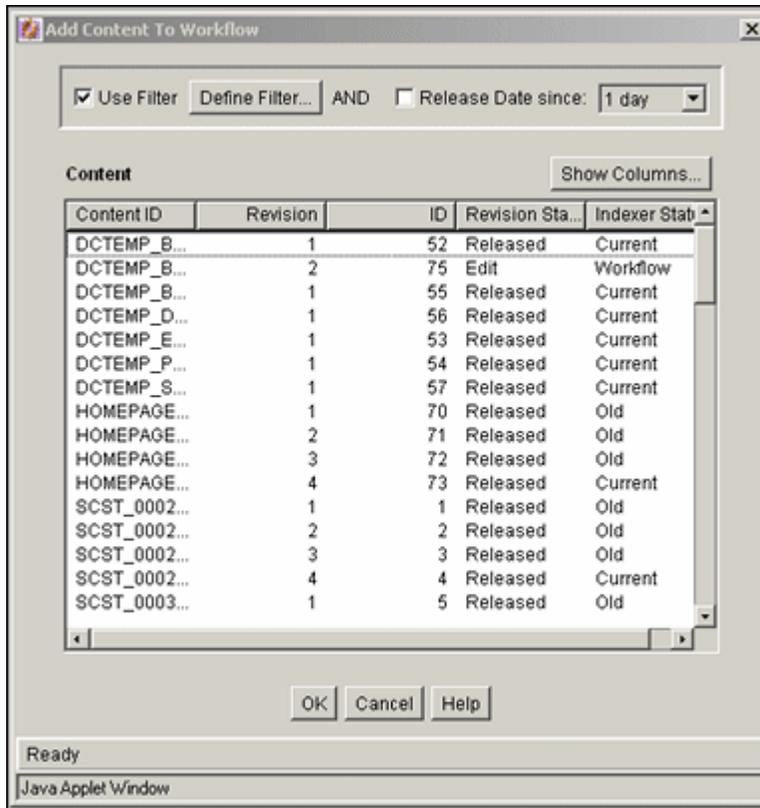


To access this screen, select a workflow in the left pane and click **New** in the Content pane of the [Workflow Admin: Workflows Tab](#).

Element	Description
Content ID	The content to add to the workflow. If using an Oracle database, all Content IDs are converted to uppercase letters automatically.

A.2.3.4 Add Content to Workflow (Existing Content) Screen

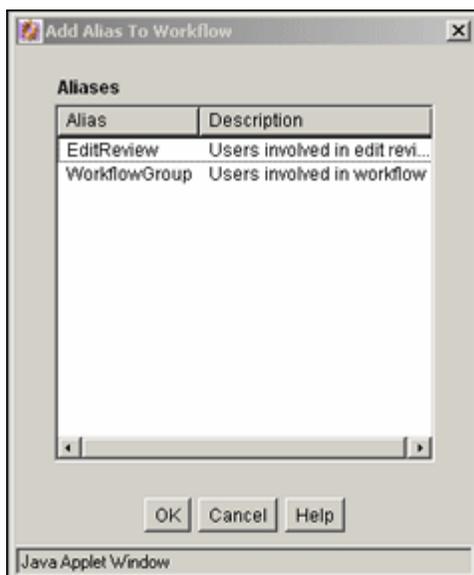
This screen is used to add existing content items to a Basic workflow.



To access this screen, select a workflow and click **Select** in the Content pane of the [Workflow Admin: Workflows Tab](#). See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns Screen"](#) for details about filtering information. To add content, select the content and click **OK**.

A.2.3.5 Add Alias to Workflow Screen

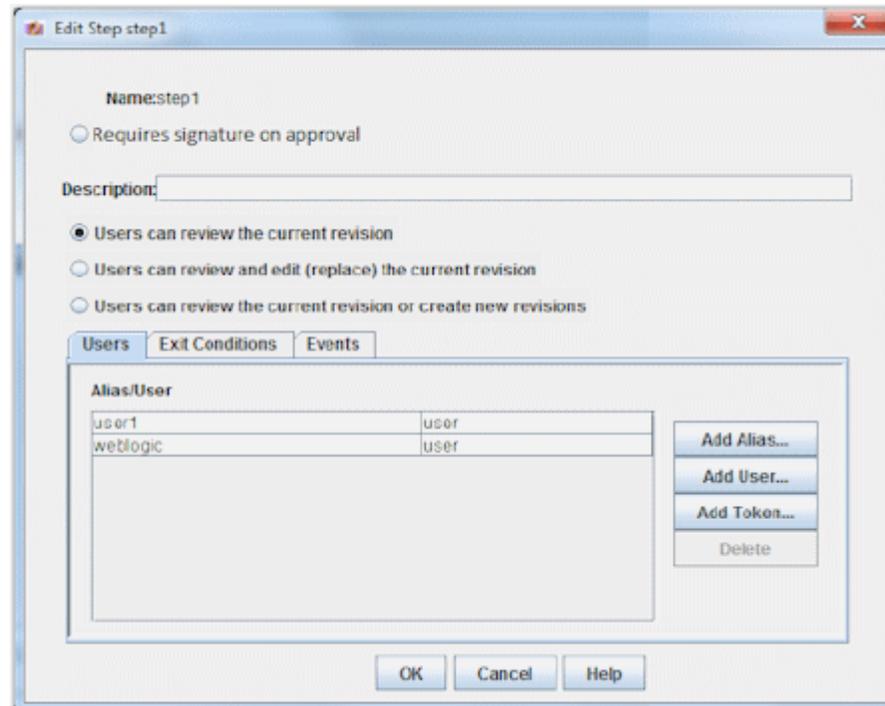
This screen is used to assign alias groups to the initial contribution step of a Basic workflow.



To access this screen, select a workflow and click **Add Alias** in the Contributors pane of the [Workflow Admin: Workflows Tab](#). To add an alias, select the alias and click **OK**.

A.2.3.6 Add New/Edit Step Screen

This screen is used to add or edit a Basic workflow review step.



To access this screen, select a workflow and click **Add** or **Edit** in the Steps pane of the [Workflow Admin: Workflows Tab](#).

Element	Description
Name	Name for the step.
Description	Description for the step.
User check boxes	Select to choose the actions users can take on an item in the workflow.

Users Tab Fields

Element	Description
Alias/User list	Lists the users, aliases, and tokens assigned to the step.
Add User, Add Alias, Add Token	Opens the appropriate screen where you can add an alias, user or a token.

Exit Conditions Tab Fields

Element	Description
Reviewers option	Determines how many users must approve the revision before the workflow passes to the next step.

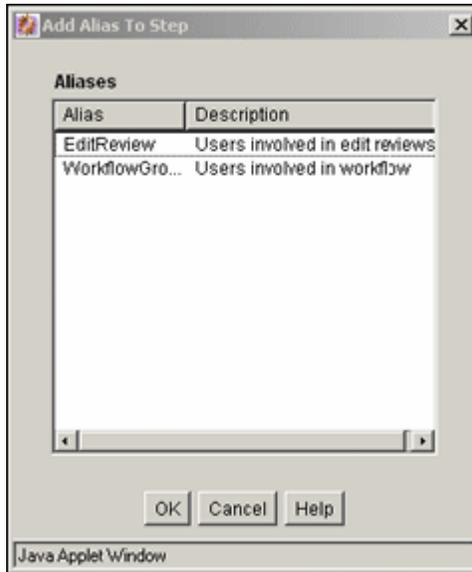
Element	Description
Use Additional Exit Condition	Lists additional conditions to be met before the workflow passes to the next step. Click Edit to open the Edit Additional Exit Condition Screen .

Events Tab Fields

For details, see [Section A.2.5.1, "Add New/Edit Step Screen: Events Tab."](#)

A.2.3.7 Add Alias to Step Screen

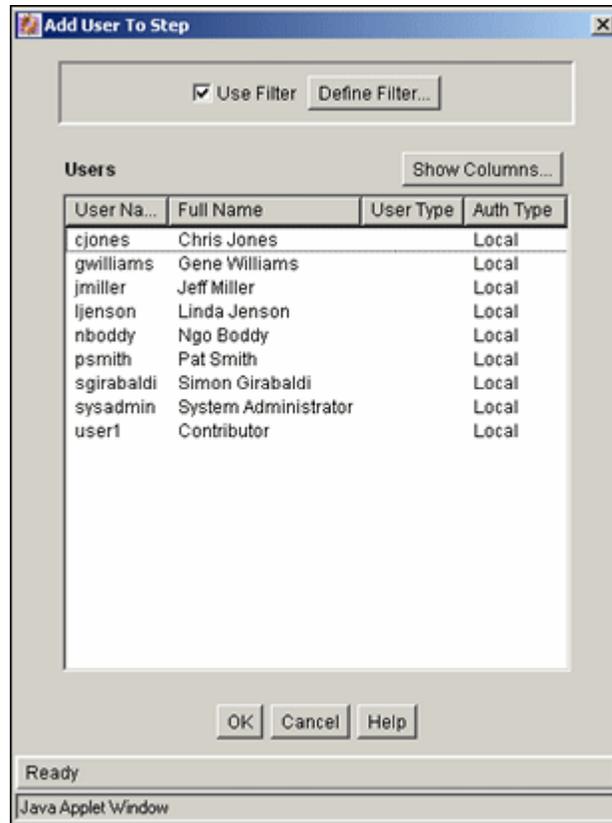
This screen is used to assign aliases to a Basic workflow review step.



To access this screen, click **Add Alias** on the [Add New/Edit Step Screen](#). To add an alias to the workflow, select the alias and click **OK**.

A.2.3.8 Add User: Basic Workflow

This screen is used to assign users to a Basic workflow step.



To access this screen, do one of the following:

- For the contribution step, select a workflow in the left pane and click **Add User** in the Contributors pane of the [Workflow Admin: Workflows Tab](#).
- For a review step, click **Add User** on the [Add New/Edit Step Screen](#).

See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns Screen"](#) for details about filtering information. To add the user, select the name and click **OK**.

A.2.3.9 Add Token: Basic Workflow

This screen is used to assign a workflow token to a Basic workflow review step.



To access this screen, click **Add Token** on the [Add New/Edit Step Screen](#). To add the token, select the token and click **OK**.

A.2.3.10 Edit Additional Exit Condition Screen

This screen is used to define exit conditions for a Basic workflow review step.

To access this screen, click **Edit** in the **Exit Conditions** tab of the [Add New/Edit Step Screen](#).

Element	Description
Field	workflow condition or metadata field to be evaluated.
Operator	Operator (such as 'Matches') to use with the field.
Value	Value for the field. Use an asterisk (*) as a wildcard to match one or more characters or a question mark (?) to match a single character. Click Select to display a list of items to use for a value in the field. This button only appears when certain metadata fields are selected.
Add	Adds the conditional statement defined by the Field, Operator, and Value fields to the exit condition clause.
Update	Changes the selected conditional statement to the statement defined by the Field, Operator, and Value fields.
Condition Clause pane	Lists the conditional statements that were added to the exit condition. You can append multiple clauses as <i>AND</i> statements.
Delete	Deletes the selected conditional statement.
Custom Condition Expression	<p>If selected, enables display and edit of the Idoc Script generated from the condition clauses. Additional conditions must be Idoc Script statements that evaluate to true or false. The code must not be enclosed in Idoc Script tags <\$ \$>.</p> <p>If unselected, the expression reverts to its original definition. All modifications are lost.</p>

A.2.3.11 Start Workflow Screen

This screen is used to start a Basic workflow and add to the e-mail message that is sent to initial contributors.



To access this screen, select a workflow and click **Start** on the [Workflow Admin: Workflows Tab](#).

A.2.4 Tokens User Interface

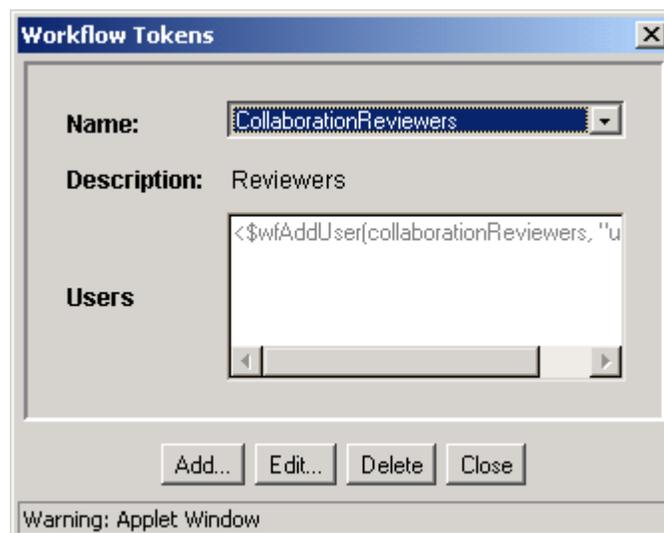
The following screens are all used in the creation and editing of tokens:

- [Section A.2.4.1, "Workflow Tokens Screen"](#)
- [Section A.2.4.2, "Add/Edit Token Screen"](#)
- [Section A.2.4.3, "Add Token User Screen"](#)

A.2.4.1 Workflow Tokens Screen

This screen is used to add, edit, and delete workflow tokens.

The predefined tokens in the Name list are associated with the sample workflow template that is included with the Workflow Admin application. Use these tokens as is, or use them as a basis to customize site-specific tokens.

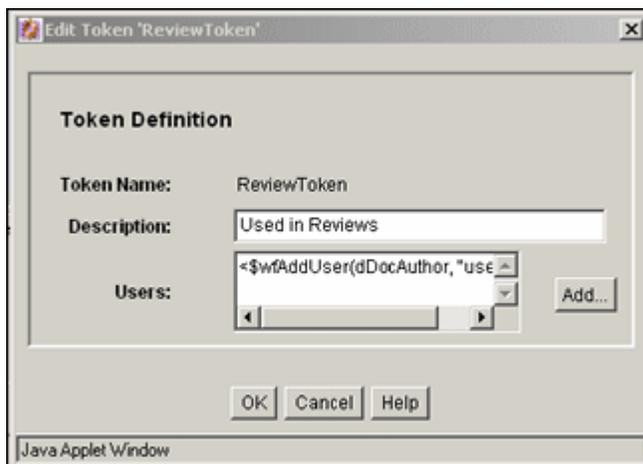


To access this screen, choose **Tokens** from the **Options** menu on the [Workflow Admin: Workflows Tab](#).

Element	Description
Name	Lists the token names.
Description	The description of the selected token.
Users pane	Shows the Idoc Script code that defines the token.
Buttons	<ul style="list-style-type: none"> ■ Add or Edit: Opens the Add/Edit Token Screen. ■ Delete: Enables deletion of the token.

A.2.4.2 Add/Edit Token Screen

This screen is used to add or edit a workflow token.



To access this screen, click **Add** or **Edit** on the [Workflow Tokens Screen](#).

Element	Description
Token Name	The name of the token.
Description	Description of the token.
Users pane	The Idoc Script code that defines the token.
Add	Opens the Add Token User Screen .

A.2.4.3 Add Token User Screen

This screen is used to add a user or alias to a workflow token.



To access this screen, click **Add** on the [Add/Edit Token Screen](#).

Element	Description
Type options	<ul style="list-style-type: none"> ■ User: An individual user login. ■ Alias: A group of users defined by an alias.
Name	The metadata corresponding to a user (dDocAuthor) or the alias.

A.2.5 The Jump User Interface

The following screens are used to create jumps:

- [Section A.2.5.1, "Add New/Edit Step Screen: Events Tab"](#)
- [Section A.2.5.2, "Edit Script for <StepName> Screen"](#)
- [Section A.2.5.3, "Script Properties Screen"](#)
- [Section A.2.5.4, "Select Target Step Screen"](#)
- [Section A.2.5.5, "Add/Edit Jump Screen Tabs"](#)
- [Section A.2.5.6, "Content Item View Screen"](#)

A.2.5.1 Add New/Edit Step Screen: Events Tab

This screen is used to add or edit step event scripts.

To access this screen, click the **Events** tab on the [Add New/Edit Step Screen](#) for a Criteria workflow or the [Add New/Edit Step Screen](#) for a Basic workflow.

Element	Description
Name field	The name for the step.
Description field	A description for the step.
User check boxes	Used to determine the actions users can take on an item in the workflow.
Entry pane	Displays the script that is evaluated when the step is entered. Buttons: <ul style="list-style-type: none"> ■ Clear: Deletes the script. ■ Edit: Opens a screen to edit or create a script.
Update pane	Displays the script that is evaluated when any of the following events occurs: <ul style="list-style-type: none"> ■ Hourly workflow update cycle ■ Update of the revision's metadata ■ Any approval of the revision ■ Any check in of the revision Buttons: <ul style="list-style-type: none"> ■ Clear: Deletes the script. ■ Edit: Opens a screen to edit or create a script.
Exit pane	Displays the script that is evaluated when the revision has completed the requirements of the workflow step. Buttons: <ul style="list-style-type: none"> ■ Clear: Deletes the script. ■ Edit: Opens a screen to edit or create a script.

A.2.5.2 Edit Script for <StepName> Screen

This screen is used to select an editing option for a step event script.



To access this screen, click **Edit** for the event on the [Add New/Edit Step Screen: Events Tab](#).

Element	Description
Edit Current	If selected, opens the Jump tab with the current script. This option is displayed only if a script exists for the event.
Create New	If selected, opens a blank Jumps tab.
Use Script Template	If selected, opens the Jumps tab with the selected script template. This option is displayed only if a script template exists.

A.2.5.3 Script Properties Screen

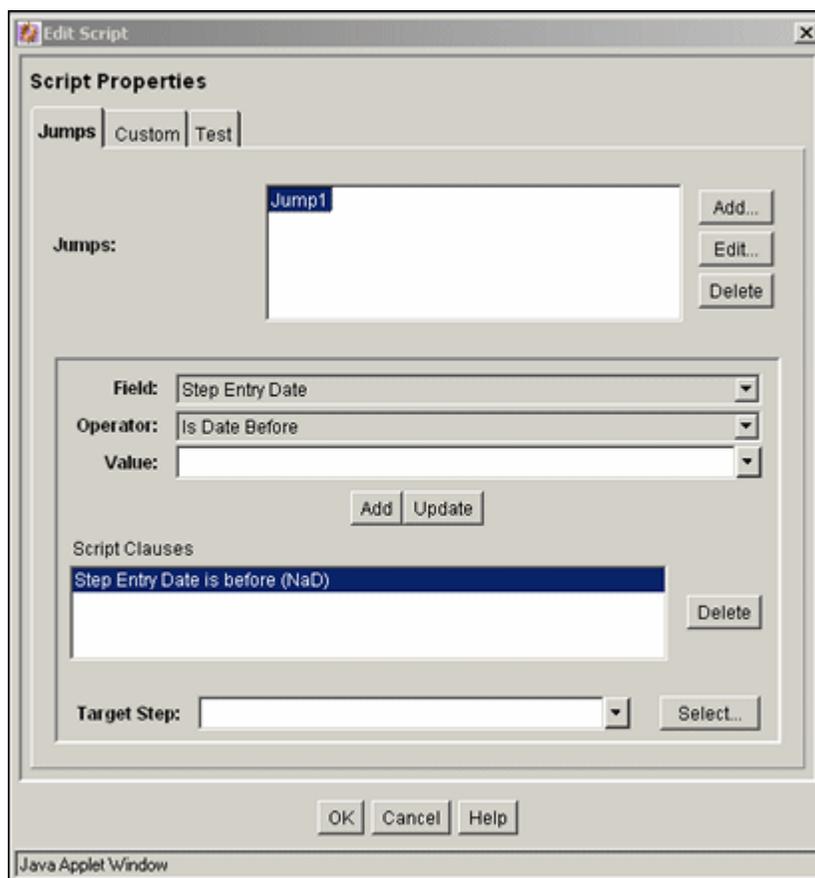
This screen is used to create, modify, and test step event scripts.

To access this screen, do one of the following:

- If an event script or script template does not exist, click **Edit** on the [Add New/Edit Step Screen: Events Tab](#).
- If an event script or script template exists, click **OK** on the [Edit Script for <StepName> Screen](#).

Script Properties: Jumps Tab

This screen is used to create step event script code.



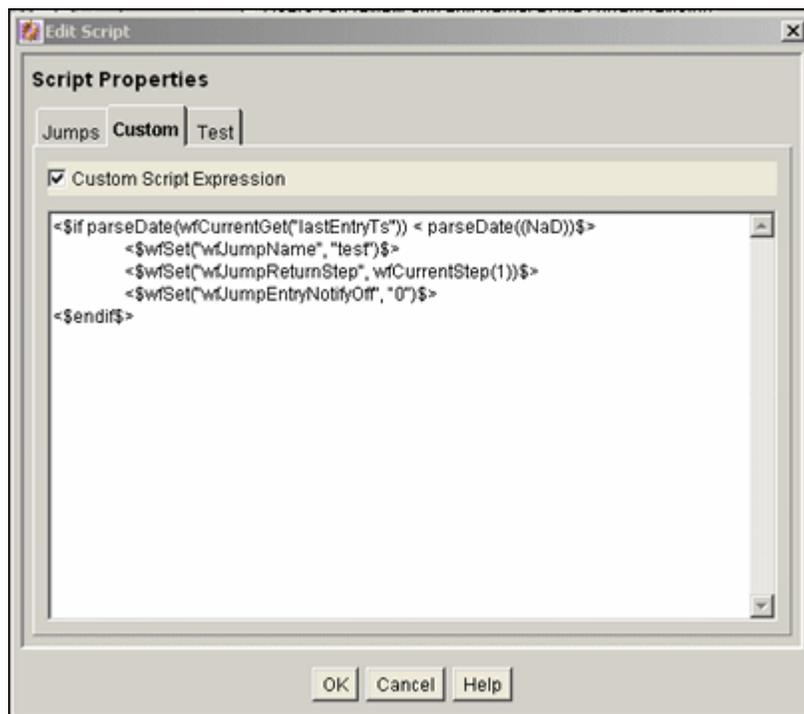
To access this screen, click the **Jumps** tab on the [Script Properties Screen](#).

Element	Description
Jumps pane	Lists the jumps included in the script. Buttons: <ul style="list-style-type: none"> ■ Add or Edit: Used to add or edit the side effects. ■ Delete: Used to delete the selected jump.
Center pane	<ul style="list-style-type: none"> ■ Field: Condition or field to be evaluated. ■ Operator: Operator to use with the field. ■ Value: Value for the specified metadata field. Use an asterisk (*) as a wildcard to match one or more characters and a question mark (?) to match a single character.
Add	Adds the conditional statement defined in the center pane to the jump.

Element	Description
Update	Changes the selected conditional statement to the statement defined in the center pane
Script Clauses pane	Lists the conditional statements added to the jump. You can append multiple clauses as <i>AND</i> statements.
Delete	Deletes the selected conditional statement.
Target Step list	Specifies a target step for the jump. Choose a value to specify a symbolic step name. Click Select to choose a step from a list.

Script Properties: Custom Tab

This screen is used to edit the script that was generated automatically by the options on the **Jumps** tab.

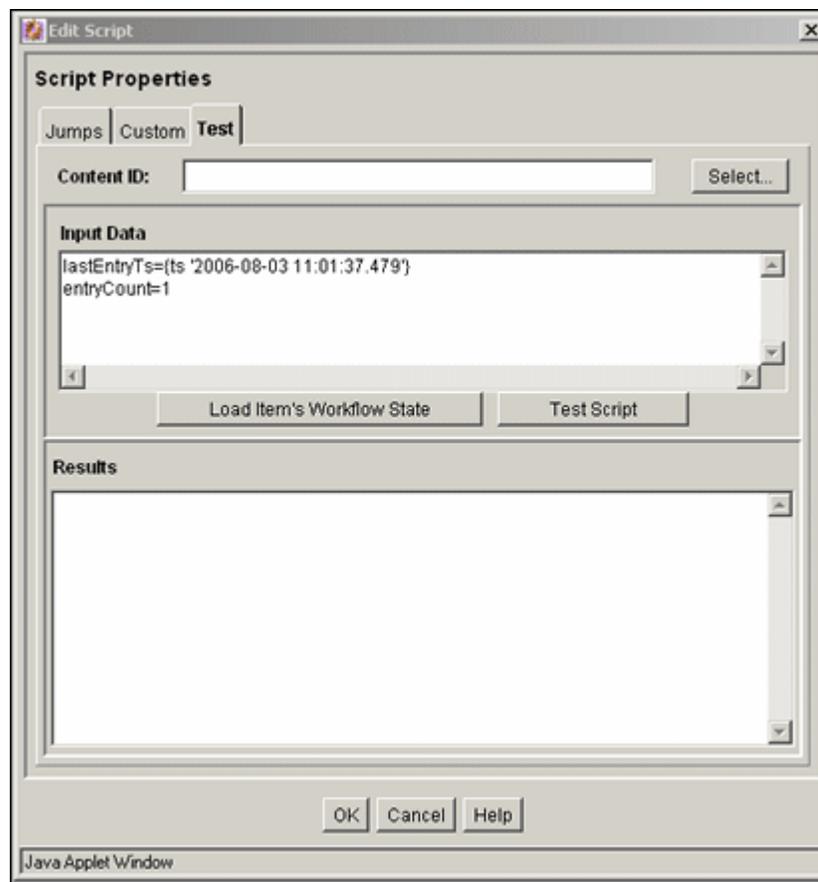


To access this screen, click the **Custom** tab on the [Script Properties Screen](#).

Element	Description
Custom Script Expression	If selected, you can edit and save the script revision. If unselected, the script reflects the statements defined on the Jumps tab. You cannot edit jumps from the Jumps tab.
Script pane	Shows the script of all jumps in the script template.

Script Properties: Test Tab

This screen is used to test a step event script.

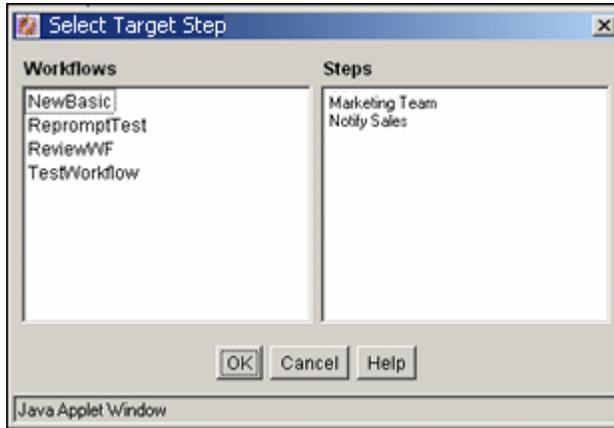


To access this screen, click the **Test** tab on the [Script Properties Screen](#).

Element	Description
Content ID	Content ID for a content item to be tested. Click Select to open a screen where you can select a content item.
Input Data pane	Displays the data that is tested when a workflow is selected and the content items's workflow state is loaded.
Load Item's Workflow State	Loads the companion file for the selected content item. If the selected content item is not in a workflow, the content item is treated like it newly entered the workflow.
Test Script	Tests the script and displays the results in the Results pane.
Results pane	Displays the results of the script test. Idoc script error messages are displayed processing errors occurred.

A.2.5.4 Select Target Step Screen

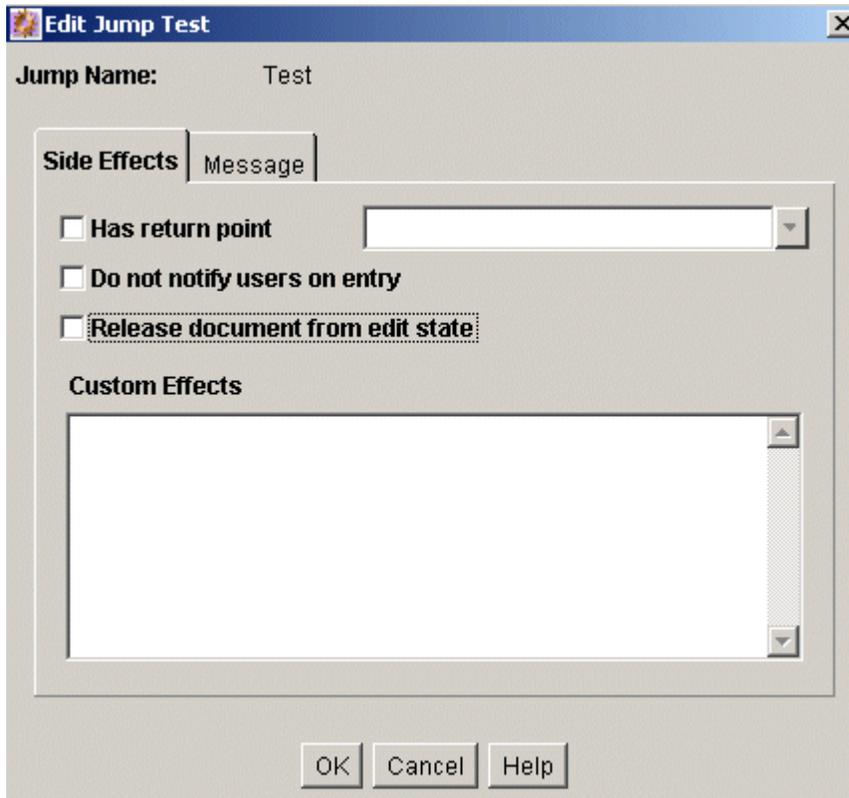
This screen is used to add a specific target step to a jump.



To access this screen, click **Select** on the [Script Properties Screen](#), Jump Tab. Choose a workflow to display the steps. Select the step to use in the target and click **OK**.

A.2.5.5 Add/Edit Jump Screen Tabs

This screen is used to add or edit jump side effects and notification messages.

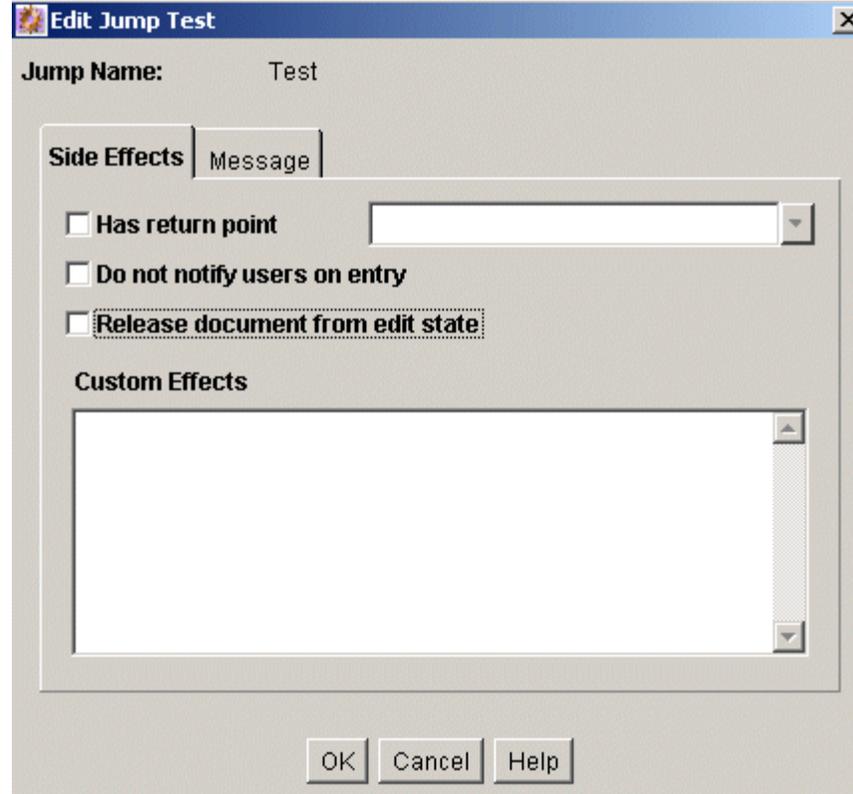


To access this screen, click **Add** or **Edit** in the Jumps pane of the [Script Properties Screen](#), Jump Tab.

