



OpenText™ Documentum™ Content Management

Records Client User Guide

Create work orders, integrate with and apply retention capabilities to the electronic record-keeping system, and manage paper assets.

EDCRM250400-UGD-EN-01

OpenText™ Documentum™ Content Management

Records Client User Guide

EDCRM250400-UGD-EN-01

Rev.: 2025-Nov-17

This documentation has been created for OpenText™ Documentum™ Content Management CE 25.4.

It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111

Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440

Fax: +1-519-888-0677

Support: <https://support.opentext.com>

For more information, visit <https://www.opentext.com>

© 2025 Open Text

Patents may cover this product, see <https://www.opentext.com/patents>.

Disclaimer

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

Table of Contents

PRE	Preface	xxi
i	Intended audience	xxii
ii	Organization	xxii
1	Overview of the Records Client	23
1.1	About Records Client	27
1.2	Usage tracking information	29
2	Records Interoperability with Content Intelligent Services (CIS)	31
2.1	About the Content Intelligent Services (CIS) integration with Retention Policy Services	31
3	Records Client common functionality	33
3.1	Work orders	33
3.1.1	Work order general overview	33
3.1.2	Work order definitions	34
3.1.3	Work order icons	36
3.1.4	About work order confirmation messages	36
3.1.5	About the OpenText Documentum Content Management (CM) Records Queue Manager	36
3.1.6	About the work order framework configuration object and each of the work order operation configuration objects	37
3.1.7	Understanding when work orders are generated	45
3.1.8	About the work order monitor job	47
3.1.9	About the operation processing order	49
3.1.10	About the application and removal of a policy	49
3.1.10.1	Applying/removing records policies to or from virtual documents and snapshots	50
3.1.11	Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report	51
3.1.11.1	Work order report overview	51
3.1.11.2	Work order breakdown report overview	56
3.1.11.3	Work order item report overview	56
3.1.11.4	Instructions to run the reports	57
3.2	Setting column preferences	77
3.3	Records auditing	78
3.3.1	Overview of auditing	78
3.3.2	Enabling auditing	80

3.3.3	Configuring the audit policy (to prevent purging audits until archived)	82
3.3.4	Verifying auditing of an event	84
3.3.4.1	Verifying the auditing of an event using the properties screen	84
3.3.4.2	Verifying the auditing of an event through the search audit of Documentum Administrator	84
3.3.5	Viewing and removing an audit	85
3.3.6	Archiving audits (declaring as formal record)	85
3.4	Records reporting	86
3.5	Records Dashboard	88
3.5.1	Dashboard overview	88
3.5.2	About Home Page	88
3.5.3	About Retention Policy Usages	89
3.5.4	About Retention Markup Usages	89
3.5.5	Physical Items Overdue for Return	90
3.5.6	Compliance Check of objects	90
4	Retention Policy Services	93
4.1	Introduction	93
4.1.1	Determining which Retention Policy Services version you are accessing	93
4.1.2	Administration components	93
4.1.3	About privileged clients and accessing repositories	94
4.1.4	Setting up Retention Policy Services	96
4.1.4.1	Configuration options	96
4.1.4.2	User preferences and column preferences	96
4.2	Retention Policy Services administration	97
4.2.1	About Retention Policy Services functionality	97
4.2.2	Retention Policy Services	98
4.2.2.1	Overview of Retention Policy Services	98
4.2.2.1.1	Retention policies and lifecycles	98
4.2.2.1.2	About retainers, lifecycle actions, and disposition actions	99
4.2.2.1.3	About retainers and retention dates	99
4.2.2.1.4	Retention policy strategy	105
4.2.2.1.5	Retention markups	106
4.2.2.1.6	Retention Policy Services navigation	107
4.2.2.1.7	Virtual documents	107
4.2.2.2	Retention Policy Services roles and functional access	108
4.2.2.3	Retention Policy Services configuration	119
4.2.2.3.1	Records check configuration option settings	119
4.2.2.3.2	System configuration options settings	121
4.2.2.3.3	Disposition configuration option settings	124
4.2.2.3.4	Qualification job filters configuration option settings	127
4.2.2.3.5	Promotion job filters configuration option settings	128

4.2.2.3.6	Disposition job filters configuration option settings	129
4.2.2.4	Work order notifications	130
4.2.2.5	Virtual document retention rules	133
4.2.2.6	Linking a record	134
4.2.2.7	Moving retained objects (unlinking objects from a retained folder)	134
4.2.2.8	Close folder operations	141
4.2.2.8.1	Overview	141
4.2.2.8.2	Closing a folder	144
4.2.2.8.3	Re-opening a folder	145
4.2.2.8.4	Revert a folder from a closed or re-opened state	145
4.2.2.9	Retention policies	146
4.2.2.9.1	Retention policy overview	146
4.2.2.9.2	Creating a retention policy	156
4.2.2.9.3	Copying, exporting, and importing retention policies	173
4.2.2.9.4	Viewing/modifying a retention policy, applied retention, or retainer properties	184
4.2.2.9.5	Enabling or disabling a retention policy	190
4.2.2.9.6	Applying a retention policy or viewing a list of retention policies	191
4.2.2.9.7	Removing an applied retention policy	197
4.2.2.9.8	Deleting a retention policy	198
4.2.2.9.9	Performing a privileged delete	199
4.2.2.9.10	Linking objects to a retained folder	200
4.2.2.10	Base dates	204
4.2.2.10.1	Deleting a base date mapping	206
4.2.2.11	Contacts	206
4.2.2.11.1	Creating a contact	207
4.2.2.11.2	Viewing or editing a contact	207
4.2.2.11.3	Deleting a contact	207
4.2.2.12	Authorities	208
4.2.2.12.1	Creating an authority	208
4.2.2.12.2	Viewing or editing an authority	208
4.2.2.12.3	Deleting an authority	209
4.2.2.13	Global conditions	209
4.2.2.13.1	Creating a global condition	210
4.2.2.13.2	Viewing or editing a global condition	210
4.2.2.13.3	Deleting a global condition	211
4.2.2.14	Conditions	211
4.2.2.14.1	Creating a condition	211
4.2.2.14.2	Viewing or editing a condition	212
4.2.2.14.3	Deleting a condition	212
4.2.2.15	Disposition run bundles	212
4.2.2.16	Qualification, promotion, and disposition	213

4.2.2.16.1	Qualification Manager	214
4.2.2.16.2	Promotion Manager	221
4.2.2.17	Disposition Manager	222
4.2.2.17.1	Overview of disposition	222
4.2.2.18	About the disposition job, strategies, actions, export and transfer locations	222
4.2.2.19	About disposition status	224
4.2.2.20	Disposition on a simple object	225
4.2.2.21	Disposition on a complex object	225
4.2.2.22	About disposition rules	226
4.2.2.23	Disposition processing behavior when multiple retainers are applied to an object	226
4.2.2.24	About terminal retention	227
4.2.2.25	About structural retention	228
4.2.2.26	About disposing physical objects	228
4.2.2.27	About disposition workflows	228
4.2.2.28	To route a document for approval (start a workflow for review and approval)	229
4.2.2.29	Running Disposition Manager	230
4.2.2.30	Retention markups	239
4.2.2.30.1	Creating a retention markup	241
4.2.2.30.2	Deleting a retention markup	245
4.2.2.30.3	Applying a retention markup	245
4.2.2.30.4	Viewing an applied retention markup	246
4.2.2.30.5	Viewing usages of a retention markup	246
4.2.2.30.6	Removing a retention markup	246
4.2.2.31	Retention Policy Services searching	246
4.2.2.32	Retention Policy Services reports	247
4.2.2.32.1	Running the retention report	247
4.2.2.32.2	Running the retention markup report	257
4.2.2.32.3	Running the retention notification report	261
4.2.2.32.4	Running the retention markup review report	264
4.2.2.32.5	Running the close folder report	267
4.2.2.32.6	Running the audit trail report	272
4.2.2.33	Retention Policy Services jobs	273
4.2.2.34	Retention Policy Services audit events	281
4.2.2.35	Retention Policy Services glossary	294
5	Records Manager	299
5.1	Records Manager Introduction	299
5.1.1	Determining which Records Manager version you are accessing	299
5.1.2	Administration components	300
5.1.3	About privileged clients and accessing repositories	301

5.1.4	Setting up Records Manager	302
5.1.4.1	Policies	302
5.1.4.2	About setting up a file plan and configuration options	302
5.1.4.3	About attribute inheritance and the file plan	306
5.1.4.3.1	Adding rules to the attribute inheritance table	307
5.1.4.4	User preferences	310
5.1.5	About customized email optional mappings	310
5.2	Records Manager administration	311
5.2.1	About Records Manager functionality	311
5.2.2	Records Manager	311
5.2.2.1	Overview of Records Manager	311
5.2.2.2	About disposition run bundles	314
5.2.2.3	Roles and functional access	315
5.2.2.3.1	About roles and permissions	315
5.2.2.3.2	Records Manager roles and functional access	316
5.2.2.3.3	Records Manager roles and functional access using Documentum Webtop	328
5.2.2.3.4	Records functionality that appears in Documentum Webtop	332
5.2.2.3.5	Documentum Webtop operations and Records Manager	333
5.2.2.4	Records overview	333
5.2.2.4.1	Functional access and permissions	337
5.2.2.5	Declaring electronic or physical documents as formal records	340
5.2.2.5.1	Entering values on the formal records form	344
5.2.2.6	Viewing document record associations	345
5.2.2.7	Creating and viewing record relationships	345
5.2.2.8	Removing a record relationship	348
5.2.2.9	Formal records, formal folders, and formal cabinets	348
5.2.2.10	Declare new version	350
5.2.2.11	Working paper	352
5.2.2.11.1	Working paper overview	352
5.2.2.11.2	Designating working papers	353
5.2.2.11.3	Cancelling working paper designations	354
5.2.2.11.4	Declaring working papers as formal records	354
5.2.2.11.5	Running a working paper report	354
5.2.2.11.6	Searching for working papers in the repository	355
5.2.2.11.7	Cleaning up working papers	355
5.2.2.12	Derived security and attribute marking sets	356
5.2.2.12.1	Derived security	356
5.2.2.12.2	Attribute markings	357
5.2.2.12.3	Attribute marking sets	358
5.2.2.13	Records policies	361
5.2.2.13.1	Overview of records policies	361

5.2.2.13.2 About policy usages and applied policies	362
5.2.2.13.3 About containment policies	363
5.2.2.13.4 About security policies	364
5.2.2.13.5 About naming policies	368
5.2.2.14 Records Manager system configuration options settings	373
5.2.2.15 Containment policies	375
5.2.2.15.1 Creating a containment policy	375
5.2.2.15.2 Creating containment policy rules for emails with attachments	378
5.2.2.15.3 Applying a containment policy	379
5.2.2.15.4 Viewing applied policies	380
5.2.2.15.5 Removing applied policies	381
5.2.2.15.6 Deleting policies and attribute markings	384
5.2.2.16 Naming policies	385
5.2.2.16.1 Creating a naming policy	385
5.2.2.16.2 Applying a naming policy	389
5.2.2.16.3 Viewing an applied naming policy	390
5.2.2.16.4 Removing an applied naming policy	390
5.2.2.16.5 Deleting a naming policy	390
5.2.2.17 Security policies	390
5.2.2.17.1 Overview of security	390
5.2.2.17.2 Creating security policy	393
5.2.2.17.3 Creating restrictive markings	395
5.2.2.17.4 Creating shared markings	395
5.2.2.17.5 Creating security levels	396
5.2.2.17.6 Creating attribute marking sets	396
5.2.2.17.7 Adding members to restrictive markings	398
5.2.2.17.8 Adding members to shared markings	398
5.2.2.17.9 Adding members to attribute markings	399
5.2.2.17.10 Adding members to security levels	400
5.2.2.17.11 Managing record security using security policies	401
5.2.2.17.12 Managing record security using security levels	401
5.2.2.17.13 Managing record security using restrictive markings	402
5.2.2.17.14 Managing record security using shared markings	403
5.2.2.17.15 Managing record security using attribute markings	403
5.2.2.17.16 Viewing applied security policies	404

5.2.2.17.1	Removing applied security policies	404
7		
5.2.2.17.1	Deleting a security policy	405
8		
5.2.2.18	Record relations	405
5.2.2.18.1	Overview	405
5.2.2.18.2	Create record relation definition	410
5.2.2.18.3	Creating your own relation types	413
5.2.2.18.4	Update record relation definition	413
5.2.2.18.5	Delete record relation definition	414
5.2.2.18.6	View record relation definitions	414
5.2.2.18.7	Create record relationship	414
5.2.2.18.8	Remove record relationship	414
5.2.2.18.9	View record relationships	414
5.2.2.19	Classification subscription lists	414
5.2.2.19.1	Overview	414
5.2.2.19.2	Creating a CSL	415
5.2.2.19.3	Deleting a CSL	416
5.2.2.19.4	Adding a location to a CSL	416
5.2.2.19.5	Removing an item from a CSL	417
5.2.2.19.6	Selecting a classification item from a CSL when declaring a record ..	418
5.2.2.20	About default forms and customized forms	418
5.2.2.21	Creating a formal cabinet	429
5.2.2.22	Creating a formal folder	434
5.2.2.23	Searching records	439
5.2.2.24	Records Manager Reports	440
5.2.2.25	Records Manager audit events	441
5.2.2.26	Records Manager jobs	445
5.3	Commonwealth administration	446
5.3.1	Overview	446
5.3.2	Create a file	449
5.3.3	Close a file	451
5.3.4	Reopen a file	451
5.3.5	Update a file	452
5.3.6	Create a file part	452
5.3.7	Close a file part	452
5.3.8	Reopen a file part	453
5.3.9	Update a file part	453
5.3.10	Import the business classification scheme (BCS)	453
5.3.11	Import a retention policy	457
5.3.12	Classify a file	460
5.3.13	Add to a file	461

5.3.14	Remove from a file	461
5.3.15	Add to a file part	461
5.3.16	Remove from a file part	462
5.3.17	Create a thesaurus term	462
5.3.18	Update a thesaurus term	464
5.3.19	RM Commonwealth audit events	464
6	Physical Records Manager	467
6.1	Introduction	467
6.1.1	Administration components	467
6.1.2	About privileged clients and accessing repositories	468
6.1.3	Setting up Physical Records Manager	469
6.1.3.1	Configuration options	469
6.1.3.2	User preferences and column preferences	469
6.2	Physical Records Manager Administration	470
6.2.1	About Physical Records Manager functionality	470
6.2.1.1	Physical Records Manager functionality	470
6.2.2	Physical Records Manager	470
6.2.2.1	Overview of Physical Records Manager	471
6.2.2.2	Physical Records Manager system configuration options settings	473
6.2.2.3	Physical Records Manager roles and functional access	474
6.2.2.4	Library requests	480
6.2.2.4.1	Overview of library requests	480
6.2.2.4.2	Library request email notifications	481
6.2.2.4.3	Making a library request	482
6.2.2.4.4	Cancel a library request	486
6.2.2.4.5	View/edit a library request	486
6.2.2.4.6	View/edit charge-outs	487
6.2.2.4.7	View/edit my charged out items	488
6.2.2.4.8	View/edit my library requests	488
6.2.2.4.9	List library requests	489
6.2.2.4.10	List charge-outs	489
6.2.2.4.11	Convert library request to charge-out	490
6.2.2.4.12	Charging in a charge-out	494
6.2.2.4.13	Send recall notice	496
6.2.2.4.14	Send overdue notice	496
6.2.2.5	Physical objects	496
6.2.2.5.1	Overview of physical objects	496
6.2.2.5.2	Create physical object (document/container/address)	497
6.2.2.5.3	View/edit physical object	500
6.2.2.5.4	Delete physical object	505
6.2.2.5.5	Export physical object	506