Element	Description
Side Effects tab	Used to specify the jump name, return point, custom side effects, and to enable notification for the jump.
Message tab	Used to enter a notification message for the jump.

Add/Edit Jump Screen: Side Effects Tab

This screen is used to add or edit jump side effects.



To access this screen, click the tab on the [Script Properties Screen](#), Jump Tab.

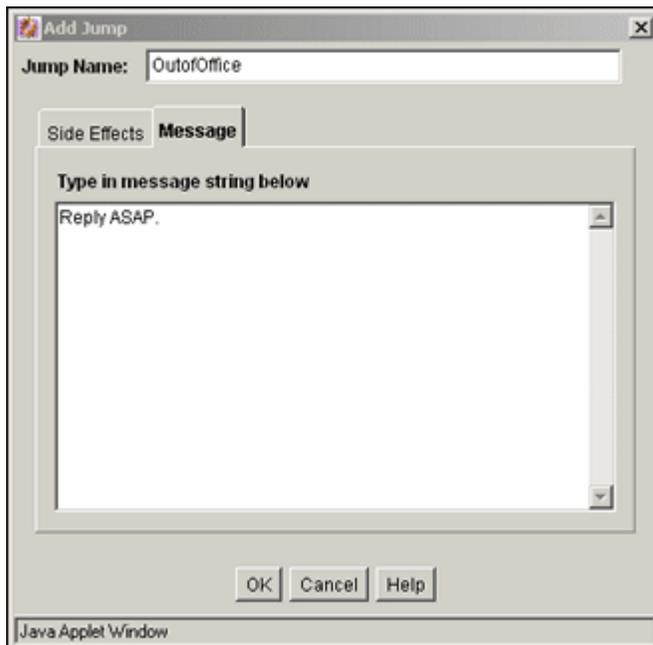
Element	Description
Jump Name field	Name of the jump.
Has return point	If selected, a return step, selected from the list, is used.
Do not notify users on entry	If selected, reviewers for the step receive the message defined on the Message tab when the jump is entered.
Release document from edit state	If selected, a document is released before approval.
Custom Effects pane	Area used to enter custom side effects using Idoc script.

Add/Edit Jump Screen: Message Tab

This screen is used to enter a notification message for the jump. To change a notification message, use Component Architecture to customize the following include files and templates. These files contain the default mail information:

- wf_approve_mail_subject include file
- wf_approve_mail_message include file
- wf_started_subject include file
- wf_rejected_subject include file
- reviewer_mail.htm template

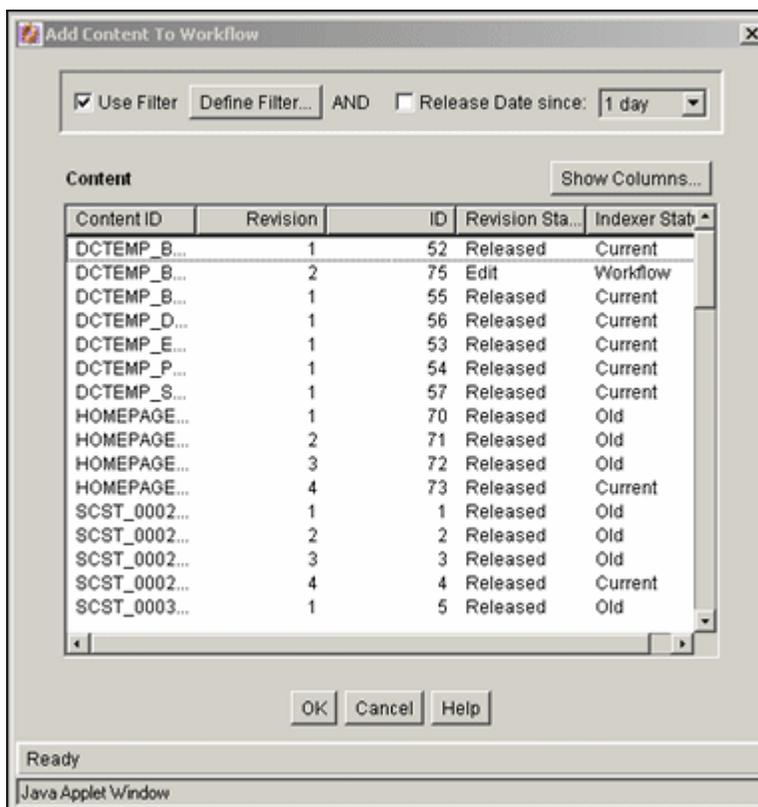
- reject_mail.htm template
- contributor_mail.htm template



To access this screen, click the **Message** tab on the [Script Properties Screen](#).

A.2.5.6 Content Item View Screen

This screen is used to select an existing revision for event script testing purposes.



To access this screen, click **Select** on the [Script Properties Screen](#), Test Tab. See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns Screen"](#) for details about filtering information. To choose a revision, select the revision and click **OK**.

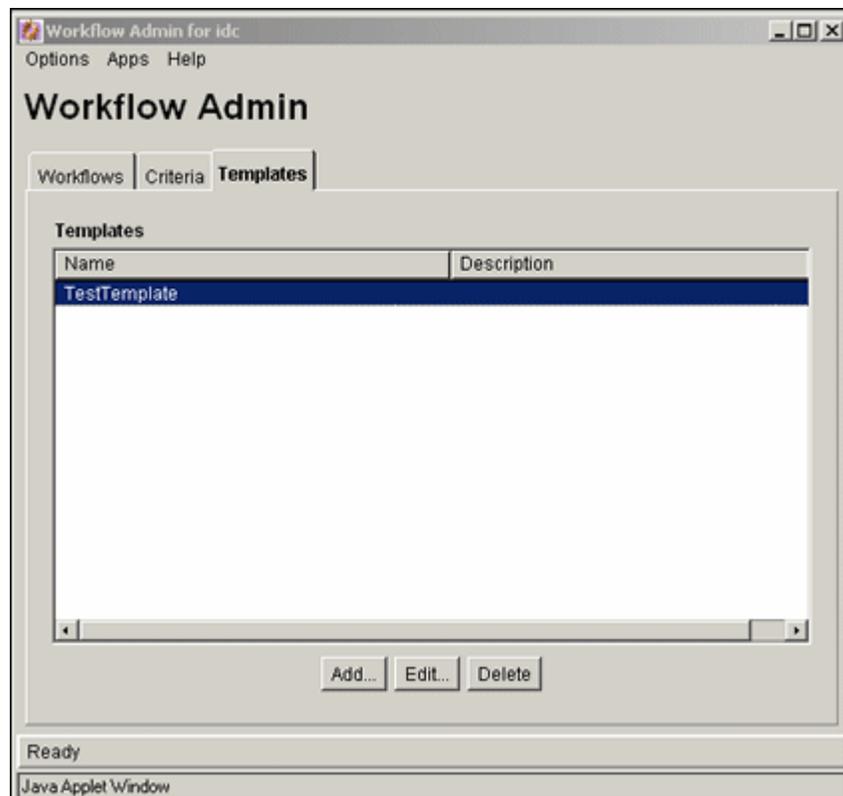
A.2.6 Workflow Template Interface Screens

The following screens are used to create templates:

- [Section A.2.6.1, "Workflow Admin: Templates Tab"](#)
- [Section A.2.6.2, "Add/Edit Template Screen"](#)
- [Section A.2.6.3, "Add New/Edit Step Screen"](#)
- [Section A.2.6.4, "Add Alias to Step Screen"](#)
- [Section A.2.6.5, "Add User to Step"](#)
- [Section A.2.6.6, "Add Token: Templates"](#)
- [Section A.2.6.7, "Edit Additional Exit Condition Screen"](#)

A.2.6.1 Workflow Admin: Templates Tab

This screen is used to add, edit, and delete workflow templates.



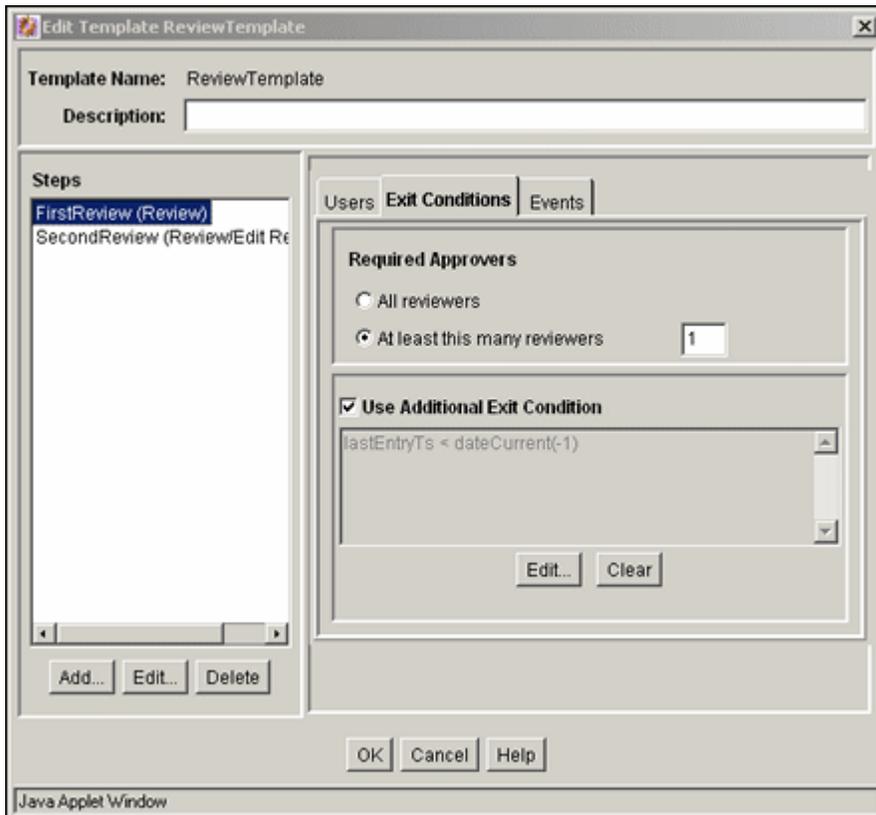
To access this screen, click the **Templates** tab on [The Workflow Admin Screen](#).

Element	Description
Columns	<ul style="list-style-type: none"> ■ Name: Workflow template names. ■ Description: Description of the template.

Element	Description
Buttons	<ul style="list-style-type: none"> ■ Add: Used to add a new template. ■ Edit: Used to edit a template. ■ Delete: Delete a template

A.2.6.2 Add/Edit Template Screen

This screen is used to add or edit a workflow template.



To access this screen, click **Add** or **Edit** on the [Workflow Admin: Templates Tab](#).

Element	Description
Template Name	Name of the template.
Description	Description of the template.
Steps pane	<p>The steps included in the workflow template.</p> <p>Buttons:</p> <ul style="list-style-type: none"> ■ Add: Used to add a new step. ■ Edit: Used to edit a selected step. ■ Delete: Used to delete a step.

Element	Description
User tab	<p>Lists the users, aliases, and tokens assigned to the selected step.</p> <p>Buttons:</p> <ul style="list-style-type: none"> ■ Add Alias, Add User, Add Token: Used to add users or tokens a step. ■ Delete: Used to delete the selected user or token.
Exit Conditions tab	<p>Lists the exit conditions to be met for the step.</p> <ul style="list-style-type: none"> ■ Reviewer options: Used to select how many users must approve a revision before the step is passed. ■ Use Additional Exit Condition: If selected, the conditions defined in the text box must be met before the workflow passes to the next step. <p>Buttons:</p> <ul style="list-style-type: none"> ■ Edit: Used to edit exit conditions. ■ Clear: Clears the Exit Condition text box.

Events Tab Fields

For details, see [Section A.2.5.1, "Add New/Edit Step Screen: Events Tab."](#)

A.2.6.3 Add New/Edit Step Screen

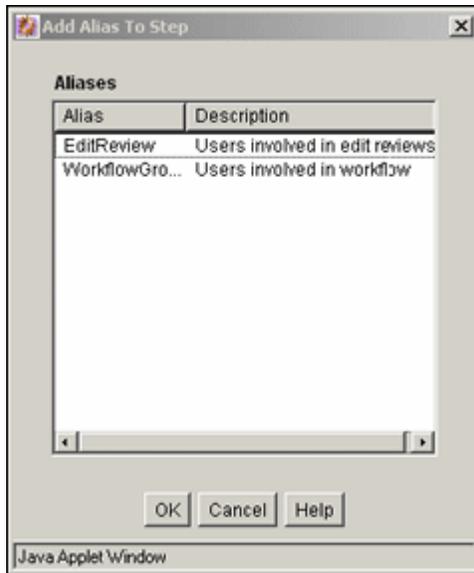
This screen is used to add or edit a step in a workflow template.

To access this screen, select a step and click **Add** or **Edit** in the **Steps** pane of the [Add/Edit Template Screen](#).

Element	Description
Name field	Name for the step.
Description field	Description for the step.
Review options	Determines the actions users can take on an item in the step.

A.2.6.4 Add Alias to Step Screen

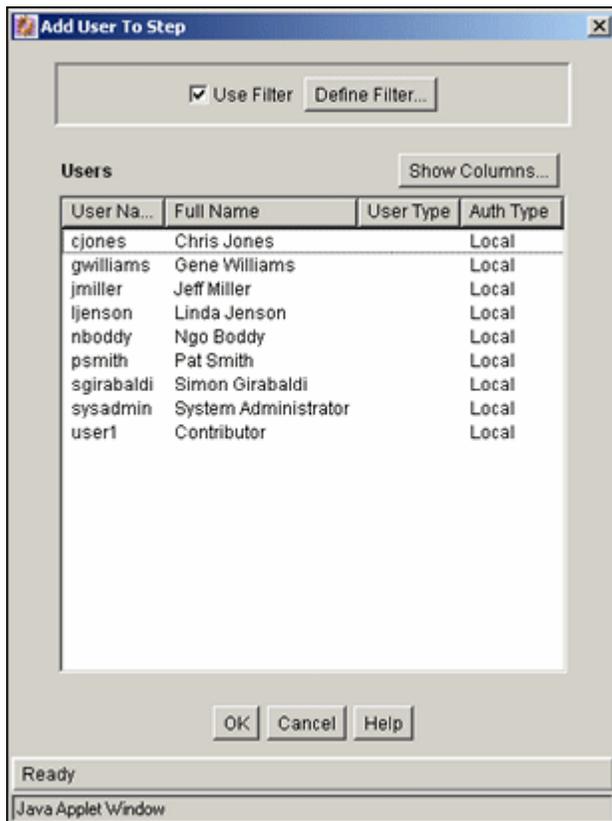
This screen is used to assign aliases to a workflow template step.



To access this screen, click **Add Alias** on the **Users** tab of the [Add/Edit Template Screen](#). To add an alias, select the alias and click **OK**.

A.2.6.5 Add User to Step

This screen is used to assign users to a workflow template step.



To access this screen, click **Add User** on the **Users** tab of the [Add/Edit Template Screen](#). See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns"](#)

[Screen](#)" for details about filtering information. To add a user, select the user and click **OK**.

A.2.6.6 Add Token: Templates

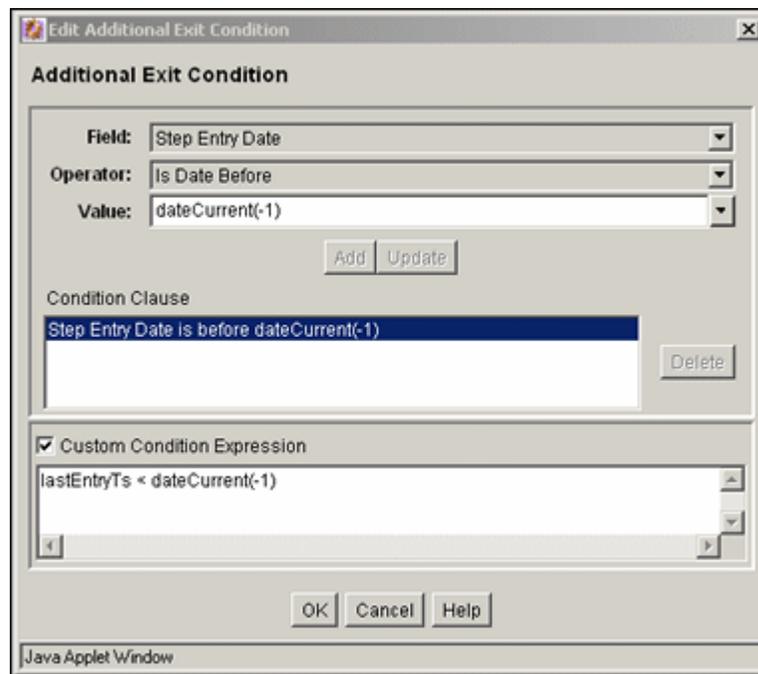
This screen is used to assign workflow tokens to a workflow template step.



To access this screen, click **Add Token** on the **Users** tab of the [Add/Edit Template Screen](#). To use a token, select the token and click **OK**.

A.2.6.7 Edit Additional Exit Condition Screen

This screen is used to define exit conditions for a workflow template step.



To access this screen, click **Edit** on the **Exit Conditions** tab of the [Add/Edit Template Screen](#).

Element	Description
Field	Workflow condition or metadata field to be evaluated.

Element	Description
Operator	Operator (such as 'Matches') to use with the field.
Value	Value for the field. Use an asterisk (*) as a wildcard to match one or more characters or a question mark (?) to match a single character. Click Select (if available) to choose a value for the field.
Add	Adds the conditional statement defined by the Field, Operator, and Value fields to the exit condition clause.
Update	Changes the selected conditional statement to the statement defined by the Field, Operator, and Value fields.
Condition Clause pane	Lists the conditional statements added to the exit condition. You can append multiple clauses as <i>AND</i> statements.
Delete	Deletes the selected conditional statement.
Custom Condition Expression	Enables display and edit of the Idoc Script generated from the condition clauses.

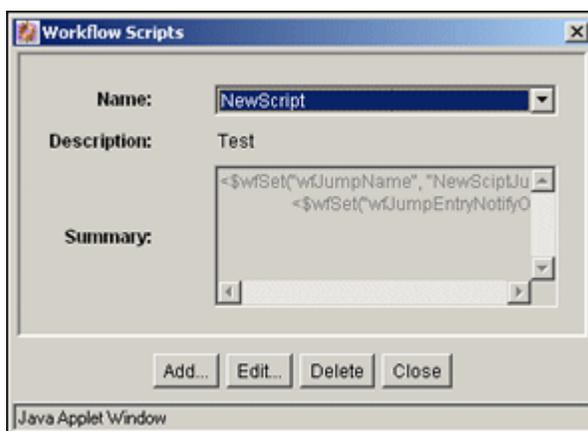
A.2.7 Workflow Scripts User Interface

The following screens are used to create workflow scripts:

- [Section A.2.7.1, "Workflow Scripts Screen"](#)
- [Section A.2.7.2, "Add/Edit Script Screen"](#)
- [Section A.2.7.3, "Add/Edit Script Screen: Jumps Tab"](#)
- [Section A.2.7.4, "Add/Edit Script Screen: Custom Tab"](#)
- [Section A.2.7.5, "Add/Edit Script Screen: Test Tab"](#)
- [Section A.2.7.6, "Add/Edit Jump Screen"](#)
- [Section A.2.7.7, "Add/Edit Jump Screen: Side Effects Tab"](#)
- [Section A.2.7.8, "Add/Edit Jump Screen: Message Tab"](#)
- [Section A.2.7.9, "Content Item View Screen"](#)
- [Section A.2.7.10, "Select Workflow Step Screen"](#)

A.2.7.1 Workflow Scripts Screen

This screen is used to add, edit, and delete script templates.



To access this screen, choose **Script Templates** from the **Options** menu in [The Workflow Admin Screen](#).

Element	Description
Fields	<ul style="list-style-type: none"> Name: Workflow template names. Description: Description of the template. Summary: Code defined for the template.
Buttons	<ul style="list-style-type: none"> Add: Used to add a new script. Edit: Used to edit a script. Delete: Delete a script

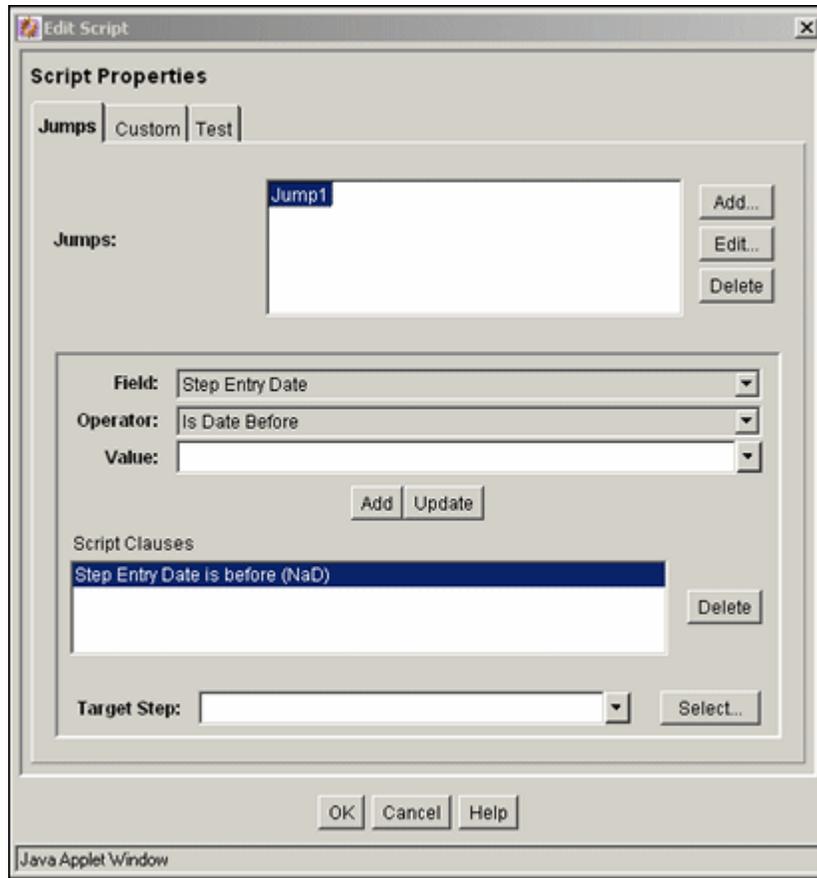
A.2.7.2 Add/Edit Script Screen

This screen is used to create, modify, and test script templates.

To access this screen, click **Add** or **Edit** on the [Workflow Scripts Screen](#).

A.2.7.3 Add/Edit Script Screen: Jumps Tab

This screen is used to create the script template code.

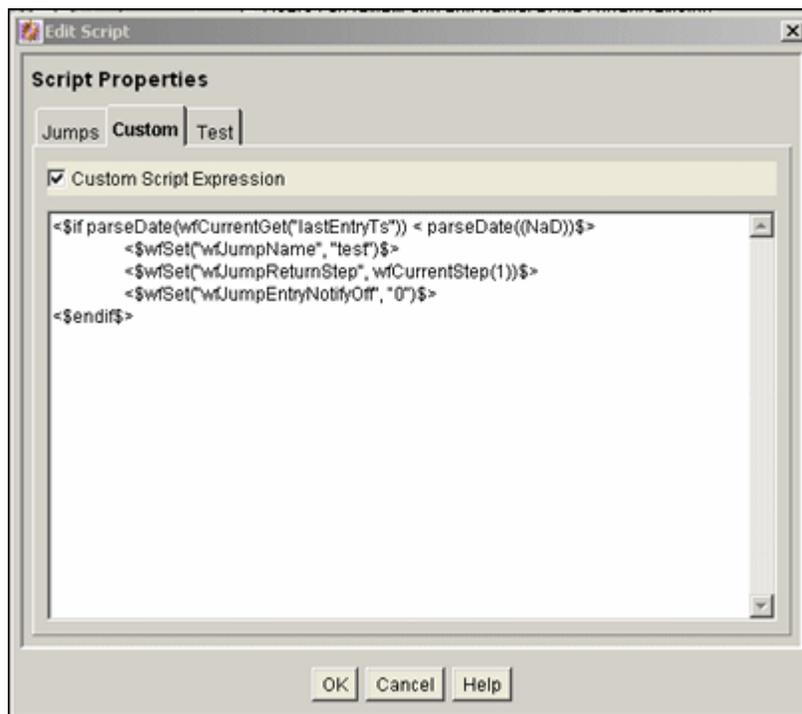


To access this screen, click the **Jumps** tab on the [Add/Edit Script Screen](#).

Element	Description
Jumps pane	Lists the jumps included in the script. Buttons: <ul style="list-style-type: none"> ■ Add or Edit: Used to add or edit the side effects. ■ Delete: Used to delete the selected jump.
Center pane	<ul style="list-style-type: none"> ■ Field: Condition or field to be evaluated. ■ Operator: Operator to use with the field. ■ Value: Value for the specified metadata field. Use an asterisk (*) as a wildcard to match one or more characters or a question mark (?) to match a single character. Buttons: <ul style="list-style-type: none"> ■ Add: Used to add the conditional statement to the jump ■ Update: Changes the selected statement to the statement defined in the pane.
Script Clauses pane	Lists the conditional statements added to the jump. You can append multiple clauses as <i>AND</i> statements. Click Delete to remove a selected statement.
Target Step	Specifies a target step for the jump. Click Select to choose a step from a list.

A.2.7.4 Add/Edit Script Screen: Custom Tab

This screen is used to edit the script that was generated automatically by the options on the **Jumps** tab.

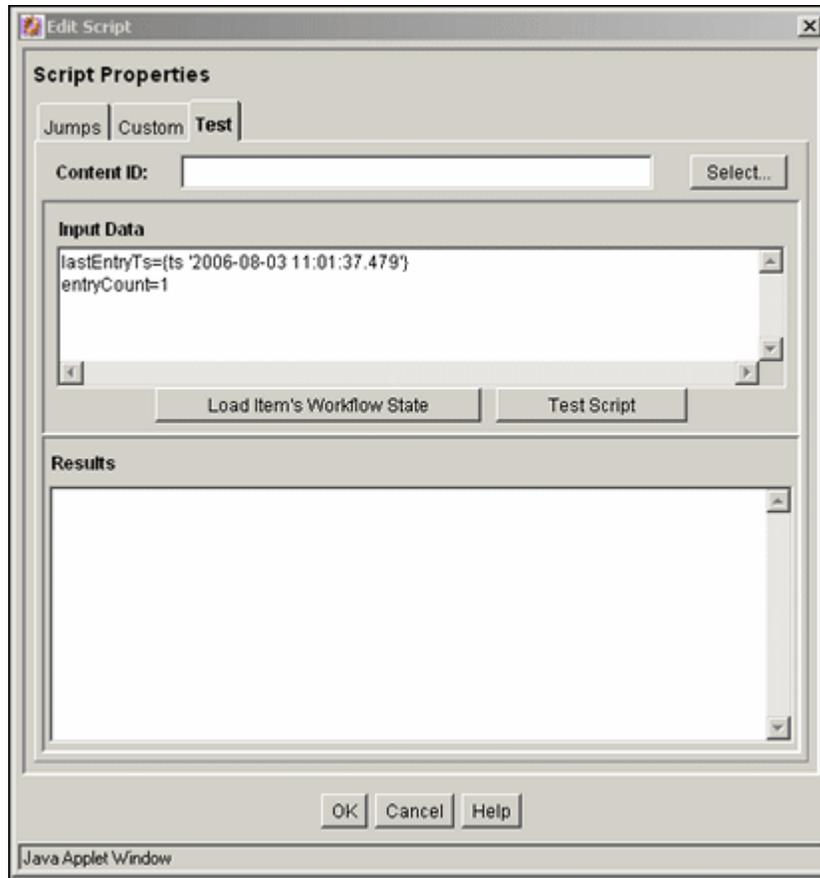


To access this screen, click the **Custom** tab on the [Add/Edit Script Screen](#).

Element	Description
Custom Script Expression	If selected, you can edit and save the script revision. If unselected, the script reflects the statements defined on the Jumps tab. The expression reverts to its original definition.
Script pane	Shows the script of all jumps in the script template.

A.2.7.5 Add/Edit Script Screen: Test Tab

This screen is used to test a script template.

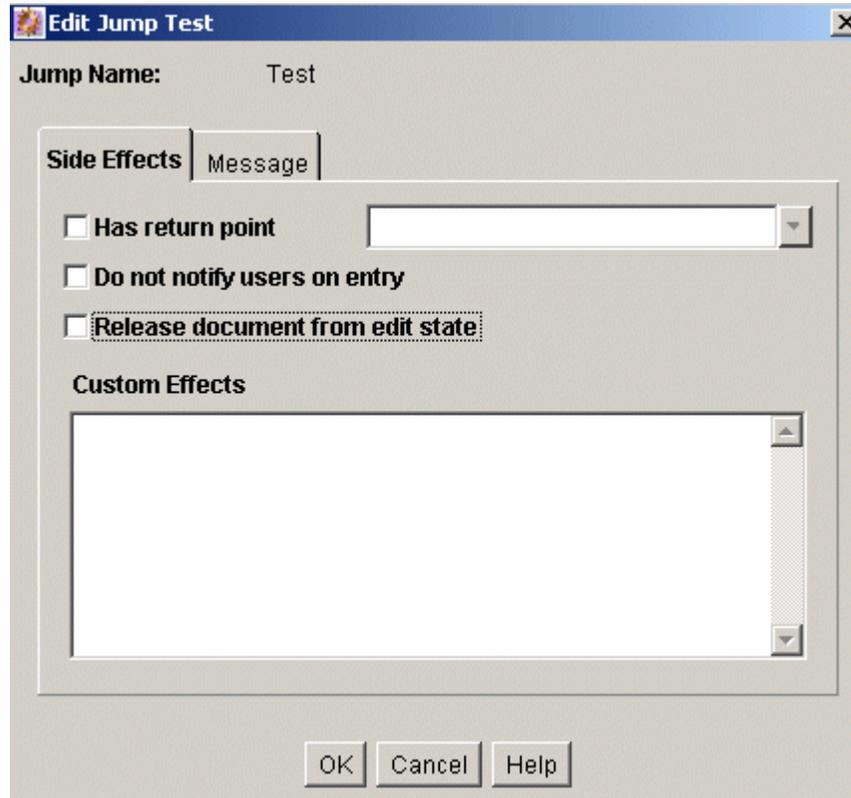


To access this tab, click the tab on the [Add/Edit Script Screen](#).

Element	Description
Content ID	The Content ID for a content item to be tested. Enter an ID or click Select to open a screen where you can select items.
Input Data pane	Shows the data that is tested when a workflow is selected and when the content items's workflow state is loaded.
Load Item's Workflow State	Loads the companion file for the selected content item. If the selected content item is not in a workflow, the content item is treated like it newly entered the workflow.
Test Script	Tests the script and displays the results in the Results pane.
Results pane	The results of the script test. Idoc script error messages are displayed if there are processing errors.

A.2.7.6 Add/Edit Jump Screen

This screen is used to add or edit jump side effects and notification messages for a script template.

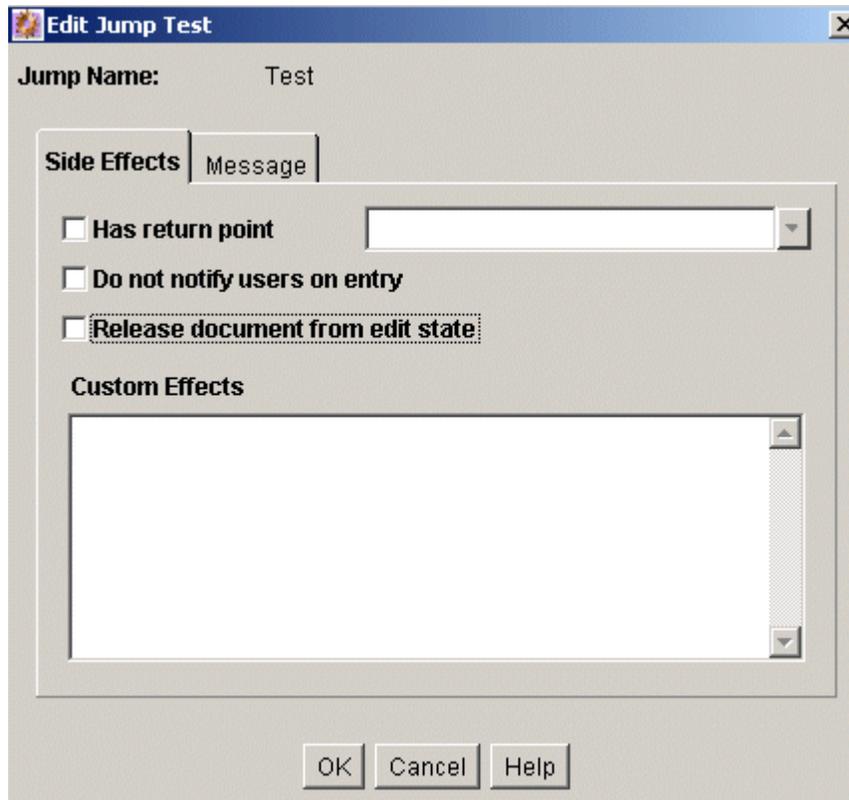


To access this screen, click **Add** or **Edit** in the **Jumps** pane of the [Add/Edit Script Screen: Jumps Tab](#).

Element	Description
Side Effects tab	Used to specify the jump name, return point, custom side effects, and to enable notification for the jump.
Message tab	Used to enter a notification message for the jump.

A.2.7.7 Add/Edit Jump Screen: Side Effects Tab

This screen is used to add or edit jump side effects for a script template.

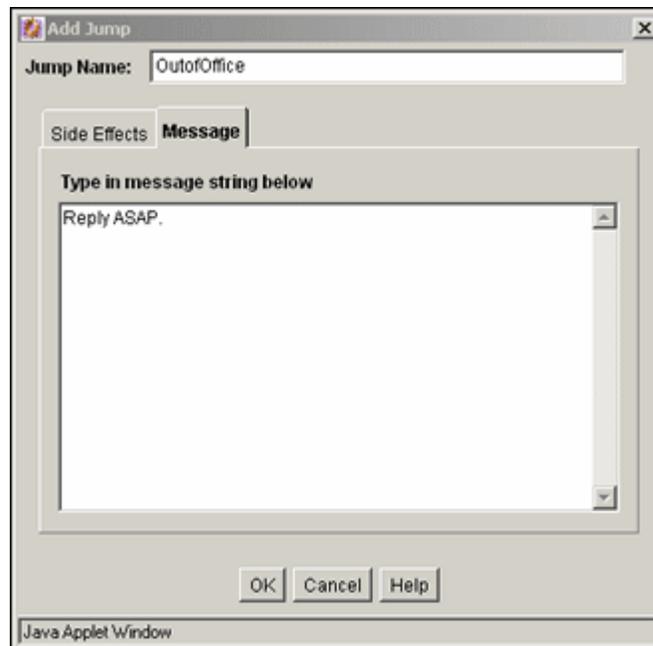


To access this tab, click the **Side Effects** tab on the [Add/Edit Jump Screen](#).

Element	Description
Jump Name	Name of the jump.
Has return point	If selected, a return step is used.
Do not notify users on entry	If selected, reviewers for the step receive the message defined on the Message tab when the jump is entered.
Release document from edit state	If selected, a document is released before approval.
Custom Effects pane	Used to enter custom side effects using Idoc script.

A.2.7.8 Add/Edit Jump Screen: Message Tab

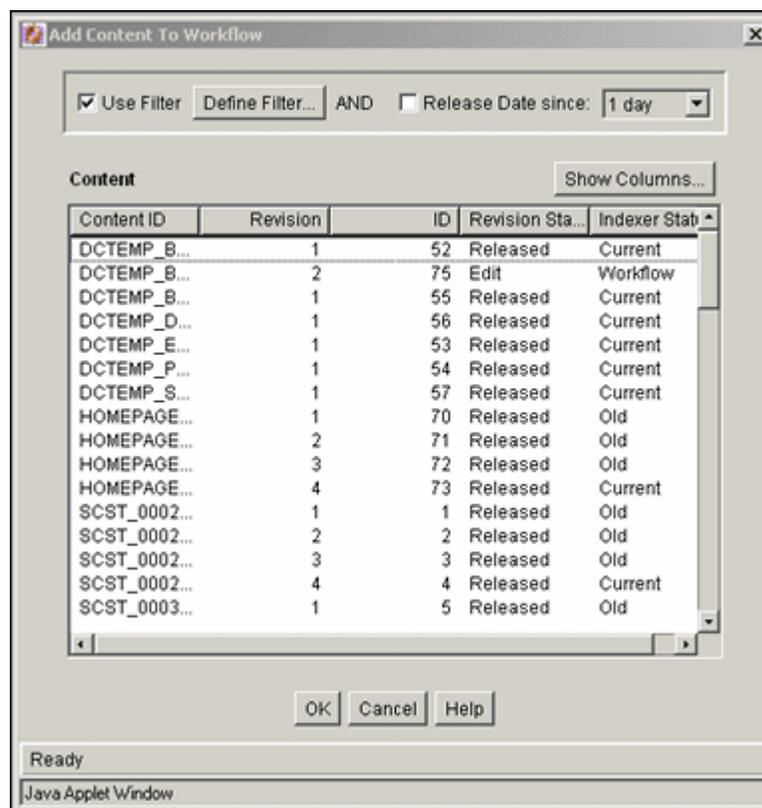
This screen is used to enter a notification message for a jump in a script template.



To access this screen, click the **Message** tab on the [Add/Edit Jump Screen](#).

A.2.7.9 Content Item View Screen

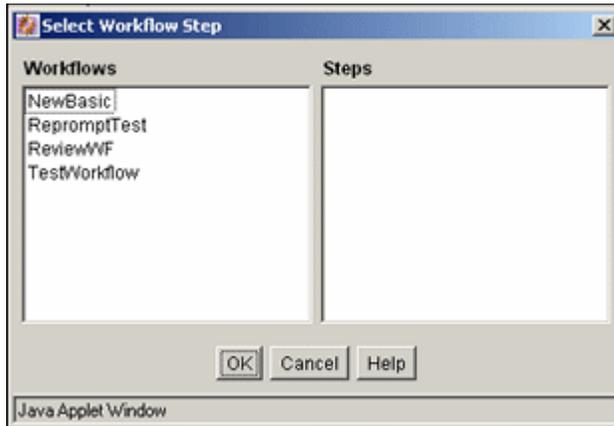
This screen is used to select an existing revision for script template testing purposes.



To access this screen, click **Select** on the [Add/Edit Script Screen: Test Tab](#). See [Section A.1.2.3, "Define Filter Screen"](#) and [Section A.1.2.4, "Show Columns Screen"](#) for details about filtering information. To use a revision, select the item and click **OK**.

A.2.7.10 Select Workflow Step Screen

This screen is used to select an existing workflow step for script template testing purposes.



To access this screen, click **Select Workflow** on the [Add/Edit Script Screen: Test Tab](#).

Element	Description
Workflows	Select a workflow to display the workflow steps in the Steps field.
Steps	The selected step is used for testing purposes.

A.3 PDF Watermark Interface

This section describes the PDF Watermark interface screens.

This section covers the following topics:

- [Section A.3.1, "PDF Watermark Administration Screen"](#)
- [Section A.3.2, "Rules Tab"](#)
- [Section A.3.3, "Add New/Edit Rule Screen"](#)
- [Section A.3.4, "Add New/Edit Criteria Screen"](#)
- [Section A.3.5, "Templates Tab"](#)
- [Section A.3.6, "Add New/Edit Template Screen"](#)
- [Section A.3.7, "Add New/Edit Text Watermark Window"](#)
- [Section A.3.8, "Add New/Edit Image Watermark Window"](#)
- [Section A.3.9, "Add New/Edit Signature Watermark Window"](#)
- [Section A.3.10, "Configuration Tab"](#)
- [Section A.3.11, "Edit Default Value Screen"](#)

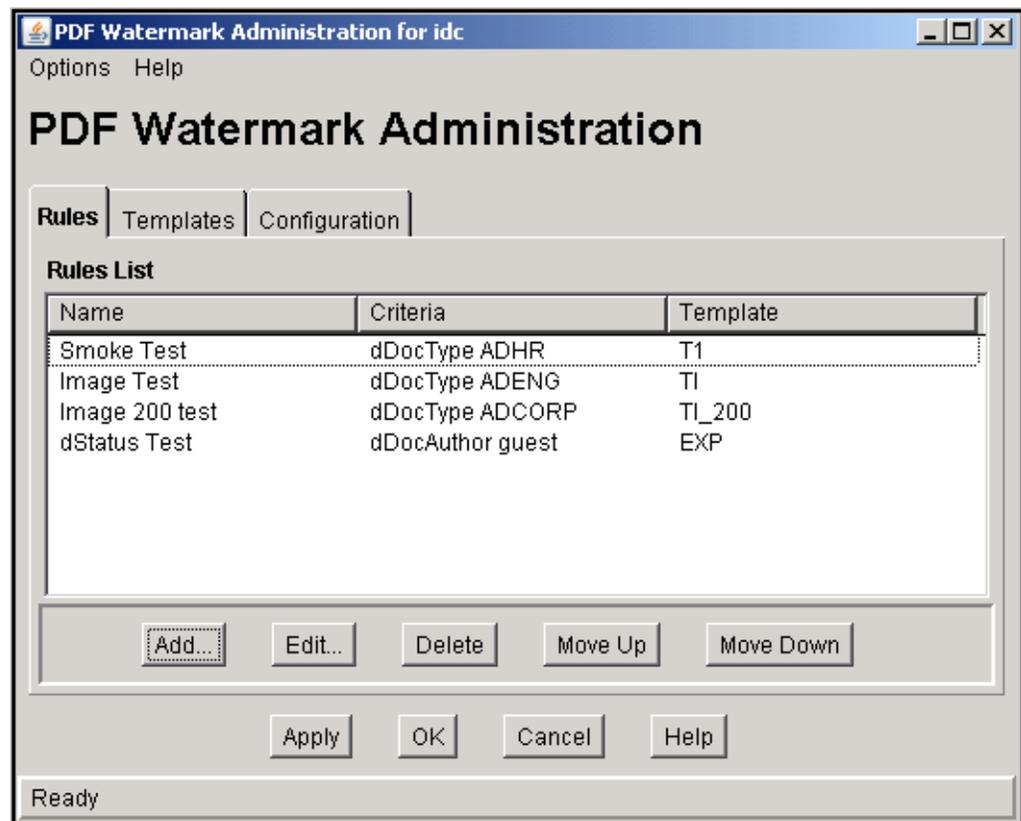
A.3.1 PDF Watermark Administration Screen

The PDF Watermark Administration screen is used to specify rules, templates, and metadata values for templates used in watermarking content. To access this screen choose **Administration** then **PDF Watermark Administration** from the Main menu.

Tabs	Description
Rules	Opens the Rules Tab .
Templates	Opens the Templates Tab .
Configuration	Opens the Configuration Tab .

A.3.2 Rules Tab

This screen is used to define a rule or ruleset, which determines which content is dynamically watermarked, upon user request.

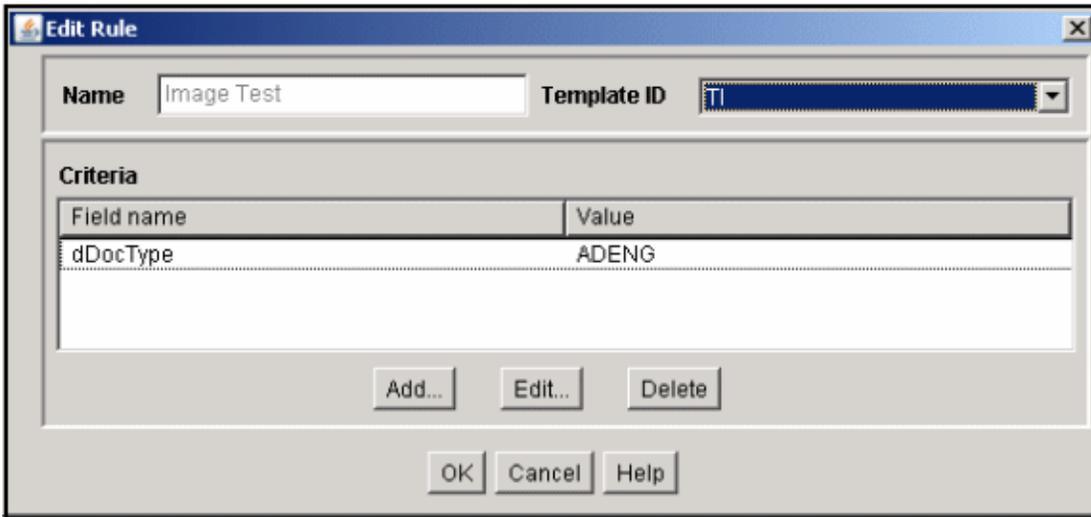


To access this screen, click the **Rules** tab on the [PDF Watermark Administration Screen](#).

Element	Description
Add or Edit	Opens the Add New/Edit Rule Screen .
Delete	Removes the selected rule from the list.
Move Up/Down	Adjusts the placement order of the selected rule relevant to its priority. The higher or lower a rule in the list, the higher or lower its priority is in the hierarchy.

A.3.3 Add New/Edit Rule Screen

This screen is used to specify a rule or edit a rule for a PDF watermark template.



To access this screen, click **Add** on the [Rules Tab](#).

Field	Description
Name	The rule name.
Template ID	Content ID of the template.
Add or Edit	Adds new criteria to the rule or displays the criteria for editing. Specify a value for any or all of the available criteria.

A.3.4 Add New/Edit Criteria Screen

This screen is used to add a new criteria or change an existing one.

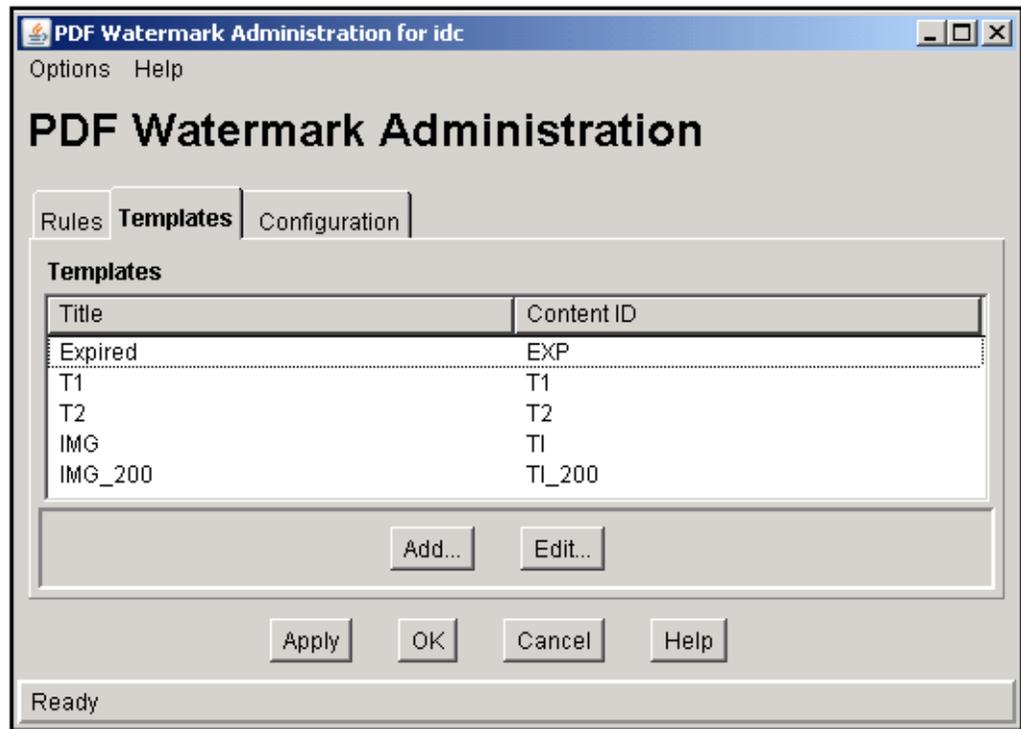


To access this screen, click **Add** or **Edit** on the [Add New/Edit Rule Screen](#).

Field	Description
Field Name	Name of the new or edited field.
Value	Name of the trigger value (criteria for use).
Options	If the field is a List, values appear on the list.

A.3.5 Templates Tab

Use this screen to design and edit watermark templates.



To access this screen, click **Templates** on the [PDF Watermark Administration Screen](#).

Element	Description
Add and Edit	Opens the Add New/Edit Template Screen .

A.3.6 Add New/Edit Template Screen

This screen is used to specify values for a template for PDF watermarks.

To access this screen, click **Add** or **Edit** on the [Templates Tab](#).

Element	Description
Title	Template title.
Content ID	Content ID for this template.
Security Level	Set to NONE (default), 40, or 128 to signify the level of bit encryption.
User or Owner Password	If security is applied, the user password is required to view the PDF. No modification of the PDF is allowed and the owner password is required to modify the PDF passwords, permissions, and security level.
Allow Print	Set to YES to allow printing. Select DEGRADED to allow printing of a low-quality version of the content.
Allow Copy	Set to YES to allow copying.
Summary tabs	Used to create, edit, or delete text and image watermarks. If you enabled the Electronic Signature component, you can also create, edit, or delete a watermark composed of electronic signature data for content items that have electronic signatures.

A.3.7 Add New/Edit Text Watermark Window

User this screen to specify values for text appearing in a PDF watermark.

To access this screen, click the **Text Watermark** tab on the [Add New/Edit Template Screen](#).

Element	Description
Text	<p>Text to appear in the watermark. The text can include embedded symbols:</p> <p>\$PAGE\$: The current page in the document.</p> <p>\$PAGE_COUNT\$: The total number of pages in the document</p> <p>\$DATE\$: The date the document is rendered.</p> <p>\$TIME\$: The time the document is rendered.</p> <p>\$USER\$: The name of requesting user.</p> <p>You can also include document information fields in the form \$\$<field_name>\$\$. For example, to include an expiration notice and the expiration date, specify the following:</p> <p>Expiration Date: \$\$dOutDate\$\$</p>
Placement and display details	<p>Specify the location and appearance of the watermark:</p> <ul style="list-style-type: none"> ▪ Location: location on the screen. ▪ X and Y coordinate: coordinate for placement specified in points. Each point = 1/72" from a baseline 0:0 location. ▪ Rotation: angle of placement, 0- through 359 degrees, counter-clockwise. ▪ Alignment: alignment on the screen. ▪ Font information: select font name, size, weight (bold, and so on), and color).

Element	Description
Layer	Places the watermark in the layer either OVER or UNDER the content. Default is OVER.
Page Range and Modifier	Pages to watermark. For example 1,2,4,10:15,19,23:LAST. Specify ranges with a colon. If left blank, all page are watermarked. Modifiers include All Pages, Odd Pages Only, Even Pages Only.

A.3.8 Add New/Edit Image Watermark Window

Use this screen to specify values for an image appearing in a PDF watermark.

To access this screen, click the **Image Watermarks** tab on the [Add New/Edit Template Screen](#).

Element	Description
Content ID	The Content ID of the image used for the watermark.
Scale Factor	Factor used to scale images with resolutions other than the default 72 dpi. The Scale Factor is expressed as a percentage based on the following formula: $\langle \text{default dpi} \rangle / \langle \text{image dpi} \rangle * 100\%$. For example, to maintain the size and resolution of a 300 dpi image, you calculate the Scale Factor as follows: $72 \text{ dpi} / 300 \text{ dpi} * 100\% = 24\%$ for a Scale Factor of 24.
Location	Location on the screen.
X Coordinate	X coordinate for placement specified in points. Each point = 1/72" from a baseline 0:0 location.
Y Coordinate	Y coordinate for placement specified in points. Each point = 1/72" from a baseline 0:0 location.
Layer	Places the watermark in the layer either OVER or UNDER the content. Default is OVER.

Element	Description
Page Range and Modifier	Pages to watermark. For example 1,2,4,10:15,19,23:LAST. Specify ranges with a colon. If left blank, all page are watermarked. Modifiers include All Pages, Odd Pages Only, Even Pages Only.

A.3.9 Add New/Edit Signature Watermark Window

Use this screen to configure a PDF watermark composed of electronic signature data. You must enable the Electronic Signature component to create a signature watermark.

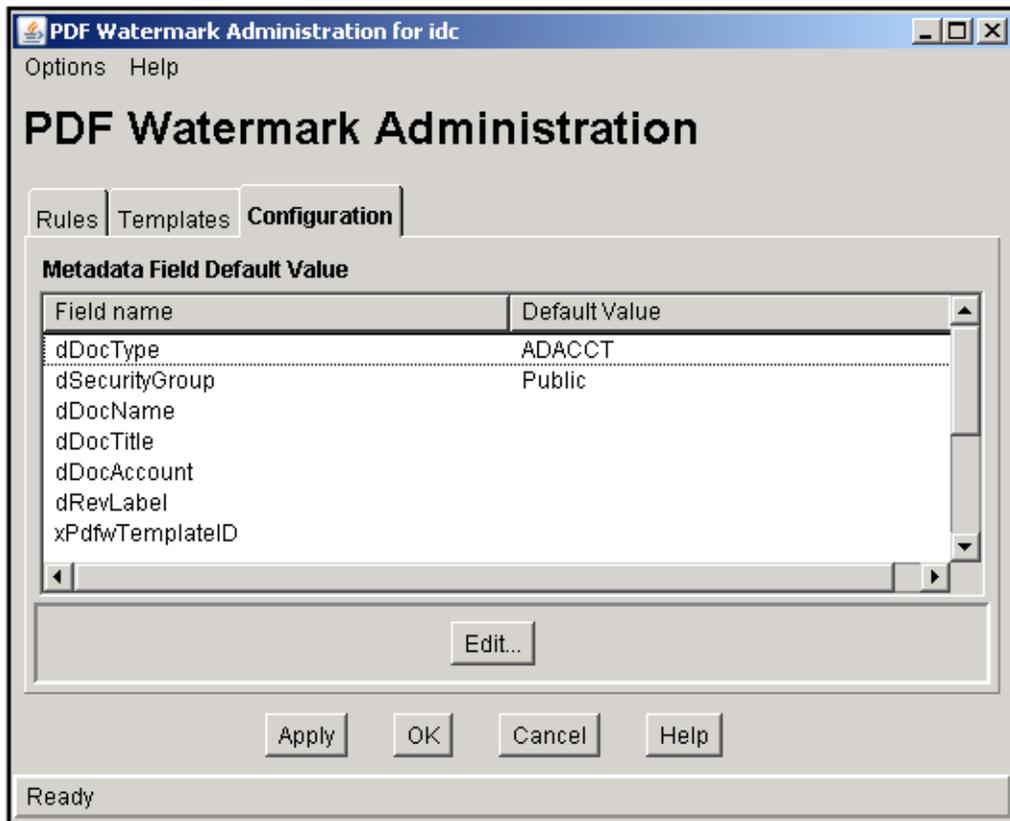
To access this screen, click the **Signature Watermark** tab on the [Add New/Edit Template Screen](#).

Element	Description
Label	Specify the text to identify the watermark.
Fields	Specify the electronic signature metadata fields to use in the watermark. The fields you specify here are the standard or user-defined fields from the Electronic Signatures table. Specify the fields as a comma-delimited list.

Element	Description
Placement and display details	<p>Specify the location and appearance of the watermark:</p> <ul style="list-style-type: none"> ■ Location: location on the screen. ■ X and Y coordinate: coordinate for placement specified in points. Each point = 1/72" from a baseline 0:0 location. ■ Rotation: angle of placement, 0- through 359 degrees, counter-clockwise. ■ Alignment: alignment on the screen. ■ Font information: select font name, size, weight (bold, and so on), and color).
Layer	Places the watermark in the layer either OVER or UNDER the content. Default is OVER.
Page Range and Modifier	<p>Pages to watermark. For example 1,2,4,10:15,19,23:LAST. Specify ranges with a colon. If left blank, all page are watermarked.</p> <p>Modifiers include All Pages, Odd Pages Only, Even Pages Only.</p>

A.3.10 Configuration Tab

This screen is used to specify default metadata field values for PDF watermarking.



To access this screen, click **Configuration** on the [PDF Watermark Administration Screen](#).

Element	Description
Edit	Used to specify a value for any or all of the available metadata field default values.

A.3.11 Edit Default Value Screen

This screen is used to edit the default values of the metadata fields for checking in new templates.



To access this screen, click **Edit** on the [Configuration Tab](#).

Element	Description
Field Name	Name of the new or edited field.
Value	Name of the trigger value.

A.4 Contribution Folders Interface

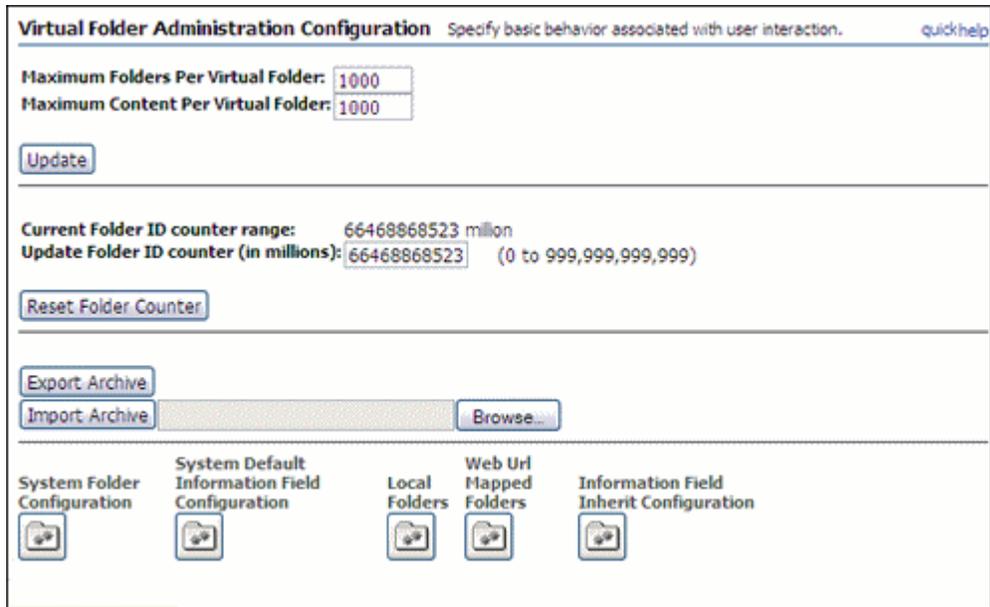
This section describes the Contribution Folders administrative interface screens.

This section covers the following topics:

- [Section A.4.1, "Virtual Folder Administration Configuration Screen"](#)
- [Section A.4.2, "System Folder Configuration Screen"](#)
- [Section A.4.3, "System Default Information Field Configuration Page"](#)
- [Section A.4.4, "Local Folders Page"](#)
- [Section A.4.5, "Information Field Inherit Configuration Page"](#)

A.4.1 Virtual Folder Administration Configuration Screen

This screen is used to provide access to the other Folder system configuration pages.

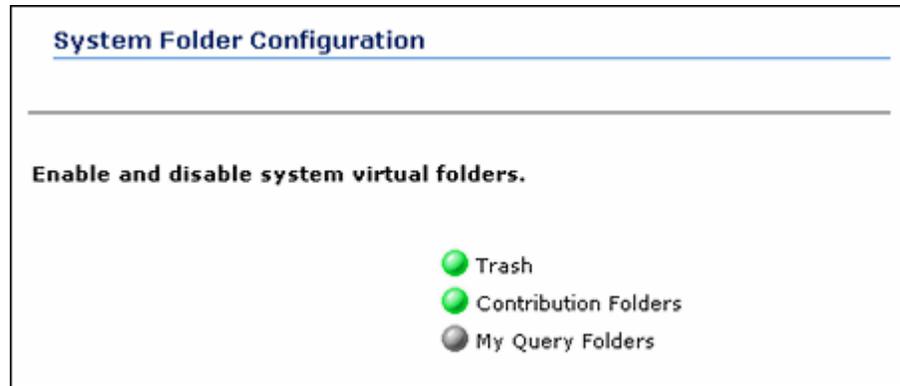


To access this screen, choose **Administration** then **Folder Configuration** from the Main menu.

Element	Description
Maximum Folders/Maximum Content Per Virtual Folder	Sets the maximum number of virtual folders any user can define and number of files that any folder can contain. Click Update to apply the changes.
Export Archive	Exports the folder hierarchy as an archive file.
Import Archive	Imports the specified folder archive. Caution: When a folder archive file is imported, all current folders are removed and replaced by the imported hierarchy. Click Browse to display a list of folders for import.
System Folder Configuration	Opens the System Folder Configuration Screen .
System Default Information Field Configuration	Opens the System Default Information Field Configuration Page .
Local Folders	Opens the Local Folders Page .
Information Field Inherit Configuration	Opens the Information Field Inherit Configuration Page .

A.4.2 System Folder Configuration Screen

This screen is used to enable and disable system-level contribution folders.



To access this page, do either of the following:

- Choose **Administration** then **Folder Configuration** from the Main menu. Choose **System Folder Configuration**.
- Click **System Folder Configuration** on the [Virtual Folder Administration Configuration Screen](#).

Element	Description
Enabled/Disabled icon	Click an icon to enable or disable the folder.

Important: Query folders are supported only for use with Check Out and Open.

A.4.3 System Default Information Field Configuration Page

This page is used to set system default metadata for contribution folders.

System Default Information Field Configuration

Specify the information field defaults that will be applied for all users.

Type

Security Group

Folder

Comments

Hidden

Read Only

Trash Delete Date

Trash Delete Location

Trash Delete Old Name

Trash Deleter

Release Date

Expiration Date

To access this page, do either of the following:

- Choose **Administration** then **Folder Configuration** from the Main menu. Choose **System Default Information Field Configuration**.
- Click **System Default Information Field Configuration** on the [Virtual Folder Administration Configuration Screen](#).