6.2.2.5.6	Mark physical object shipped (or picked up) for charge-out	508
6.2.2.6	Disposition of physical objects	509
6.2.2.6.1	Overview	509
6.2.2.6.2	Completing disposition for a paper object with a Destroy all strategy	510
6.2.2.6.3	Completing disposition for a paper object with Destroy content strategy	510
6.2.2.6.4	Completing disposition for a paper object with a Export all, Destroy all strategy	510
6.2.2.6.5	Completing disposition for a paper object with Export all, Destroy content strategy	511
6.2.2.6.6	Completing disposition for a paper object with Export all strategy	511
6.2.2.6.7	Completing disposition for a paper object with a NARA Transfer, Destroy all strategy	511
6.2.2.6.8	Completing disposition for a paper object with NARA Transfer, Destroy content strategy	512
6.2.2.7	Barcodes	513
6.2.2.7.1	Copying a record	513
6.2.2.7.2	Barcode generation rules	513
6.2.2.7.3	Generating and regenerating barcodes	515
6.2.2.7.4	Scanning and transferring scanned barcodes into the system (barcode manager)	516
6.2.2.7.5	Change barcode	516
6.2.2.8	Label printing rules	517
6.2.2.8.1	Overview	517
6.2.2.8.2	View/edit a list of label printing rules	518
6.2.2.8.3	Create a label printing rule	518
6.2.2.8.4	Print a label	519
6.2.2.9	Batch processing using a portable scanner	519
6.2.2.9.1	Overview	519
6.2.2.9.2	To manually upload a batch processing file for bulk operations	521
6.2.2.9.3	To view the operation status and/or to view the report for an operation	522
6.2.2.9.4	Batch processing notifications	522
6.2.2.10	Pass-along requests	523
6.2.2.11	Physical Records Manager reports	524
6.2.2.11.1	Running a physical record report	524
6.2.2.11.2	Running a library request report	530
6.2.2.12	Physical Records Manager jobs	531
6.2.2.13	Physical Records Manager audit events	533
7	Core OpenText Documentum CM functionality	537
7.1	Repositories	537
7.1.1	Log in to a repository	537
7.1.1.1	Log in as an express user	539

7.1.1.2	Log into another repository	539
7.1.1.3	Log out of all repositories	539
7.1.1.4	Set your favorite repositories	539
7.1.2	Navigate a repository	540
7.1.2.1	Select the columns that appear in lists	541
7.1.2.2	Navigate categories	542
7.1.3	Locate an item in a selection dialog box	543
7.1.4	Set your preferences	543
7.1.5	Open an additional repository window	545
7.1.6	Drag-and-drop	545
7.1.7	Right-click	546
7.1.8	View messages	546
7.1.9	View the status of background operations	546
7.1.10	Refresh page	546
7.1.11	Select HTTP or UCF content transfer	547
7.1.12	Use modal dialogs	548
7.1.13	Work with repository documents offline through My Documentum	548
7.1.14	View product information	548
7.2	Files and folders	549
7.2.1	Create a file	549
7.2.2	Create a folder	549
7.2.3	Create a cabinet	550
7.2.4	Set properties	550
7.2.5	Check out and edit files	551
7.2.5.1	Overview of check out and edit	551
7.2.5.2	Check out a file	552
7.2.5.3	Check in a file	553
7.2.5.3.1	Checkin information	553
7.2.5.3.2	Versions	555
7.2.5.3.3	Replace a repository file with a different file	556
7.2.5.4	Cancel checkout of a file	556
7.2.5.5	View currently and recently checked-out files	557
7.2.6	View a file in read-only mode	557
7.2.7	Change the format associated with a type of file	558
7.2.7.1	Restore associated file formats to the defaults	559
7.2.8	Import files to the repository	559
7.2.9	Import OLE linked objects	560
7.2.10	Export files from the repository	561
7.2.10.1	Deep export	562
7.2.11	Delete an item from the repository	563
7.2.12	Move an item to a new location in the repository	563
7.2.13	Copy an item to a new location in the repository	564

7.2.14	View your clipboard	564
7.2.15	Links	565
7.2.15.1	Link an item to another location in the repository	565
7.2.15.2	Link an item to another repository	565
7.2.15.3	View all locations to which an item is linked	566
7.2.15.4	Link a repository item to your computer	567
7.2.15.5	Add a document or folder to your browser's bookmarks or favorites ..	567
7.2.15.6	Use email to send a link to a repository item	568
7.2.15.7	Convert Desktop DRLs to Documentum Webtop URLs	568
7.2.15.8	Open a link sent by email	569
7.2.15.9	Access the DRL of a document version that is deleted from the repository	569
7.2.16	Subscriptions	570
7.2.17	Receive notification when a file is read or changed	570
7.2.18	Export the information displayed in a list	571
7.2.18.1	Export specific search results as a CSV file	571
7.3	Using the Brava! HTML Viewer	572
7.4	Email messages	573
7.4.1	Changes in email processing	573
7.4.2	Operations supported on email messages	573
7.4.3	Importing email messages to the repository	573
7.4.4	Exporting email messages from the repository	576
7.4.5	Viewing email messages	577
7.4.6	Transforming email messages	577
7.4.7	Searching email messages	577
7.4.8	Locating and opening an email attachment	577
7.4.9	Locating the email to which an attachment belongs	578
7.5	Search	578
7.5.1	Run a simple search	578
7.5.1.1	Further define search terms	579
7.5.2	Run an advanced search	582
7.5.2.1	Enter values for an advanced search	583
7.5.3	View search results	587
7.5.3.1	Smart navigation	587
7.5.3.2	Monitor search results in real time	588
7.5.3.3	Save search results from external sources	589
7.5.4	View your most recent results but do not relaunch the search	590
7.5.5	Improve your search experience	590
7.5.5.1	How configuration can impact your search experience	590
7.5.5.2	Index a repository	592
7.5.5.3	Searchable items	592
7.5.6	Saved searches	593

7.5.6.1	Save a search to run again later	593
7.5.6.2	Run a saved search	593
7.5.6.3	View the results of a saved search but do not relaunch the search ...	594
7.5.6.4	Edit a saved search	594
7.5.6.5	Copy a saved search	594
7.5.7	Search templates	595
7.5.7.1	Run a search from a search template	595
7.5.7.2	Create a search template	596
7.5.7.3	Edit a search template	596
7.5.7.4	Modify a search template definition	597
7.5.7.5	Copy a search template	598
7.5.8	Set search preferences	598
7.6	Inbox	599
7.6.1	Inbox overview	599
7.6.2	Open a task or notification	599
7.6.3	Perform a task	599
7.6.4	Complete a task	600
7.6.5	Accept a task that has been assigned to multiple users	601
7.6.6	Reject a task	602
7.6.7	Delegate a task	602
7.6.8	Repeat a task	603
7.6.9	Change your availability for tasks	603
7.6.10	Work queue tasks	604
7.6.10.1	Manage tasks in your queue Inbox	604
7.6.10.2	Get the next available task in a work queue	605
7.6.10.3	Select a task from the queue	605
7.7	Workflows and quickflows	606
7.7.1	Start a workflow	606
7.7.2	Send a quickflow	608
7.7.3	View workflows	609
7.7.4	Pause a workflow	609
7.7.5	Resume a paused workflow	610
7.7.6	Stop a workflow	610
7.7.7	Email the workflow supervisor or a workflow performer	610
7.7.8	Process a failed task in a workflow	611
7.7.9	Change the workflow supervisor	611
7.7.10	Save workflow information as a Microsoft Excel spreadsheet	612
7.7.11	View aggregated report for workflow performance	612
7.7.12	Create a workflow template	612
7.8	Work queues	613
7.8.1	Work queue roles	613
7.8.2	Setting up queue management	614

7.8.3	Set up a new work queue	615
7.8.4	Set up work assignment matching	615
7.8.4.1	Set up skill profiles in the process template	616
7.8.4.2	Define work assignment matching filters	616
7.8.4.3	Add work assignment matching filters to a work queue	617
7.8.5	Work queue policies	618
7.8.5.1	Priorities of tasks	619
7.8.5.1.1	Set dynamic priority and aging logic for tasks	619
7.8.5.2	Create or modify a queue policy	620
7.8.6	Define a queue category	621
7.8.7	Define a work queue	622
7.8.8	Define work queue override policies	624
7.8.9	Manage work queue users	625
7.8.9.1	Add a user or group to a work queue	625
7.8.9.2	Remove a user or group from a work queue	625
7.8.9.3	Add skills to work assignment processor profiles	626
7.8.9.4	Update the processor profile in a work queue	628
7.8.10	Monitor work queues	628
7.8.10.1	Assign or reassign a work queue task to a specific user	630
7.8.10.2	Unassign a work queue task from a user	631
7.8.10.3	Move a work queue task to another work queue	631
7.8.10.4	Suspend a work queue task	632
7.8.10.5	Unsuspend a work queue task	632
7.8.10.6	Enable users to select tasks from the queue	632
7.8.11	Create business calendars	633
7.9	Lifecycles	635
7.9.1	View Lifecycles	635
7.9.2	Assign a lifecycle to a file	635
7.9.3	Remove a lifecycle from a file	636
7.9.4	Promote a file to the next lifecycle state	636
7.9.5	Demote a file to its previous lifecycle state	636
7.9.6	Suspend a file from its current lifecycle state	637
7.9.7	Resume a suspended file	637
7.10	Collaborate with other users	637
7.10.1	Create and edit formatted text	637
7.10.2	Discussions	638
7.10.2.1	View discussions	639
7.10.2.2	Add and edit comments	639
7.10.2.3	Delete comments	640
7.10.2.4	Discussions in search results	640
7.10.3	Notes	641
7.10.4	Contextual folders and cabinets	642

7.10.5	Calendars	643
7.10.5.1	Create calendars and events	643
7.10.5.2	Specify recurring event properties	645
7.10.5.3	View calendars and events	647
7.10.5.4	Edit calendars and events	647
7.10.5.5	Delete calendars and events	647
7.10.5.6	Calendars in search results	648
7.10.5.7	Export and import with calendars	648
7.10.6	Data tables	648
7.10.6.1	Create data tables and entries	649
7.10.6.2	View data tables	652
7.10.6.3	View data table entries	652
7.10.6.4	Edit data tables	653
7.10.6.5	Edit data table entries	654
7.10.6.6	Delete data tables	654
7.10.6.7	Import and export with data tables	654
7.10.7	Rooms	655
7.10.7.1	Visit a room	655
7.10.7.2	Link to a room	656
7.10.7.3	Objects governed by rooms	656
7.10.7.3.1	Ungovern objects from a room	656
7.10.7.4	Create a room	657
7.10.7.5	Edit the properties of a room	658
7.10.7.6	About room membership	659
7.10.7.7	Copy a room	660
7.10.7.8	Move or link to a room	661
7.10.7.9	Delete a room	661
7.10.8	Manage room membership	662
7.10.9	Manage users as a non-administrator	664
7.10.9.1	Create new users	665
7.10.9.2	Modify users	666
7.10.9.3	Unlist users (conceal members)	667
7.10.9.4	Restricted folders	667
7.11	Forms	668
7.11.1	Enter data in a form	668
7.11.2	Format text in a form	668
7.11.3	Create a new form	670
7.11.4	Save As functionality	671
7.12	Virtual documents	671
7.12.1	Virtual documents overview	671
7.12.2	Create a virtual document	671
7.12.3	View the structure of a virtual document	672

7.12.4	View the content of a virtual document	672
7.12.5	Add a descendant to a virtual document	673
7.12.6	Rearrange descendants in a virtual document	675
7.12.7	Remove a descendant from a virtual document	676
7.12.8	Specify that a certain version of a descendant is always used	677
7.12.9	Set a version label for a virtual document	678
7.12.10	Create an archive of a virtual document	678
7.12.11	Convert a virtual document to a simple document	679
7.12.12	Set your virtual document preferences	679
7.13	PDF annotations	681
7.13.1	PDF annotations overview	681
7.13.2	Configure PDF Annotation Service to open when user views a PDF ..	681
7.13.3	Add comments to a PDF document	682
7.13.4	View comments in a PDF document	682
7.14	Relationships	682
7.15	Renditions and transformations	683
7.15.1	Renditions and transformations overview	683
7.15.2	Viewing a list of the different renditions of a file	684
7.15.3	Importing a rendition	685
7.15.4	Transforming a document to PDF or HTML format	685
7.15.5	Creating a rendition through transformation	686
7.15.6	Creating a related file through transformation	687
7.16	Presets	688
7.16.1	Presets overview	688
7.16.2	Create a preset	689
7.16.3	Edit an existing preset	689
7.16.4	Edit preset rules	690
7.16.5	Preset rules	690
7.16.6	Remove a preset from an item	693
7.16.7	Delete a preset	693
7.16.8	The Documentum Webtop Express preset	693
7.17	Permission sets	694
7.17.1	Permission sets overview	694
7.17.2	Basic permissions	694
7.17.3	Extended permissions	695
7.17.4	Create or edit a permission set	695
7.17.5	Edit permissions	696
7.18	Users, groups, and roles	699
7.18.1	Users	699
7.18.1.1	Locate a user	699
7.18.1.2	Create or edit a user	699
7.18.1.3	User properties	700

7.18.1.4	Import users from information contained in an input file	701
7.18.1.4.1	Input file for new users	702
7.18.1.5	Make a user active or inactive	703
7.18.1.6	Change the home repository of a user	703
7.18.1.7	View the groups to which a user belongs	704
7.18.1.8	Reassign one user's items to another user	704
7.18.1.9	Delete a user	704
7.18.1.10	View user management logs	705
7.18.2	Groups	705
7.18.2.1	Create or edit a group	705
7.18.2.2	Group properties	706
7.18.2.3	Add or remove members in a group	708
7.18.2.4	Reassign one group's items to another group	708
7.18.2.5	View the groups to which a group belongs	709
7.18.2.6	Sort Groups and members within groups	709
7.18.2.7	Delete a group	709
7.18.3	Roles	709
7.18.3.1	Create or edit a role	710
7.18.3.2	Role properties	710
7.18.3.3	Add or remove members in a role	711
7.18.3.4	Reassign one role's items to another role	711
7.18.3.5	View the groups to which a role belongs	712
7.18.3.6	Delete a role	712
A	Records Troubleshooting Tips, Limitations and FAQs	713
A.1	Applying a retention policy using our public API	713
A.2	Special characters	714
A.3	Why can I no longer log in to a repository using my Privileged DFC instance	715
A.4	How to identify your Privileged DFC instance from other instances on the same host	715
A.5	Why my Privileged DFC instance does not show up in Documentum Administrator	717
A.6	How to test that your instance of Privileged DFC is properly configured	717
A.7	Digital shredding	718
A.8	Auditing	718
A.9	Why is Declare Formal Record disabled?	718
A.10	Why is the node for Records Manager, Retention Policy Services, Physical Records Manager, or Records Manager Commonwealth Edition missing?	719
A.11	Creating formal records, cabinets, and folders	720
A.12	Why can I not create new objects in a folder after I upgrade Records (only if Security Policy is applied)	720

B	Keyboard Shortcuts for Microsoft Windows and Mac Operating Systems	721
C	Records Manager and Department of Defense functionality	723
C.1	Overview of Department of Defense functionality	723
C.2	Classification guides	724
C.2.1	About classification guides	724
C.2.1.1	Creating classification guides for classified records	725
C.3	Disposition run bundles	729
C.3.1	Overview of disposition run bundles	729
C.3.2	To open a disposition run bundle and view the details, and when necessary to view the details of the work order and perform recovery actions	731
C.3.3	To confirm or to reject a NARA transfer run	732
C.3.4	To view the last transferred item list	734
C.3.5	To view the manifest of a transfer run or, to export the manifest or declare it as a formal record	734
C.4	Declaring Department of Defense formal records	736
C.4.1	Entering values on the applicable Department of Defense form when declaring Department of Defense formal records	738
C.4.1.1	Entering values on the Department of Defense standard records form	738
C.4.1.2	Entering values on the Department of Defense email records form ...	743
C.4.1.3	Entering values on the Department of Defense classified records form	747
C.5	Running the Department of Defense declassification report	759
C.6	Records - XML export and XML import operations	760
D	XML Report examples against View Input and View Results	763
E	Optional attributes	765

Preface

Preface

The Records Client is a unified client with integrated OpenText™ Documentum™ Content Management Retention Policy Services, OpenText™ Documentum™ Content Management Records Manager, and OpenText™ Documentum™ Content Management Physical Records Manager capabilities. The records product suite consists of OpenText Documentum Content Management (CM) Retention Policy Services and OpenText Documentum Content Management (CM) Records Manager. Once one or more of these products is purchased, then the appropriate functionality appears within the Records Client according to the role that the user is in. For example, members in the Retention Manager role would see the administration node for Retention Policy Services but would not see the administration nodes for Records Manager or for OpenText Documentum Content Management (CM) Physical Records Manager.

 **Note:** Each records product is role based and therefore all users and administrators must be in the correct role for the expected functionality to work properly. It is equally important that each instance of the Records Client, which hosts each of the records products, is registered for Privileged DFC.

Records Manager includes two optional feature packs: Records Manager Commonwealth Edition (RMCE) and Department of Defense (DoD). Documentum Webtop functionality is always available regardless of the records products that are installed. Although these products are deployed from a single war file, they are usable only when the respective dar files are installed. For complete details about deployment and installation, refer to the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*.