Element	Description
Information fields	Defines the metadata values applied to content checked in through a contribution folder if values are not defined for the folder or by the user. The values are applied on initial check-in. You can use Idoc Script. If Release Date is not specified, the current date and time is used.

A.4.4 Local Folders Page

This page is used to map a contribution folder structure to a local file system.

Local Folders

Specify virtual folders to be replicated to directories on host system.

Folder	Local Directory		
/Contribution Folders/ »	C:\Website	<input type="button" value="Rebuild"/>	<input type="button" value="Remove"/>

Folder	<input type="text"/>	<input type="button" value="Browse..."/>	
Local Directory	<input type="text"/>		

To access this page, do either of the following:

- Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Local Folders**.
- Click **Local Folders** on the [Virtual Folder Administration Configuration Screen](#).

Element	Description
Rebuild	Deletes the existing local directory structure and re-creates the folder structure. Any subdirectories and files are deleted then re-copied to the local directory.
Remove	Removes the local directory from the file system.
Folder	Contribution folder to be mapped to a local directory. Click Browse to select a folder to be mapped.
Local Directory	Directory where the folder structure is replicated.
Add	Replicates the folder to a specified directory on the file system.

A.4.5 Information Field Inherit Configuration Page

This page is used to select which metadata values are propagated from a contribution folder to its subfolders and content items.

Information Field Inherit Configuration

Select information fields that are to be propagated to content.

- Title
- Author
- Type
- Security Group
- Release Date
- Expiration Date
- Folder
- Comments
- Hidden
- Inhibit Propagation
- Read Only
- Trash Delete Date
- Trash Delete Location
- Trash Delete Old Name
- Trash Deleter

To access this page, do either of the following:

- Choose **Administration** then **Folder Configuration** from the Main menu. Choose **Information Field Inherit Configuration**.
- Click **Information Field Inherit Configuration** on the [Virtual Folder Administration Configuration Screen](#).

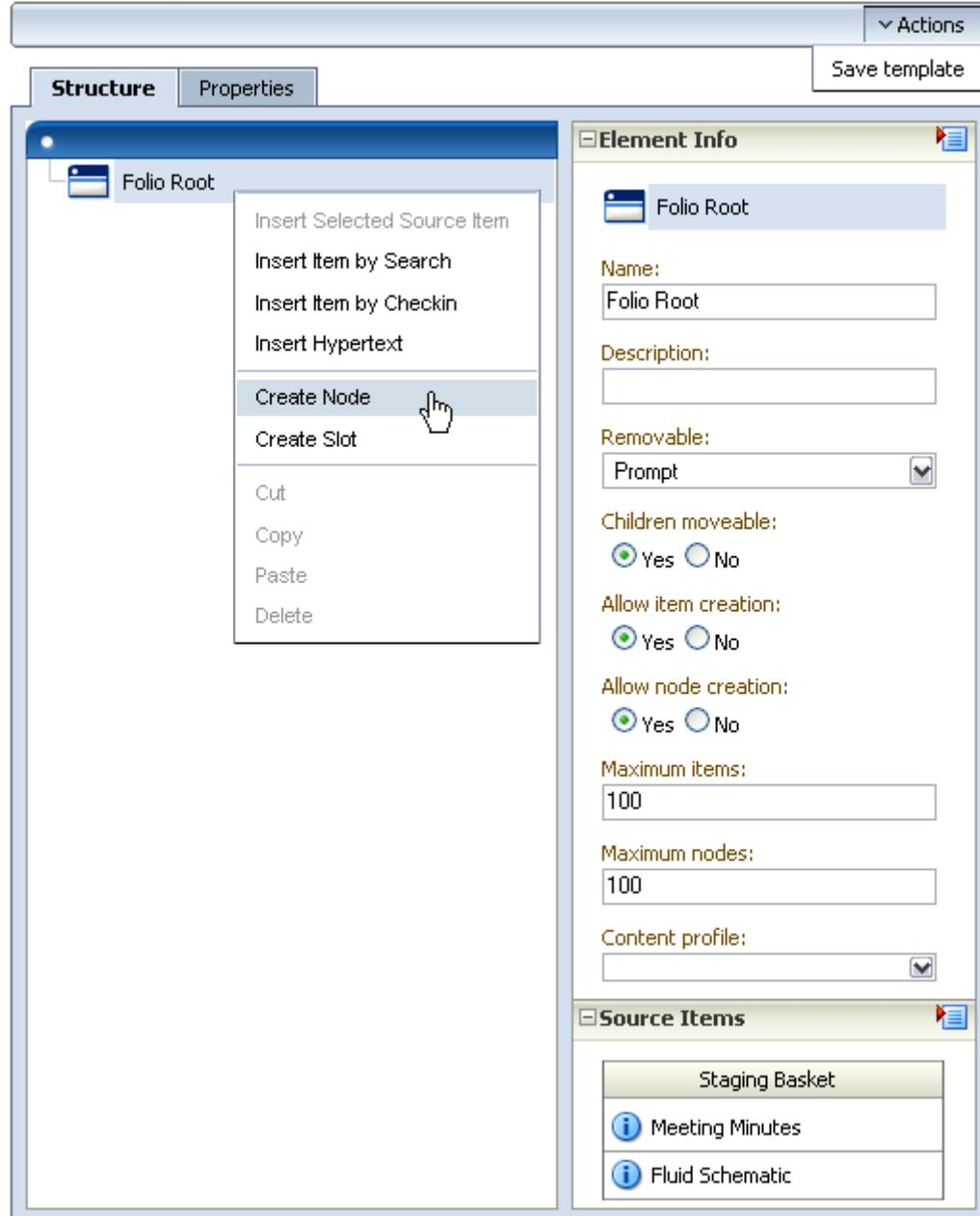
Element	Description
Information Field check boxes	Selects the metadata fields to be propagated.

A.5 Create/Edit Folio Template Page

This page is used to create template with a predefined structure that users select when they create an advanced folio. It is made up of two tabs:

- [Section A.5.1, "Structure Tab"](#)
- [Section A.5.2, "Properties Tab"](#)

Edit Folio Template



To access this screen, choose **Administration** then **Folio Administration** from the Main menu. Select **Create Folio Template**.

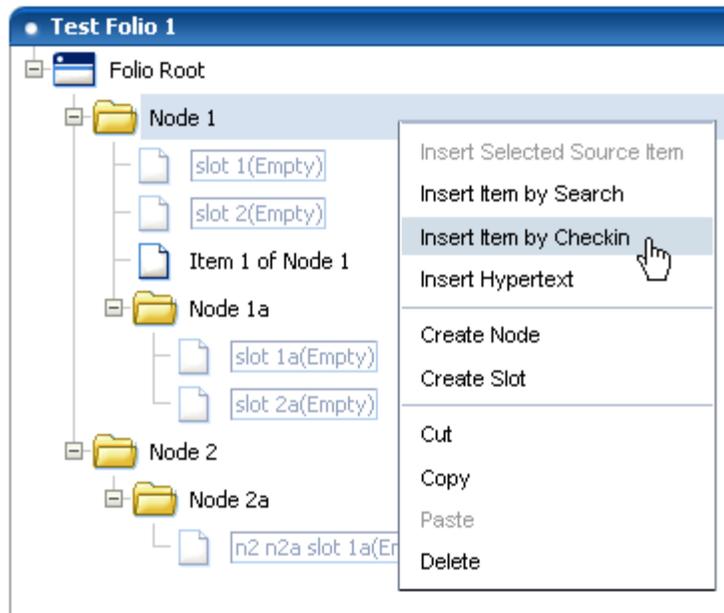
A.5.1 Structure Tab

The **Structure** tab is divided into the following sections:

- [Section A.5.1.1, "Folio Structure Pane"](#)
- [Section A.5.1.2, "Element Info Pane"](#)
- [Section A.5.1.3, "Source Items Pane"](#)

A.5.1.1 Folio Structure Pane

This pane is used to define the objects that compose the folio hierarchy.



This pane is part of the [Create/Edit Folio Template Page](#). Unless otherwise noted, information is applicable to all elements (nodes, items, slots).

Item	Description
Insert Selected Source Item	Inserts the selected item from the Source Items Pane .
Insert Item by Search	Opens a window to search for an item to add to the node or slot.
Insert Item by Checkin	Opens a window with a content check-in form used to check in an item for use in the selected node or slot.
Remove Content Item	(item only) Removes a content item from a slot.
Insert Hypertext	Creates a new item in the folio structure that can establish a hypertext link to the specified URL.
Create Node or Slot	Creates a new node or slot in the folio structure.
Cut, Copy, Paste	Cuts an object from the structure for copying or pasting.
Delete	Deletes an object.

A.5.1.2 Element Info Pane

Use this pane to define the details of each element of the XML template file checked in to define the folio.

This pane is part of the [Create/Edit Folio Template Page](#). Fields are displayed for all elements (items, slots, and nodes) unless otherwise noted.

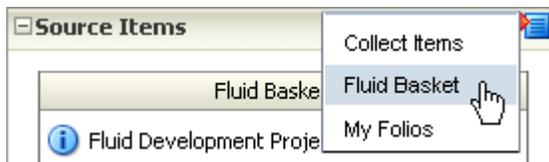
Important: The element information is unique to the folio template, not to the content item associated with the template. A content item can be associated with several different folio templates, and the element information about that item can be different in each template. If the element information is changed in one template, it does not change in another.

Information	Description
Name	Name given the element.
Description	Description of the element to help identify its intended use.

Information	Description
Attributes (slots and items)	Allowable uses and limitations of an element. Options include: <ul style="list-style-type: none"> ▪ Allow empty ▪ Lock content ▪ Removable ▪ Allow external ▪ Restrict formats ▪ Allow folio ▪ Content profile ▪ Clone Item
Attributes (nodes)	Default attributes for nodes. Options include: <ul style="list-style-type: none"> ▪ Removable ▪ Children movable ▪ Allow item creation ▪ Allow node creation ▪ Maximum Items ▪ Maximum Nodes ▪ Content Profile
Content ID	(items and slots) Unique identifier of a content item.
Create Date	(items and slots) Date a content item was created.
last modified	(items and slots) Date changes were made to the item.
link	(hyperlinks only) URL of the hyperlink.

A.5.1.3 Source Items Pane

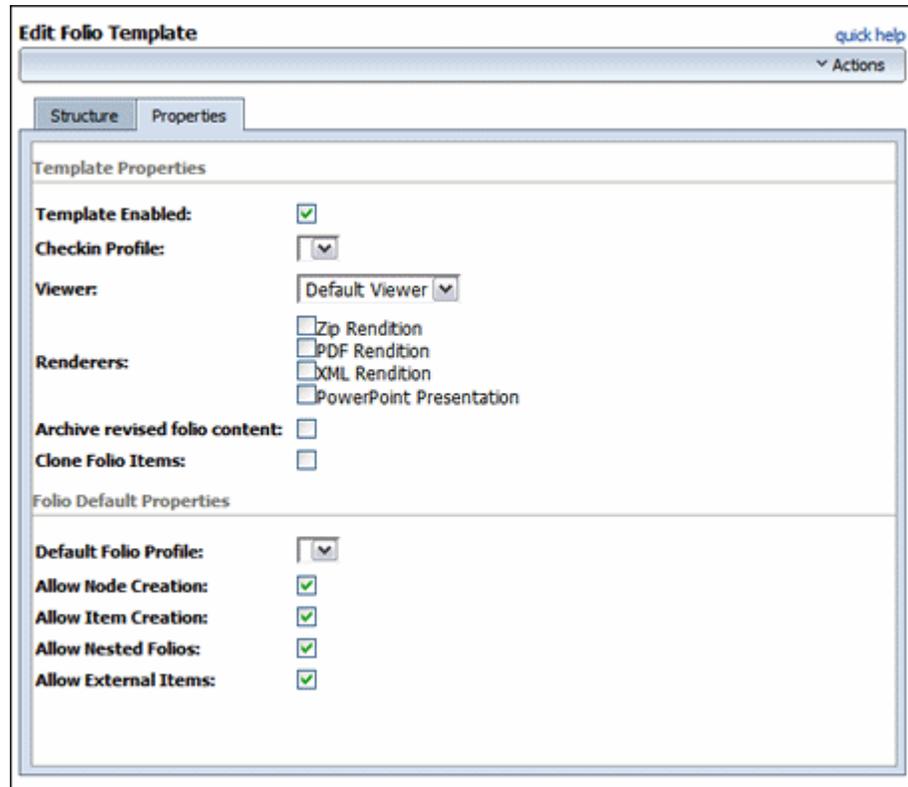
This pane collects checked-in items for use in the folio. Search results are displayed and you can select items for insertion into the folio.



Use the selection menu to choose a content basket to display in the tray.

A.5.2 Properties Tab

This screen is used to define the default folio template properties and enable a folio template.



To access this screen, click the **Properties** tab on the [Create/Edit Folio Template Page](#).

Form Element	Description
Template Enabled	If selected, enables the template for the user when creating an advanced folio.
Checkin Profile	Specifies the profile to be used when a user checks in a newly created folio based on this template. Choosing a profile here suppresses the option for the user to select one on check in.
Viewer	Specifies the viewer to use for the View Folio page.
Renderers	Specifies what options are available in the Renderers menu on the Edit Folio page. Options are: <ul style="list-style-type: none"> ■ zip rendition ■ pdf rendition ■ XML rendition
Archive revised folio content	If selected, causes the current revisions of folio content to be compressed into a flat file and stored as the native file of the folio revision each time it is locked or a snapshot is made. Default: disabled.
Clone Folio Items	If selected, causes any content items specified in the template to be cloned when a folio is created from the template. Cloning an item creates a copy and checks it in as a new content item. If this is not enabled, any content item specified in the template is associated with the folio using the existing content ID.

Form Element	Description
Default Folio Profile	Specifies the profile to be used for searching and checking in when adding content items to the folio.
Allow Node Creation	If selected, you can create nodes.
Allow Item Creation	If selected, you can create items.
Allow Nested Folios	If selected, you can add other folios as an item to the folio.
Allow External Items	If selected, you can add external links to the folio.

A.6 Content Tracker Interface

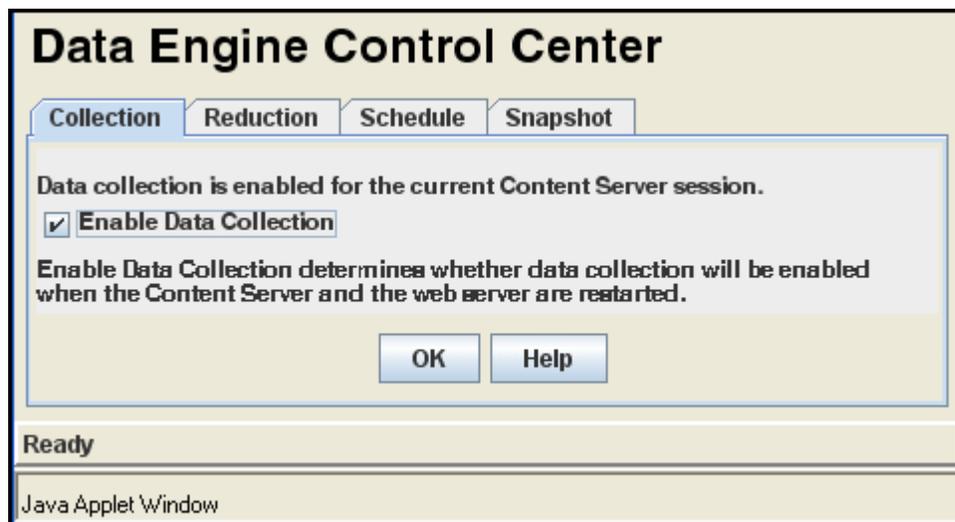
This section describes the Content Tracker interface screens.

This section covers the following topics:

- [Section A.6.1, "Data Engine Control Center"](#)
- [Section A.6.2, "Content Tracker Report Generator Main Page"](#)

A.6.1 Data Engine Control Center

This screen provides access to the user-controlled functions of the Content Tracker Data Engine.



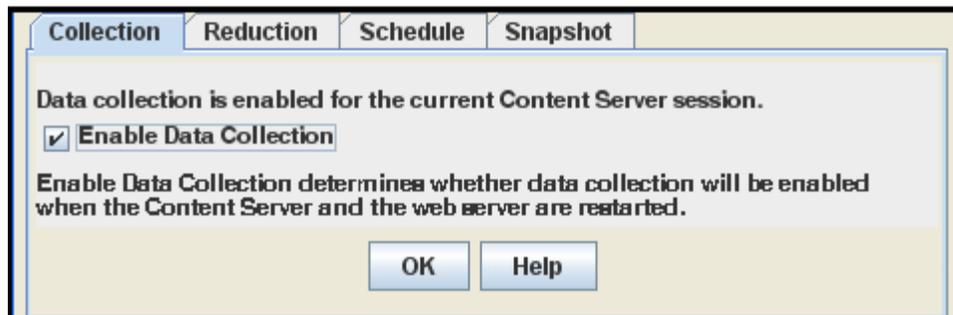
To access this screen, choose **Administration** then **Content Tracker Administration** from the Main menu. Click **Data Engine Control Center**.

This section describes the following tabs accessible through this page:

- [Section A.6.1.1, "Collection Tab"](#)
- [Section A.6.1.2, "Reduction Tab"](#)
- [Section A.6.1.3, "Schedule Tab"](#)
- [Section A.6.1.4, "Snapshot Tab"](#)
- [Section A.6.1.5, "Services Tab"](#)
- [Section A.6.1.6, "Extended Services Tracking Screen"](#)
- [Section A.6.1.7, "Field Map Screen"](#)

A.6.1.1 Collection Tab

This screen is used to enable Web traffic data collection for a session.

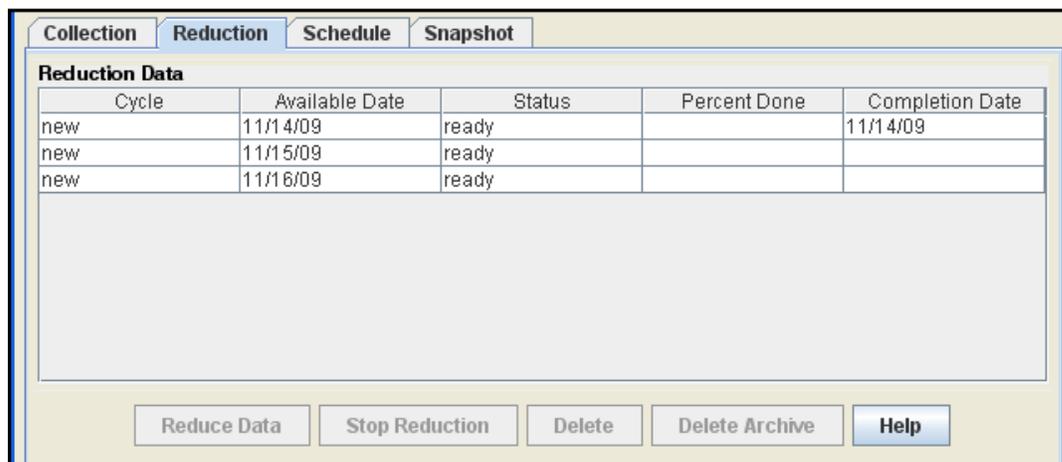


To access this screen, click the **Collection** tab on the [Data Engine Control Center](#).

Element	Description
Enable Data Collection	If selected, enables data collection. Oracle WebCenter Content Server and the Web server must be restarted before any changes take effect.

A.6.1.2 Reduction Tab

This screen is used to start and stop data reduction manually, to monitor progress of a data reduction operation, and to delete the raw data files from which the table rows are generated.



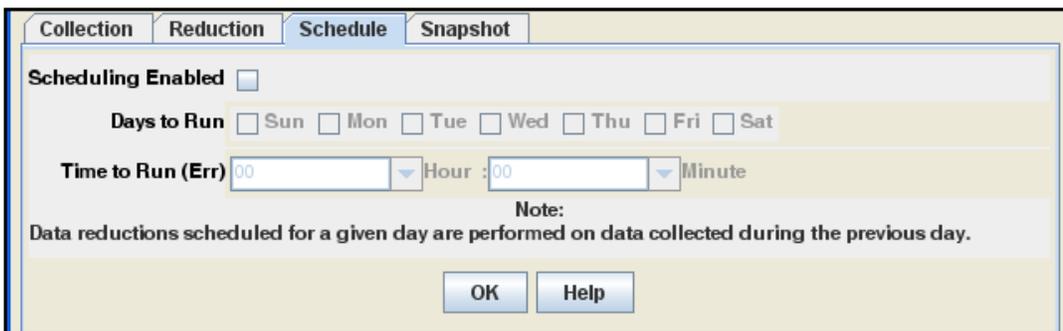
To access this screen, click the **Reduction** tab on the [Data Engine Control Center](#).

Element	Description
Cycle	The state of the input data. Values can include: <ul style="list-style-type: none"> ▪ new ▪ recent ▪ archive
Available Date	The date when the input data was collected.

Element	Description
Status	The status of the reduction data. <ul style="list-style-type: none"> ▪ ready ▪ running ▪ archiving
Percent Done	Progress of the reduction process.
Completion Date	Date and time when the data reduction process completed.
Reduce Data	Initiates the data reduction process on the selected data.
Stop Reduction	Terminates a running reduction process.
Delete	Deletes the selected input data. If raw data is deleted, any reduced data in the tables is unaffected.
Delete Archive	Deletes the input data in the archive cycle. If raw data is deleted, any reduced data in the tables is unaffected.

A.6.1.3 Schedule Tab

This screen is used to enable automatic data reduction.



To access this screen, click the **Schedule** tab on the [Data Engine Control Center](#).

Element	Description
Scheduling Enabled	If selected, data reduction runs automatically.
Days to Run	If selected, data reduction runs on the days chosen.
Time to Run	Used to select the hour and minute when data reduction runs.

A.6.1.4 Snapshot Tab

This screen is used to selectively enable and automatically assign specific activity metrics to pre-defined, custom metadata fields.

To access this screen, click the **Snapshot** tab on the [Data Engine Control Center](#).

All fields are case-sensitive. Make sure all field values are spelled and capitalized correctly.

Element	Description
Enable Snapshot post-processing	<p>If selected, activates the metrics functions and enables users to individually select and assign functions to applicable metadata fields. Default: disabled.</p> <p>Before you select this option, create the custom metadata fields to associate with each metric.</p>
Enable Last Access updates	<p>If selected, activates the associated search relevance metadata field and the Autoload check box. Enter the internal name of the metadata or custom metadata field to be linked to this activity metric.</p> <p>Some applications require that the Last Access field always contains a valid value.</p> <p>Click Autoload to start a query that populates any empty Last Access metadata fields in the DocMeta database table.</p>
Enable Short or Long Access Count updates and intervals	<p>If selected, activates the associated search relevance metadata fields and time interval fields. Enter the internal name of the metadata field to be linked to the activity metric. Specify the interval in days for the activity metric count.</p>

A.6.1.5 Services Tab

This screen is used to log additional service calls with data values relevant to the associated services.

Service Name	Calling Product	Event Type	Reference	Field Map
SCT_LOG_EVENT	Content Tracker	Log Service Event		
SCT_LOG_SERVICE	Content Tracker	Log Service Direct		
GET_FILE_BY_NA...	Core Server	Content Access		
GET_DYNAMIC_U...	Core Server	Content Access		
GET_DYNAMIC_C...	Core Server	Content Access		
GET_EXTERNAL_...	Core Server	Content Access		
GET_ARCHIVED_F...	Core Server	Content Access		
COLLECTION_GE...	Folders	Content Access		
COLLECTION_GE...	Folders	Content Access		
GET_ASSOCIATED...	Threaded Discussi...	Content Access		

To access this screen, click the **Services** tab on the [Data Engine Control Center](#).

This tab is not displayed if Content Access Only mode is set to ON (the default).

Element	Description
Services	Names and result set values of services logged by Content Tracker.
Add or Edit	Opens the Extended Services Tracking Screen .
Delete	Deletes the selected service.

A.6.1.6 Extended Services Tracking Screen

This screen is used to configure service entries in the ServiceExtraInfo ResultSet that is included in the SctServiceHandler.hda file.

To access this screen, click **Add** on the [Services Tab](#).

Element	Description
Service Name	Name of the service to be logged (for example, GET_FILE).
Calling Product	String that is copied to the SctAccessLog table when the service is logged. Usually set to Core Server for all standard entries.
Event Type	String that is copied to the SctAccessLog table when the service is logged. Usually set to Content Access for all standard entries.
Reference	Used to set the sc_scs_reference field in the SctAccessLog table. If blank, the internal getReference logic is used.
Field Map	Name of the field map ResultSet that is added to the SctServiceFilter.hda file. Required if the extended service call tracking function is used. You can log DataBinder field information to the general purpose columns in the SctAccessLog table. You can set a configuration variable to write out the object when the service is called. You can see what data is available at the time the event is recorded. Click Add to map a field.
Field pane	Lists each set of data field, location, and table column names associated with a field map ResultSet.

A.6.1.7 Field Map Screen

This screen is used to configure the field map ResultSets linked to the service entries and included in the SctServiceHandler.hda file.

To access this screen, click **Add** on the [Extended Services Tracking Screen](#).

You can set the `SctDebugServiceBinderDumpEnable` configuration variable to configure the service handler filter to write out the service DataBinder objects into dump files. See the Oracle WebCenter Content Idoc Script Reference Guide for details.

Element	Description
Field Name	Name of the data field.
Field Location	Section in the Oracle WebCenter Content Server service DataBinder where the data field to be logged is located. Values include: <ul style="list-style-type: none"> ▪ Local Data ▪ Environment ▪ Binder ResultSet
Column Name	Column in the SctAccessLog table where data values are logged.

A.6.2 Content Tracker Report Generator Main Page

This screen is used to select a pre-defined report.

Content Tracker Report Generator

Start Date:

End Date:

Rows per Page: 25 **Total Pages:** 10

Criteria:

Content Usage Reports

- Top Content
- Top Content Items by Format
- Top Access Modes by Format
- Top Content by Content Type
- Top Content Items by Author
- Top Content Items by User Role
- Top Content Items by User Type
- Top Content Items by Day

User Access Reports

- Content Items seen by user
- Users who have seen Content
- Users who have seen Security Group
- Users who have seen Content Items by Author
- Users who have seen Content Items by dID
- Users by User Type
- Users by User Role

Admin Reports

- Content Items not accessed in period
- Users not active in period

Custom Reports

To access this screen, choose **Administration** then **Content Tracker Reports** from the Main menu.

Field	Description
Date fields and menu	Start and end of a specific time period for records to be searched. Use the date menu to enter relative dates in the field(s): <ul style="list-style-type: none"> ■ Yesterday ■ Latest Week ■ Latest Month ■ Latest Year
Rows per Page	Specifies the number of results rows for each page of the report.
Total Pages	Specifies the maximum number of results pages for the report.
Criteria	Filters the search results and immediately accesses the applicable drill-down report.
Content and User	Lists content and user according to the selected criteria.

A.7 Content Categorizer Interface

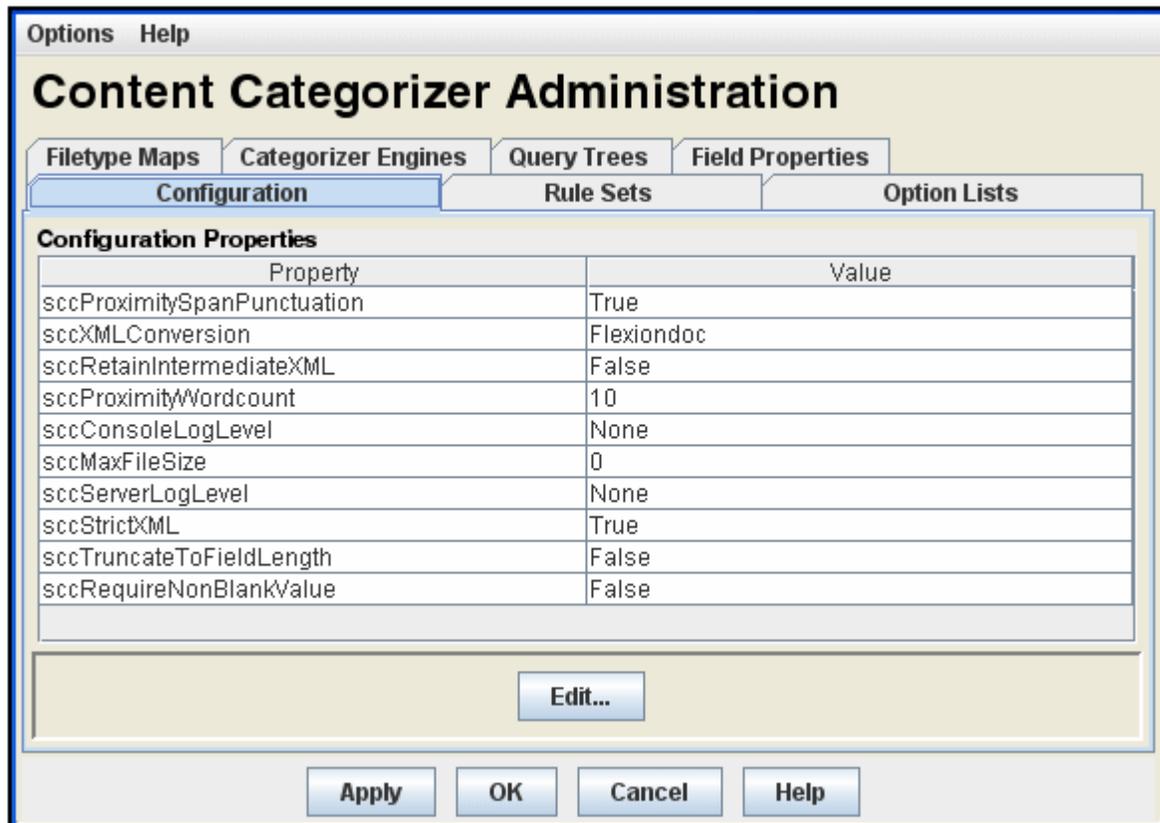
This section describes the Content Categorizer interface screens.

This section covers the following topics:

- [Section A.7.1, "Content Categorizer Administration Page"](#)
- [Section A.7.3, "Rule Sets Tab"](#)
- [Section A.7.4, "Option Lists Tab"](#)
- [Section A.7.5, "Filetype Maps Tab"](#)
- [Section A.7.6, "Categorizer Engines Tab"](#)
- [Section A.7.7, "Query Trees Tab"](#)
- [Section A.7.8, "Field Properties Tab"](#)
- [Section A.7.9, "Batch Categorizer Screen"](#)
- [Section A.7.10, "Categorize Existing Screen"](#)

A.7.1 Content Categorizer Administration Page

This screen is used to define the configuration and search rules for Content Categorizer, register categorizer engines, and build query trees.