Retention Policy Services and Records Manager bring records management discipline and Enterprise Content Management (ECM) power to the handling of all business records and messages, to:

- Reduce the risk of non-compliance and litigation; through uniform, standards-compliant policies and systems for record and message retention, access, and disposition.
- Control the cost of managing large volumes of records and messages in compliance with statutes, regulations, and established business practices.
- Manage physical records in one or more warehouses.

i Intended audience

This document is intended for individuals who manage records, administer the record keeping system, and who use records in their work.

ii Organization

This guide is divided into three product-specific parts for Records preceded by a fourth part that covers Records functionality that is common to the three product-specific parts. Part 5 covers core OpenText Documentum Content Management (CM) functionality, which is always available regardless of the three records products that are installed.

Chapter 1

Overview of the Records Client

The Records Client is a WDK-based application that provides a unified solution for administering records products. The Records Client leverages the strengths of OpenText Documentum CM, is built on top of Documentum Webtop, and consists of the following records products:

- Retention Policy Services
- Records Manager
- Physical Records Manager

Retention Policy Services, Records Manager, and Physical Records Manager are uniquely suited to provide complete record, retention, and physical object capabilities in a single unified user interface. Total records management functionality as a result, is available at your finger tips.

There are two ways of creating records:

- Declaratively, when you select a document for example and declare it as a formal record from the Records menu Declare Formal Record. Declaring an object as a formal record means that a form has to be filled out. A formal record is a construct (a snapshot that contains all of the record components (usually documents) and is associated to a form. All formal records have a form with metadata associated to it.
- Passively, by linking a document for example, into a policy managed folder or by applying a policy directly to the document, which results in a typical record. Typical records are not associated to a form with metadata and are only policy managed, by at least one policy.

Retention Policy Services allows the management of records by applying retention policies as well as litigation holds to manage the controlled aging process.

Records Manager is used primarily to declare formal electronic records and to administer them within a policy managed file plan. Any type of content can be stored as either a formal record or a typical record. Records Manager Commonwealth Edition and Department of Defense are optional feature packs available with the purchase of Records Manager. Commonwealth Administration was developed to meet Records Manager requirements of the Australian State and Federal Governments and other organizations. It is based on policies of National Archives of Australia (NAA) and closely related to ISO 15489, VERS, and MoReq.

Physical Records Manager provides enhanced records management to account for any physical assets, that is real-world objects which are represented as physical objects in Physical Records Manager. It includes functionality to manage warehouse

inventories, to reserve and borrow physical objects, generate reports, and manage barcodes.

All components of the integration are deployed from a single war file. Deployment based on the records.war file makes it possible to activate any one or more of the records products from a single client. Core OpenText Documentum CM functionality (for example, ECM functionality) however, is always available regardless of the product that is activated. Records Manager Commonwealth Edition is available with the purchase of Records Manager. The Commonwealth Administration node however, is displayed only when the Records Manager Commonwealth Edition dar file is installed. Similarly, Department of Defense functionality is only available when the Department of Defense dar files are installed.



Note: The version of the OpenText™ Documentum™ Content Management Server must match or exceed the version of the Retention Policy Services dar file being installed. The dar installer performs a pre-installation check and it will notify you if the version of the OpenText Documentum CM Server is incorrect.

Refer to the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*, to install dar files for any of the records products or the optional feature packs (Records Manager Commonwealth Edition and Department of Defense).



Note: You cannot successfully install Records Manager or Physical Records Transformation Services independently without first installing Retention Policy Services, Records Manager, and Physical Records Transformation Services functionality are dependent on Retention Policy Services. Records Manager and Physical Records Transformation Services are the plug-ins to Retention Policy Services. If you want to install Records Manager for its functionality only, install the Retention Policy Services dar files first then the Records Manager dar files. If you want Records Manager Commonwealth Edition functionality, install the Records Manager Commonwealth Edition dar file after the Records Manager dar files are installed. If you want Department of Defense functionality, install the Department of Defense dar files after the Records Manager dar files are installed. If you want to install Physical Records Transformation Services for its functionality only, install the Retention Policy Services dar files first then the Physical Records Manager dar files. Only Retention Policy Services can stand on its own, requiring only the Retention Policy Services dars. Dar files must be installed in a specific order according to instructions in the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*.

Online help can be viewed for the three records products and for Documentum Webtop, regardless of the product that is installed.

You can purchase Retention Policy Services to begin with and then when ready, upgrade to Records.

Available clients and online help

All records products are supported in one unified client. Users and administrators do not have to worry about which client, online help, or guide to obtain or reference. The content in either format is divided into product-specific parts. The PDF copy of the help file can also be downloaded from <https://support.opentext.com>.

This guide documents Records Manager, Records Manager Commonwealth Edition, Retention Policy Services, Physical Records Manager, and Documentum Webtop functionality in one unified client user guide.

OpenText Documentum Records Activator for Microsoft Outlook - User Guide (EDCRMCOOUT-UGD) documents the RA functionality.



1. End users and administrators must be in the proper Retention Policy Services, Records Manager, or Physical Records Manager role and must also have the appropriate permissions to gain the functional access needed. Functional access is tailored or limited according to the permissions you are assigned and the Retention Policy Services, Records Manager, or Physical Records Manager role you are in. Members in Records Manager, Retention Manager, or Physical Records Manager roles do not need Delete on every object to manage them. Members in the manager roles are given dynamically the ability to dispose or privilege delete retained records. They are also given Browse All to view the records and perform operations on them. Users must have Write permissions on objects they want to declare as formal records. Whether users need Write on the target folder is not entirely dependent on the security policy. Users must have Write permissions on the target folder when folder security is turned *On*. When folder security is enabled, a user must have Write permission (or greater) on the:
 - Target folder to create, import, copy, or link an object into the folder.
 - Source folder to unlink (move) or delete an object from a folder.

Folder security is set to *On* by default. The folder security setting of a repository is recorded in the folder_security property in the docbase config object.

All roles and functional access are further described in “[Roles and functional access](#)” on page 315.

Regardless of the role or the client, the user also must be in the form_user group to create formal records, formal cabinets, and formal folders. If the user is not in the form_user group, menu options for Declare Formal Record, **File > New > Formal Cabinet**, and **File > New > Formal Folder** are not enabled for the user.

2. If only Retention Policy Services dar is installed, then Retention Policy Services Retention Managers, Compliance Officers, and Power Users will have Browse All permission.

If Records Manager is also installed along with Retention Policy Services, then only Retention Policy Services Retention Managers will have Browse All permission. Compliance officers and power users will not have Browse All permission.

3. Use the Administration node to set the permissions for a user, assign a role, and to add the user to a group if necessary.

For more information on administering users, groups, and roles, refer to [“Users, groups, and roles” on page 699](#). You need Administrator client capability to modify role membership.

The Records Client is ideally suited to manage all aspects of records management requirements for an organization. Requirements can include file plans, security, immutability, access controls, retention requirements, and the ability to manage physical records.

Since the records client is role-based, users have access to the set of functionality associated to the role they are in.

With the Records Client, you can:

- Define records policies, that is create and administer policies needed for file plans or managed folders to limit containment and access by the policies applied.
- Create a file plan and manage folders
- Access all end user and administrator functionality in all three major functional areas: records, retention, and content
- File formal records and typical records

Formal records are declared to a file plan, associated to a form, and are encapsulated within a snapshot. The form selected to declare a formal record captures metadata and provides advanced functionality. A form is defined and available for general use and there are forms that have been customized specifically to match Department of Defense requirements. A typical record is not declared using the declarative process, is not associated to a form, and is not encapsulated in a snapshot. An example of a typical record is a document with a retention policy applied to it (whether applied directly or indirectly from the folder based on inheritance).

- Define policies for file plans
- Promote a record within an Retention Policy Services lifecycle from one phase to the next, until it reaches the final phase for disposition
- Run disposition on records as part of the disposal schedule
- Prevent a record from reaching disposition if necessary
- Generate reports
- View audit trails and generate audit trail reports
- Check out and check in electronic records

- Charge-out and charge-in physical records
- Reserve a physical record as a library request

Optional integrations and applications

It is also possible, whenever needed, to integrate additional WDK-based applications such as Transformation Services, Collaboration Services, Subscription Services, and Workflow Services. Such additions require that the appropriate .dar file is installed on Records Manager.

You can declare Department of Defense email records using Records Activator for Microsoft Outlook client. Records Activator is an integration that allows users to create formal email records directly from Microsoft Outlook. You can declare email records only when Records Activator for Microsoft Outlook is configured and the standard record dar file is installed on Records Manager. Though Records Activator for Microsoft Outlook is not a WDK-based integration, the standard record dar file must be installed for Records Manager.



Note: To declare email records directly from Records Activator for Microsoft Outlook , refer to *OpenText Documentum Records Activator for Microsoft Outlook - User Guide (EDCRMCOOUT-UGD)*.

Records Manager also works within My Documentum for Microsoft Outlook for declaring typical records.

1.1 About Records Client

After you log in, to view the About Records Client details, click **File > About Records Client**.

Each administrative node is displayed only if the respective product is installed and users are assigned appropriate roles in the same OpenText Documentum CM repository. Any administrative node selected in the navigation pane lists all of its administrative items with a description in the content pane. Administrative nodes can be seen by users only if they are in a role that allows them to see the node. The same administrative items can be displayed in the navigation pane by expanding the node in the navigation pane. All objects displayed in the content pane are right-click enabled. Options you can select from, for the action you need, are displayed in a list box when you right-click an object.

Use the Administration node to provide individual members or members of a group the necessary permissions required to perform their roles. The Administrator cannot add users to the roles that require super user privilege.



Note: Refer to “[Users, groups, and roles](#)” on page 699 for complete details.
Only the Role Administrator can modify role membership.

The Records Client provides online help for Retention Policy Services and Records Manager, regardless of which is installed. Although both products are deployed from a single records war file, `records.war`, their respective DAR files must be installed for them to operate properly.

Use Retention Policy Services to retain records (that is, to age and dispose of records in a controlled manner) and when necessary to place retention markups, holds for example, to suspend aging for legal purposes. The administration node in Retention Policy Services is labeled Retention Policy Services which is used to administer/manage the following Retention Policy Services components:

- Base Dates
- Contacts
- Authorities
- Global Conditions
- Conditions
- Retention Policies
- Disposition Run Bundles
- Retention Markups

Use Records Manager to declare formal electronic records. The administration node in Records Manager node is labeled Records Manager which is used to administer/manage the following Records Manager components:

- Containment Policies
- Security Policies
- Derived Security
- Restrictive Markings
- Shared Markings
- Security Levels
- Attribute Marking Sets
- Attribute Markings
- Classification Guides (Department of Defense specific node, available only if Department of Defense dars are installed)
- Naming Policies
- Record Relation Definitions
- Classification Subscription Lists

Use Records Manager to manage physical inventories, that is physical objects in warehouses for example and to create barcodes. Physical record objects in Records

Manager are electronic representations of real-world objects. The Physical Records Manager node is used to administer/manage the following components:

- Library Requests
- Charge-outs
- Barcode Generation Rules
- Label Printing Rules
- Pass-along Requests

1.2 Usage tracking information

Documentum CM Server tracks software usage by recording login times. The Documentum CM Server global registry contains a record of the first and latest login time for each user of each application that connects to Documentum CM Server. Documentum CM Server periodically generates basic reports to indicate usage. These reports are available to the Documentum CM Server administrator. The *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS-AGD)* contains more information about usage tracking reports.

Since the licenses are allocated to users through OpenText Directory Services (OTDS), you can also track the license usage through OTDS. For more information, see *OpenText Directory Services - Web Client Help (OTDS-H-AWC)*.

Users can access work order reports through Retention Policy Services and the Records Manager Commonwealth Edition functionality through Records Manager.

Chapter 2

Records Interoperability with Content Intelligent Services (CIS)

2.1 About the Content Intelligent Services (CIS) integration with Retention Policy Services

The CIS option named Cascade To Subcategories provides functionality for classifying content in a repository into user-defined taxonomies. The option is displayed for retention policies, only if CIS is enabled and when Cascade To Subfolders is selected. A taxonomy is a specific hierarchy of categories and subcategories into which you organize content. Taxonomies provide alternate organizational schemes from the scheme found in the repository folders. For example, a taxonomy might create categories based on your organization's departments. Content created by the Engineering department would be assigned to the Engineering category; content created by the Public Relations department would be assigned to the PR category; and so on.

Cascading of retention policies applied to a file plan, as result of this option, can be controlled against both folders and categories. The CIS option allows a Records Manager to set, per retention policy, whether the policy when applied to a folder (or cabinet) or to a category should propagate to all subfolders or subcategories or not.

When CIS is enabled in the repository, retention policies can be created with a setting that can be used to allow or to prevent retention from cascading to subcategories. Cascading is controlled by setting the Cascade Rule when a retention policy is created. The cascading (or propagation) rules are as follows:

- Cascade To Everything (default setting)
- Cascade To Subcategories
- Cascade To Subfolders
- Do Not Cascade

Retention policies by default cascade to everything, that is to both subfolders and subcategories. Although a retention policy (retention) can be allowed to cascade down a file plan hierarchy, it can be prevented from cascading beyond a certain point. For example, in a simple file plan that consists of some folders followed by a category and then one or more folders, cascading from folders above the category could be prevented at the category to prevent further cascading to any folders on the other side of the category. Assume a file plan as shown in [Figure 2-1](#), where F1, F2, and F3 are folders and C1 is a category. Also, assume that the retention policy propagation rules are set to cascade to subfolders but not to subcategories. If the policy is directly applied to folder F1, then F2 would inherit the policy and C1

would not. Since F3 is a subfolder of C1 it would not have retention applied since propagation is prevented by C1.

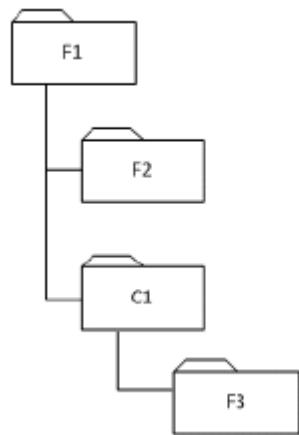


Figure 2-1: File plan with folders and a category

Contained items that are not a type of folder, category, or subtype of folder, or category always inherit the retention policy.

The Structural Retention Type option on the retention policy when the policy is being created (or when it is being modified from its properties) is displayed only when the value for the Retention Strategy is set to Linked. This allows a retention or records manager to place a linked retention on a folder or category and to have it go through disposition without destroying itself, only the contents therein. The folder is reset after the disposition run, and aging starts over. Only those retention policies, that have no rollover retention policies specified, support Structural Retention Type. The container object (folder, category, or physical container) is also destroyed along with its children, if Structural Retention Type is turned off (deselected).

Both Cascade To Subcategories and Structural Retention Type options are further described in the procedure for “[Creating a retention policy](#)” on page 156.

Chapter 3

Records Client common functionality

This chapter describes functionality that is common to all of the Records Client products, Retention Policy Services and Records Manager. The following topics are described:

3.1 Work orders

3.1.1 Work order general overview

Work order functionality provides increased processing performance within a framework that can scale to meet the request for processing a large quantity of items against any Records operations, that are supported. Work orders allow users to start multiple operations without having to wait for an operation to finish. Users can also monitor any of the operations while they are being processed as well as perform recovery actions to resume an operation, without starting all over again if the operation encounters a problem. The Work Order Report is included for monitoring and recovery. Work order configuration objects are also available for tuning performance.

Work order functionality pertains to all of the records products and therefore a work order may be created for any supported records operation using Retention Policy Services or Records Manager. All supported records operations are listed in “[Work order report overview](#)” on page 51.

Work orders are created by the Work Order Framework (WOF) for asynchronous processing to better process large requests with possibly millions of objects. For example, applying retention to a folder with millions of items, such as documents and subfolders, would be divided up into workable sizes or chunks by the Work Order Framework.

The primary interactive feature of work orders is the three work order reports—Work Order Report, Work Order Breakdown Report, and Work Order Item Report. Any operation/request defined within a work order is processed by the Work Order Framework. The work orders may be processed immediately within the local space of the framework or remotely by the OpenText™ Documentum™ Content Management Records Queue Manager. Work order configuration objects are available for tuning work order performance. The work order reports are described in “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51. Work orders are processed in the background and therefore, users and administrators can move onto other tasks without having to wait for the operation to complete.

Work orders:

- Are discrete amounts of work which are self-contained, of manageable sizes, and are processed concurrently.
- Spawn other work orders if necessary, during the discovery of identifying items to process in the initial work order request.

Work order features include:

- Scalability
- Discovery
- Reporting and Monitoring
- Recovery

The Work Order Report is essentially the master work order report. It includes two other reports users can launch from it whenever necessary, the Work Order Breakdown Report and the Work Order Item Report, and it is used for monitoring and recovery.

3.1.2 Work order definitions

The work order hierarchy is depicted as shown in [Figure 3-1](#). There are three work order types: master, reference, and partitioned. Reference and partitioned work orders are subwork orders. The three work order types are described as follows:

- A master work order is always *created* when a request is delegated to the framework.
Contains the request and information for the entire operation and binds together all of the spawned work orders that satisfy the request. Reference and partitioned work orders are those spawned by a master work order. The master work order and all subwork orders spawned by it are referred to as a collection of work orders.
- A reference work order is created for each folder. Some operations such as promotion and qualification do not create reference works orders for folders since the children of folders for those operations are not affected.
Contains an object that has to be processed, but which, by itself, also controls other objects to which the operation has to be propagated (for example, a folder from which retention cascades to its children). The dependent objects are allocated to other work orders.
- A partitioned work order, is always *spawned* from reference work orders but could also be spawned from the master work order depending on the setting for the Work Order Size.
Contains a number of allocated objects that fit within the predetermined Work Order Size.

For example:

If the requested (selected) object for an operation is only a folder object, a master work order is created from which a reference work order is spawned. A partitioned

work order is spawned from the reference work order only if the number of documents in the folder exceeds the Work Order Size configured for the operation.

When a reference work order is partitioned, a number of partitioned work orders are created (zero if an empty folder). Each partitioned work order has at most the number of items defined as the work order size. For example, by default the work order size is 1000. If a folder has 5,341 items, 6 partitioned work orders will be created (the first 5 will have 1000 items and the last one will have 341 items). Any subfolders will cause a reference work order to be created. If a partitioned work order is created, it will spawn a reference work order against each folder. If a partitioned work order is not spawned, the documents will then be processed immediately and a reference work order will be spawned from the master work order against each folder.



Note: The input and the results of the Work Order Report, the Work Order Breakdown Report, or in a work order notification, can be viewed in an XML file when you right-click a work order and select View Input or View Results. Work order notifications can also be configured optionally for completed work orders, whether they are successfully processed or not.

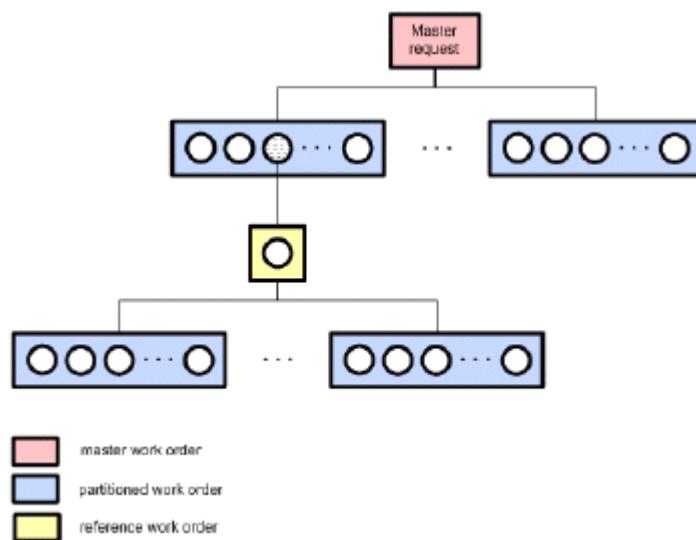


Figure 3-1: Work order hierarchy

3.1.3 Work order icons

- represents a master work order.
- represents reference work orders.
- represents partitioned work orders.
- represents the work order framework configuration object.
- represents a work order operation configuration object.
- represents a machine that processed a work order.

3.1.4 About work order confirmation messages

Success, and error messages are displayed in the status bar at the bottom of the page. If a message is longer than the status bar display area:

- Hover the mouse cursor over it to make the message scroll to the right so you can see the rest of the wording (the full message).
- The same message can also be viewed in its entirety by selecting **Tools > View Messages**. Previous messages can also be viewed using this option.

3.1.5 About the OpenText Documentum Content Management (CM) Records Queue Manager

The Records Queue Manager is used for remote processing of work orders. Each Records Queue Manager server represents a worker (each worker can define how many threads can process items) that can process work orders. The queue items are stored in the repository so that multiple instances of Records Queue Manager can collaborate to process spawned work orders. By using the repository, it is possible that if a Records Queue Manager server is shut down (power outage), other Records Queue Manager systems can continue the work and then that Records Queue Manager server can resume after it is restarted. Customers can later add additional Records Queue Manager systems to increase throughput. The Records Queue Manager frees up the Application server so that processing can be distributed.

You must install Records Queue Manager on a separate host other than the Application server and Documentum CM Server to avoid contention for resources. To install Records Queue Manager, refer to *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*. To enable remote processing, if Records Queue Manager is installed, refer to “[About the work order framework configuration object and each of the work order operation configuration objects](#)” on page 37.

Work orders can be configured per operation to initiate remote processing (assuming that remote processing is enabled) when a specific number of items in a request is reached or exceeded. The number of items specified for the work order size, against an operation, is used to determine when remote processing is initiated. For example, if a user is applying retention to a folder with five documents, the

processing could be done locally. If the folder instead had 1,000,000, processing would be completed remotely. Once partitioning is done, multiple Records Queue Manager processors each pull off the queue any of the partitioned work orders that were routed for processing. It is also possible to configure the system to always process everything remotely by setting the local thresholds to zero. Refer to “[About the work order framework configuration object and each of the work order operation configuration objects](#)” on page 37.

3.1.6 About the work order framework configuration object and each of the work order operation configuration objects

The attribute settings, that are modifiable on these configuration objects, should not be changed unless the impacts are well understood. Work order processing of all supported records operations is dependent on these configuration files.

 **Note:** If any of the values, as set out-of-the-box for supported records operations, are changed post installation, they will not be reverted to the defaults if the Retention Policy Services DAR is reinstalled.

Although there is only one Work Order Framework Configuration object to manage the framework, there are many Work Order Operation Configuration objects, one for each supported records operation. The framework configuration object is stored in Cabinets/System/Applications/RPSConfig/Workorder Configuration. The work order operation configuration objects are stored in Cabinets/System/Applications/RPSConfig/Workorder Operations Configuration.

Table 3-1: Work order framework configuration attributes

Attribute	Default Setting	Description
Name	Work Order Framework Configuration Object	The name assigned to this configuration object.
Owner Name	Install Owner	The account that installed the Retention Policy Services DAR.
Enable Remote Processing	False	Determines whether the Records Queue Manager can be used or not. If you wish to use Records Queue Manager, this option must be selected. If the checkbox is deselected, all operations would be processed locally. Remote processing is not enabled by default.

Attribute	Default Setting	Description
Asynchronous Local Processing	False	If the operation is to be processed locally, this option if selected, allows local processing to be done asynchronously. Note, if the operation is being done in a transaction (for example, clipboard operations), this setting will be ignored and the operation will be done synchronously. Local processing is asynchronous by default.
Route Timeout (in seconds)	14400 (4 hours)	This attribute, displayed when you select Show all properties , sets a threshold for the length of time or to limit the time a work order remains on the queue before the system determines it is down. It is meant to prevent work orders from sitting on the queue indefinitely. A setting of 0 disables this option. The value is set to 1,4400 seconds by default.  Note: This attribute is also used for the Waiting Timeout that is used by the Work Order Monitor Job, except that this value is interpreted in minutes rather than seconds.
Successful Work Order Cleanup Duration (in days)	30	All successfully processed master work orders are deleted after the specified duration. Only work orders that were completed successfully can be destroyed.

Attribute	Default Setting	Description
Failed Work Orders Cleanup Duration (in days)	60	All failed work orders are deleted by the work order monitor job after the specified duration. Only work orders that fail completely can be destroyed. Any work order that partially succeeds can be recovered, for example a transfer run within a disposition run bundle.
Update Batch Size	250	<p>Indicates how many items to process before providing a processing status update. A value of 250 for example, means that an update is provided whenever 20 items have been processed. If the value for the update batch size is the same as the value for the work order size, then only one update is provided when all of the items in the work order have been processed.</p> <p>This setting affects the Last Update Time that can be displayed optionally on the Work Order Report. A work order that fails to update itself after the time interval specified for the Update Timeout means that it is not able to finish processing the number of items specified for this attribute. It could be that the processor is hung or that the value for this attribute should be reduced. Chances are that the processor is hung as the default values assigned for all operations, provide sufficient margin for success.</p>
Work Order Size	1000	Indicates the number of items that are permitted in a partitioned work order. Determines when the master work order needs to be partitioned.

Attribute	Default Setting	Description
Session Timeout (in minutes)	120 minutes (2 hours)	This attribute is used to set the <code>login_ticket_timeout</code> of the work order. It is required because the work orders are in queue before getting picked up for processing and the login ticket generated gets outdated over time. The login ticket that will be used by the work order framework will expire only after the <code>session_timeout</code> (in minutes) value elapses.
Notification Base URL	<code>http://localhost:8080/records</code>	The link to the work order for recipients of e-mail notifications. To create work order notifications, refer to "Work order notifications" on page 130 . Set the URL to reflect the host of the Application server for the Records Client. The port may need to be changed (or if a different port is used). The last part (<code>records</code>) may also be changed if your organization wishes to name the location differently.
Notification Date Format	Medium	Determines the format of the start and end dates within the message added to the notification under the Instructions heading. Options include: <i>Full</i> , <i>Long</i> , <i>Medium</i> , or <i>Short</i> . The exact result depends on the locale, but generally: <ul style="list-style-type: none"> - SHORT is completely numeric, such as 12.13.52 or 3:30pm- MEDIUM is longer, such as Jan 12, 1952 - LONG is longer, such as January 12, 1952 or 3:30:32pm - FULL has it completely specified, such as Tuesday, April 12, 1952 AD or 3:30:42pm PST.

Attribute	Default Setting	Description
Router Module Name (Read-only)	com.documentum.workorder.create.WorkOrderCtsRouter com.documentum.web., com.documentum.webtop., com.documentum.webcomponent.,	Indicates the name of the module that will be used for remote routing.
User operation origin packages core (Read-only)	com.documentum.rps.library., com.documentum.prm.library., com.documentum.rmce.library., com.documentum.rm.library.	The Java packages for core applications that will be used by instrumented operations to identify the operation origin for intercepted actions that generate master work orders.
User operation origin packages custom		The administrator can define additional Java packages that will be used by instrumented operations to identify the operation origin for intercepted actions that generate master work orders.

 **Warning**

If either the Update Batch Size or the Work Order Size settings on the Work Order Operation Configuration object is set to 0, the respective settings on the Work Order Framework Configuration object is referenced instead. System administrators can choose to make all operations reference their respective operation configuration object or the configuration object of the framework. Settings can be maintained centrally as a result, if necessary. For example, if you want to control (maintain) the Update Batch Size or the Work Order Size or both centrally, that is for all operations, set the value to 0 on the operation configuration object for each operation. Then set the desired value for the respective attribute on the framework configuration object.

Table 3-2: Work order operation configuration objects

Attributes	Description
Name (Read-only)	Name of the operation. Each work order operation configuration object has a unique value that corresponds to a supported operation. For example, Apply/Remove Records Policy.

Attributes	Description
Authorized Roles (Read-only)	Indicates all of the roles that are authorized for this operation.
Children Depend on Reference Item (Read-only)	Children will only be processed if the folder object is successfully processed, when set to T (True). For example, retention applied to a folder will cascade to its children only if retention is successfully applied to the folder. Children will be processed whether the folder object is processed successfully or not, when set to F (False). This attribute pertains to reference work orders, which are spawned from the master work order or a partitioned work order when a folder object is encountered.
Context Switch Helper (Read-only)	The module name of the WorkOrderContextSwitchHelper implemented for the applicable operation.
Item Processor (Read-only)	The module name of the WorkOrderItemProcessor implemented for the applicable operation.
Master Processor (Read-only)	The module name of the MasterWorkOrderProcessor implemented for the applicable operation.
Reference Item Depends on Children (Read-only)	The folder object will only be processed if the children are successfully processed, when set to T (True). For example, a folder object will be disposed of only if the children (contents) are successfully disposed. The folder object will be processed whether the children are processed successfully or not, when set to F (False). This attribute also pertains to reference work orders, as described for Children Depend on Reference Item.
Reference Item Process Order (Read-only)	This attribute is defined on only the operation configuration object for each supported records operation. This attribute setting affects the processing order of an operation against container objects and the items contained within, a folder and the documents within for example. The value can be set to process the folder first and then the documents within (before children) or to process the documents first and then the folder (after children).
Update Batch Size	Refer to “ Work order framework configuration attributes ” on page 37 for the description.

Attributes	Description
Update Timeout	<p>This attribute is defined on only the operation configuration object for each supported records operation. The value entered is in seconds. The value can be set to either 0, which means there will not be a timeout; or equal to or greater than 300 seconds (5 minutes). A work order that does not update after processing the number of items according to the Update Batch Size will timeout if the number of seconds specified has elapsed. For example, if the Update Batch Size is set to 250 and the Update Timeout is set to 300, the work order will timeout if 250 items could not be successfully processed within 300 seconds (5 minutes).</p> <p> Note: The Update Batch Size and the Update Timeout attributes are interdependent. Make sure any changes to their settings to fine tune performance, for the expected work volume, is appropriate. If 5,000 items with 5 partitions consisting of 1,000 items against an Update Timeout of 300, 250 items is easily processed. Each item according to these figures should be processed within 1.2 seconds (300 divided by 250). You would not want to change only one without considering whether or not to change the other. Setting the Update Batch Size to 500 for example, and leaving the Update Timeout at 300 allows less than 1 second (0.6) to process an item which would be more likely to fail. The lesser processing time is allocated, the greater the chances become for failure.</p>
Work Order Size	<p>Refer to “Work order framework configuration attributes” on page 37 for the description.</p>

Attributes	Description
Local Processing Threshold	<p>This attribute is defined on only the operation configuration object for each supported records operation. Determines whether the work order will be routed to the local queue for immediate processing, assuming that Records Queue Manager is enabled which by default is not. A value of 50 for example, means that a work order with more than 50 items will be queued for external (asynchronous) processing as opposed to being queued for local (synchronous) processing which is generally done immediately. If set to 0, no local processing, all work orders for the operation would be queued for external processing. The default setting out-of-the-box is 100.</p>
Include All Children	<p>Indicates whether the work order framework should discover all objects in a hierarchy, including those which the user has no permission to access. True means discover all objects whether the user has permissions to access them or not. The user must be a member of dmc_rps_contributor role.</p>
Work Order Parameters Factory	<p>The module name of the WorkOrderParametersFactory is implemented to handle the creation and processing of the specific work order parameter type expected by the processor. It interprets the encoding of parameters in the work order.</p>
Enable to Suppress Successful Work Order Results	<p>If you select this attribute, the work order framework generates work order results only for the items whose processing has failed or is in warning state. It does not generate results for successfully processed items. Also, the work order item report does not display the successfully processed items.</p> <p>If you do not select this attribute, the work order framework generates work order results for all the processed items (including succeeded, failed or items in warning state).</p> <p>By default, this attribute is selected ONLY for COMPLIANCE_CHECKER and REPORT_OVERDUE_DISPOSITION work order operation configuration objects.</p>

Attributes	Description
Destroy Successful Work Orders	If you select this attribute, the work order monitor job cleans the successful work orders. Else they are retained. You can view the retained successful work orders in the Work Order Report.

All work orders provide regular updates, up the hierarchy, to the master work order until all work orders are processed. All work orders can be monitored for their progress from the Work Order Report as further described in “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51.

3.1.7 Understanding when work orders are generated

The general rule is that a work order is created when many items, possibly thousands or millions of items in a folder or subfolders, are requested for an operation. When making a Retention Markup, Retention Policy or Records Policy direct change through the Records Client UI, the specified items are processed immediately for the change while folder children are routed for processing using existing rules. The following table lists the conditions under which a work order will or will not be generated:

Table 3-3: Conditions for generating work orders

Condition	Work Order Generated	Notes
Apply/remove a policy to one or more items directly.	Yes	One work order for all items processed.
Linking an empty folder or a document into a policy managed folder and/or into a folder with markups applied.	No	
Linking a folder with content into a policy managed folder and/or into a folder with markups applied.	Yes	One work order will be created for processing Records Policy application operations. And, one work order will be created for processing Retention Markup application (if applicable) operations.
Setting or removing one or more attribute markings on an empty formal folder or formal record.	No	
Setting or removing one or more attribute markings on a folder with items.	Yes	One work order for all attribute markings processed.