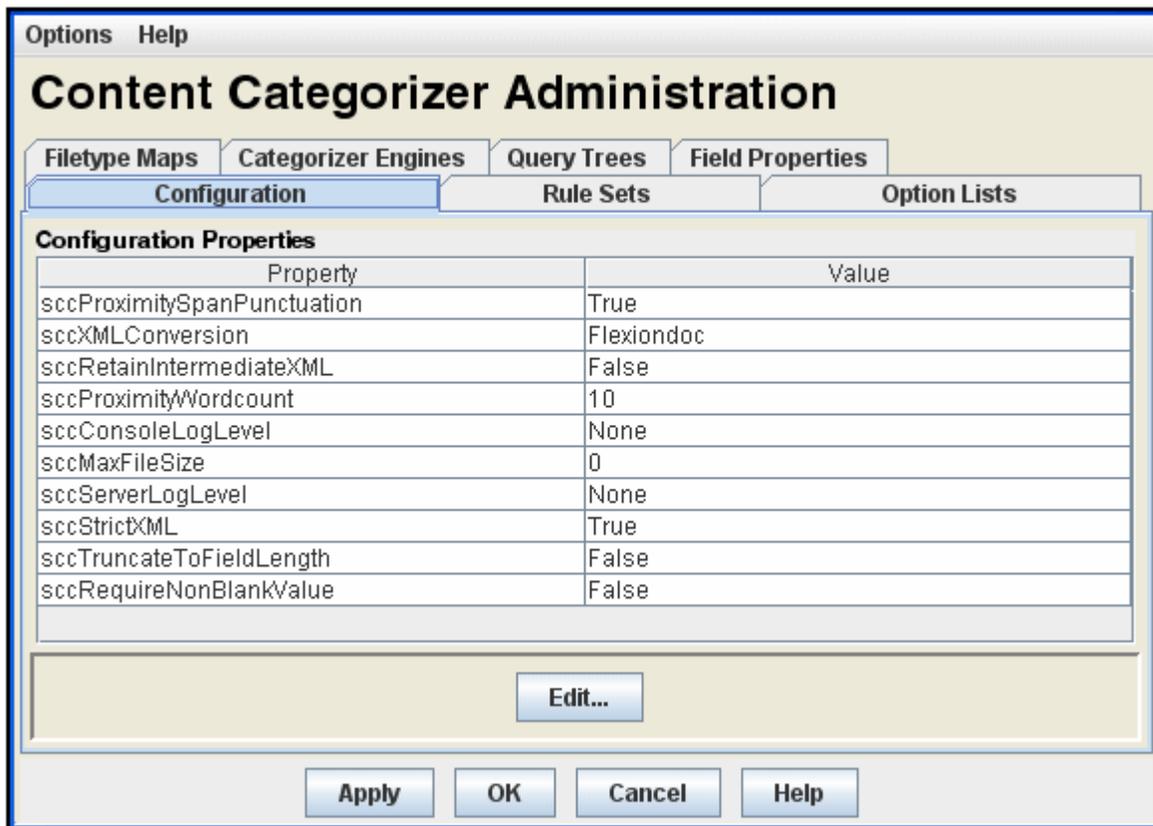
To access this screen, choose **Administration** then **Content Categorizer Administration** from the Main menu.

Element	Description
Options menu	Provides options to save changes or exit the application.

Element	Description
Tabs	<p>The individual tabs are used to manage the software:</p> <ul style="list-style-type: none"> ▪ Rule Sets Tab ▪ Option Lists Tab ▪ Filetype Maps Tab ▪ Categorizer Engines Tab ▪ Query Trees Tab ▪ Field Properties Tab

A.7.2 Configuration Tab

This screen is used to set Content Categorizer run-time configuration settings.



To access this screen, click the **Configuration** tab on the [Content Categorizer Administration Page](#).

Element	Description
Property	<p>Lists properties that can be configured:</p> <ul style="list-style-type: none"> ■ sccRetainIntermediateXML: If set to true, all temporary files are retained and INFO trace entries in the server log map the temp files to the content. ■ sccConsoleLogLevel: Level of execution trace information that appears in the console window when Oracle WebCenter Content Server is run as a foreground process, not started as a background service. ■ sccServerLogLevel: Level of execution trace information that appears in the Oracle WebCenter Content Server log. ■ sccProximityWordcount: Number of words that can lie between two keywords in an Option List search rule for the keywords to be considered "near" each other. Default: 10. ■ sccStrictXML: Set to true if XML includes have no leading whitespace.) ■ sccRequireNonBlankValue: If set to true, search results do not return blank metadata values if XML tags are empty. ■ sccProximitySpanPunctuation: If set to true, leading and trailing punctuation is eliminated from strings during the normalization process. ■ sccTruncateToFieldLength: If set to true, XML tag contents too long for their target metadata fields are automatically truncated to fit. If set to false, XML tag contents too long for their target metadata fields produce errors. ■ sccXMLConversion: Name of the XML conversion method used to convert native documents into XML when operating in Interactive mode or Batch mode.
Value	Current value for each property.
Edit	Opens the Field Map Screen for a selected property.

A.7.2.1 Property Config Screen

This screen is used to edit the value of the property.

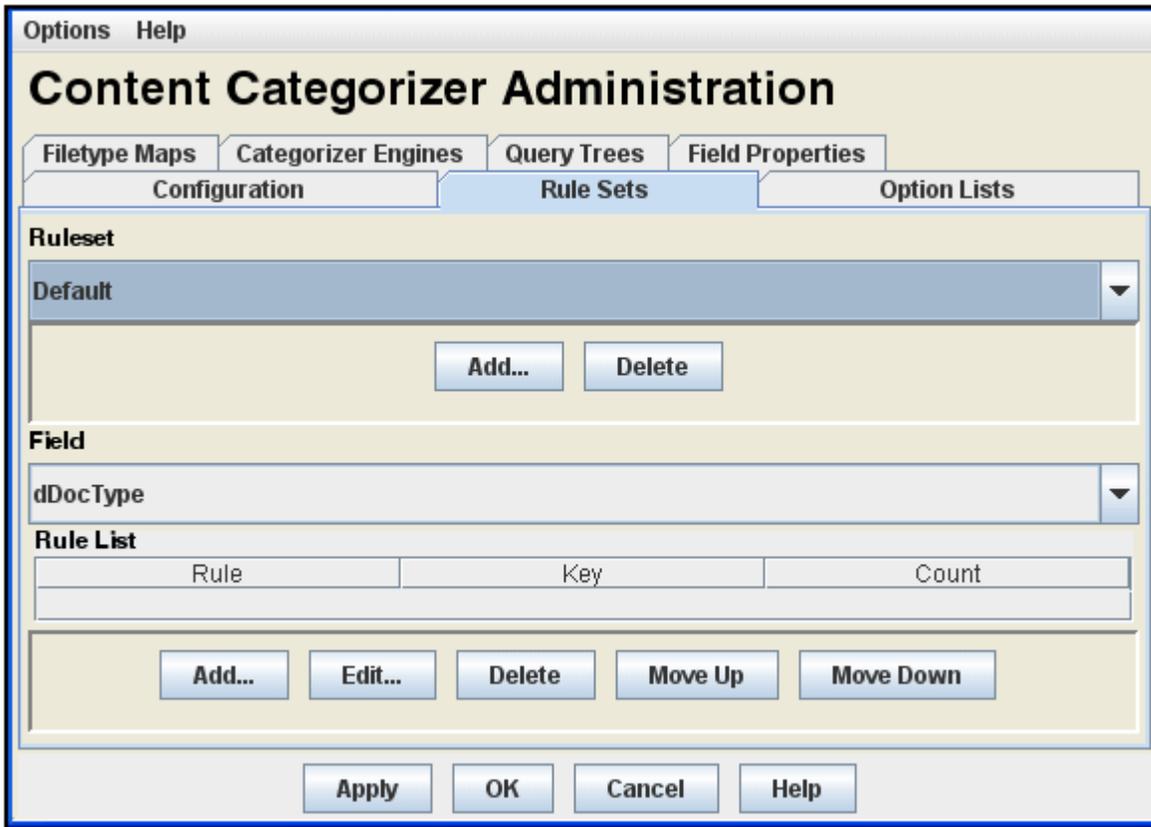


To access this screen, highlight a property on the [Configuration Tab](#) and click **Edit**.

Element	Description
Property field	Changes the setting of the selected property.

A.7.3 Rule Sets Tab

This screen is used to define the search rules that Content Categorizer uses to find metadata values.

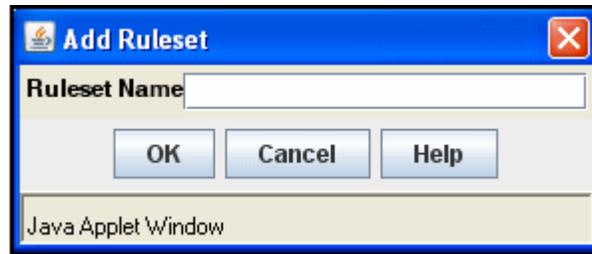


To access this screen, click the **Rule Sets** tab on the [Content Categorizer Administration Page](#).

Element	Description
Ruleset list	Defined search rulesets. You cannot include one ruleset in another and you can apply only one ruleset to a given document.
Add (Ruleset)	Opens the Add Ruleset Screen .
Delete (Ruleset)	Deletes the selected search ruleset. You cannot delete the default ruleset.
Field list	Selects a metadata field for viewing or defining search rules. Only the metadata fields that allow search rules are included in the list.
Rule List	Defined search rules for the metadata field. Searches are run in the order shown, from the top of the list to the bottom.
Columns	Shows the type of search rule, the search key, and the count.
Edit (Rule List)	Opens the Add/Edit Rule for Field Screen .
Delete (Rule List)	Deletes the selected search rule.
Move Up/Down (Rule List)	Moves the selected search rule up or down in the list.

A.7.3.1 Add Ruleset Screen

This screen is used to define a new search ruleset.



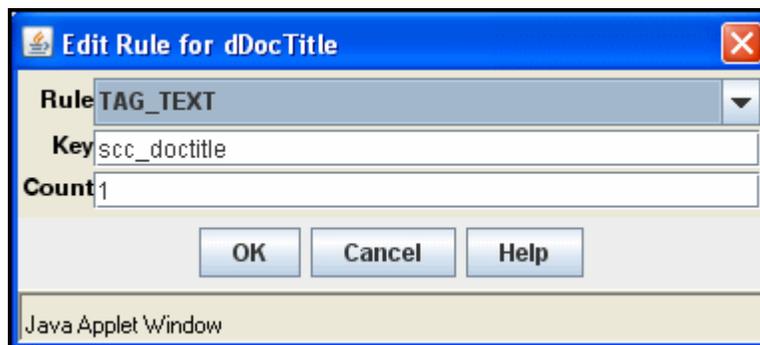
To access this screen, click **Add** on the [Content Categorizer Administration Page](#).

Important: Content Categorizer requires a non-empty rule set for any file type (.doc, .txt, .xml, and so on) it is called to examine. If no rules exist for a given file type, Content Categorizer throws an exception. The easiest way to protect against this is to add at least one rule to the Default rule set. The Default rule set is used for all file types which do not have a custom rule set assigned.

Element	Description
Ruleset Name	Used to add a ruleset name.

A.7.3.2 Add/Edit Rule for *Field* Screen

This screen is used to define a new search rule or edit a rule.

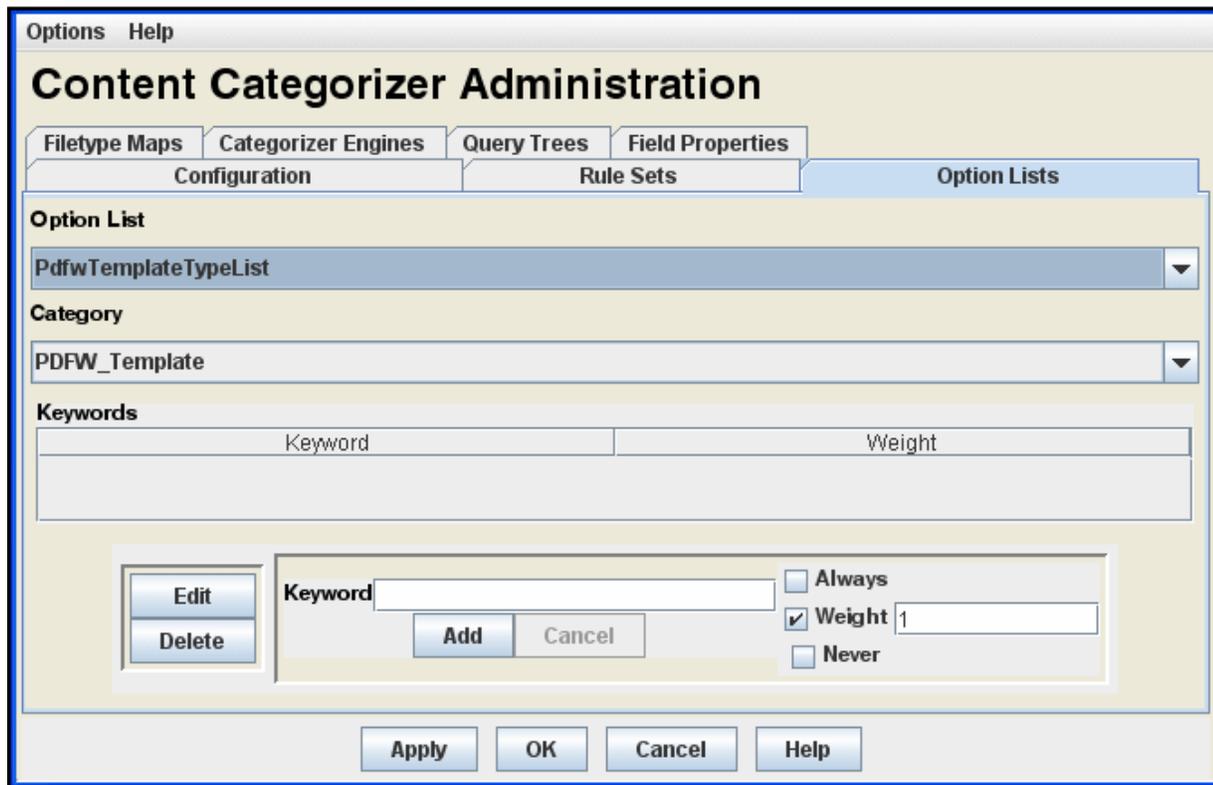


To access this screen, click **Add** or **Edit** on the [Rule Sets Tab](#).

Element	Description
Rule list	Selects the type of search rule.
Key	Defines the search key for the search rule.
Count	Defines the count for the search rule.

A.7.4 Option Lists Tab

This screen is used to define the keywords and weights for search rules.

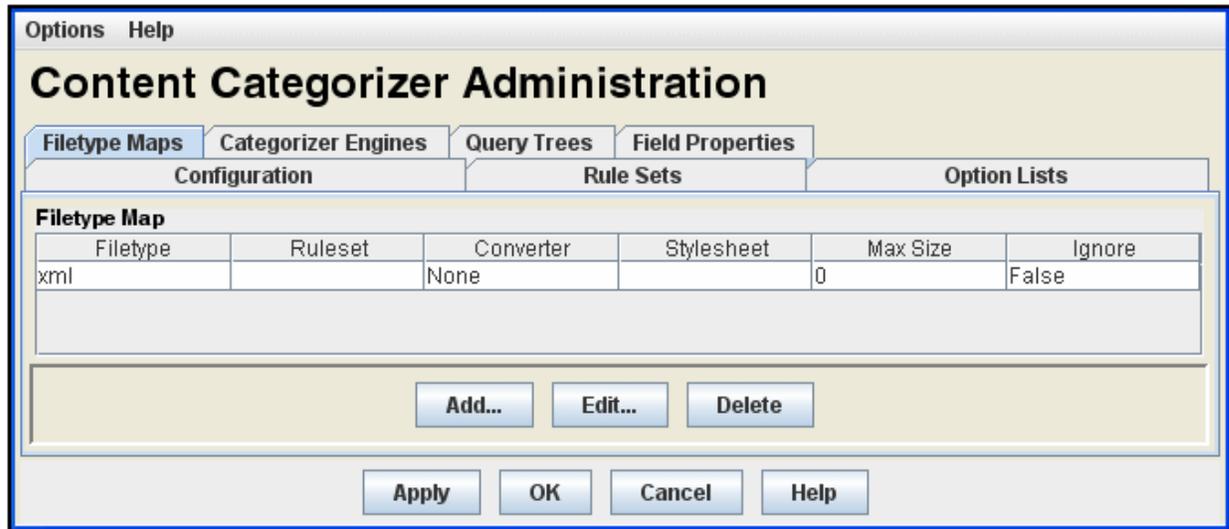


To access this screen, click the **Option Lists** tab on the [Content Categorizer Administration Page](#).

Element	Description
Option List	Selects the list.
Category	Selects a value on the selected list.
Keyword	Keywords associated with the selected category and their weight.
Edit	Changes the Add button to Update and enters the selected keyword and weight in the editing area.
Delete	Deletes the selected keyword.
Keyword box	Used to add or edit a keyword. Click Add to add the keyboard and weight value or apply changes to the selected keyword.
Cancel	Changes the Update button to Add without saving changes to the selected keyword and weight value.
Weight options	Defines the weight assigned to the keyword.

A.7.5 Filetype Maps Tab

This screen is used to create and modify a filetype map.

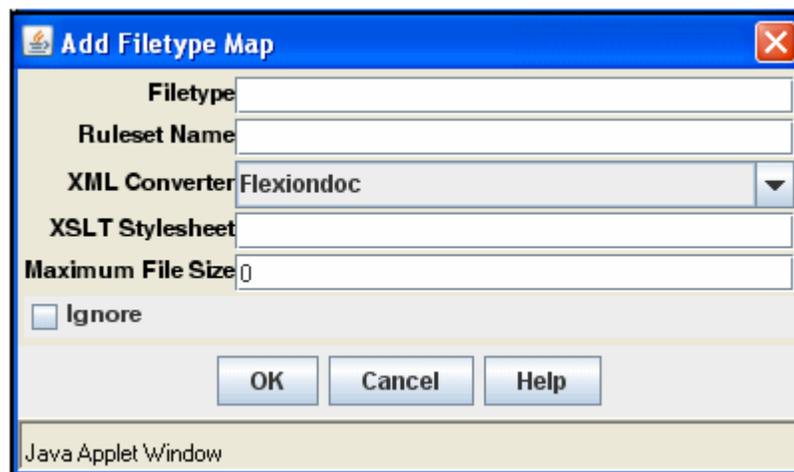


To access this screen, click the **Filetype Maps** tab on the [Content Categorizer Administration Page](#). If no Filetype Map entry is defined for a particular content item, then the default ruleset, XML Converter, style sheet, and maximum size values are used.

Element	Description
Filetype Map	Defined filetype maps and their properties, including: <ul style="list-style-type: none"> Filetype name Ruleset Converter Style sheet
Add or Edit	Opens the Add/Edit Filetype Map Screen .
Delete	Deletes the selected filetype map.

A.7.5.1 Add/Edit Filetype Map Screen

This screen is used to define a new filetype map or edit a map.



To access this screen, click **Add** or **Edit** on the [Filetype Maps Tab](#).

Defining a filetype entry for a particular content file type allows content-specific processing alternatives. For example, you could use a custom ruleset for a specific content type, set a maximum file size, or direct Content Categorizer to ignore files.

Element	Description
Filetype	Specifies the filetype (such as doc, txt, xls). Enter \$\$NONE\$\$ to define a map entry for files with no filetype.
Ruleset Name	Used to specify the ruleset to be applied. If no ruleset is specified, the default ruleset are used.
XML Converter	Lists the applicable XML converter. Three values are available: Flexiondoc, SearchML, and None. (None is available if the content is in XML format either currently or when the custom XSLT style sheet completes its processing.) The default value is set as a configuration parameter.
XSLT Stylesheet	Used to specify the file path (absolute or relative) of the XSLT style sheet to be applied. XSLT style sheets are stored in the <i>IntradocDir/custom/ContentCategorizer/stylesheets/</i> directory. You can use customized, content-specific XSLT translation style sheets as the back-end of the XML conversion. The selected steeliest is used in a transformation operation after the XML conversion (if any) is complete. Style sheets allow document properties and content to be isolated with he results extracted to a metadata field. The style sheet to be used for a given content item is determined by a set of specifiers that includes the document type (doc, txt, xls, and so on). The default value for XSLT Stylesheet depends on the XML converter actually used. Flexiondoc uses flexion_to_scc.xsl and SearchML uses searchml_to_scc.xsl.
Maximum File Size	Used to establish the maximum file size for a given file type (doc, txt, xls, and so on). Files of this type that exceed the maximum size are ignored by Content Categorizer.
Ignore	If selected, directs Content Categorizer to disregard a particular file type (doc, txt, xls, and so on).

A.7.6 Categorizer Engines Tab

This screen is used to register a third-party categorization engine for integration with Content Categorizer.

To access this screen, click the **Categorizer Engines** tab on the [Content Categorizer Administration Page](#). The values needed to register an engine are normally provided by the third-party categorization vendor.

Element	Description
Categorizer Engines	Defined Categorizer Engines.
Properties	Shows the following properties for a Categorizer Engine: <ul style="list-style-type: none"> ▪ Engine Name ▪ Indexer Class ▪ Indexer Configuration ▪ Extractor Class ▪ Extractor Configuration ▪ Description
Add or Edit	Displays the Add/Edit Categorizer Engine Screen .
Delete	Deletes the registration for the selected engine.
Move Up/Down	Moves the position of the selected engine in the list.

A.7.6.1 Add/Edit Categorizer Engine Screen

This screen is used to add a categorizer engine.

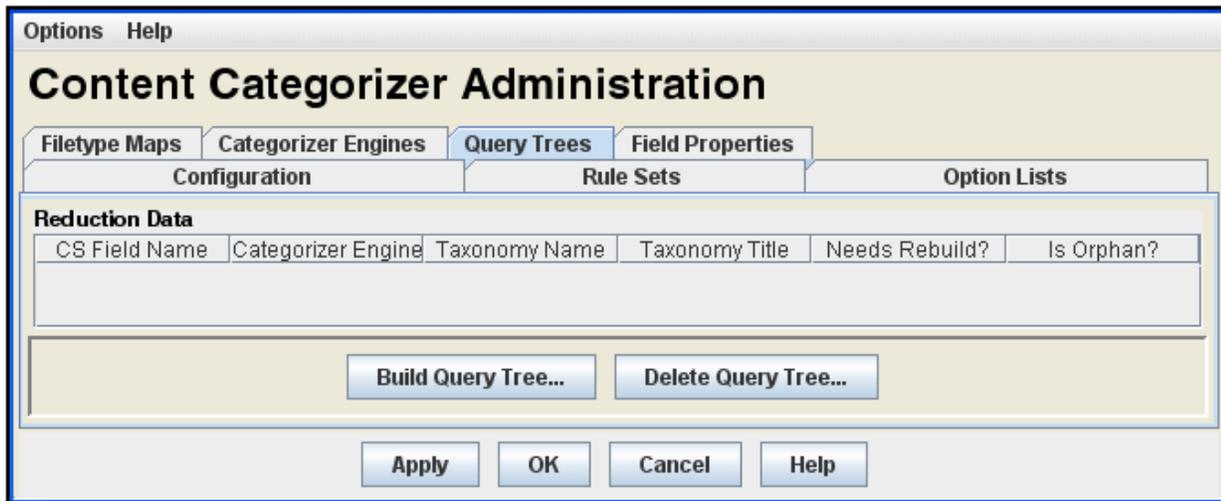
To access this screen, click **Add** on the [Categorizer Engines Tab](#).

Element	Description
Engine Name	Identifier for a categorization engine for which SCC has an adaptor module. This identifier is used in the Key field of a CATEGORY rule, for example, " <i>EngineName/TaxonomyName</i> ".
Indexer Class	Name of the Java class in an SCC adaptor module used to ask the categorizer engine to categorize document(s).
Indexer Configuration	String passed to the Indexer Class's <code>setup()</code> method. Usually a comma-delimited list of engine-specific initialization parameters.
Extractor Class	Name of the Java class in an SCC adaptor module used to ask the categorizer engine for the set of categories in a given taxonomy.

Element	Description
Extractor Configuration	String passed to the Extractor Class's doExtract () method, usually a comma-delimited list of engine-specific initialization parameters.
Description	Description of the categorization engine.

A.7.7 Query Trees Tab

This screen is used to create a browsable hierarchy of categorized documents.

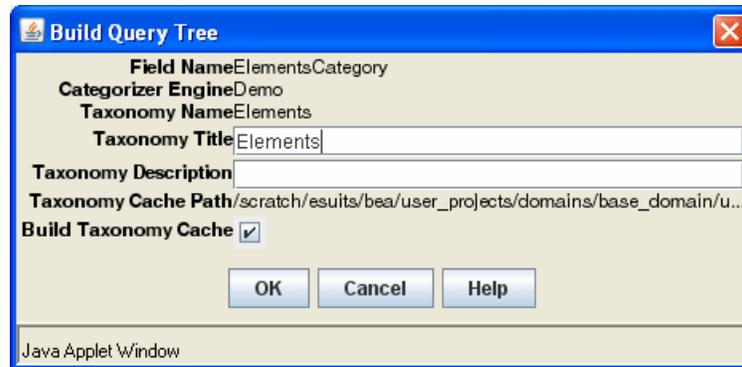


To access this screen, click the **Query Trees** tab on the [Content Categorizer Administration Page](#).

Element	Description
Query Trees	Defined Query Trees.
Properties	Shows the following properties and status for a Query Tree: <ul style="list-style-type: none"> ■ CS Field Name ■ Categorizer Engine ■ Taxonomy Name ■ Taxonomy Title ■ Needs Rebuild? If Yes, the taxonomy cache, the Library page link to the cache, or both, are old or do not exist. A rebuild of the query tree is necessary. ■ Is Orphan? If Yes, the taxonomy cache, the Library page link to the cache, or both, are orphans w no CATEGORY rules that refer to them. Check the rule associated with the query tree.
Build Query Tree	Displays the Build Query Tree Screen .
Delete Query Tree	Displays the Delete Query Tree Screen .

A.7.7.1 Build Query Tree Screen

This screen is used to build a query tree.

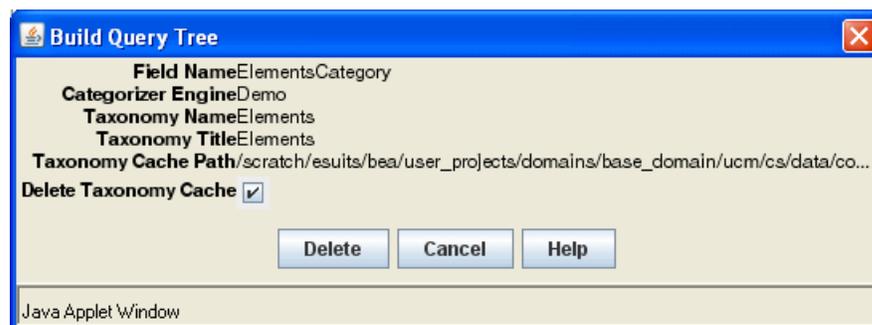


To access this screen, click **Build Query Tree** on the [Query Trees Tab](#).

Element	Description
Field Name	Metadata field for which the CATEGORY search rule was defined.
Categorizer Engine	Categorizer engine specified for the CATEGORY search rule that was defined for the metadata field.
Taxonomy Name	Taxonomy specified for the CATEGORY search rule that was defined for the metadata field.
Taxonomy Title	Title of taxonomy.
Taxonomy Description	Description of taxonomy, which is used under the root link on the Library main page and in the Description field of the Query Link Definition screen.
Taxonomy Cache Path	Path to the taxonomy cache: <i>IntradocDir/data/contentcategorizer/taxonomies/engine_name/taxonomy_name/</i>
Build Taxonomy Cache	If selected, click OK to build or rebuild the taxonomy cache.

A.7.7.2 Delete Query Tree Screen

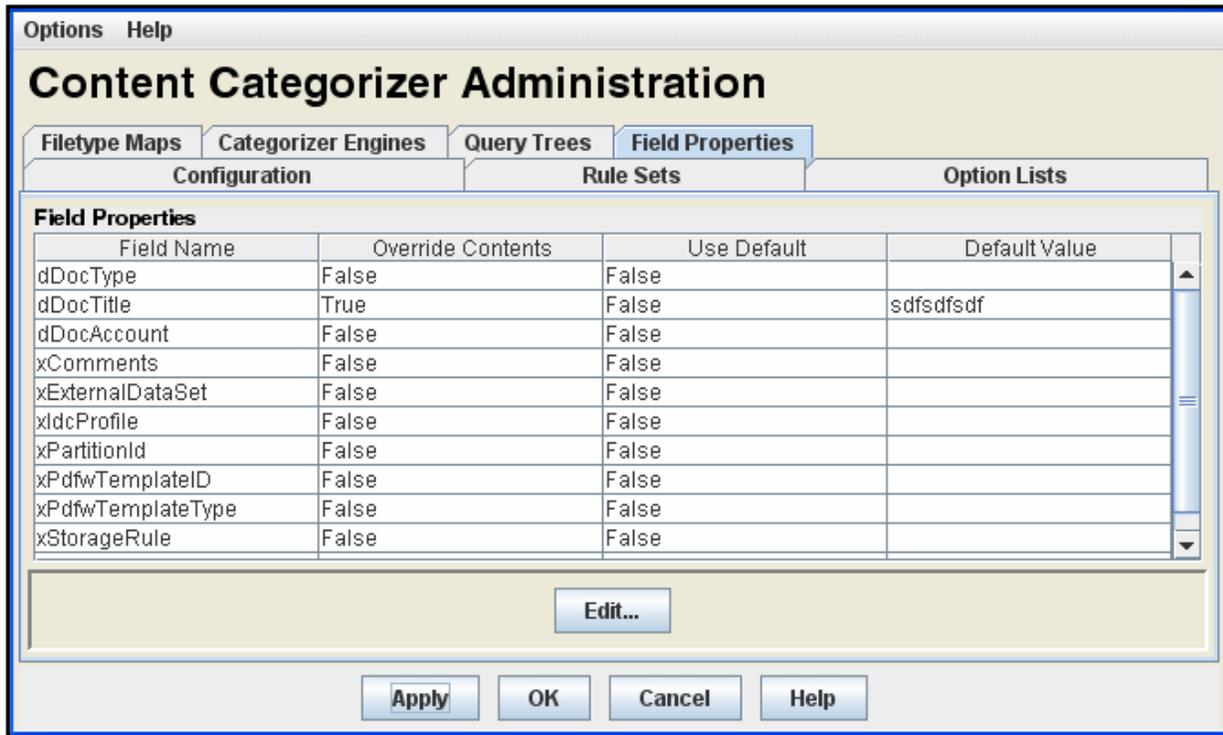
This screen is used to delete a query tree.



To access this screen, click **Delete Query Tree** on the [Query Trees Tab](#). For details about the fields on this screen, see [Section A.7.7.1, "Build Query Tree Screen."](#)

A.7.8 Field Properties Tab

This screen is used to set override and default properties used during Batch mode.