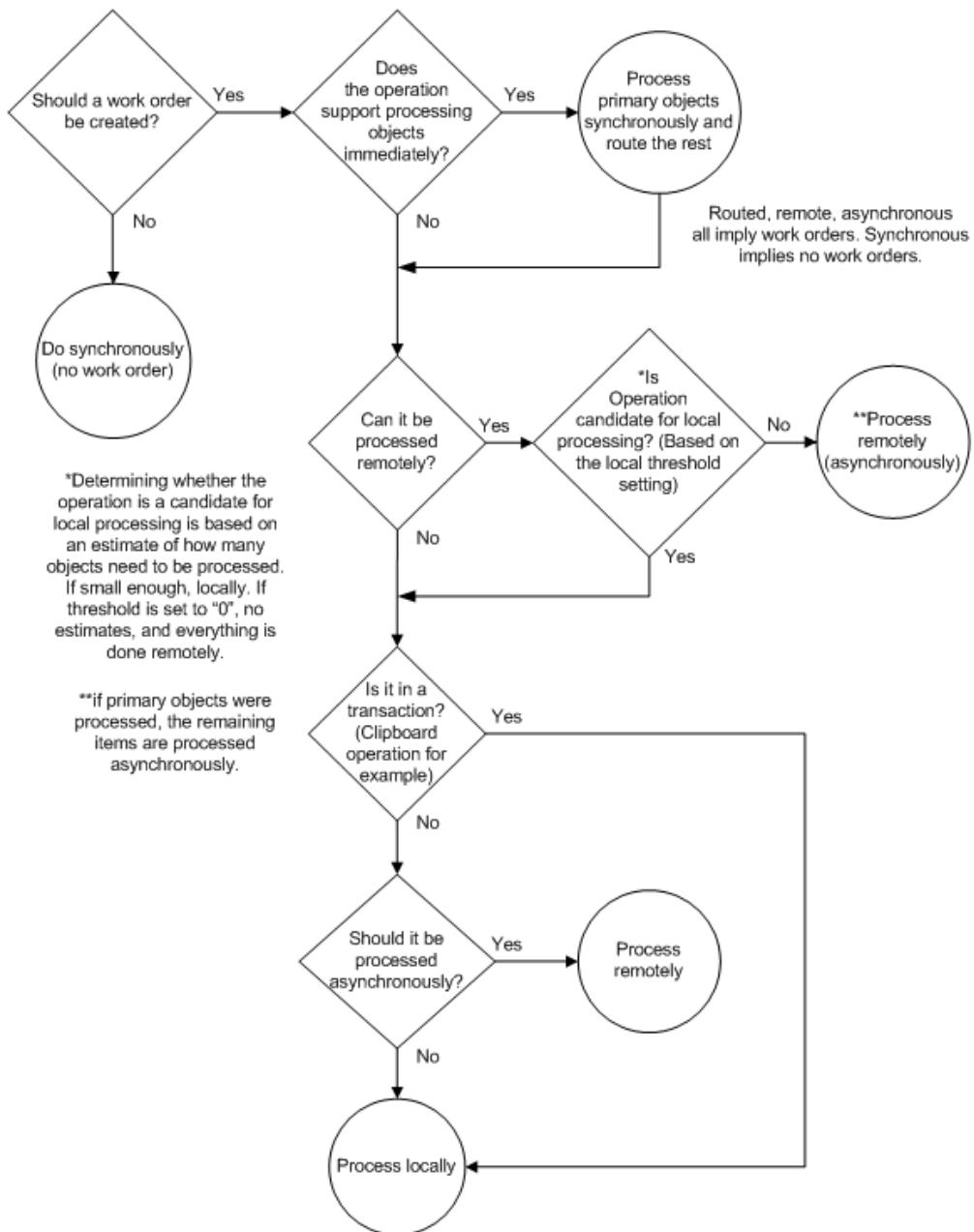


Figure 3-2: Work order processing flow

3.1.8 About the work order monitor job

The Work Order Monitor Job (dmc_rps_WorkOrderMonitorJob), when it runs (every 15 minutes), does three things:

- Terminates any work order that is stuck on the work order queue, before it is passed to a processor for processing, based on the Route Timeout (route_timeout) attribute.
- Terminates any work order that is stuck in processing, after it has been picked up off the queue, based on the Update Timeout (update_timeout) attribute.

Running work orders that have not provided an update time within the allotted interval since the last update time, are terminated. For example, a work order that should be able to process 1,000 items within 10 minutes, is terminated if it does not. The processing capacity, depending on the complexity of an operation, is different from one operation to another. A work order that is being processed has a Processing Status of *Running*.

The Processing Status of a master work order can be determined from the Work Order Report. Although it is an optional column, you can always display it from the Column Preferences dialog. The possible values that can be displayed are (For additional details, refer to “[Instructions to run the reports](#)” on page 57):

- CREATED - master work order has been created but not routed.
- ROUTED - master work order has been routed for processing.
- RUNNING - master work order is now actively being processed.
- WAITING - master work order is waiting for its children to complete processing.
- COMPLETED - master work order (including all of its subwork orders) has finished processing.
- Terminates any work orders that are in the waiting state, that are stuck, based on the Route Timeout (route_timeout) attribute times 60.
- Destroys work orders that were completed successfully, based on the Cleanup Duration interval, whereby all of the items in a request were processed successfully.

Details regarding either of these actions can be obtained from the work order monitor Job Report. That is, when you right-click dmc_rps_WorkOrderMonitorJob and select View Job Report, under Job Management in Documentum Administrator.

Although the frequency at which the job runs can be increased or decreased, decreasing it would mean a longer interval before a hung work order is detected.

Any work order that is interrupted in the middle of processing, becomes a candidate for recovery using the Work Order Report. Although any work order, master or subwork order, can be terminated by the work order monitor job, only the master work order can be recovered. This implies that only the Work Order Report has the

Recover menu option, the Work Order Breakdown Report and the Work Order Item Report do not.

The following attributes, with the exception of the clean-up attribute, are used to determine the running state of a work order and whether it should or should not be terminated:

Table 3-4: Attributes referenced by the work order monitor job

Attribute	Description
<ul style="list-style-type: none"> • update_batch_size • cleanup_duration_in_days • cleanup_duration_failed_wos <p>The cleanup_duration_in_days and cleanup_duration_failed_wos attributes are defined on the dmc_rps_work_order_config configuration object</p>	<p>dmc_rps_work_order_config: There is only one instance of this work order configuration object in the repository. For monitoring purposes, this file contains the default value for the update_batch_size. The default value implies that the value assigned on this configuration object for the update_batch_size is the value that will be used if the value for the update_batch_size on the dmc_rps_work_order_op_cfg configuration object is set to 0. This object is referenced for the default value in cases when the update_batch_size for a given operation is set to 0.</p>
	<p>update_batch_size: Defines the default number of items, for each supported records operation, that must be processed to trigger an update.</p>
	<p>cleanup_duration_in_days: Defines the number of days before successfully processed work orders are destroyed. It is intended to prevent excessive build up of successfully processed work orders. The default value is set to 30 days.</p>
	<p>cleanup_duration_failed_wos: Defines the number of days before failed work orders are destroyed. It is intended to prevent excessive build up of failed work orders. The default value is set to 60 days.</p>
<ul style="list-style-type: none"> • update_timeout • update_batch_size • destroy_success_work_orders <p>Defined on the dmc_rps_work_order_op_cfg configuration object</p>	<p>dmc_rps_work_order_op_cfg: Each supported records operation is defined with this work order configuration object. There is one for each supported records operation. The list box of the Operations filter on the Work Order Report displays all of the supported records operations.</p>
	<p>update_timeout: Represents the minimum time that a work order is permitted to have a value of <i>Running</i> in its processing_status attribute.</p>

Attribute	Description
	update_batch_size: Defines the number of items, for each supported records operation, that must be processed to trigger an update.
	destroy_success_work_orders: The work order monitor job excludes the successful work orders from being cleaned up if this flag is turned off for any of the operations.

The attributes on the work order monitoring job reference the work order configuration objects and their attributes.

3.1.9 About the operation processing order

Each supported records operation is associated with a processing order that is specified on the respective operation configuration object as before_children or after_children. A before_children setting implies a top down approach, to process the immediate documents of the selected folder before the documents in a subfolder. An after_children setting implies the opposite, a bottom up approach, to process the documents in the subfolder before the immediate documents. Objects in a folder for example, are processed in a bottom up approach when the disposition operation is run whereas, a top down approach is taken if a retention policy is applied. Retention processing must cascade down the folder structure whereas, with disposition processing, the opposite must occur, since the objects in the folder must be processed before the parent folder. In either case, the system waits until content of the subfolder or of the parent folder is processed before returning to process content of the other.

3.1.10 About the application and removal of a policy

A records policy, that is a retention policy or any of the Records Manager policies, can be applied to an object directly or by inheritance. A directly applied policy implies that a policy is selected and applied directly to the selected object. Both the object and the policy must be selected explicitly. Inherited policies reference a policy that is directly applied. Objects that are linked into a policy managed folder for example, inherit and enforce rules by referencing the policy that is directly applied to the folder. Policies are also inherited as a result of cascading, if the policy is set to allow cascading.



Notes

- When retention is being applied to a folder which does not have all its objects successfully applied with retention, the Work Order Report will show failed counts and actions for the items with no retainers. However, on the removal of the retention from this folder, the Work Order Report will show warning counts with no action for the items with no retainers.

- Application of policies and other actions such as creating a record relationship or performing a checkout for example, are disabled for work orders and their configuration objects.
- Removing a Retention Policy from an object may spawn work orders to remove related retainers. A related retainer could be due to a rolled over retention policy.

3.1.10.1 Applying/removing records policies to or from virtual documents and snapshots

Although a virtual document or a snapshot are each considered to be a single object, processed results in a work order could return multiple objects. Multiple objects could be returned since a formal record can be a snapshot of one or more documents.

Virtual documents and snapshots are unique instances of container-like objects. Work orders can process the application or removal of a policy (Process Records Policy) or retention markup (Process Retention Markup) as follows:

- All policies and retention markups can be applied to, or removed from, snapshots.
- Only retention policies can be applied to, or removed from, both snapshots and VDMs.

To determine the cascading behavior of the sub-operations for processing a records policy or retention markup, refer to “[Sub-operation cascade behavior for applying/removing records policies and retention markups](#)” on page 50. For example, the Policy Rules defined for a retention policy determine whether retention will cascade to the only the root or to the root and children of a virtual document or a snapshot.



Note: Policy and markup application and removal on complex objects will fail for all children if it fails for any one child, when the process is driven by a work order. A rollback of the apply or remove operation is performed if a child of a snapshot or virtual document fails during work order processing. The first failure of a child encountered, results in a rollback. The operation can be recovered only after the problem, that caused processing of the child to fail, is fixed. Fix the problem and then perform recovery.

Table 3-5: Sub-operation cascade behavior for applying/removing records policies and retention markups

Operation	Sub-operation	Cascade to Folders	Cascade to VDM Children	Cascade to Snapshot Children
Process Records Policy	Apply/remove retention policy	Configurable per policy	Configurable per policy	Configurable per policy

Operation	Sub-operation	Cascade to Folders	Cascade to VDM Children	Cascade to Snapshot Children
	All other apply/ remove sub- operations: - Containment Policy - Naming Policy - Security Policy - Security Level - Security Markings- Attribute Markings	Yes	No	Yes
Process Retention Markup	Apply/remove retention markup	Configurable per markup	No	Yes

3.1.11 Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report

The Work Order Report is an advanced feature for monitoring the processing of Records operations and performing recovery actions when necessary.

3.1.11.1 Work order report overview

The Work Order Report reports on master work orders which are created by the Work Order Framework for asynchronous processing. It is used primarily for monitoring and recovering master work orders and for launching the Work Order Breakdown Report or the Work Order Item Report to drill into an operation for recovery purposes or to examine results for performance tuning purposes. The Work Order Item Report can be launched from the Work Order Report or from the Work Order Breakdown Report. Any work order, or more specifically subwork order (referenced or partitioned) reported in the breakdown report can also be further broken down (drilled into) by launching another Work Order Breakdown Report. You can continue drilling into subwork orders, such as the subwork orders spawned by a partitioned work order, until there are no other subwork orders.

To determine throughput:

- The master work order has information about the number of items processed per minute.
- Each work order including the master work order stores six time values (Start Time, Route Time, Start Processing Time, Wait Time, Return Time, Finish Time). For additional details, refer to “[Instructions to run the reports](#)” on page 57.
- It is possible for each work order that processed at least one item to view the XML results and determine the time when the item was processed. Note that

master work orders may not process any items if partitioning was required or if all of the primary items were folders.

The breakdown report reports the subwork orders (partitioned and reference work orders) spawned by a master work order. The item report goes further to report the actual items contained in the request for the operation in question. For further details about these two reports, refer to the respective overview. For an overview of work orders, refer to “[Work orders](#)” on page 33.

The screenshot shows the 'Work Order Report' interface. At the top, there are filters for 'Owner' (Select Owner), 'Operations' (All), 'Completion Status' (All), 'Number' (text input), 'Start Time' (checkbox checked, Any Time), 'End Time' (checkbox checked, Any Time), and a 'Reset Filters' button. Below the filters is a link '[+] Show Advanced'. The main area displays 87 results from Jan 15, 2013, at 3:40:06 PM. A table lists operations with columns: Name, Operation, Operation Origin, Sub-operation Details, Version, Owner, and Completion Status. Row 79, 'Disposition' (User origin), has a context menu open, with 'View Breakdown' highlighted. Other options in the menu include 'View Input', 'View Results', 'Properties', and 'Delete'. The table data is as follows:

Name	Operation	Operation Origin	Sub-operation Details	Version	Owner	Completion Status
87	Process Records Policy	User	Apply Retention Policy 'KW_NARA_LinkedDA'	1.0,CURRENT	Administrator	Processing
86	Disposition	External		1.0,CURRENT	dcmbao6	Succeeded
85	Disposition	User		1.0,CURRENT	dcmbao6	Succeeded
84	Evaluate Retention Date	External		1.0,CURRENT	dcmbao6	Succeeded
83	Promotion	User		1.0,CURRENT	dcmbao6	Succeeded
82	Process Records Policy	User	Apply Retention Policy 'KW_NARA_LinkedDA'	1.0,CURRENT	dcmbao6	Succeeded
81	Process Records Policy	User	Apply Retention Policy 'KW_NARA_LinkedDA'	1.0,CURRENT	dcmbao6	Failed
80	Process Records Policy	User	Apply Retention Policy 'link_cond_destroyEKT'	1.0,CURRENT	dcmbao5	Failed
79	Disposition	External	View Breakdown	1.0,CURRENT	dcmbao6	Succeeded
78	Disposition	User	View Items	1.0,CURRENT	dcmbao6	Succeeded
77	Evaluate Retention Date	External	Properties	1.0,CURRENT	dcmbao6	Succeeded
76	Promotion	User	Delete	1.0,CURRENT	dcmbao6	Succeeded
75	Process Records Policy	User	Recover	1.0,CURRENT	dcmbao6	Succeeded
74	Disposition	Automated		1.0,CURRENT	Administrator	Failed

Figure 3-3: Work order report default settings

The screenshot shows the 'Advanced Settings' dialog for the Work Order Report. It contains two sections: 'Sub-Operations' with a checkbox 'Any Sub-Operation' checked, and 'Operation Origins' with a checkbox 'Any Operation Origin' checked. There is also a link '[+] Hide Advanced' at the top left.

Figure 3-4: Work order report advanced settings

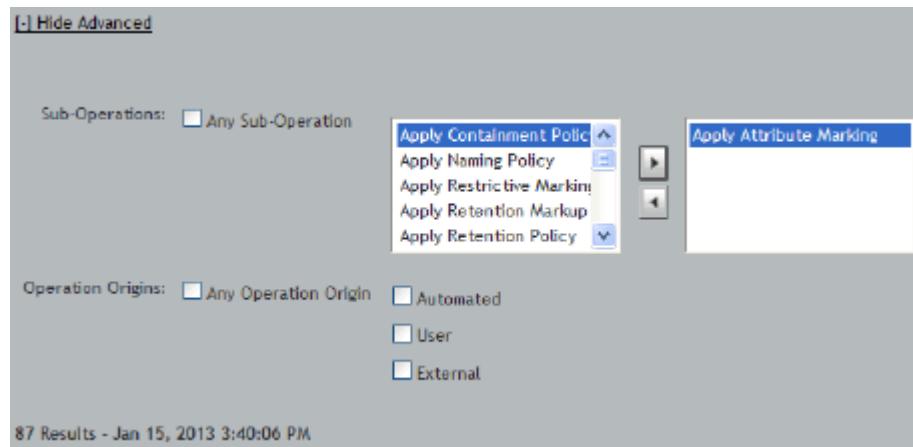


Figure 3-5: Work order report sub-operations and operation origin selectors

Obtaining a report using the default filter settings returns results against all work orders and the state that each is in. Results can be narrowed based on any combination of filter settings. The report filters and the columns that display the results are described in the tables within the “[Instructions to run the reports](#)” on page 57. Results against all work orders reported can be monitored to determine whether a work order requires recovery or not. Work orders that have stopped providing regular updates (due to a processor that suddenly goes inactive, times out, hangs, or is inadvertently shut down) or that have a completion status of Failed or Partially Succeeded, are candidates for recovery.

The recover menu option when you right-click a master work order is available only if the completion status is either partially succeeded or failed.

- **Compliance Checker**

You can select this option and click **Report** to view the results of executing the compliance check job. The compliance check job scans only those items that meet the filter criteria selected in Records Check Configuration options during its execution. An item is considered to be non-compliant by the compliance check job if

- The item has not inherited all the expected Retention Policy Services retainers from its parent folders
- The item has inherited one or more Retention Policy Services retainers, although it is not expected to inherit those retainers/markups from any of its parent folders
- The item has not inherited all the expected Retention Policy Services retention markups from its parent folders
- The item has inherited one or more Retention Policy Services retention markups, although it is not expected to inherit those markups from any of its parent folders.

- Destroy Master Work Order
- Disposition
- Evaluate Retention Date
- Process Records Policy

Process implies application or removal. Records policy implies retention policies, containment policies, naming policies, security policies, and security markings. Security markings include attribute markings, restrictive markings, shared markings, and security levels.

- Process Retention Markup
Process for this operation also implies application or removal.
- Promotion
- Qualification
- Overdue for Disposition

You can select this option and click **Report** to view the results of executing the Disposition overdue job. Only the items that are under retention and all their retainers in final phase are considered for overdue disposition checks. Each item goes through the following checks and report is generated accordingly if:

- The item is checked out.
- The item has hold mark-up attached.
- The item has permanent mark-up attached.
- The item has structural retainer.
- The item has terminal retainer.
- There is no export directory configured or export directory is not a network location (only if the export action is applicable).
- The item has review disposition strategy.
- Disposition approval required.
- (applicable only for NARA transfer strategy) The disposition run bundle is not enabled.
- The container has structural linked policy applied.
- The items have NARA transfer disposition strategy applied on them. To report these items, there is grace period configured in Grace Waiting Period (in Days) (grace_waiting_period attribute) of Records Check Configuration object.

Report is generated for physical objects if:

- The item is marked as lost
- The item is charged-out

- The physical export location is not available (this is considered only if the export action is applicable for the disposition strategy)
- The physical item is waiting for physical markings. To report these types of items there is grace period configured in Grace Overdue Period (in Days) (`grace_overdue_period` attribute) of Records Check Configuration object.

To view the entire list of sub-operations, change the Operation filter setting to *All*.
The sub-operations include:

- Apply Attribute Marking
- Apply Containment Policy
- Apply Naming Policy
- Apply Restrictive Marking
- Apply Retention Markup
- Apply Retention Policy
- Apply Security Level
- Apply Security Policy
- Apply Shared Marking
- Remove Attribute Marking
- Remove Containment Policy
- Remove Naming Policy
- Remove Restrictive Marking
- Remove Retention Markup
- Remove Retention Policy
- Remove Security Level
- Remove Security Policy
- Remove Shared Marking

All of the items in the list except Apply Retention Policy and Remove Retention Policy are not available unless the Records Manager DAR is installed.

Although there is only one Work Order Framework Configuration object in the repository, each supported operation has its own Work Order Operation Configuration object which are each named to match the operation. The Notifications tab on each Work Order Operation Configuration object is only visible to users who are members of the `dmc_rps_work_order_admin` role. For further details about the work order configuration objects, refer to “[Work orders](#)” on page 33.



Note: The Work Order Report is role based and therefore only members in either the Work Order Administrator role (`dmc_rps_work_order_admin`) or

the Work Order User role (dmc_rps_work_order_user) can run the report. Members in the Work Order Administrator role can view all of the work orders in the system, their own and those of others, and can delete work orders. Users that are only in the work order user role will only see their own work orders.

3.1.11.2 Work order breakdown report overview

The Work Order Breakdown Report reports on the subwork orders (partitioned and reference work orders) spawned by a master work order. It is used primarily to determine processing status and how efficiently processor resources are being utilized. Additional resources can be added or adjustments can be made to the work order configuration objects to improve efficiency.



Note: The Work Order Breakdown Report reports the breakdown of a master work order. It does not return results for any non-master work orders. The breakdown report does not return results for partitioned work orders that have no items.

To run the Work Order Breakdown Report, the Work Order Report must be run first. A master work order must be selected on the Work Order Report to run (launch) the Work Order Breakdown Report. The Work Order Breakdown Report is used to drill into a collection of subwork orders (spawned by a master work order) allowing you to see any work orders that were spawned.

3.1.11.3 Work order item report overview

The Work Order Item Report reports the items that were processed in a work order. By default only the primary objects that were selected for the operation are reported. The associated icon of each of the items reported is also displayed. Items reported are not actionable, that is no right-click functionality is available for any selected item. This report shows historical information and the objects in the repository may no longer exist or may have been moved out of the parent folders.

The following details against the Disposition operation for example can be determined from the Message column; any one or more of these details could be included in the message:

- The items that were processed. This can include documents, folders, and physical objects. You would be able to determine exactly what was in a container object, at the time the operation was done.
- If any actions were taken. For example, if on the first disposition run a physical object was marked for destruction whereas on the second run it would not.
- If a terminal retainer was applied.
- If a document was held or skipped.
- If structural retention was involved and if it was reset.
- If a job was responsible for the disposition run.
- If a document was not processed because it was checked out.

- If a folder (container object) was not disposed because it was not empty.

Also, whether the remaining items in the folder are retained and if there are folders that must be disposed separately.

3.1.11.4 Instructions to run the reports

To run the Work Order Report (WOR) or the Work Order Breakdown Report (WOBR) or the Work Order Item Report (WOIR):

1. To run the **Work Order Report**, select **Records > Reports > Work Order Report**.

To run the **Work Order Breakdown Report**, right-click a master work order reported in the **Work Order Report** and select **View Breakdown**.

To run the **Work Order Item Report**, right-click a work order reported in either the **Work Order Report** or the **Work Order Breakdown Report** and select **View Items**. Results in these reports are generated automatically against the default filter settings. Click the **Report** button if you change the default filter settings.



Note: A breadcrumb mechanism is added to the upper left-hand corner of the **Work Order Breakdown Report** and **Work Order Item Report**.

A count and timestamp are also displayed in the upper left-hand corner when a query is submitted, that is when you click the **Report** button, or when a column is added or removed. It can be determined at a glance when the report was last generated. The count and the timestamp are updated each time the **Report** button is clicked. Although the count may not change, that is if filter settings remain the same, the timestamp will change. Even if the filter settings do remain the same the count could increase, if for example more work orders were created since the last reported time. Also, the plus sign (+) next to the count means that there are more results to page through. The actual count, if there is more than one page of results, can be determined when you go to the last page.

2. Click **Report** to obtain results according to the default settings or change the filter settings to create your own custom report and then click **Report**.

Calendars for the **Start Time** and the **End Time** on the **Work Order Report** are displayed when the checkboxes for **Any Time** are deselected. The filters for the three work order reports are described in the following table:

Table 3-6: All work order reports filter descriptions

Filter Name	WOR	WOBR	WOIR	Description
Owner	x			Filters work orders against any user that is selected. One or more users can be selected. The default value is set to <i>All</i> . This filter is displayed only to users who are members of the Work Order Administrator role. Users in the Work Order User role can filter (see) only their own work orders.

Filter Name	WOR	WOB R	WO IR	Description
Operation	x			Filters work orders against all operations or any one particular operation.
Start Time	x			<p>Filters master work orders against the date and time an operation was initiated by the user or the work order job. Although Any Time is the default date range, deselecting the checkbox allows you to specify a specific date range. A value specified against only the From field returns results from that date and time to the current date and time. Similarly, a value specified against only the To field returns results up to the current date and time.</p> <p> Note: The date and the time entered (in hours, minutes, and seconds) represents Documentum CM Server time which could be different from your local time if the Documentum CM Server is located in a different time zone.</p>
End Time	x			<p>Filters master work orders based on the date and time they were completed. Completion of a master work order implies completion of the requested operation. The Any Time filter is used in the same manner as described for the Start Time.</p> <p> Notes</p> <ul style="list-style-type: none"> • Use the last update time against a particular work order to determine if it is progressing or not. Compare the last update time to the current time. The time reported is updated whenever work is completed by any of the subworker orders. If the report is still waiting and the update time has not changed for several minutes, it could mean that the work order is stuck or the work order monitoring job is not running. • The date and the time entered (in hours, minutes, and seconds) represents Documentum CM Server time which could be different from your local time if the Documentum CM Server is located in a different time zone.

Filter Name	WOR	WOB R	WO IR	Description
Completion Status	x			<p>Filters work orders against their status. Choices include: <i>All</i>, <i>Processing</i>, <i>Succeeded</i>, <i>Partially Succeeded</i>, and <i>Failed</i>.</p> <p><i>Processing</i> - The master work order has been taken from the queue and is currently being processed. Returns a list of work orders that have not yet completed and therefore have a Processing Status of either <i>Created</i>, <i>Routed</i>, <i>Running</i>, <i>Waiting</i>, or <i>Completed</i>.</p> <p><i>Succeeded</i> - The master work order has been successfully processed. Returns a list of work that have been completed without any errors.</p> <p><i>Partially Succeeded</i> - Not all items in the master work order or one or more of the work order children could be processed successfully or got skipped. Returns a list of work orders that have been completed with some errors and at least one success</p> <p><i>Failed</i> - Although the work order was picked up off the queue for processing, the processing could not be initiated or if initiated failed to complete due to a hung processor or inadvertent shut down. Returns a list of work orders that have completely failed.</p>
Number	x			All master work orders when they are created are assigned a unique id number which you can filter against to report only specific master work orders. One or more id numbers, if you know the number, can be typed into the text box using just a comma or both a comma and a space delimiter between each number as follows: 5321, 5587, 991020, and so forth. Do not include commas in the number itself. The host name or IP address, depending on the DNS server configuration, on which processing was performed can also be determined if you add the Processor Host column from the Column Preferences dialog. The Processor Host column is not displayed by default.
Reset Filters	x			Clears all entries and returns all filters to their default settings.
Show Advanced/Hide Advanced	x			Shows or hides advanced filters when selected.

Filter Name	WOR	WOB R	WO IR	Description
Sub-operations	x			<p>Filters those operations that can be associated with more than one operation. For example, <i>Process Records Policy</i> can be associated with an <i>Apply Records Policy</i> sub-operation or a <i>Remove Records Policy</i> sub-operation. <i>Process Retention Markup</i> as well can be associated with an <i>Apply Retention Markup</i> sub-operation or a <i>Remove Retention Markup</i> sub-operation. Any Sub-Operation is selected by default to report on all sub-operations against the selected Operation. One or more sub-operations can be selected, added or removed, when the checkbox for Any Sub-Operation is deselected.</p> <p> Note: The list box, on the selector displayed when Any Sub-Operation is deselected, displays all possible sub-operations when the Operation is set to <i>All</i>. Only the applicable sub-operations are listed against the selected Operation. Only Retention Policy Services sub-operations are listed if Retention Policy Services alone is installed. If Records Manager is also installed, its sub-operations will also be listed. Furthermore, the sub-operations listed is restricted to the role you are member of.</p>

Filter Name	WOR	WOB R	WO IR	Description
Operation Origin	x			<p>Filters master work orders based on the process that initiated the creation of a master work order. Any Operation Origin is selected by default. Once deselected any single option or combination can be selected.</p> <p>Automated - indicates the master work order was created by a job, the qualification, promotion, or disposition jobs.</p> <p>User - indicates the master work order was created as a result of any one of the following internal operations: applying/removing a policy, managing records security, applying a retention markup, deleting a work order, running the qualification, promotion, or disposition managers. When using a known client application, a link, move or unlink operation in that client application will specify the USER operation origin for any work order generated to process the change for child items (such as the case of moving a folder that has documents or folders within it).</p> <p>External - indicates the master work order was created as a result of any one of the following external operations: clipboard operations, Link/Unlink/Move with respect to policy managed folders, web services, OpenText™ Documentum™ Content Management client, changing an attribute that has been configured for a security attribute marking (Department of Defense- Supplemental Markings, Project Name), lifecycle and workflow initiated operations, all other operations not listed anywhere else.</p>
Processor Hosts		x		Filters work orders against one or more specific processors. Only those work orders processed by the hosts selected are reported.
Any Processing Status		x		Filters against one or more of the processing statuses Created , Routed , Running , Waiting , and Completed .
Any Completion Result		x	x	Filters against one or more of the completion results Succeeded , Warning , and Failure .
Any Additional Information		x	x	Can be set to filter work orders that have skipped items or which have action items.

Filter Name	WOR	WOBR	WOIR	Description
Show All Descendants	x	x		<p>When selected, reports all of the work orders spawned by the selected work order in the Work Order Report or in the Work Order Breakdown Report. The breakdown report can be run against a master work order selected on the Work Order Report or against a spawned work order that is reported and selected on the Work Order Breakdown Report. The breakdown report is the means by which you can drill into a collection of work orders.</p> <p> Note: Only the primary objects selected in a request against a supported operation are reported by default unless this option is selected. Although results are reported automatically, without having to click the Report button, when the Work Order Item Report is opened, the Report button will have to be clicked if this option is selected.</p>

Columns can be added or removed as necessary and reorganized from left to right to suit your viewing preferences using the Column Preferences dialog. Any column width by default will display a string of up to 50 characters. If results include more than 50 characters, you can stretch the column header to the right to expose the rest of the string. Results in any of the columns Results are returned under the following default column headings:

Table 3-7: Work Order Report, Work Order Breakdown Report, and Work Order Item Report column descriptions

Column Heading	WOR	WOBR	WOIR	Description
Name	x	x	x	The name on the WOR is the number assigned to a master work order. On the WOBR it is the id of the reference or partitioned work order. On the WOIR it is the original name assigned to each object listed.
Checked Out			x	<p>The header for this column does not say Checked Out, the key icon is used instead. It is however spelled out in the Column Preferences. The key is displayed for any item that is checked out. Keep in mind that the reading is historical and therefore the item may well have been checked in recently.</p> <p> Note: This column is displayed as the first column by default.</p>

Column Heading	WOR	WOBR	WOIR	Description
Master ID	x	x		The number assigned to a master work order. All master work orders are associated with a unique numerical identifier that is assigned sequentially to each master work order created. Only the master work orders are assigned a unique integer.
Operation	x	x		Indicates the name of the operations that were processed or are being currently processed. Operations that are currently supported include: <i>Qualification, Promotion, Disposition, Process Records Policy, Process Retention Markup, Compliance Checker, Destroy Master work order, Overdue for Disposition, Evaluate Retention date, Link/Move Folder</i> . A report can be obtained against any operation when <i>All</i> is selected.
Operation Origin	x			The process that initiated the creation of a master work order. The 3 possible values that can be displayed: <i>Automated, User, and External</i> . Each are described in the preceding table that describes the filters.
Sub-operation Name	x			Identifies the name of the sub-operation that was performed against an operation. Examples: If the Operation column displays <i>Process Records Policy</i> , the Sub-operation Name column would display either <i>Apply Retention Policy</i> or <i>Remove Retention Policy</i> . If the Operation column displays <i>Process Retention Markup</i> , the Sub-operation Name column would display either <i>Apply Retention Markup</i> or <i>Remove Retention Markup</i> .
Sub-operation Details	x			Identifies which records policy or retention markup, that is the name of the policy or markup, that was either applied or removed. Examples: If the Operation column displays <i>Process Records Policy</i> and the Sub-operation Name displays <i>Apply Retention Policy</i> or <i>Remove Retention Policy</i> , the Sub-operation Details would identify the name of the policy that was applied or removed. If the Operation column displays <i>Process Retention Markup</i> and the Sub-operation Name displays <i>Apply Retention Markup</i> or <i>Remove Retention Markup</i> , the Sub-operation Details would identify the name of the retention markup that was applied or removed.

Column Heading	WOR	WOBR	WOIR	Description
Version	x		x	<p>Although the following description pertains to the Work Order Report, it is the version of the object that was processed that pertains to the Work Order Item Report. Distinguishes recovered master work orders from the original master work order. A version of 1.0 displayed against a work order represents the original processing run. A version of 1.0, CURRENT displayed, represents the first recovery attempt, 2.0, CURRENT represents the second recovery attempt, and so forth until SUCCEEDED for the Completion Status is achieved. CURRENT is no longer displayed when subsequent recoveries are performed, for example:</p> <ul style="list-style-type: none"> • 1.0 • 2.0 • 3.0, CURRENT <p>The Recovery menu option is available against only the CURRENT versions. All copies of a master work order will display a Master Id that is the same as that displayed for the original. Therefore, to determine which original a master 2.0, CURRENT version belongs to, if several instances are displayed for example, refer to the Master ID column.</p>
User	x			All users who started an operation are reported by default unless a particular user is selected to narrow the results.