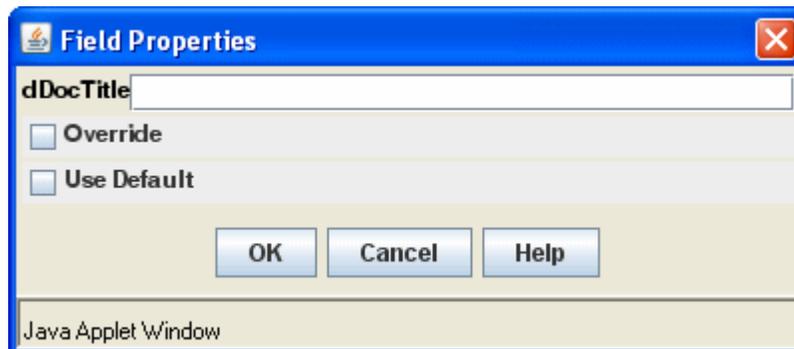


To access this screen, click the **Field Properties** tab on the [Content Categorizer Administration Page](#).

Element	Description
Field Properties	Standard and custom metadata fields and their property settings including: <ul style="list-style-type: none"> ▪ Name ▪ Override Contents: If true, the value returned by the categorization process overrides an existing value. ▪ Use Default: If true, a default value is used. ▪ Default Value: The default value for each field.
Edit	Opens the Field Properties Screen .

A.7.8.1 Field Properties Screen

This screen is used to edit settings for a field selected in the Field Properties list.

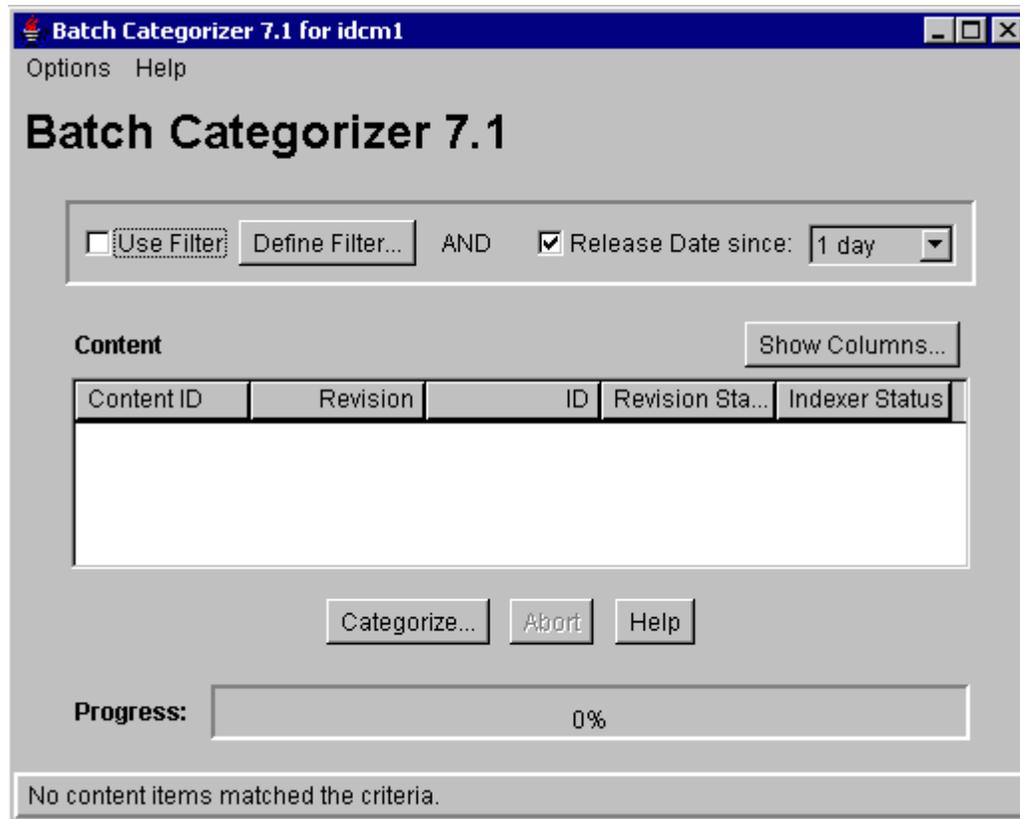


To access this screen, click **Edit** on the [Field Properties Tab](#).

Element	Description
Metadata field	Used to change the default value of the selected field.
Override	If selected, sets Override to true.
Use Default	If selected, sets Use Default to true.

A.7.9 Batch Categorizer Screen

This screen is used to run Content Categorizer in Batch mode.

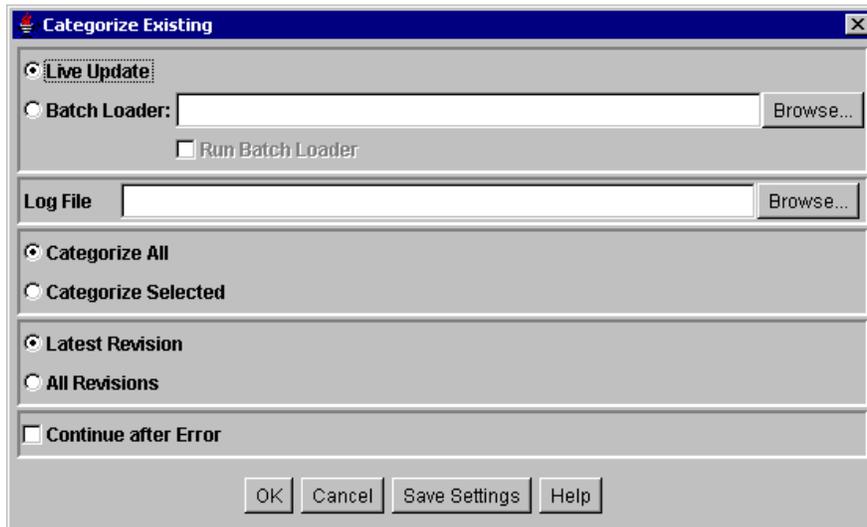


To access this screen, run the BatchCategorizer application.

Element	Description
Use Filter and Release Date	If selected, enables filtering of content based on any defined filters and release date filter (if specified).
Define Filter	Opens the Define Filter Screen .
Content list	Content items in the repository.
Show Columns	Opens the Show Columns Screen .
Content list properties	Shows properties for each content item such as Content ID, Revision, and so on.
Categorize	Opens the Categorize Existing Screen .
Progress bar	Shows the progress of the batch process.

A.7.10 Categorize Existing Screen

This screen is used to categorize existing content.



To access this screen, click **Categorize** on the [Batch Categorizer Screen](#).

Element	Description
Live Update or Batch Loader	If selected: <ul style="list-style-type: none"> Live Update: categorizes and updates existing selected content. Batch Loader: categorizes existing content and writes update records to the control file. Specify the control file name or click Browse to locate the file.
Run Batch Loader	If selected, runs the utility.
Log File	Defines the location and file name for the Categorizer log file. Click Browse to select a location.
Categorize options	<ul style="list-style-type: none"> Categorize All: All content items are categorized. Categorize Selected: Only selected items are categorized.
Revision options	<ul style="list-style-type: none"> Latest Revision: Latest content revisions are categorized. All Revisions: All revisions are categorized.
Continue after Error	If selected, the Batch Categorizer continues processing when it encounters an error and logs the error. Otherwise, processing stops when an error is encountered.

A.8 Web Layout Editor Interface

This section describes the screens used to create Web pages with the Web Layout Editor.

This section covers the following topics:

- Section A.8.1, "Web Layout Editor Page"
- Section A.8.2, "Add Page Link Screen"
- Section A.8.3, "Add Web Page Screen"
- Section A.8.4, "Edit Local Page Link Screen"

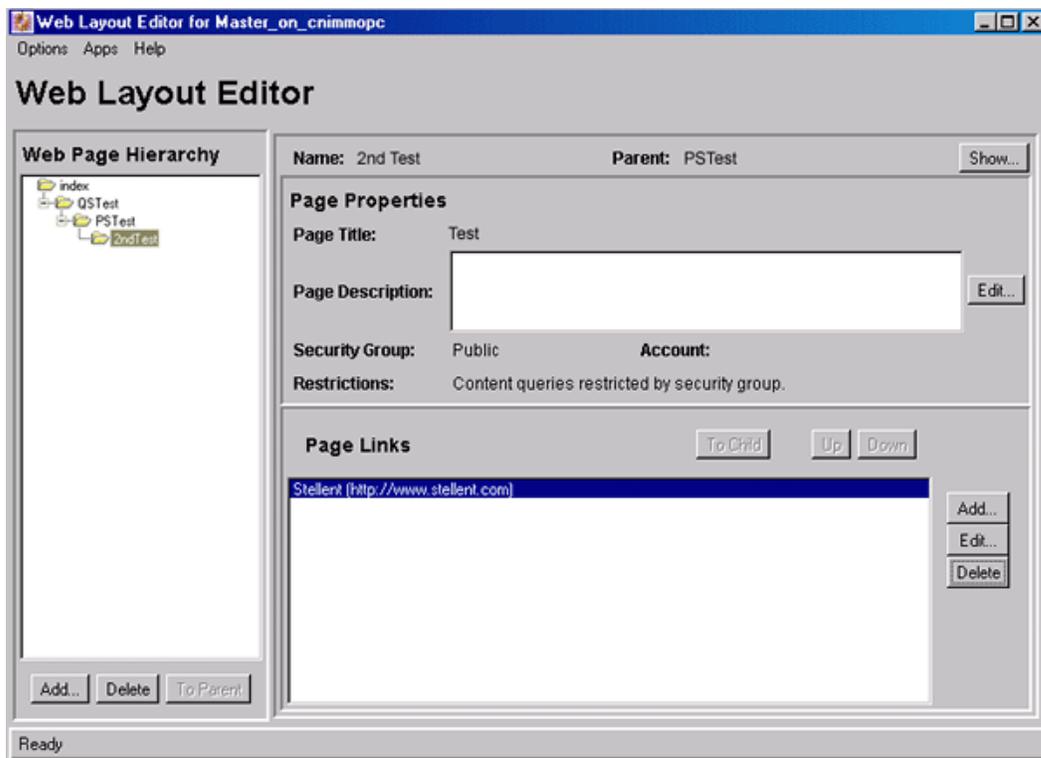
- Section A.8.5, "Edit External URL Screen"
- Section A.8.6, "Edit Page Properties Screen"

The following screens are used to create and edit queries through the Web Layout Editor.

- Section A.8.7, "Edit Active Report Query Screen"
- Section A.8.8, "Create Historical Report Screen"
- Section A.8.9, "Query Link Definition Screen"
- Section A.8.10, "Add/Edit Query Results Page"

A.8.1 Web Layout Editor Page

This page is used to design a Web layout.



To access this page, choose **Administration** then **Admin Applets** from the Main menu. Click **Web Layout Editor**.

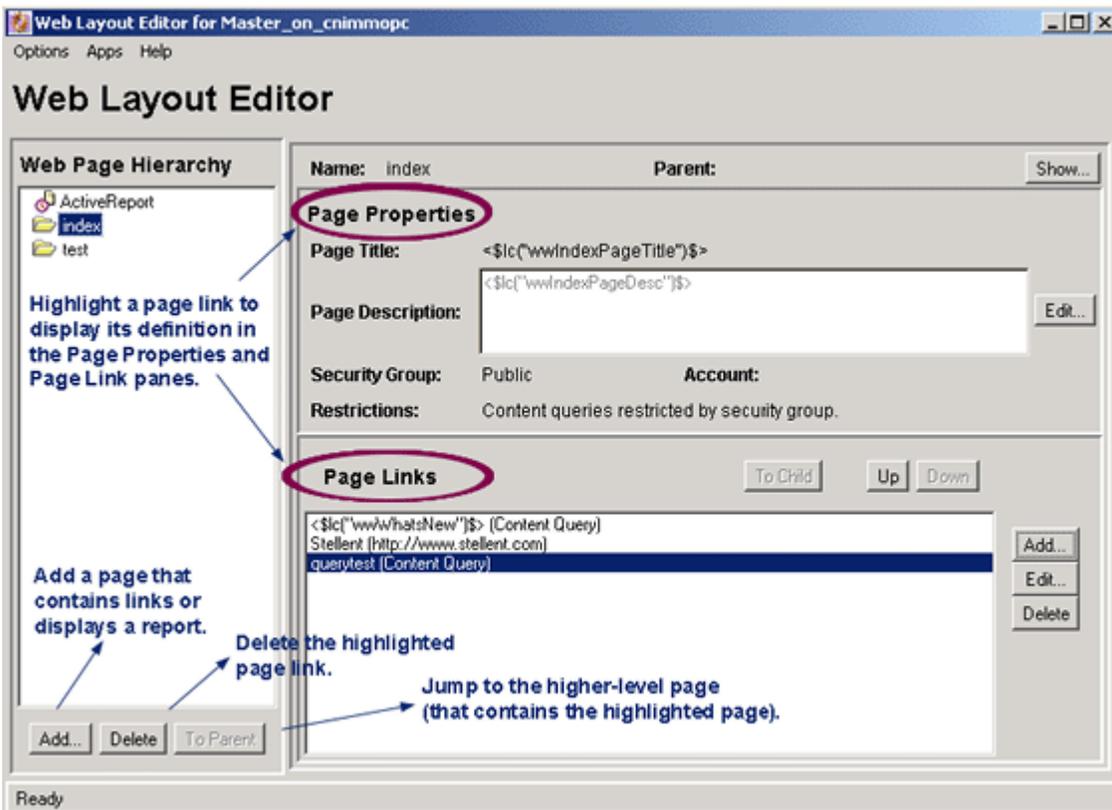
This page contains three panes: the Web Page Hierarchy pane, the Page Properties pane, and the lower page (usually the Page Links pane).

Element	Description
Web Page Hierarchy Pane	Opens the Web site structure and relationship between pages.
Page Properties Pane	Defines the page header text and the security group that filters the content for the page.

Element	Description
Lower pane	<p>Determines what is displayed in the lower pane:</p> <ul style="list-style-type: none"> Page Links Pane displays the contents of the selected link (URLs, local pages, queries). Active Report Specification Pane and Historical Report Specification Pane display information about the selected report.

A.8.1.1 Web Page Hierarchy Pane

This pane displays the organization of the local Web pages in the Library. Child pages are shown in the parent's folder. A page must be selected in this pane to edit it.

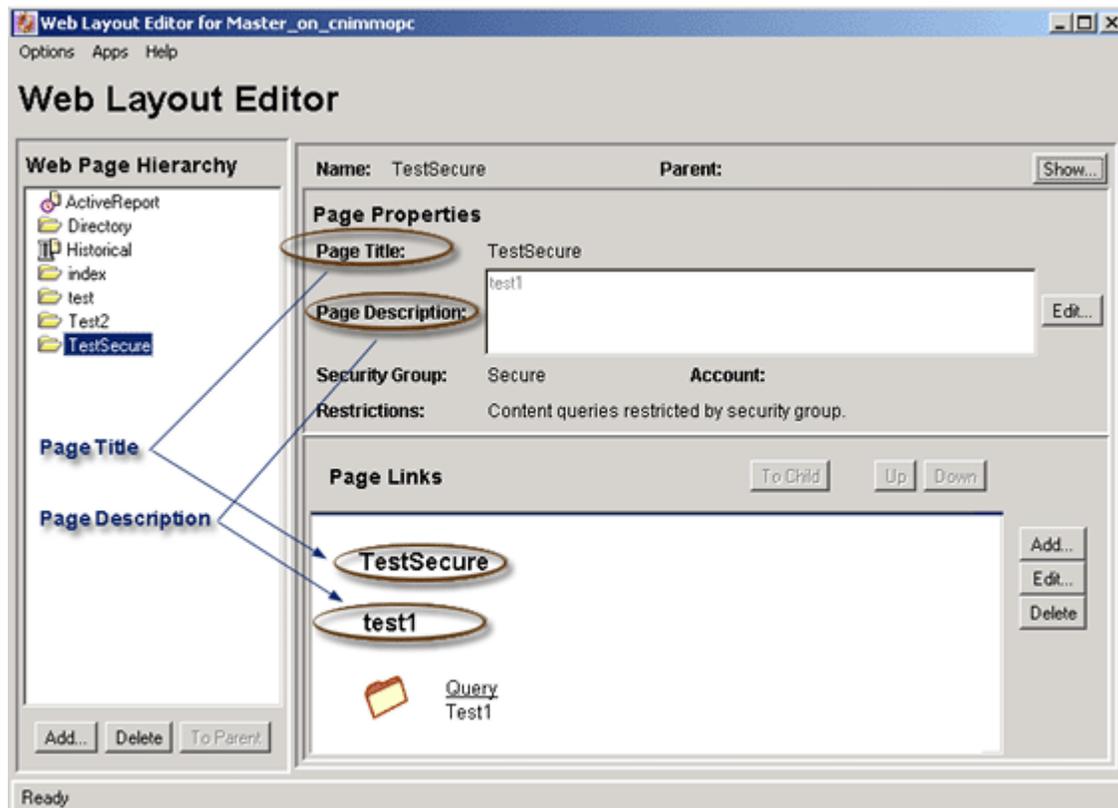


For subadministrators to see a page in this pane, they must be able to view its parent. For subadministrators to delete a page, the page must be a directory page and the subadministrator must have access to that page and all of its children.

Element	Description
Add	Adds a page that contains links or opens a report.
Delete	Deletes the highlighted page link.
To Parent	Jumps to the higher-level page containing the highlighted page.

A.8.1.2 Page Properties Pane

This pane controls page header text and the security group that filters its content.

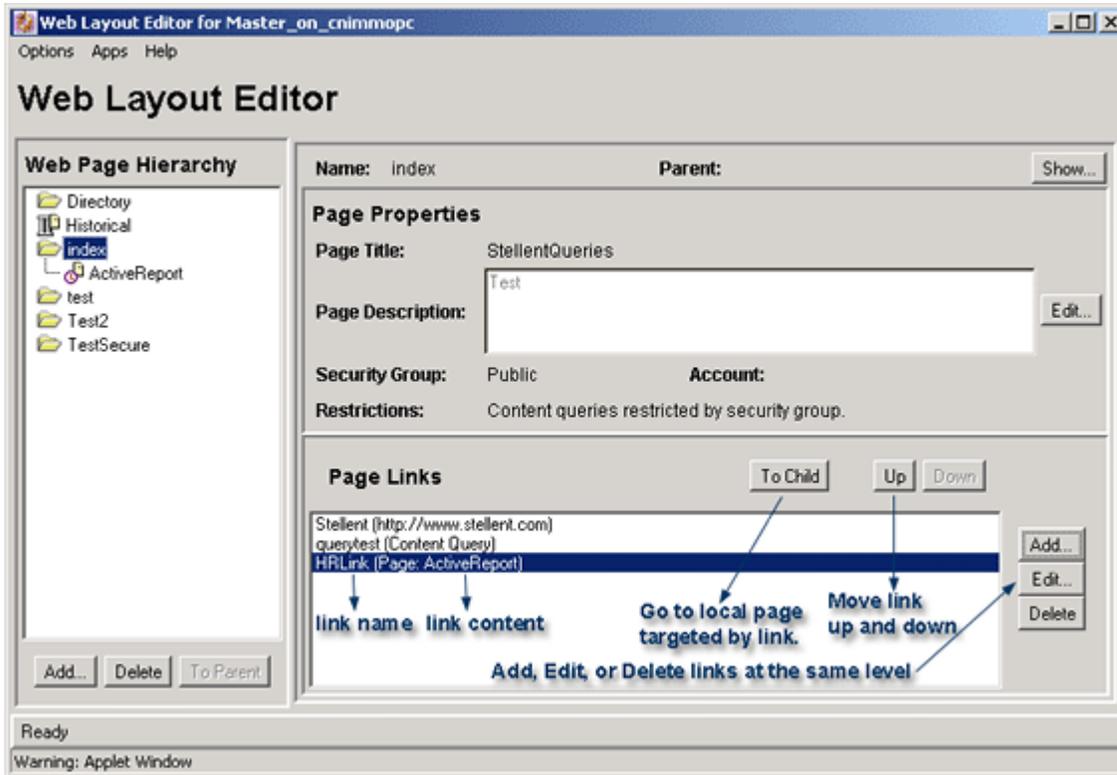


For subadministrators to edit a page, it must be a directory page, and the subadministrator must have admin access to that page and all of its children. This prevents a subadministrator from editing a public page that has links to secure pages.

Element	Description
Name	Page name as it appears in the Web Page Hierarchy pane.
Parent	Parent page, if the page has a parent.
Show	Opens the Web page.
Page Title	Title of the Web page.
Page Description	Description of the Web page.
Security Group	Names of the security groups that filter the files appearing on the Web page. Only files within the security group for which end user has permission are displayed.
Account	Assigns the account to the page. Only users with Read permission to the account can access this page.
Restrictions	Shows any restrictions, such as whether content queries are restricted by security group or account.

A.8.1.3 Page Links Pane

This pane opens the contents of the local page selected in the [Web Page Hierarchy Pane](#).



For subadministrators to see the contents of a page, they must have Read access to that page and all of its parents. This prevents the subadministrators from seeing a page that they cannot get to through the Library link.

Element	Description
To Child	Goes to the local page targeted by the link selected in the Page Links pane.
Up or Down	Moves the selected link up or down in the list of links.
Lower pane	The page selected in the Web Page Hierarchy pane determines what is displayed in the lower pane: <ul style="list-style-type: none"> Page Links Pane opens the contents of the selected link (URLs, local pages, queries). Active Report Specification Pane and Historical Report Specification Pane display information about the selected report, such as Data Source, Report Template, Report Creation Date, and Rows Per Page.
Add	Opens the Add Page Link Screen .
Edit	Displays the relevant screen for editing a link at the same level. For example, when editing a query, a Query Link Definition page opens, or when editing a URL, an Edit URL page opens.
Delete	Deletes the selected link at the same level.

A.8.2 Add Page Link Screen

This screen is used to start the process of setting up a link to a new Web page.

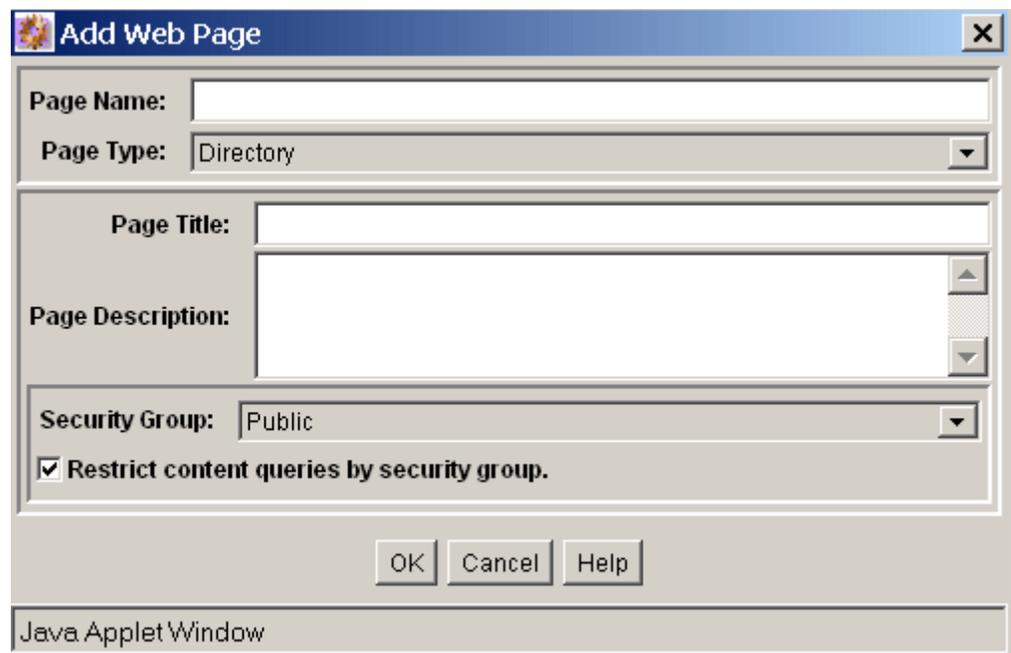


To access this screen, click **Add** on the [Page Links Pane](#).

Element	Description
Link Type	Specifies which type of page link to add to the Web page: <ul style="list-style-type: none"> Local Page: Links page to a local page. External URL: Links page to an External URL. Query: Links page to a report query.

A.8.3 Add Web Page Screen

This screen is used to add a new Web page.



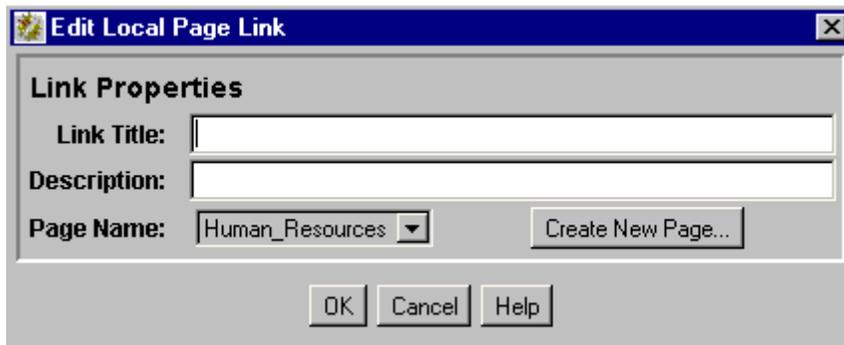
To access this screen, click **Add** on the [Web Page Hierarchy Pane](#).

Element	Description
Page Name	Name appearing in the Web Page Hierarchy pane.
Page Type list	<ul style="list-style-type: none"> Directory: A Web page that contains links to other pages, links to URLs, or runs a query. Active Report: A Web page that displays current information from the database. Historical Report: Similar to an Active Report, but captures and saves the information at the time when it was last created.

Element	Description
Page Title and Page Description	Appear on the Page Properties Pane .
Security Group	Filters the files that appear on the Web page. Only files within the security group for which an end user has permission are displayed.
Restrict content queries by security group	If selected, the security group applies to all queries that originate from this page. All queries inherit the security group of this page.
Account	Assigns the account to the page. Only users with Read permission to the account can access this page.
Restrict content queries by account	If selected, the account applies to all queries that originate from this page.

A.8.4 Edit Local Page Link Screen

This screen is used to enter information about a local page.

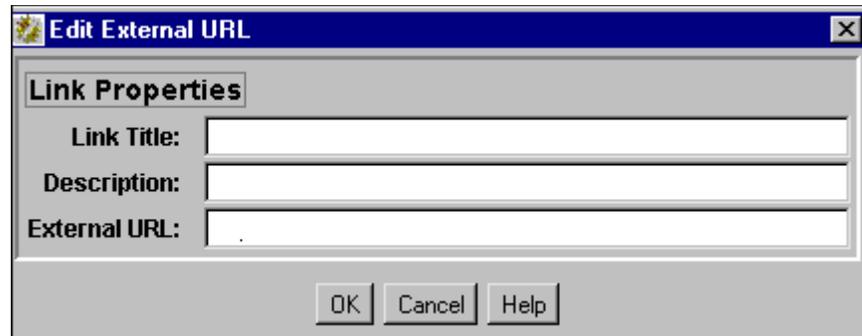


To access this screen, click **Add** then **Local Page** in the [Web Page Hierarchy Pane](#) of the [Page Links Pane](#).

Element	Description
Link Title	Text displayed as the link.
Description	Optional field text or HTML displayed under the link to provide additional description about the destination.
Page Name	The page where the link appears.
Create New Page	Opens the Add Web Page Screen .

A.8.5 Edit External URL Screen

This screen is used to specify information for an external URL.



To access this screen, click **Add** then **External URL** from the [Page Links Pane](#) in the [Web Page Hierarchy Pane](#).

Element	Description
Link Title	Text displayed as the link.
Description	Optional field text or HTML displayed under the link to provide additional description about the destination.
External URL	Address of the link's destination, starting with <code>http://</code> .

A.8.6 Edit Page Properties Screen

This screen is used to modify the page properties for a Web page.



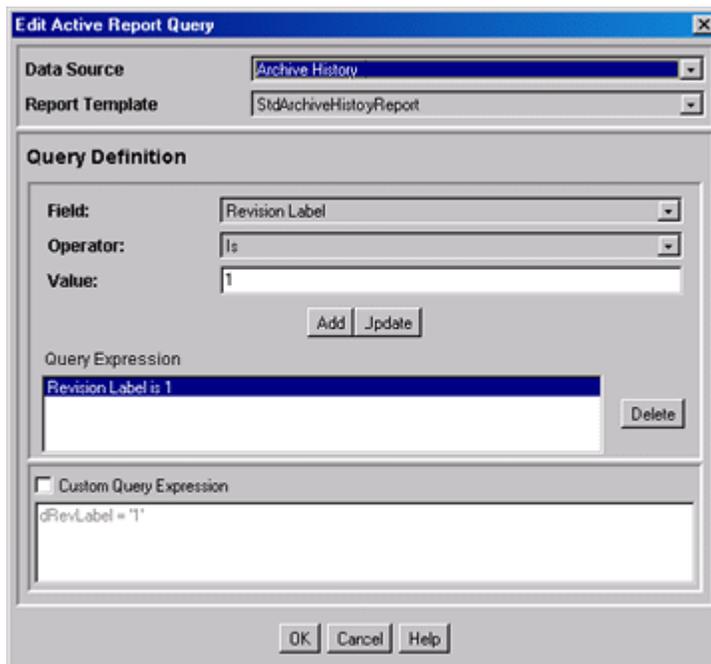
To access this page, select a page in the [Web Page Hierarchy Pane](#) then click **Edit** in the [Page Properties Pane](#).

Element	Description
Page Title	Title of the Web page.
Page Description	Describes the Web page.
Security Group	Specifies the security group for the Web page.

Element	Description
Restrict content queries by security group	If selected, content queries are restricted to users assigned to the specified security group.
Account	Assigns the account to the Web page. Only users with Read permission to the account can access this page.
Restrict content queries by account	If selected, content queries are restricted to users assigned to the specified account.

A.8.7 Edit Active Report Query Screen

This screen is used to define the data source, template, and query definition for an active report.



To access this screen, select an active report page in the [Web Page Hierarchy Pane](#) and click **Edit Report Query** in the Active Report Specification pane.

Element	Description
Data Source	Type of report to create: <ul style="list-style-type: none"> ■ Archive History ■ Content Types ■ User ■ Information Fields ■ Content History ■ Workflow Items ■ Workflow History
Report Template	List of templates that control the query links display.

Query Definition pane	Description
Field	Field the query searches, dependent on the Data Source selected.
Operator	Query operators. Available operators are the result of the field selected.
Value	Target data for the query, dependent on the Field selected.
Add	Enters the query into the Query Expression box. You can append one or more query lines
Update	Updates the selected query line.
Query Expression	Displays each query as a single line when added by the Add button.
Custom Query Expression	If selected, enables display and editing of SQL code generated from the query expression. If unselected, the expression reverts to its original definition and modifications are lost.
Delete	Deletes a selected query line.

A.8.8 Create Historical Report Screen

This screen is used to specify the information to be included in an historical report.