Column Heading	WOR	WOBR	WOIR	Description
Completion Status	x	x		<p>Displays the current state of a master work order created for an operation. A master work order could be in one of the following states:</p> <ul style="list-style-type: none"> <i>Processing</i> - the work order is being processed (has a processing status of Created, Routed, Running, Waiting, or Completed). <i>Succeeded</i> - the work has been completed without errors. <i>Partially Succeeded</i> - the work has been completed and there were some errors but at least one success <i>Failed</i> - none of the operations were successful. <p>A completion status of <i>Succeeded</i>, <i>Partially Succeeded</i>, and <i>Failed</i> implies that processing of all the items for the given operation is finished.</p> <p>A completion status of <i>Processing</i> means that the work orders spawned from the master work order are in any of the 5 states where at least one of them is not listed as <i>Completed</i>. The 5 states are described below, against the Processing Status.</p> <p> Note: Warnings against NARA transferred items, due to any skipped items, could still result in <i>Succeeded</i> if the items are disposed successfully. Skipped items in a transfer does not prevent disposition.</p>

Column Heading	WOR	WOBR	WOIR	Description
Start Time	x	x		<p>Displays the time at which a work order is created against the objects requested for an operation. Once a master work order is created, it is then routed and queued for processing. The Route Time is then registered. The Route Time column however is not displayed by default. Use Column Preferences if you want to add it. Once the master work order is picked up off the queue, the Start Processing Time is registered. It is also not displayed by default. If any reference work orders are created, a Wait Time and Return Time would also be registered. These two columns are also not displayed by default, only the Start Time and End Time. The recommended order for displaying these columns from left to right is: Start Time Route Time Start Processing Time Wait Time Return Time End Time .</p> <p>All of these time registries can be used to calculate the route duration, processing duration, and wait durations for assessing performance and improving it with additional resources. For further details about these durations, refer to Average Route Duration, Average Processing Duration, and Average Wait Duration which are also listed in this table.</p>
End Time	x	x		The time at which processing of the requested operation finished. The value is blank until processing of the operation is completed.
Processor Host	x	x		Identifies the processor that is either processing or has processed a master work order. A blank is a valid value which indicates that the work order has either been created or routed and no processing has been done.
Estimated Completion (%)	x			Indicates the amount of work, in percentage, that has been completed. A display of 100 for example, means the work order is 100% completed. <i>Estimate Not Available</i> is displayed only if the work order cannot estimate the number of items to process.
Processed Items Per Minute	x			Indicates the average number of items that are processed in one minute.

Column Heading	WOR	WOBR	WOIR	Description
Total Items to Process Estimate	x			Indicates the total number of items that need to be processed by the master work order. The total number of items to process may increase as the work order discovers which items need to be acted on. For example, applying a retention markup may cascade to subfolders, so as each folder is processed the work order processor may discover more items.
Total Items Processed	x			Indicates the number of items that have been processed by a master work order. The number displayed may not equal the number of items listed on the Work Order Item Report, which could be due to any skipped items. Skipped items in a folder will not show up in the Work Order Item Report. A reference work order that is terminated by the work order monitor job, could also cause a mismatch.
Total Items Successful	x			<p>The sum of all Items Successful in the collection of subwork orders spawned by a master work order. Indicates the number of items that have been processed successfully. The Total Items Successful, Total Items Warned, and Total Items Failed pertain to the completion results. The Completion Result on the Work Order Breakdown Report includes checkboxes for filtering against: Success, Warning, and Failure.</p> <p> Note: One or more actions could be displayed against any of the 3 results, though generally against items warned. For example, an action against a physical object that needs to be marked for destruction, before it can be destroyed.</p>

Column Heading	WOR	WOBR	WOIR	Description
Total Items Warned	x			The sum of all Items Warned in the collection of subwork orders spawned by a master work order. Indicates the number of items that may or may not have been done. Items that are warned will not be processed during a recovery. A warning against an item means it cannot be recovered. For example, if a folder with 10 items is undergoing disposition and one of the items is privilege deleted before disposition processing reaches it, a warning is displayed against the item. The item is gone and can never be recovered. Similarly, a physical object that is going to be destroyed, based on the disposition operation, will have a warning if it has not been marked for destruction. The Total Items with Actions column would display at least 1 action, possibly more, and that would be to have it marked for destruction.
Total Items Failed	x			The sum of all Items Failed in the collection of subwork orders spawned by a master work order. Indicates the number of items that could not be processed by a work order. Items that failed will be retried if the master work order is recovered.
Total Items Skipped	x			The sum of all Items Skipped in the collection of subwork orders spawned by a master work order, including the master work order. Two reasons for skipped items: 1) Work order was terminated 2) Operation determined that an item could not be acted on. For example, when disposing a folder, if a subfolder was not ready for disposition (retainer not in final phase), this would cause a skip.
Total Items with Actions	x			The sum of all Items with Actions in the collection of subwork orders spawned by a master work order. The number displayed indicates the number of actions you are prompted to take.

Column Heading	WOR	WOBR	WOIR	Description
Average Process Duration	x			<p>Indicates the average processing duration time of all the work orders in the collection of work orders spawned by the master including processing of the master itself. If a master work order has only folders to process, no processing time is spent on it, only on the reference work order spawned to process the documents in the folder. Only the documents in the folder are processed unless more subfolders (folder objects) are discovered among the documents. If so more work orders are spawned.</p> <p><i>Processing duration</i>, is the difference between the Start Processing Time and End Time or between the Start Processing Time and Wait Time or between Wait Time (the time waiting starts) and End Time of a work order. Processing durations are used to calculate the Average Processing Duration of a master work order. All work orders spawned by a master, including the master if it does any processing, are used in the calculation. A master work order will not have anything to process if only folders are selected for the request, unless both documents and folders are requested (selected) for the operation.</p>
Average Route Duration	x			<p>Indicates the average route duration time of all the work orders in the collection of work orders spawned by the master including routing of the master itself. The route duration time of a master work order is the time between its creation time and the time it was queued for processing.</p> <p>The <i>Route duration</i>, is the difference between the Route Time and Start Processing Time of a work order. Route durations are used to calculate the Average Route Duration of a master work order. All work orders spawned by a master, including the master, are used in the calculation.</p>

Column Heading	WOR	WOBR	WOIR	Description
Average Wait Duration	x			<p>Indicates the average wait duration time of all the work orders in the collection of work orders spawned by the master including the master itself.</p> <p>The <i>Wait duration</i>, is the difference between the Wait Time and Return Time. Wait durations are used to calculate the Average Wait Duration of a master work order. All work orders spawned by a master, including the master, are used in the calculation. Wait and return times are relevant only if the requested items are documents and folders. If the folder requested for example, has both documents and folders (subfolders), a wait time is registered while contents of the subfolders are processed. A return time is registered when the system returns to process the immediate documents of the folder requested. Depending on a configuration setting for each of the supported operations, it might be that the documents get processed before the folder. The processing order defined for each operation is based on the <code>before_children</code> or <code>after_children</code> setting.</p>
Elapsed Time	x			The elapsed time is the entire time taken to create and process a master work order and all of the work orders spawned from it or that in other words, is in its collection of subwork orders. It is basically the difference between the End Time and the Start Time .

Column Heading	WOR	WOBR	WOIR	Description
Last Update Time	x	x		Shows the last time any running work order was updated. (The value displayed is based on the work order that was the last one to provide an update. A work order that has a Processing Status of <i>Running</i> with a value for the last update time that is not so recent compared to the current time, means that processing has for one reason or another, stopped. A difference of an hour for example, between the current time and that shown for the last update time should alert you to take recovery action. The interval should typically amount to only minutes or possibly seconds, not hours. If you click the Report button and see that the last update time occurred 10 minutes ago, wait a couple of minutes and click the Report button again to see if a new update time is registered. The last update could be from any one of the work orders in the collection spawned from the master or from the master itself. This column can be monitored for regular updates.
Maximum Process Duration	x			The longest time taken to process a work order in a collection of work orders.
Maximum Route Duration	x			The longest time taken to route a work order in a collection of work orders.
Maximum Wait Duration	x			The longest time a work order waited in a collection of work orders.
Number of Work Orders	x			The number of work orders spawned by a master work order.
Object Id	x	x		All work order objects created or spawned are assigned a unique id.

Column Heading	WOR	WOBR	WOIR	Description
Process Duration	x	x		<p>The length of time taken to process a master work order, specifically the immediate documents, not the documents of subfolders if the request includes any subfolders. This includes time taken to create the master work order, the time taken to spawn any subwork orders, and the time taken to process the immediate documents, if any. Processing is virtually 0 if there are no immediate documents to process in the master. If the requested object for an operation is a folder with only subfolders and no documents, the master has no documents to process, only work orders to spawn. The Elapsed Time however, which implies total processing duration, also accounts for the processing of any subwork orders (and their documents). The Elapsed Time is therefore always greater than the Process Duration.</p> <p>The time is displayed in units of seconds as s, minutes as m, hours as h, and possibly days as d. For example, 6s means 6 seconds, 3m 48s means 3 minutes and 48 seconds, 1h 3m 48s means 1 hour 3 minutes and 48 seconds, 2d 1h 3m 48s means 2 days 1 hour 3 minutes and 48 seconds.</p>

Column Heading	WOR	WOBR	WOIR	Description
Processing Status	x	x		<p>Displays the current processing state of a master work order.</p> <p>A work order with a completion status of <i>Processing</i> can have a Processing Status of:<i>Created</i> - a master work order is created. <i>Routed</i> - the master work order is queued, on Records Queue Manager. <i>Running</i> - the master work order is being processed. <i>Waiting</i> - a work order, master or any subwork orders (spawned from the master), shows it is in waiting regardless of whether the items associated with the parent are processed first or whether the items associated with the children are processed first. For example, a folder that contains documents and a folder. Either the documents in the parent folder are processed first or that of the subfolder. Either way, one of the folders waits until the other is processed. <i>Completed</i> - processing of the master work order has finished.</p> <p>The Processing Status can be determined from the Properties of a work order when you right-click a master work order and select Show all properties.</p>
Return Time	x	x		<p>The time at which a work order returns to process those items based on the before or after children setting selected for each operation.</p> <p>The Return Time and Wait Time are related in the sense that while one set of items is under processing the other set waits idling until the system returns to process them. Although work orders are processed concurrently, items in the work order are processed serially.</p>
Route Duration	x	x		<p>The length of time a work order spends on the queue before being taken for processing. It is the difference between the Route Time and the Start Process Time.</p>
Route Time	x	x		<p>The time at which a work order is queued.</p>
Start Process Time	x	x		<p>The time at which a work order is taken off the queue for processing.</p>
Wait Duration	x	x		<p>The time a portion of the items in a work order spend waiting while other items in the work order are being processed. The items that are in waiting start to be processed upon the Return Time.</p>

Column Heading	WOR	WOBR	WOIR	Description
Wait Time	x	x		The time at which the items in a work order start to wait while other items get processed before the system returns to process them. See further details in the Return Time.
Items Failed		x		The number of items in a subwork order that could not be processed successfully.
Items Skipped		x		The number of items in a subwork order that processing could not get to. Refer to Total Items Skipped for further details.
Skipped			x	Indicates whether the item bypassed processing or not by displaying Yes or No.
Items Successful		x		The number of items in a subwork order that processed successfully.
Items Warned		x		The number of items in a subwork order that had a warning.
Items with Actions		x		The number of items in a subwork order that have preliminary or follow up actions to be performed.
Number Processed		x		The number of items in a subwork order that were actually processed, taken off the queue.
Number to Process		x		The number of items in a subwork order that will have to be processed, put on the queue.
Type		x	x	For the breakdown report, identifies the type of subwork order spawned by a master work order, as either a partitioned or reference work order. On the item report, it represents the type of item that was acted on.
Name			x	The name of the primary objects that were requested (selected) against an operation.
Parent Folder			x	Identifies the path and folder from which the primary objects were selected for an operation.
Skipped			x	Indicates whether an item was processed or not.
Primary			x	Indicates whether an item is the primary item or not. Only the primary objects in a request are displayed unless the Show All Descendants filter is selected.
Result			x	Indicates whether the item was successfully processed or not. The result can be <i>Success</i> or <i>Failure</i> .

Column Heading	WOR	WOBR	WOIR	Description
Message			x	<p>Displays the message that is associated with the Result. For example: [An exception was encountered while processing this reference work order, [DMC_RPS_PRIVILEGE] User does not have proper privilege to Apply Hold Retention Markup], could be the message displayed for the Process Retention Markup operation that resulted in a <i>Failure</i>. If there is an action to be performed, it would be displayed in the Action Item column.</p> <p>Limited to 450 characters. If longer than 450 characters, view the results of the corresponding work order that processed this item to see the full message (and any associated exceptions).</p>
Action Item			x	Any action that needs to be taken, whether the operation fails or succeeds, would be displayed in this column.

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

You can also right-click a work order and select **Properties** to view its results. The properties of a work order include the following tabs:

- Info
- Permissions
- History

3. Optionally, to recover a work order, right-click a work order which has a **Completion Status** of either *Partially Succeeded* or *Failed* and a version label which indicates that it is current, and then select **Work Order Action > Recover**. Only failed or partially succeeded work orders that are current, are eligible for recovery. The label displayed in the **Version** column should indicate *CURRENT* next to the version number for the selected work order. For example, 1.0,CURRENT, 2.0,CURRENT, and so on.

Recovery attempts to reprocess all failed items in whatever work orders processed them. FAILED and PARTIALLY_SUCCESSFUL work orders are candidates for recovery. A new version of the master is created for each recovery performed. The **Completion Status**, as a result, should change to *Processing* and then eventually to *Succeeded*, if all goes well. The recovery however, could fail again or could be partially succeeded. Therefore, perform the recovery against each new version until recovery succeeds.

The other work order actions, regardless of the **Completion Status** against the selected work order, allow you to view the input, results, breakdown, and

aggregate results. These four work order actions are displayed in the list box as **View Input**, **View Results**, **View Breakdown**, and **View Items**.

- **View Input**, displays an XML report of the items that the work order is acting on as well as the input parameters associated with a particular operation. Input parameters associated with the **Process Records Policy** operation for example, would identify the affected objects and the policy that is being applied or removed.
- **View Results**, displays an XML report that lists the details against all of the items the work order acted on. Although it is possible to view the results in any of the reports, the XML reports provide further details. In a promotion operation for example, you can determine the retainer Id along with the phase the retainer is promoted from and the phase it is promoted to. In a qualification operation, you could similarly determine the retainer Id along with the phase it was qualified in and the qualification date.

The number of items skipped, if there are any terminated work orders for example, is also listed. The count in the results against items skipped pertains to the primary objects in the request. For example, if there are 5 items requested for an operation, 2 folders and 3 documents for instance, and the master work order timed out (never updated its status), only the 5 items would be listed. Items in the 2 folders would not be counted. For apply/remove policies and markups, reference work orders are created and if any are terminated, each reference work order would add to its skipped count, the number of immediate children.



Note: For an example of both XML reports, refer to [Appendix D, XML Report examples against View Input and View Results on page 763](#).

- **View Breakdown**, opens the **Work Order Breakdown Report** which allows the user to drill into a collection of work orders. For example, on the **Work Order Report** you can select a master work order and select **View Breakdown** to display all of the work orders in its collection. When viewing the results in the breakdown you can then select a work order in the breakdown report to continue drilling into the collection of work orders associated with a subwork order. All of the work orders that belong to a collection have the same **Master ID** as that of the master selected. All of the columns displayed for the **Work Order Breakdown Report** are described . The same columns displayed for the **Work Order Report** can be displayed for the **Work Order Breakdown Report**. The filters on the **Work Order Breakdown Report** are described in [“All work order reports filter descriptions” on page 57](#).
- **View Items**, opens the **Work Order Item Report** which allows the user to view the items in a master work order or in a subwork order.

All five menu options are available only if the selected work order is a master work order. Only the first two options are available if the selected work order is either a partitioned or reference work order. Both partitioned and reference work orders can be referred to as subwork orders. The master and its subwork orders can be called a collection of work orders.

Work orders in search results or wherever they are visible, whether you use the Records Client, Documentum Webtop (if it is records enabled), or the Work Order Report, allow right-click capability.

The **Delete** menu option is available against only the *CURRENT* versions. All versions of a master work order that are not CURRENT can only be deleted when the CURRENT version is deleted. The **Delete** option is therefore not displayed for versions other than the CURRENT version. Work order administrators can delete a CURRENT master work order if its **Processing Status** is *Completed*. Users can only delete CURRENT master work orders that have a **Completion Status** of *Succeeded*.