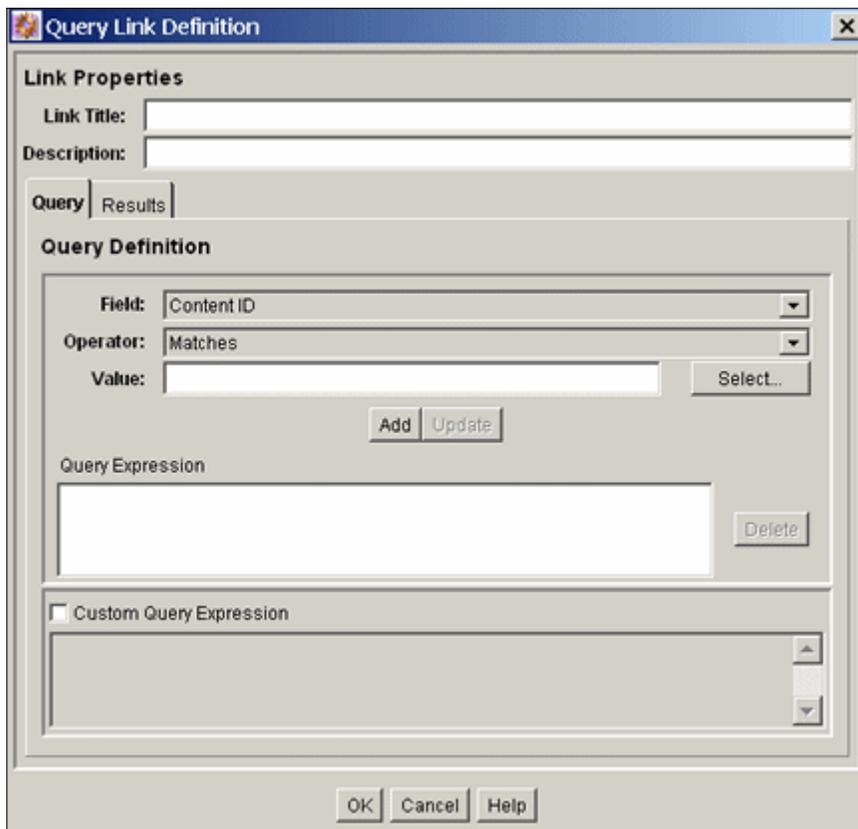
To access this screen add a new Web page and specify that it be a historical report. When Historical Report Specification is shown in the lower pane of the Web Layout Editor, click **Create Report Data**.

Element	Description
Data Source	Select Archive History from the list of data sources.

Element	Description
Report Template	This field is automatically populated with the tdArchiveHistoryReport selection.
Rows Per Page	The rows per page in the report.
Field	Metadata field the query searches.
Operator	The method for searching the metadata fields. The selected field determines the set of available values: <ul style="list-style-type: none"> ■ Is ■ Is Not ■ Begins With ■ Contains
Value	Target data for the query.
Add	Enters the query into the Query Expression box. You can append one or more query lines.
Update	Updates the selected query line.
Query Expression box	Displays each query as a single line.
Delete	Deletes the selected query line.
Custom Query Expression	If selected, enables display and edit of Idoc Script generated from the query expression. If unselected, the expression reverts to its original definition and modifications are lost.

A.8.9 Query Link Definition Screen

This screen is used to specify the information to be used in a query.



To access this screen click **Add** or **Edit** in the [Web Layout Editor Page](#).

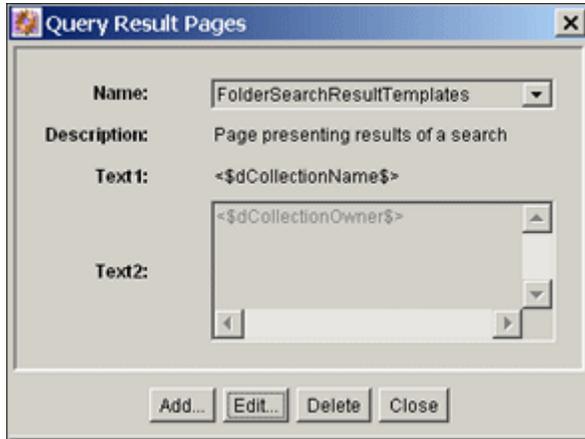
Element	Description
Link Title	Text displayed as the link.
Description	Text displayed under the link to provide a description about the link destination (optional field).
Query Tab	
Query Tab	Description
Field	Metadata field the query searches.
Operator	Specifies the method for searching the metadata fields. The selected field determines the set of available values.
Value	Target data for the query.
Select	Opens the Content Item View screen or User View screen, used to select content items or users.
Add	Enters the query into the Query Expression box. You can append one or more query lines.
Update	Updates the selected query line.
Query Expression pane	Displays each query as a single line.
Delete	Deletes the selected query line.
Custom Query Expression	If selected, enables display and edit of Idoc Script generated from the query expression. If unselected, the expression reverts to its original definition and all modifications are lost.

Note: You can directly edit the following fields to add Idoc Script variables and HTML tags.

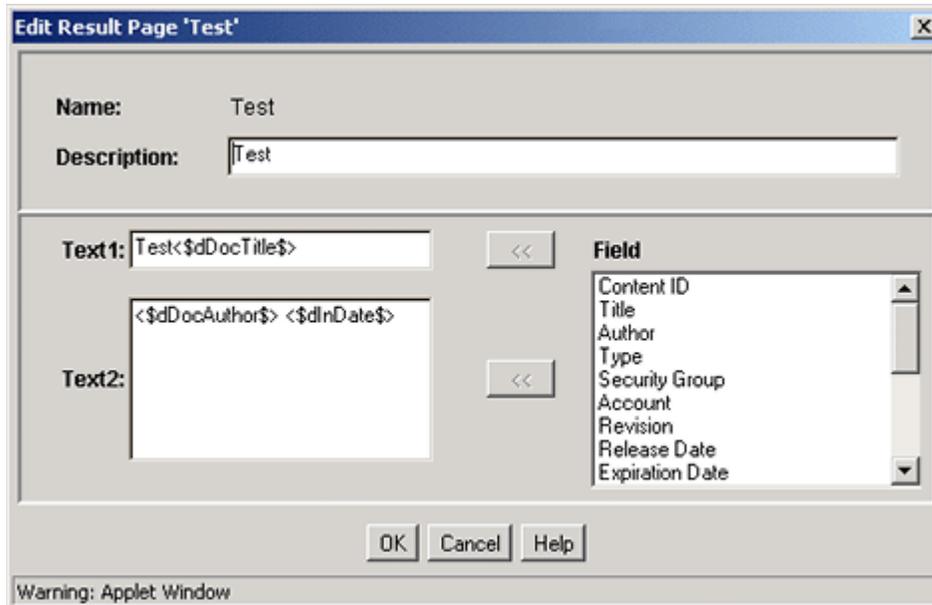
Results Tab	Description
Page Title	Heading of the query results page.
Sort Results By	The metadata field by which the list of results is sorted.
Sort Order	The order of search results.
Results Template Page	Templates that control how the query links are displayed. The list contains a Standard Results page and any templates created with the Query Results Pages screen.
Use Customized Text	If selected, displays custom text for each row on the query results page.
Text 1, Text 2	Text that is displayed as the first or second line in each row on the query results page.*
Arrows	Moves the selected field from the Field list to the Text 1 or Text 2 field.
Field list	Lists the metadata fields available for display on the query results page.

A.8.10 Add/Edit Query Results Page

This page is used to add or edit specifications for query results.



To access this screen select **Options** then **Query Result Pages** from the [Web Layout Editor Page](#).



To add a query result page, click **Add** on the [Add/Edit Query Results Page](#).

Note: You can edit these fields directly to add Idoc Script variables and HTML tags.

Element	Description
Name	The name for the Query Results Page. You can select this name from the Results Template Page Properties.
Description	Helps identify the results page. This text is not displayed on a Web page.
Text 1, Text 2 field	Text that is displayed as the first or second line in each row on the query results page.
Arrows	Moves the selected field from the Field list to the Text 1 or Text 2 field.
Field	Lists the metadata fields available for display on the query results page.

When adding Idoc Script variables and HTML tags to the Text 1 and Text 2 fields, keep in mind that any resulting HTML tags can affect the display of the search results page. See the *Oracle WebCenter Content Idoc Script Reference Guide* for more information.

Building a Web Site

This appendix describes the Web Layout Editor and how it is used to build a Web site.

The following topics are covered:

- [Section B.1, "Planning a Web Site"](#)
- [Section B.2, "Working with Web Pages"](#)
- [Section B.3, "Managing Web Pages"](#)
- [Section B.4, "Working with Reports"](#)
- [Section B.5, "Writing Queries"](#)

B.1 Planning a Web Site

Administrators are responsible for planning the Web site. Subadministrators with WebLayout rights can create directory pages for groups and accounts if they have permissions for those groups and accounts.

This section covers these topics:

- [Section B.1.1, "The Web Layout"](#)
- [Section B.1.2, "Defining the Site Structure and Displaying Criteria"](#)
- [Section B.1.3, "Task Sequence"](#)

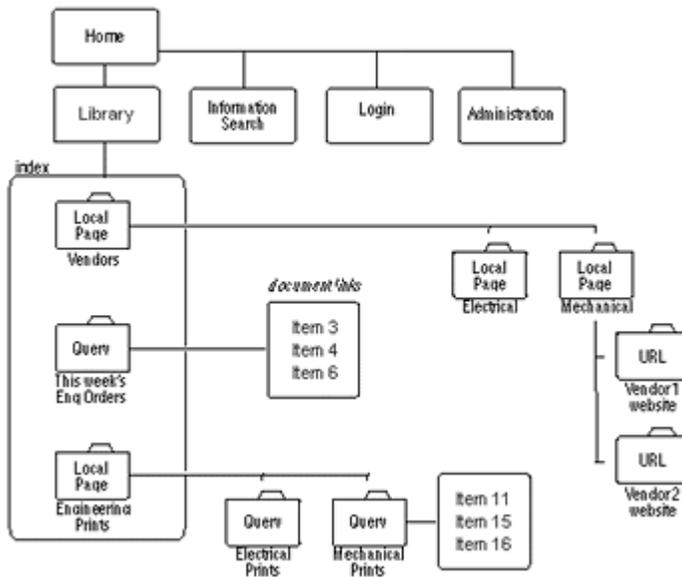
B.1.1 The Web Layout

From the Home page, the Library (Table of Contents) link displays the top level of your Web layout. Although a Web layout is not required and might not be necessary for all applications, it provides an effective means for grouping files and navigating. When a Web layout is not created, the Search function provides the only access to files in the core Oracle WebCenter Content Server. However other products like Site Studio, and extras like Folders and Categorization Folders provide other means of navigation.

Active and Historical reports are other features introduced later in this section. Web viewable files always have lowercase names.

[Figure B-1](#) shows an example of a Web layout using Local Pages, URLs, and Queries as site-building features.

Figure B-1 Web Layout Example



On the Library Web pages, these features are displayed as links with a title next to a file-folder icon. When you click a folder that represents a query, the result produces a set of links to files that match the query's criteria.

B.1.2 Defining the Site Structure and Displaying Criteria

Define the Web site structure in the Web Hierarchy pane of the Web Layout Editor. Then define criteria to display specific files when the user clicks a folder (or link). The criteria for each link is based on the metadata for each file. Besides executing a query, links can jump to another page of links, go to a URL, or display a report. The following examples demonstrate how links are setup to display files.

- **Example 1:** To enable users to access engineering forms from a link named Forms, create a content type named Forms using the Configuration Manager. For details, see [Section 2.1, "Content Types."](#) Then, create a query with Type equal to Forms using the Web Layout Editor.
- **Example 2:** To enable users to access specific Standard Work Procedures, create a content type called SWP, and create a query of Type equal to SWP and Content Name substring of 7200.

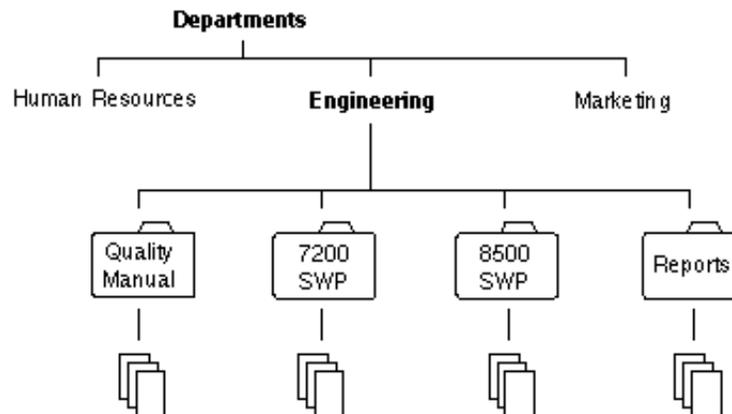
B.1.3 Task Sequence

The following steps demonstrate the typical sequence of tasks for creating a Web site with the Web Layout Editor:

1. **Gather Information.** The first step is to gather information about how your users would intuitively retrieve information; what do they want and how would they typically search for it? How does this impact security?
2. **Customize Metadata.** If necessary, customize your site's metadata by creating any additional fields that might be useful (described in [Section 2.2, "Custom Fields."](#))
3. **Define Content Types.** Define the content types to support your site (described in [Section 2.1, "Content Types."](#))

4. **Define Security Groups, Users, and Roles.** Create security groups and users, and assign roles to users to establish their permissions (described in the *Oracle WebCenter Content System Administrator's Guide for Content Server*).
5. **Design the Web Site.** Create the Web site layout. Although a Web site provides a structure that allows navigation to locate and display files, it is not required. Some companies prefer users to use only the search engine to find files, others prefer to use both a navigation structure and a search engine. To design the Web site, it is helpful to first draw a Web site structure as shown in [Figure B-2](#).

Figure B-2 Example Web Structure



B.2 Working with Web Pages

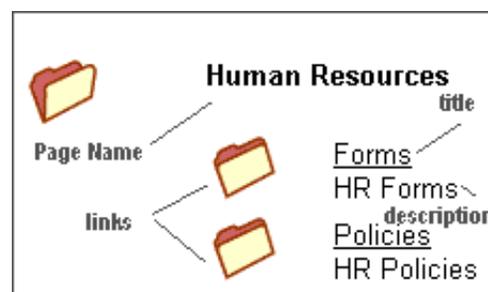
After completing the initial plan, build the Web site and determine how it functions. Revise it if it does not perform properly or is not manageable. Continue this process until you have a design that is going to work for you and the users.

The links on a page jump to one of these:

- Local page
- URL
- Query
- Report

The links all look similar and can be combined on the same page as shown on the local page in [Figure B-3](#):

Figure B-3 Links in Example Local Page



A *local page* is one of two types: a directory or a report. A local page that is a directory can contain links that open another local page, open a URL, or run a query. Only administrators can create a local page that is a report. Administrators or subadministrators with appropriate rights can create a local page that is a directory.

An *external URL* is a link to a specified URL (Web address). You can link to any URL address or Web page on the intranet or internet.

A *search query* produces a page containing links to files that meet the criteria of a defined query. The page looks the same as a page resulting from a content search.

Important: Queries can inherit the security group, the account or both that the page links are on. If the security group or account is inherited, it automatically restricts the query to files in that security group or account.

Reports are either Active or Historical. Active reports appear as a file folder link and perform a database query each time they are run, generating a display of current information. Like Active Reports, Historical Reports appear as a file folder link, but they contain information that was queried at the time they were initially run. They do not perform a database query each time they are opened, and the report is only changed if it is updated.

B.3 Managing Web Pages

Subadministrators do not have access to the Query Result Pages function in the Options menu nor to any applications for which they do not have rights. Additionally, subadministrators have viewing, editing, and deleting restricted rights as described in these sections:

- [Section B.3.1, "Adding a New Web Page"](#)
- [Section B.3.2, "Editing Web Page Properties"](#)
- [Section B.3.3, "Creating a Local Page Link"](#)
- [Section B.3.4, "Creating an External URL Link"](#)
- [Section B.3.5, "Editing a Hierarchical Web Page Structure"](#)

B.3.1 Adding a New Web Page

To add a new Web page to the Web layout:

1. In the [Web Page Hierarchy Pane](#), click **Add**.
The [Add Web Page Screen](#) opens.
2. Enter information about the new page.
3. Click **OK**.

B.3.2 Editing Web Page Properties

To edit the properties of a Web page:

1. Select the page in the [Web Page Hierarchy Pane](#).
2. Click **Edit** in the [Page Properties Pane](#).
The [Edit Page Properties Screen](#) opens.

3. Edit the properties.
4. Click **OK**.

B.3.3 Creating a Local Page Link

To create a local page link:

1. Select the page in the [Web Page Hierarchy Pane](#) under which you want to locate the new local page.
2. In the [Page Links Pane](#), click **Add**.
The [Add Page Link Screen](#) opens.
3. Select **Local Page**, and click **OK**.
4. Enter information about the new local page into the [Edit Local Page Link Screen](#).
5. When done, click **OK**.

B.3.4 Creating an External URL Link

To create an external URL link:

1. Select the page in the [Web Page Hierarchy Pane](#) under which you want to locate the new URL.
2. In the [Page Links Pane](#), click **Add**.
The [Add Page Link Screen](#) opens:
3. Select **External URL**, and click **OK**.
4. Enter information about the URL into the [Edit External URL Screen](#).
5. When done, click **OK**.
6. Refresh the browser to display the new page.

B.3.5 Editing a Hierarchical Web Page Structure

To edit a hierarchical Web page structure, the objective is to insert a page, making it the new parent of the hierarchical page.

For example:

1. Create a structure.
2. Select **QSTest** directory with the Page Link **PCTest** also selected.
3. Click **Page LinksDelete**.
4. Select the **Index** directory and select **Page LinksAdd**.
5. Create a new page.
 - Title the page *NewEngPage*.
 - Type a Description as *NewEngPage*.
6. Click **OK**.
The *NewEngPage* opens in the [Web Page Hierarchy Pane](#).
7. Select **QSTest** and click **Page LinksAdd**.
8. Select **Local Page**.

9. Click **OK**.

The NewEngPage now appears under QSTest.

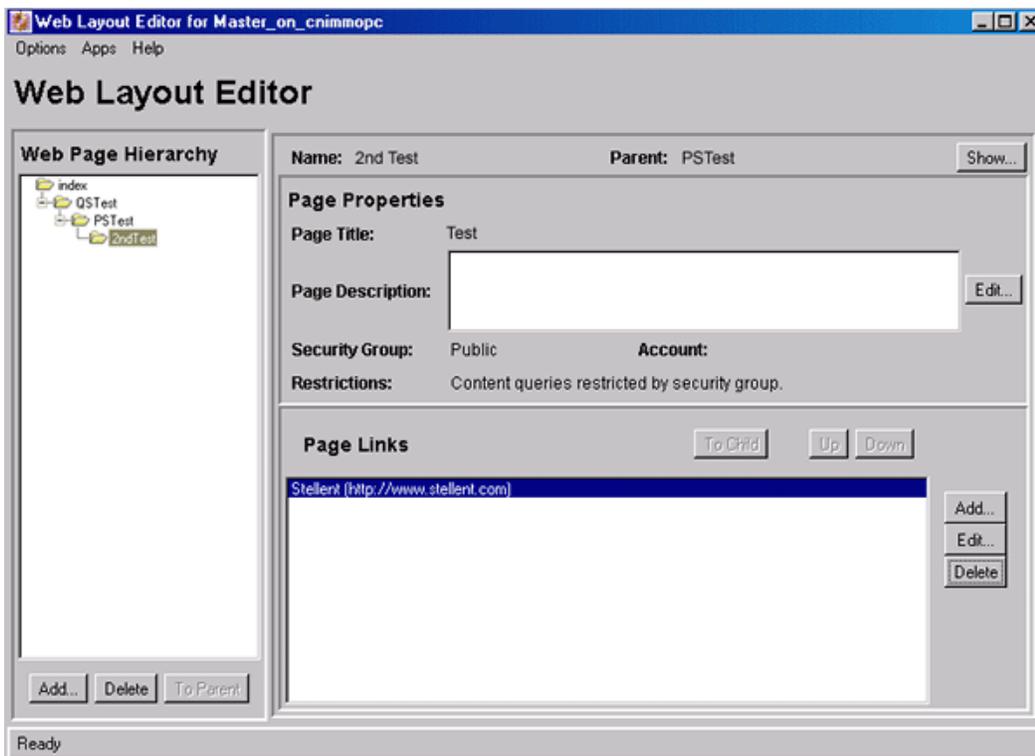
10. Select NewEngPage and click **Page LinksAdd**.

11. Select **Local PageOK**.

Note that the Page name is PCTest.

The NewEngPage has now been entered with PCTest as its child and the External URL in 2ndTest has been preserved.

The following image shows a hierarchical Web page structure created by this example procedure.



B.4 Working with Reports

This section covers these topics:

- [Section B.4.1, "About Reports"](#)
- [Section B.4.2, "Defining an Active Report"](#)
- [Section B.4.3, "Defining a Historical Report"](#)
- [Section B.4.4, "Editing a Query Expression in an Active Report"](#)

B.4.1 About Reports

You can define two types of reports with the Web Layout Editor: Active Reports and Historical Reports.

- Active Reports appear as a file-folder link and perform a database query each time they are run, generating a display of current information. You can define active reports and edit their query expressions.

- Like Active Reports, Historical Reports appear as a file-folder link, but they contain information that was queried at the time they were initially run. They do not perform a database query each time they are opened, and the report is changed only if the database is updated. The procedure for creating a Historical Report is almost the same as creating an Active Report. The only difference is the Create Historical Report screen has an extra field (Rows Per Page) to specify the number of rows each page of the report can contain.

B.4.2 Defining an Active Report

To define an active report:

1. In the Web Layout Editor, add a new Web page, and select **Active Report** as the Page Type.
2. In the Active Report Specification pane of the Web Layout Editor, click **Edit Report Query**.
3. Define the query by entering information on the [Edit Active Report Query Screen](#).
4. Click **OK**.

B.4.3 Defining a Historical Report

To prepare an Archive Historical Report:

1. In the WebLayout Editor, add a new Web page and select **Historical Report** as the Page Type.
2. In the Historical Report Specification pane of the Web Layout Editor, click **Create Report Data**.
3. When you create the report data in the [Create Historical Report Screen](#), specify **Archive History** for the data source.
4. Write a query for the report that returns the data you want to retrieve. For example, specify the Content ID.
5. When done specifying information for the report, click **OK**.

B.4.4 Editing a Query Expression in an Active Report

To edit the query expression in an active report:

1. In the [Web Page Hierarchy Pane](#), select the report you want to edit.
2. In the Active Report Specification pane, click **Edit Report Query**.
3. In the Query Expression window on the [Edit Active Report Query Screen](#), select the query line to edit.
4. Make changes to the query as necessary, and click **Update**.

Caution: If you clear the Custom Query Expression check box, the expression reverts to its original definition; all modifications are lost.

5. Click **OK**. If a query is not specified, all values are returned.

B.5 Writing Queries

This section covers these topics:

- [Creating a Query Link](#)
- [Editing the Query Expression in a Query Link](#)
- [Adding a Query Results Page](#)
- [Editing a Query Results Page](#)
- [Deleting a Query Results Page](#)

You can write custom query expressions when you define query links. The method you use to write custom queries varies depending on the kind of query you write.

To write directory custom queries, use Idoc Script, a proprietary scripting language. To write report queries, you can use SQL script and Idoc Script. Idoc Script is described in detail in the *Oracle WebCenter Content Idoc Script Reference Guide*. Basic SQL script is briefly described below.

Note: Your SQL syntax is dependent on your database. Different databases expect different syntax for items like wildcards, and so forth. See your database documentation for specific syntax information.

SQL script involves operators, which are words that show logical relationships between the words in your query. The following table contains some basic operators and their use.

Operator	Use
AND	Returns files that contain the specified words.
OR	Returns files that contain at least one specified word.
=	Equal
<> or !	Not equal
<	Less than
>	Greater than
<+	Less than or equal to
>+	Greater than or equal to
IN	Finds a position in a table.
BETWEEN	Finds a value in a range.
NOT	Excludes the files that contain the specified condition.

The following are examples of SQL script:

- Finds all files that have an internal revision ID less than 50000:

```
dID < '50000'
```
- Finds all files that have a Content ID between 10000 and 50000:

```
dDocName BETWEEN '10000' AND '50000'
```

B.5.1 Creating a Query Link

To create a query link:

1. In the [Web Page Hierarchy Pane](#), select the page where you want to locate the new query link.
2. In the Page Links pane, click **Add**.
The [Add Page Link Screen](#) opens.
3. Select **Query**, and click **OK**.
The [Query Link Definition Screen](#) opens.
4. Enter information into the screen.
5. When done, click **OK**.

When adding Idoc Script variables and HTML tags to the Text 1 and Text 2 fields, keep in mind that any resulting HTML tags can affect the display of the search results page. See the *Oracle WebCenter Content Idoc Script Reference Guide* for more information.

B.5.2 Editing the Query Expression in a Query Link

To edit the query expression in a query link:

1. In the [Page Links Pane](#) of the Web Layout Editor, select the query you want to edit.
2. Click **Edit**.
The [Query Link Definition Screen](#) opens.
3. In the Query Expression area, select the query line to edit.
4. Make changes to the metadata, Operator, metadata Value fields as necessary, then click **Update**.
5. Click **OK**.

Caution: If you clear the Custom Query Expression check box, the expression reverts to its original definition; all modifications are lost.

B.5.3 Adding a Query Results Page

Follow these instructions to add a query results page. This task is available for administrators, not for subadministrators with WebLayout rights:

1. From the Web Layout Editor menu, select **Options**, then select **Query Results Pages**.
The Query Result Pages screen opens.
2. Click **Add** to display the Add Result Page.
3. Enter information for the new page. Observe the field descriptions for [Add/Edit Query Results Page](#).
4. Click **OK**.

B.5.4 Editing a Query Results Page

Follow these instructions to edit a query results page. This task is available for administrators, not for subadministrators with WebLayout rights:

1. From the Web Layout Editor menu, select **Options**, then **Query Results Pages**, then select the name of the page.
2. Click **Edit**.
The [Add/Edit Query Results Page](#) opens.
3. Make the necessary changes, and click **OK**.

B.5.5 Deleting a Query Results Page

Follow these instructions to delete a query results page. This task is available for administrators, not for subadministrators with WebLayout rights:

1. From the Web Layout Editor menu, select **Options**, then **Query Results Pages**, then select the name of the page.
2. Click **Delete**.
3. When prompted, click **OK** to verify the deletion.

Symbols

\$\$AND\$\$, 9-11
\$\$AND_NOT\$\$, 9-11
\$\$NEAR\$\$, 9-11
\$\$OR\$\$, 9-11

A

Abstract search rules, 9-10
access control of WebDAV, 6-29
accessibility, xix
Account field, 2-4
Activation Condition - Clause tab
 content profiles, A-69
Activation Condition - Conditions tab
 content profiles, A-66
Activation Condition - Custom tab
 content profiles, A-70
Activation Condition - General tab
 content profiles, A-68
activation conditions
 in content profiles, 3-13
 modifying in content profiles, 3-27
Active Reports
 defining, B-7
 editing query expression, B-7
 overview, B-6
Activity metrics
 about, 8-18, A-136
 creating custom metadata fields, 8-19
 editing settings, 8-22
 enabling, 8-19
 linking to custom metadata fields, 8-21
 post-reduction processing, 8-7
Add Alias to Step screen, A-80, A-88, A-103
Add Alias to Workflow screen, A-86
Add Content to Workflow screen
 Existing Content, A-85
 New Content, A-85
Add Content Type screen, A-9
Add Custom Info Field screen, A-17
Add Custom Info screen, A-16
Add File Extensions screen, A-12
Add Jump screen, A-110
 Message tab, A-112
 Side Effects tab, A-111
Add New Content Item screen, A-31
Add New File Formats screen, A-12
Add New Step screen, A-79, A-87, A-103
 Events tab, A-93
Add New Subscription Type screen, A-39
Add New Workflow screen, A-84
Add Page Link screen, A-158
Add Profile "name" screen, A-59
Add Profile screen, A-59
Add Rule "name" screen, A-64
Add Rule "name" screen - Fields tab, A-65
Add Rule Field "name" screen, A-72
Add Rule Field screen, A-71
Add Rule screen, A-61
Add screen, A-42
Add Script screen
 Custom tab, A-109
 Jumps tab, A-107
 Test tab, A-109
Add Template screen, A-102
Add Token screen, A-92
Add Token to Step screen, A-81, A-89, A-105
Add Token User screen, A-92
Add User to Step screen, A-80, A-88, A-104
Add Web Page screen, A-159
AddCCToArchiveCheckin (optional
 component), 9-4
AddCCToNewCheckin (optional component), 9-5
administrators, 1-3
aliases
 definition, 4-3
application
 API, 8-2
 fields, 2-3
 running as applets, 1-4
 running in standalone mode, 1-4
architecture of WebDAV, 6-26
Archive Historical Report, B-7
Archive tables
 deleting rows, 8-14
 description, 8-14
 reduction data file, 8-14
archiving folders, 6-17, 6-23
 exporting folder hierarchy, 6-23
 importing folder hierarchy, 6-24

- ASCII characters in WebDAV properties, 6-27
- associating file types with conversion
 - programs, 2-10
- Audit trails, 8-25
- Author field, 2-4
- AuthorDelete variable, 6-8
- Auto-Contribution step, 4-2
- Automatic data reduction
 - setting, 8-10
- automatic replication of workflow items, 4-46

B

- Basic subscriptions, 2-19
- Basic workflows
 - changing, 4-21
 - process, 4-16
 - set-up tips, 4-17
 - status, 4-6
 - usage, 4-7
 - user interface, A-82
- Batch Categorizer, A-153
- Batch mode, 9-1
- batch mode
 - overview, 9-3
 - process, 9-3
- browsers, A-2
- browsing and system performance, 6-18
- browsing performance, 6-20
- building
 - web sites, B-1

C

- Case-sensitivity
 - metadata in Oracle and DB2 databases, 8-25
 - Snapshot tab fields
 - Snapshot tab, 8-22
- Categorize button, 9-1
- Check In/Search Link - Add Condition screen, A-61
- Check In/Search Link- Conditions tab, A-61
- Check Out Item screen, A-33
- checking in
 - new content item, 2-13
- checkout
 - undo, 2-16
 - with Repository Manager, 2-16
- choosing workflow type, 4-7
- clients for WebDAV, 6-25
- Clusters
 - tracking limitations, 8-15
- Collection tab
 - about, A-135
 - terminology definition, 8-3
- CollectionReleasedOnly, 6-16
- combined output table, 8-11
- Comments field, 2-5
- companion files
 - contents, 4-4
 - location, 4-4

- components
 - Content Tracker, 8-1
 - ExtranetLook, 6-31
- conditional statements
 - setting up for jump, 4-30
 - setting up for script template, 4-35
- configuration
 - Content Categorizer, 9-5
 - Folders, 6-20
 - Information Field Inherit Configuration, A-127
 - local folders, 6-22, A-126
 - maximum number of folders and files, 6-20
 - metadata propagation, 6-21
 - System Default Information Field
 - Configuration, A-125
 - system default metadata, 6-21
 - System Folder Configuration page, A-124
 - system folders, 6-20
 - Virtual Folder Administration Configuration
 - page, A-123
- Configuration Manager
 - content types, 2-2
 - Content Types tab, A-9
 - editing metadata fields, 2-5
 - File Formats tab, A-10
 - Profiles tab, A-58
 - Rules tab, A-63
 - setting metadata, 2-2
- configuration parameters
 - CollectionReleasedOnly, 6-16
 - formatting metadata fields in profiles, 3-30
 - MaxQueryRows, 9-3
- Configuration Tab, A-142
- Configure Thumbnail Options screen, A-13
- connection issues to WebDAV virtual folder, 6-30
- consumers, 1-3
- Content Categorizer
 - overview, 9-1
 - setup, 9-5
- Content Dashboard
 - terminology definition, 8-3
- Content ID field, 2-4
- content item
 - adding, 2-13
 - deleting, 2-16
 - deleting all revisions, 2-16
 - metadata, 8-14
 - revisions, 6-16
 - revisions in folders, 6-6
 - security, 6-14
 - unsubscribing, A-38
 - viewing, A-3
 - WebDAV and workflows, 6-32
- Content Item Subscribed screen, A-41
- Content Item View screen, A-3, A-100, A-113
- content profiles
 - Activation Condition - Clause tab, A-69
 - Activation Condition - Conditions tab, A-66
 - Activation Condition - Custom tab, A-70
 - Activation Condition - General tab, A-68

- activation conditions, 3-13, 3-27
 - Add Profile "name" screen, A-59
 - Add Profile screen, A-59
 - Add Rule "name" screen, A-64
 - Add Rule "name" screen - Fields tab, A-65
 - Add Rule Field "name" screen, A-72
 - Add Rule Field screen, A-71
 - Add Rule screen, A-61
 - adding header to metadata field group, 3-26
 - Check In/Search Link - Add Condition screen, A-61
 - Check In/Search Link - Conditions tab, A-61
 - Content Item View screen, A-3
 - creating, 3-32
 - Edit Default Value - Conditions tab, A-61, A-73, A-74
 - Edit Default Value - Select Field screen, A-74
 - Edit Derived Value - Conditions tab, A-74
 - Edit Group Header screen, A-65
 - Edit Profile "name" screen, A-59
 - Edit Restricted List screen, A-74
 - Edit Rule "name" screen, A-64
 - Edit Rule "name" screen - Fields tab, A-65
 - Edit Rule Field "name" screen, A-72
 - Edit Trigger Field screen, A-59
 - formatting configuration variables, 3-30
 - grouping metadata fields, 3-17, 3-26
 - metadata field attributes, 3-29, 3-30
 - metadata fields in rules, 3-13
 - metadata reordering, 3-20
 - modifying, 3-32
 - overview, 3-11
 - Preview Profile screen, A-61
 - Preview Results screen, A-62
 - previewing, 3-33
 - Profile Links screen, A-60
 - Profiles tab, A-58
 - rules, 3-12, 3-24
 - Rules tab, A-63
 - trigger field
 - disabling, 3-32
 - overview, 3-11
 - selecting, 3-31
 - troubleshooting, 3-34
 - User View screen, A-4
 - Content Tracker
 - access permissions, 8-17
 - component, 8-1
 - custom reports, 8-36
 - data collection, 8-4
 - data output overview, 8-13
 - data processing overview, 8-4
 - data reduction overview, 8-6
 - drill-down reports, 8-35
 - event logs, 8-11
 - logging service, 8-5
 - query reports, 8-27
 - Report Generator, 8-34, A-139
 - sctAccessLog table, 8-11
 - troubleshooting, 8-37
 - content types, 2-1
 - contribution folders
 - see also 'folders'
 - administration, 6-20
 - archiving, 6-17, 6-23
 - configuration, 6-20
 - connection issues, 6-30
 - content item revisions, 6-16
 - criteria workflow, 4-47
 - for Site Studio, 6-32
 - metadata inheritance, 6-15
 - overview, 6-13
 - performance, 6-18
 - security, 6-14
 - structure, 6-13
 - system folders, 6-20
 - trash bin, 6-15
 - contribution step, 4-2
 - contributors, 1-3
 - conversion
 - associating file types with programs, 2-10
 - custom, 2-11
 - native file, 2-9
 - specifying native file, A-9
 - status, A-6
 - cookies, WebDAV, 6-29
 - count, 9-7
 - Create Historical Report screen, A-163
 - criteria subscriptions, 2-19
 - Criteria workflows
 - user interface, A-76
 - criteria workflows
 - changing, 4-15
 - disabling, 4-15
 - process, 4-10
 - setting up, 4-12
 - status, 4-6
 - usage, 4-7
 - custom conversion, 2-11
 - custom fields, 2-2
 - custom reports, 8-36
- ## D
-
- Data collection
 - Content Tracker logging service, 8-5
 - log, 8-11
 - operational summary, 8-2
 - overview, 8-4
 - SctAccessLog, 8-11
 - SctIgnoreFileTypes, 8-11
 - service handler filter, 8-5
 - terminology definition, 8-3
 - web server filter, 8-5
 - Data Engine Control Center
 - about, A-134
 - Collection tab, A-135
 - Schedule tab, A-136
 - Services tab, A-137
 - Snapshot tab, 8-18, A-136

- terminology definition, 8-3
- Data output
 - content item metadata, 8-14
 - reduction log files, 8-15
 - SctAccounts table, 8-14
 - SctGroups table, 8-14
 - SctUserAccounts table, 8-14
 - SctUserGroups table, 8-15
 - SctUserInfo table, 8-15
 - user metadata, 8-14
- Data processing
 - data reduction process, 8-6
 - overview, 8-4
 - post-reduction processing, 8-7
 - with activity metrics, 8-7
 - without activity metrics, 8-6
- Data reduction
 - access counts and random order of data
 - reduction, 8-22
 - automatic, 8-10
 - contents of SctAccessLog, 8-11
 - log, 8-11
 - logging, 8-11
 - manual, 8-9
 - operational summary, 8-3
 - overview, 8-6
 - process flow overview - with activity metrics, 8-7
 - process flow overview - without activity metrics, 8-6
 - reduced data files, 8-11
 - set file types with SctIgnoreFileTypes, 8-11
 - terminology definition, 8-3
- Database tables
 - archive, 8-14
 - naming structure, 8-14
 - primary, 8-14
 - reduction data file, 8-14
- DB2 database
 - metadata case-sensitivity, 8-25
- DCL, 3-1
- default metadata
 - defining system, 6-21
- Define Filter screen, A-41
- defining
 - Active Report for Web Layout Editor, B-7
 - business processes, 4-7
- Delete All Revisions screen, A-36
- Delete Revision screen, A-35
- Dependent Choice List, 3-1
- designing workflows, 4-8
- digital signatures
 - acquiring, 4-38
 - setup, 4-38
- directory queries, B-8
- DisablePersonalFolderFormat variable, 6-9
- DONE status, 4-6
- double-byte characters in file names, 6-31
- Drill-down reports, 8-35
- dynamic option list, 3-8
- Dynamic Watermarking, 5-1

E

- Edit Active Report Query screen, A-162, B-7
- Edit Additional Exit Condition screen, A-81, A-90, A-105
- Edit Content Type screen, A-9
- Edit Criteria Workflow screen, A-78
- Edit Custom Info Field screen, A-17
- Edit Default Value - Conditions tab, A-61, A-73
 - content profiles, A-74
- Edit Default Value - Select Field screen, A-74
- Edit Derived Value - Conditions tab, A-74
- Edit External URL screen, A-160
- Edit File Extension screen, A-12
- Edit File Format screen, A-12
- Edit Folio page
 - Element Info tray, A-130
 - Source Items tray, A-132
- Edit Group Header screen, A-65
- Edit Jump screen, A-110
 - Message tab, A-112
 - Side Effects tab, A-111
- Edit Local Page Link screen, A-160
- Edit Page Properties screen, A-161
- Edit Profile "name" screen, A-59
- Edit Restricted List screen, A-74
- Edit Rule "name" screen, A-64
- Edit Rule "name" screen - Fields tab, A-65
- Edit Rule Field "name" screen, A-72
- Edit Script screen
 - Custom tab, A-109
 - Jumps tab, A-107
 - Test tab, A-109
- EDIT status, 4-6
- Edit status, troubleshooting, 4-49
- Edit Step screen, A-79, A-87, A-103
 - Events tab, A-93
- Edit Subscription Type screen, A-39
- Edit Template screen, A-102
- Edit Token screen, A-92
- Edit Trigger Field screen
 - content profiles, A-59
- Edit Type Script screen, A-94
- Edit Workflow screen, A-84
- Element Info Tray, A-130
- entry count variable, 4-28
- entry script, 4-5
- event scripts
 - update, 4-29
- events, 4-4, 4-26
- examples
 - Abstract search rules, 9-10
 - jumps, 4-29
 - Option List search rule, 9-11
 - Pattern Matching search rules, 9-7
 - workflow token, 4-24
- executing Repository Manager functions, 2-13
- exit conditions, 4-3
- exit script, 4-5
- Expiration Date field, 2-5
- exporting archives, 6-23

- External reporting tools
 - generating custom reports, 8-28
- external URL
 - creating link, B-5
- extracting URL links
 - process overview, 2-23
- extractLinks
 - Link Manager filter, 2-27
- ExtranetLook component, 6-31

F

- Field map ResultSet, 8-3
- Fields screen, A-39
- fields, editing, 2-5
- file conversion, native, 2-9
- file formats, naming, 2-10
- file system
 - mapping local folders to, 6-22
- file types, associating with conversion programs, 2-10
- files
 - double-byte characters in file name, 6-31
 - maximum number, 6-20
 - number sign in file name, 6-31
 - zero bytes, 6-30
- filters
 - extractLinks, 2-27
 - for Link Manager, 2-27
 - linkParseService, 2-27
 - sortAndDecodeLinks, 2-28
- Firefox, supported versions, A-2
- FIRST_PARAGRAPH, 9-10
- FIRST_SENTENCE, 9-10
- FldDefaultFilesLoadCount variable, 6-9
- FldDefaultFoldersLoadCount variable, 6-9
- FldEnableInProgressIndicator variable, 6-9
- FldMigrateDefaultSecurityGroup variable, 6-10
- FldMigrateRootBaseName variable, 6-10
- FldPersonalFolderFormat variable, 6-9
- FldShowAutoPropagateOption variable, 6-9
- Flexiondoc, 9-1
 - interactive mode requirements, 9-3
- FolderMigrateExcludeList variable, 6-10
- folders
 - see also 'contribution folders'
 - configuration variables, 6-8
 - metadata, 6-6
 - migration variables, 6-9
 - overview, 6-2
 - personal, 6-6
 - propagation, 6-6, 6-7
 - query folders, 6-4
 - retention, 6-5
 - retention rules, 6-10
 - security, 6-6
 - shortcuts, 6-3
 - versioning, 6-6
 - WebDAV variables, 6-10
- FoldersDefaultDocType variable, 6-9

- FoldersIndexParentFolderValues variable, 6-9
- folio
 - definition, 7-1
 - structure tray, A-130

G

- GENWWW status, 4-6
- GenWWW status
 - workflow items stuck in --, 4-49
- Google Chrome, supported versions, A-2

H

- hierarchical folders, see 'contribution folders'
- Historical Reports, B-6
- HTTP methods used by WebDAV, 6-27

I

- Idoc variables, modifying, 4-41
- importing archives, 6-24
- improving system performance, 6-18
- index
 - rebuilding, 2-5
 - status, A-6
- Information Field Inherit Configuration page, A-127
- information fields, see 'metadata'
- inheritance of metadata, 6-15, 6-19
- Internet Explorer
 - considerations, A-2
 - supported versions, A-2

J

- jump
 - changing, 4-31
 - completing, 4-30
 - creating, 4-29
 - errors, 4-33
 - overview, 4-26
 - purpose, 4-3
 - scripts, testing, 4-31
 - setting up conditional statement, 4-30
 - setting up side effects, 4-30
 - step variables, 4-28

K

- key
 - Pattern Matching search rules, 9-7
- keys, workflow, 4-4

L

- language support, 6-27
- Last Access, 8-19
- last entry variable, 4-28
- link evaluation rules
 - default examples, 2-26
 - overview, 2-25

- table columns, 2-25
- link extraction
 - process, 2-23
- link management
 - in Site Studio, 2-28
- Link Manager
 - filters, 2-27
 - link extraction process, 2-23
 - overview, 2-22
 - refreshing, 2-29
 - search options, 2-22
- link status
 - valid or invalid, 2-24
- LinkManagerPatterns
 - lkpAccept column, 2-26
 - lkpAction column, 2-26
 - lkpContinue column, 2-26
 - lkpDescription column, 2-25
 - lkpEnabled column, 2-26
 - lkpLinkType column, 2-26
 - lkpName column, 2-25
 - lkpOrder column, 2-26
 - lkpParameters column, 2-26
 - lkpType column, 2-26
 - table columns, 2-25
- linkParseService
 - Link Manager filter, 2-27
- local folders
 - configuration, 6-22, A-126
 - mapping, 6-22
 - overview, 6-16
 - rebuilding, 6-23
 - removing, 6-23
- Local Folders page, A-126
- local page
 - creating link, B-5
- local pages, B-4
- login cookie, 6-29
- Long Access Count, 8-19

M

- Managed Links Administration page
 - overview, A-44
- ManagedLinks table
 - overview, 2-27
 - refreshing, 2-29
- Manual data reduction
 - running, 8-9
- mapping local folders, 6-22
- maximum number of folders and files, 6-20
- MaxQueryRows, 9-3
- metadata
 - case-sensitivity, 8-25
 - content item metadata, 8-14
 - creating custom metadata fields for activity
 - metrics, 8-19
 - custom fields, 2-3
 - defining field properties, 9-5
 - defining system default, 6-21

- editing, 2-5
- folder, 6-6
- inheritance, 6-6, 6-15, 6-19
- propagation, 6-15, 6-21
- reordering on content server pages, 3-20
- search rules, 9-5
- standard fields, 2-3
- updating, 2-14
- metadata fields
 - editing, 2-5
 - predefined, 2-3
- MIME types
 - identifying, 2-10

N

- naming
 - file formats, 2-10
- native file conversion, 2-9, A-9
- new content
 - search rules for metadata values, 9-5
- New Criteria Workflow screen, A-78
- non-ASCII characters in WebDAV properties, 6-27
- non-reviewer approval, 4-45
- Non-secure mode reports
 - custom reports, 8-31
 - example of, 8-30
 - pre-defined reports, 8-30
 - report queries for, 8-29
 - security mode selection process, 8-31
- Non-secure reports
 - customizing the report query file, 8-33
- number sign, in virtual folder name or file name, 6-31

O

- operating modes
 - batch mode, 9-3
 - batch mode process, 9-3
 - Flexiondoc requirements in interactive mode, 9-3
 - interactive mode, 9-3
 - interactive mode process, 9-4
 - interactive mode requirements, 9-2
 - overview, 9-3
 - SearchML requirements in interactive mode, 9-3
- optimizing system performance, 6-18
- Option List screen, A-20
- Option List search rule, 9-11
- option lists, 2-7
- Optional Component
 - AddCCToArchiveCheckin, 9-4
 - AddCCToNewCheckin, 9-5
- Oracle database
 - metadata case-sensitivity, 8-25

P

- pages
 - Information Field Inherit Configuration, A-127
 - Local Folders, A-126

- System Default Information Field
 - Configuration, A-125
- System Folder Configuration, A-124
- Virtual Folder Administration
 - Configuration, A-123
- parallel workflows, 4-39
- parent/child relationship, 3-1
- passthru, 2-11
- Pattern Matching search rules, 9-7
- PDF Optimization, 5-1
- PDF Watermark
 - metadata fields, 5-1
- PENDING status, 4-6
- performance of Folders, improving, 6-18
- planning
 - web sites, B-1
- predefined metadata fields, 2-3
- Preview Profile screen, A-61
- Preview Results screen, A-62
- Primary tables
 - description, 8-14
 - reduction data file, 8-14
- process
 - Basic workflow, 4-16
 - Criteria workflow, 4-10
 - workflow step, 4-5, 4-33
- process of WebDAV requests, 6-26
- Profile Links screen, A-60
- profile rules
 - see 'content profile'
- Profiles tab, A-58
- propagation of metadata, 6-15, 6-21
- protocol used by WebDAV, 6-25
- publishing cycle interval, 3-7

Q

- queries
 - writing directory, B-8
 - writing report, B-8
- query expression
 - editing Active Reports, B-7
 - editing Query link, B-9
- query folders, 6-4, A-125
- Query link
 - creating, B-9
 - editing query expression, B-9
- Query Link Definition screen, A-164
- Query reports
 - drill-down reports, 8-35
 - generating, 8-27, 8-34
 - overview, 8-26
 - pre-defined, A-139
- query results page
 - adding, B-9
 - deleting, B-10
 - editing, B-9

R

- rebuilding
 - search index, 2-5
- rebuilding local folders, 6-23
- recursive table
 - for multiple trees - creating, 3-9
- Reduction data file
 - storage, 8-14
- Reduction log files
 - overview, 8-15
- Reduction tab
 - terminology definition, 8-3
- refresh activity
 - recompute links, 2-29
 - sortAndDecodeLinks filter, 2-28
 - updating counts, 2-30
 - using Managed Links Administration page, A-44
- Reject Revision screen, A-37
- Release Date field, 2-5
- RELEASED status, 4-6
- removing local folders, 6-23
- RepMan rights, 2-12
- Report generation
 - about, 8-24
 - operational summary, 8-3
 - See also Content Tracker Report Generator and External reporting tools
- report queries
 - writing, B-8
- Report query file
 - customizing for security mode, 8-33
- reports
 - Archive Historical, B-7
 - defined with Web Layout Editor, B-6
- Repository Manager, 2-12
 - adding new content items, 2-13
 - deleting a revision, 2-16
 - functions, 2-13
 - Subscriptions tab, 2-20
 - undoing a checkout, 2-16
 - unsubscribing, A-38
 - updating metadata, 2-14
- retention
 - query folders, 6-5
- retention scheduling, 6-11
- return step, 4-28
- reverse proxy server
 - web beacon feature, 8-23
- REVIEW status, 4-6
- Review status
 - workflow items stuck in --, 4-50
- Review/Edit Revision step, 4-2
- Reviewer step, 4-2
- reviewers not in workflow, 4-45
- Review/New Revision step, 4-2
- Revision field, 2-5
- revision status, A-6
- revision, deleting, 2-16
- rule types
 - Abstract, 9-10

- Option List, 9-11
- Pattern Matching, 9-7
- rules
 - adding metadata fields, 3-24
 - content profiles, 3-13
 - link patterns, 2-25
 - table columns, 2-25
- Rules tab, A-63
- run-time configuration parameter
 - setting XML conversion method, 9-5

S

- Safari, supported versions, A-2
- sccXMLConversion
 - configuration setting values, 9-1
- Schedule tab
 - about, A-136
 - terminology definition, 8-3
- schema
 - adding metadata fields, 3-7
 - and DCL, 3-1
 - changing publishing cycle, 3-7
 - creating, 3-5
 - creating relationships, 3-6
 - creating schema view, 3-6
 - creating structure, 3-5
 - directory structure, 3-4
 - dynamic option lists, 3-8
 - enabling the schema, 3-7
 - example, 3-5
 - hierarchical structure, 3-1
 - interface screens, A-45
 - mapping feature, 3-1
 - overview, 3-1
 - parent/child relationship, 3-1
 - publishing cycles, 3-5
 - recursive table for multiple trees, 3-9
 - relationships, 3-4
 - selecting tables, 3-6
 - tables, 3-2
 - views, 3-3
- script templates
 - changing, 4-35
 - creating, 4-34
 - setting up conditional statement, 4-35
 - setting up side effects, 4-34
 - testing, 4-35
- scripts
 - testing workflow jump, 4-31
 - update event, 4-29
- SctAccessLog
 - contents of, 8-11
- sctAccessLog table
 - Content Tracker event logs, 8-11
- SctAccounts table
 - field names and definitions, 8-14
 - metadata contents, 8-14
- SctGroups table
 - field names and definitions, 8-14
 - metadata contents, 8-14
- sctLog files
 - raw event logs, 8-11
- SctUserAccounts table
 - metadata contents, 8-14
- SctUserGroups table
 - field names and definitions, 8-15
 - metadata contents, 8-15
- SctUserInfo table
 - field names and definitions, 8-15
 - metadata contents, 8-15
- search
 - folders and files, 6-4
- search index
 - rebuilding, 2-5
- search options
 - in Link Manager, 2-22
- Search relevance fields
 - See Activity metrics, 8-19
- search rule override
 - applied to fields during content check in, 9-2
- search rules
 - Abstract, 9-10
 - defining, 9-16
 - guidelines, 9-6
 - metadata values, 9-5
 - Option List, 9-11
 - overview of types, 9-2
 - types, 9-7
- searching in workflow step, 4-48
- SearchML
 - interactive mode requirements, 9-3
- Secure mode reports
 - custom reports, 8-31
 - customizing the report query file, 8-33
 - example of, 8-30
 - pre-defined reports, 8-30
 - report queries for, 8-29
 - security mode selection process, 8-31
- security
 - content items, 6-14
 - folders, 6-14
 - workflow issues, 4-8
- Security checks
 - custom reports, 8-31
 - examples of security modes, 8-29
 - manually changing the preference variable value, 8-31
 - pre-defined reports, 8-30
 - report queries and security modes, 8-29
 - security mode selection process, 8-31
- Security Group field, 2-4
- security of WebDAV, 6-29
 - access control, 6-29
 - login cookie, 6-29
 - session timeout, 6-29
- Select Alias screen, A-43
- Select Root Node for Tree
 - metadata fields, A-22
- Select Target Step screen, A-97

- Select User screen, A-42
- Service definitions, 8-3
- Service entry, 8-3
- Service handler filter, 8-5
- Services tab
 - about, A-137
 - terminology definition, 8-3
- session timeout, 6-29
- Short Access Count, 8-19
- Show Columns screen, A-7
- ShowFolderMigrationMenu variable, 6-10
- site structure, B-2
- Site Studio
 - completely managed links, 2-28
 - link management, 2-28
 - provisionally managed links, 2-29
 - web activity reporting reports, 8-26
 - web beacon feature, 8-23
 - and WebDAV, 6-15, 6-21, 6-32
- Snapshot tab, 8-22
 - about, 8-18, A-136
 - editing snapshot configuration, 8-22
 - enabling snapshot function and activity metrics, 8-19
 - error checking, 8-22
 - linking activity metrics to custom metadata fields, 8-21
 - terminology definition, 8-3
- sortAndDecodeLinks filter, 2-28
- Source Items Tray, A-132
- standalone mode, running applications, 1-4
- Start Workflow screen, A-91
- static inheritance, preventing --, 6-19
- Static URLs
 - false positives, 8-17
 - wrong dID reported, 8-16
- static watermarking, 5-1
- status, workflow, 4-6
- step name variable, 4-28
- steps
 - auto-contribution, 4-2
 - contribution, 4-2
 - review, 4-2
 - review/edit revision, 4-2
 - review/new revision, 4-2
- Stop Reduction button, A-135
- structure of Folders, 6-13
- subadministrators, 1-3
- subscriptions
 - adding, 2-20
 - adding users, 2-21
 - deleting, 2-21
 - editing, 2-21
- sub-workflows, 4-15
- suppressing notification, 4-48
- syntax, workflow token, 4-24
- System Default Information Field Configuration page, A-125
- system default metadata, 6-21
- System Folder Configuration page, A-124

- system folders, 6-20
- system performance, 6-18

T

- tables used in schema, 3-2
- TAG_ALLTEXT, 9-7
- TAG_TEXT, 9-7
- target step, 4-28
- templates
 - changing script, 4-35
 - creating script, 4-34
 - testing workflow script, 4-35
 - workflow, 4-33
- testing
 - workflow jump script, 4-31
 - workflow script template, 4-35
- Text Search, 9-7
- TEXT_ALLFULL, 9-7
- TEXT_ALLNEXT, 9-7
- TEXT_ALLREMAINDER, 9-7
- TEXT_FULL, 9-7
- TEXT_NEXT, 9-7
- TEXT_REMAINDER, 9-7
- thumbnail
 - configuration, A-13
 - overview, 2-11
- title allocation
 - WebDAV, 6-28
- Title field, 2-4
- token
 - screens, A-91
- tokens
 - creating, 4-24
 - definition, 4-3
 - syntax, 4-24
- Top content items, 8-3
- Tracking limitations
 - in single-box clusters, 8-15
- Trash Bin
 - disabling, 6-21
 - function, 6-15
- tray
 - Element Info, A-130
 - folio structure, A-130
 - Source Items, A-132
- trigger field
 - content profile, 3-11
 - disabling, 3-32
 - selecting, 3-31
- troubleshooting
 - connection issues to WebDAV virtual folder, 6-30
 - content items "stuck" in workflow, 6-32
 - deleting content from Site Studio contribution folders, 6-32
 - double-byte characters in file name, 6-31
 - ExtranetLook component, 6-31
 - number sign in virtual folder name or file name, 6-31
 - WebDAV, 6-29

- WebDAV drag and drop does not work with
 - Windows 2000, 6-33
 - zero-byte files, 6-30
- Troubleshooting Content Tracker
 - mechanisms, 8-37
 - PLUGIN_DEBUG support, 8-38
 - setting PLUGIN_DEBUG, 8-38
- Type field, 2-4

U

- Undo Check Out screen, A-34
- undoing a checkout, 2-16
- UNIX
 - running standalone application on, 1-5
 - services, 1-5
- unsubscribing, A-38
- Update Content Info screen, A-32
- Update Database Design screen
 - metadata fields, A-23, A-24
- update scripts, workflow, 4-29
- URL
 - creating external link, B-5
- URL link patterns
 - default examples, 2-26
 - overview, 2-25
 - table columns, 2-25
- URL links
 - search options, 2-22
- User credentials audit tracking
 - failed logon attempts, 8-25
- user interface (Folders)
 - Information Field Inherit Configuration page, A-127
 - Local Folders page, A-126
 - System Default Information Field Configuration page, A-125
 - System Folder Configuration page, A-124
 - Virtual Folder Administration Configuration page, A-123
- user interface (WebDAV)
 - virtual folders in Windows Explorer, 6-27
- User metadata
 - See also Metadata
 - overview, 8-14
 - SctAccounts table, 8-14
 - SctGroups table, 8-14
 - SctUserAccounts table, 8-14
 - SctUserGroups table, 8-15
 - SctUserInfo table, 8-15
- User permissions audit tracking
 - failed attempts to access content items, 8-25
- User View screen
 - content profiles, A-4
- users
 - ad hoc, 4-40
 - adding to subscription, 2-21
 - types, 1-3
- Users Subscribed screen, A-40

V

- variables, see 'configuration parameters', 6-16
- vault, 2-1
- views, 3-3
- Virtual Folder Administration Configuration page, A-123

W

- web beacon
 - with reverse proxy server, 8-23
 - with Site Studio, 8-23
- web browsers, A-2
- web layout, 2-1
- Web Layout Editor
 - about, B-1
 - Active Reports, B-6
 - adding
 - query results page, B-9
 - web pages, B-4
 - creating
 - external URL link, B-5
 - local page link, B-5
 - Query link, B-9
 - web sites, B-2
 - defining
 - Active Reports, B-7
 - criteria to display files, B-2
 - site structure, B-2
 - deleting
 - query results page, B-10
 - editing
 - Active Report query expression, B-7
 - Query link query expression, B-9
 - query results page, B-9
 - web page properties, B-4
 - web page structure, B-5
 - Historical Reports, B-6
 - interface, A-154
 - main page, A-155
 - Page Hierarchy pane, A-156
 - Page Links pane, A-157
 - Page Properties pane, A-156, A-157
 - planning web sites, B-1
 - tasks, B-2
 - using the, B-4
 - Web Page Hierarchy pane, A-156
 - working with reports, B-6
 - working with web pages, B-3
 - writing
 - report queries, B-8
- web pages
 - adding in Web Layout Editor, B-4
 - editing properties, B-4
 - editing structure, B-5
 - working with, B-3
- Web server filter
 - overview, 8-5
- Web site
 - building, B-1

- defining criteria to display files, B-2
- planning, B-1
- WebDAV
 - administration, 6-28
 - architecture, 6-26
 - clients, 6-25
 - folders, 6-27
 - functions, 6-25
 - HTTP methods used, 6-27
 - multiple concurrent language support, 6-27
 - overview, 6-25
 - process, 6-26
 - protocol, 6-25, 6-27
 - requesting missed accesses, 8-17
 - security, 6-29
 - and Site Studio, 6-32
 - technology, 6-25, 6-26
 - title allocation, 6-28
 - troubleshooting, 6-29
 - troubleshooting drag and drop functionality with
 - Windows 2000, 6-33
 - workflows, 6-32
- wfAction, 4-23
- wfAdditionalExitCondition, 4-22
- wfAddUser, 4-22
- wfCurrentGet, 4-22
- wfCurrentSet, 4-22
- wfCurrentStep, 4-22
- wfDisplayCondition, 4-22
- wfExit, 4-22
- wfGet, 4-22
- wfGetStepTypeLabel, 4-22
- wfIsReleasable, 4-22
- wfJumpEntryNotifyOff, 4-23
- wfJumpMessage, 4-22
- wfJumpName, 4-23
- wfJumpReturnStep, 4-23
- wfJumpTargetStep, 4-23
- wfMailSubject, 4-23
- wfMessage, 4-23
- wfNotify, 4-23
- wfParentList, 4-23
- wfReleaseDocument, 4-23
- wfSet, 4-23
- wfStart, 4-23
- wfupdateMetaData, 4-23
- Windows
 - running standalone application on, 1-5
- Windows Explorer
 - and WebDAV security, 6-29
- workflow
 - escalation, 4-42
 - pre-design questions, 4-7
 - replication, 4-46
 - scenarios, 4-45
 - step process, 4-33
- Workflow Admin
 - Criteria tab, A-77
 - Templates tab, A-101
 - tool, 4-33
- Workflows tab, A-83
- Workflow Revisions, 2-16
- Workflow Scripts screen, A-106
- Workflow Tokens screen, 4-24, A-91
- workflows
 - actions, 4-5
 - Basic
 - changing, 4-21
 - process, 4-16
 - set-up, 4-18
 - tips, 4-17
 - user interface, A-82
 - companion file, 4-4
 - Criteria
 - based on folder, 4-47
 - changing, 4-15
 - disabling, 4-15
 - process, 4-10
 - set-up, 4-12
 - user interface, A-76
 - customizing, 4-22
 - designing, 4-8
 - e-mail templates, 4-40
 - events, 4-4, 4-26
 - items in wrong workflow, 4-51
 - items stuck in Edit status, 4-49
 - items stuck in GenWWW status, 4-49
 - items stuck in Review status, 4-50
 - jumps
 - completing, 4-30
 - creating, 4-29
 - setting up conditional statement, 4-30
 - setting up side effects, 4-30
 - testing scripts, 4-31
 - keys, 4-4
 - modifying, 4-9
 - overview, 4-1
 - process, 4-5, 4-33
 - script templates
 - changing, 4-35
 - creating, 4-34
 - overview, 4-33
 - testing, 4-35
 - security issues, 4-8
 - status, 4-6
 - step types, 4-2
 - sub-workflow type, 4-1
 - sub-workflows
 - changing, 4-15
 - disabling, 4-15
 - templates
 - changing, 4-33
 - tokens
 - creating, 4-24
 - WebDAV, 6-32
 - working with
 - Basic workflow user interface, A-82
 - Criteria workflow user interface, A-76

X

XML, 9-7

XML conversion

overview, 9-2

sccXMLConversion configuration setting, 9-1

setting conversion method, 9-5

Z

zero-byte files, 6-30