4. Optionally, to export all of the results reported to CSV or to export results against only one or more selected work orders, click **Tools > Export to CSV** or **Tools > Export Selected Row to CSV**.

3.2 Setting column preferences

Column preferences functionality associated with the records products can be used to control an administrator's or end user's personal view of what results to view and the order in which to view them. Columns can be added and removed as necessary and can also be organized from left to right as necessary. Column preferences is available with the following features:

- Qualification manager
- Promotion manager
- Disposition manager
- Barcode manager
- All of the reports
- Commonwealth files
- Commonwealth file parts

To modify the attributes displayed in the content pane, select the column preferences icon to the far right of the column headings. You can add to the columns that are displayed by default and reset to the defaults when necessary, using the **Reset to defaults** button. Any column width by default, in any of the reports, will display a string of up to 50 characters. If results include more than 50 characters, you can stretch the column header to the right to expose the rest of the string.

3.3 Records auditing

Audit procedures that are common to Retention Policy Services and Records Manager are documented in this section:

- “Overview of auditing” on page 78
- “Enabling auditing” on page 80
- “Configuring the audit policy (to prevent purging audits until archived)” on page 82
- “Verifying auditing of an event” on page 84
- “Viewing and removing an audit” on page 85
- “Archiving audits (declaring as formal record)” on page 85

Audit events are listed and described in the product-specific parts of this document, and in the online help that matches this document:

- “Records Manager audit events” on page 441
- “RM Commonwealth audit events” on page 464
- “Retention Policy Services audit events” on page 281
- “Physical Records Manager audit events” on page 533

An Audit Trail Report is also available to report against audit events of all the records products. To run the Audit Trail Report, refer to “Running the audit trail report” on page 272.



Note: The Audit Trail Report can be used to declare a formal record of the audit trails reported.

3.3.1 Overview of auditing

Auditing of the records events, which consists of Retention Policy Services events, Records Manager events, Records Manager Commonwealth Edition events, and Physical Records Manager events, rely on Retention Policy Services. Retention Policy Services is the base regardless of the Records Client product purchased.

You can register audit events to track the value changes of attributes. For example, on a system dm_save event, leave the Application Code empty. Select the Include all subtypes checkbox if necessary. Click the Select Attributes link. Then select the required attributes from the resulting locator.

Auditing is primarily done through the auditing framework built into Documentum CM Server. For a more detailed discussion of the framework, refer to the *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS-AGD)*.

There are two types of audit events from the perspective of Documentum CM Server: *system events* and *application events*. System events are defined by

Documentum CM Server and are recognized automatically by Documentum CM Server (for example, checkin, save, destroy). These usually have dm_ prefixes. The list of auditable system events can be found in Appendix B of the *OpenText Documentum Content Management - Foundation Java API Development Guide (EDCPKCL-DGD)*.

All application events of the records products are distinguished from one another based on prefixes assigned to the beginning of the audit events. Retention Policy Services audit events are defined with dmc_rps_ prefixes, Records Manager with dmc_rm_ prefixes, Records Manager Commonwealth Edition with dmc_rmc prefixes, and Physical Records Manager with dmc_prm_ prefixes. Application events are categorized according to the Application Code they belong to, as follows:

- All Retention Policy Services and Physical Records Manager audit events prefixed with dmc_rps and dmc_prm can be enabled against the Application Code = dmc_rps.
- All Records Manager audit events prefixed with dmc_rm can be enabled against the Application Code = dmc_rm.
- All Records Manager Commonwealth Edition audit events prefixed with dmc_rmc can be enabled against the Application Code = dmc_rmc.

Each part of this document (or, in online help) provides a chapter that lists the audit events for the product it covers:

- “Records Manager audit events” on page 441
- “RM Commonwealth audit events” on page 464
- “Retention Policy Services audit events” on page 281
- “Physical Records Manager audit events” on page 533

For any event (both system and application) to be audited, the event must be enabled (registered) in the repository used by the application. A registry is created in the repository in the process. Audit events must be enabled using Documentum Administrator.

Auditing gathers statistics relating to actions performed by the respective application. Use Documentum Administrator to configure auditing for a particular product. To view audit trails however, use the Retention Policy Services Audit Trail Report feature. “[Running the audit trail report](#)” on page 272 provides information for reporting an audit trail against Retention Policy Services events.

For information about Documentum Administrator auditing, refer to *Audit Management of the OpenText Documentum Content Management - Administrator User Guide (EDCAC-UGD)*.

3.3.2 Enabling auditing

An audit trail is generated only when an audit event is enabled/registered and the event has occurred. Audit trails can also be archived and/or purged once the schema for dm_audit_policy is activated. To activate the dm_audit_policy schema, refer to “Configuring the audit policy (to prevent purging audits until archived)” on page 82. Although you can view audits in Documentum Administrator, use Retention Policy Services to run an audit trail report. To run an audit trail report, refer to “Running the audit trail report” on page 272.

Auditing is enabled from the Documentum Administrator user interface. Once enabled, audit trails are logged against the events selected when the event is run.

After auditing is enabled, you can report on audit events generated by the system. A report can be generated by either of two means :

- Retention Policy Services reporting feature (Records > Audit Trail Report)
- Documentum Administrator audit trail report feature (Audit Management > Search Audit)

To enable auditing:

1. Log in to the repository through Documentum Administrator.
2. Navigate to **Administration > Audit Management**.
3. Click **Manage Auditing by Object Type** in the content pane. If the link is inactive, the user account must be assigned the **Extended Privilege of Config, View and Purge Audit**.
4. Select the object type, for the events that you want audited, from the list displayed in the locator and click **OK**. The object selected for this step represents the Target Object for each of the audit events listed for a records product, Records Manager, Records Manager Commonwealth Edition, Retention Policy Services. You can clarify this by referring to any one of the tables that list audit events.

The **Register Audit** screen is first displayed with the selected target object type. If necessary, you can click **Select** to change the target object type.

5. Click **Add Audit** to select one or more events associated with the selected target object type.

The **Register Audit** screen refreshes displaying options to select one or more events for the selected target object type.

6. Type in the appropriate value for the **Application Code** according to following guidelines:
 - For Retention Policy Services audit events, type *dmc_rps*.
 - For Physical Records Manager audit events, type *dmc_rps*. Physical Records Manager and Retention Policy Services share the same application code.

- For Records Manager audit events, type *dmc_rm*.
- For Records Manager Commonwealth Edition audit events, type *dmc_rmc*.
- For system events, leave it empty.

You can select a particular lifecycle related to Retention Policy Services and also target a specific state or phase of the selected lifecycle. A specific attribute associated with the selected event can also be selected.

The checkboxes can be ignored. Select **Include all subtypes** when the target object type selected is *dm_sysobject*.

7. Click **Add** to select/add an event.

The **Event Filter** on the resulting **Choose an event** locator is set to **All Events** by default. Select **Custom Events**. If necessary, change the **Items per view** to see more of the list when the list is large and spread across more than one page.

8. Select all the events needed and click **OK** on the locator to accept the selections. Selections accepted from the locator are listed in the Register Audit screen. You can add more events to the object type already selected or click **OK**.

Increase the number of items shown per page if you cannot see all your selections listed. Although the events you selected could consist of both custom and non-custom events, you can change the view from **All Events** to view only **Custom Events** if necessary.

9. Click **OK** when you are done adding all the events needed for the selected object type.

The **Register Audit** screen is again refreshed summarizing the events for each object type added.

You can register events against a different application code for the same object type when you click **Add Audit**.

For a complete list of audit events associated to a particular records product, click the appropriate link:

- “Records Manager audit events” on page 441
- “RM Commonwealth audit events” on page 464
- “Retention Policy Services audit events” on page 281
- “Physical Records Manager audit events” on page 533

10. Click **OK** to register the events listed.
11. Repeat the procedure starting at step 3 only if you have to register events for a different object type.

3.3.3 Configuring the audit policy (to prevent purging audits until archived)

Audit trails can be archived and/or purged from a repository once the dm_audit_policy schema is activated. The dm_audit_policy schema supports:

- The ability to archive and purge audit trail entries.

To archive audits, refer to “[Archiving audits \(declaring as formal record\)](#)” on page 85.

To activate the dm_audit_policy schema:

1. On the Documentum CM Server, determine if the schema is already activated or not through this query:

Special configuration is required to enable the schema required for audit trail purge prevention:

```
select * from dm_audit_policy
```

If the query returns something, even an empty result set, then the schema is activated.

If the query returns nothing, then activate the schema by performing one of the following substeps:

- a. Run the following IAPI command on Documentum CM Server against your repository:

```
apply,c,NULL,APPLY_D66_SCHEMA_CHANGES,START_VSTAMP,I,O
```

- b. Run the ondemand_schema_changes.ebs script located at DM_HOME/bin using this command:

```
dmbasic -f dm_ondemand_schema_changes.ebs -e Entry_Point --  
docbase_name docbase_user user_password
```

2. Log in to the Records Client as a super user and create a user, *author 7* for example, with privileges as shown in [Figure 3-6](#):

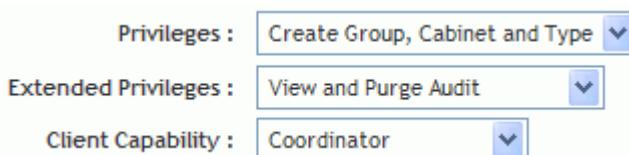


Figure 3-6: Audit trail user privileges

3. Add the user to dmc_rm_recordmanager role.
4. Log in to Documentum Administrator as the install owner and from the Audit Management page select **Audit Policies**.

5. On the **Audit Policy Properties** page, create an audit policy for the user created in step 2, *author 7* for example.

An instance of the Documentum CM Server object type *dm_audit_policy* is created, part of the schema activated in step 1. A policy is created that allows only its members to purge audit trail events based on certain attributes of *dm_audittrail* objects.



Note: The Records Manager system changes the value of the *i_is_archived* attribute of *dm_audittrail* to *True* after an audit trail report containing that audit trail event is successfully declared as a formal record.

When the schema of step 1 is activated, the server prevents purging of audit trail events. Only users or groups named as an accessor of a *dm_audit_policy* object can purge an audit policy when the attributes of the *dm_audit_trail* have values equal to what the *dm_audit_policy* specifies.

The Documentum CM Server (system) may not automatically prevent the purging of audit trails when the *dm_audit_policy* schema is activated. Purging is dependent on the *i_is_archived* attribute setting on both the schema object and the audit trail object. The system does not prevent users or groups, members of the policy, from purging if *i_is_archived* on the schema (policy criteria) is set to *True* when the audit trail has it set to *False*. The value for the *i_is_archived* attribute on both these objects must be set to *False* to prevent any purging.

The name of the audit policy has no material effect on the business logic of purging audit policies. A user can choose any name when creating and configuring an audit policy.

6. From Documentum Administrator configure and activate some audit events as follows:

- a. Go to the **Administrator Access** node and grant the Records Manager (*dmc_rm_recordsmanager*) **Audit Management** capabilities.

The system is now ready for testing.



Note: Make sure that users who declare formal records from audit reports, and who purge audit events are not super users or system administrators.

To run an audit trail report, refer to “[Retention Policy Services audit events](#)” on page 281.

3.3.4 Verifying auditing of an event

There are two ways to verify if an application event was audited. One is through the Properties screen of the audited object. The other is through the Search Audit facility of Documentum Administrator.

3.3.4.1 Verifying the auditing of an event using the properties screen

To verify auditing of an event from the properties of an object:

1. Right-click the object against which you ran the audit event and select **Properties**.
2. Click the **History** tab. All audit events ever performed against the object are displayed along with the details. If nothing is listed, it could mean that the object never experienced an audit event or that no audit events have been enabled.
3. Click **OK** or **Cancel**.

3.3.4.2 Verifying the auditing of an event through the search audit of Documentum Administrator

Documentum Administrator is helpful in the case of an audited event against an object that has no properties GUI. Objects that have already been removed from the repository (for example, disposed) can also be listed from Documentum Administrator. Documentum Administrator also has a facility that allows you to search the audit trail table.

Documentum Administrator also displays details that are not shown in the history tab.

To verify auditing of an event using search audit:

1. Navigate to **Administration > Audit Management** and select **Search Audit** in the content pane.
The **Search Criteria** screen allows you to search either by **Search Criteria** or by **DQL**.
2. Using the **Search Criteria** option, selected by default, specify the parameters for the audit trail you want to see and click **OK**. Select an event for example, and click **OK** to keep it simple, or refine the search criteria using a combination that narrows the query.
Audit trail entries are listed that satisfy the criteria. Select **Properties** of any entry to view more details.

3.3.5 Viewing and removing an audit

A list of audits can be obtained for viewing. Using the **Unaudit** feature, you can stop or remove an audit. Use this procedure to view or remove an audit.

To view or remove an audit:

1. Navigate to **Administration > Audit Management** and select **Manage Auditing by Object Type** in the content pane.

2. Select **dm_sysobject** in the locator displayed and click **OK**.

The **Register Audit** screen is displayed listing all existing audit events that are registered against **dm_sysobject**. If audit events are registered against dmc_rps and dmc_rm application codes, two listings of audit events would be displayed for dm_sysobject. Physical Records Manager audit events, prefixed with dmc_prm, are listed with Retention Policy Services audit events.

3. Click **dm_sysobject** listed under the **Object Name** column and click **Edit**. The **Register Audit** screen is refreshed and now provides **Add** and **Remove** buttons.

4. Select the events you would like to remove from the registry and click **Remove**.

The screen refreshes and the selected event is no longer displayed in the registry.

5. Click **OK** to accept the changes or **Cancel** to ignore the changes.

3.3.6 Archiving audits (declaring as formal record)

This functionality is only available if Records Manager is installed. This procedure is required if the audit policy has been configured to prevent purging audits until they are archived. To configure the audit policy refer to “[Configuring the audit policy \(to prevent purging audits until archived\)](#)” on page 82.

To archive audits:

1. Run the Audit Trail Report.

2. Specify your search criteria.

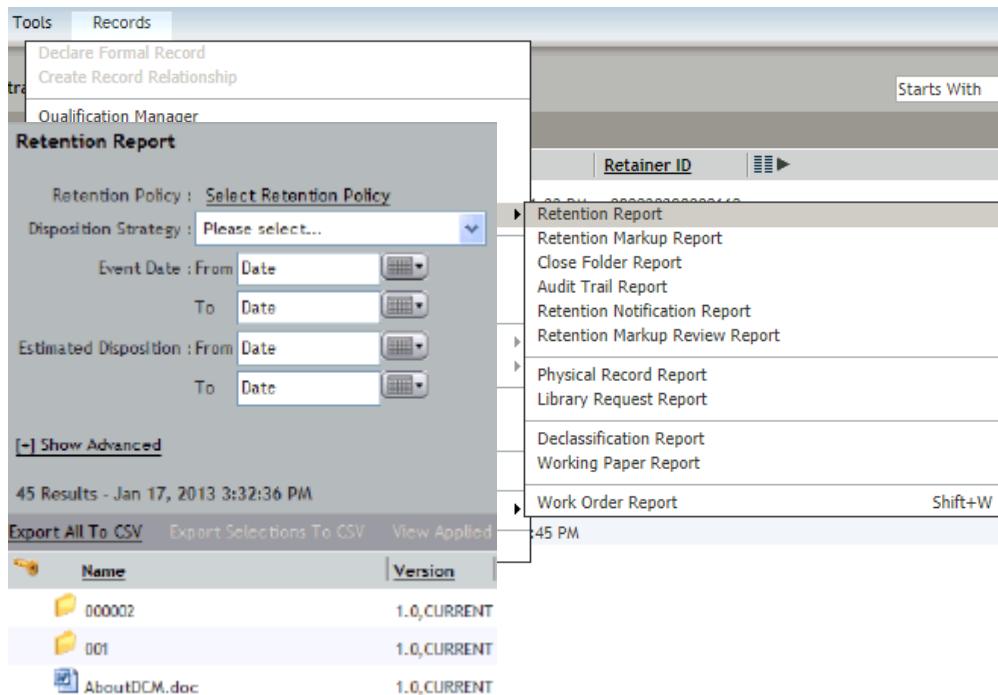
3. Click **Report**.

4. Click the **Declare formal Record** action and then follow instructions for declaring formal records, .

To verify that the audits have been marked Archived it is possible to choose a column preference that displays the Archived status.

3.4 Records reporting

All reports associated with the records products (Records Manager or Retention Policy Services) are accessible on the Records menu.



Note the following features on ALL records reports:

- Although all records reports always display the **Export All To CSV** action and makes it available by default, the other actions are displayed only when one or more results are listed. The other actions are made available depending on the items selected from the results.
- The number of results and the timestamp in the lower left corner is displayed only when the **Report** button is clicked, whether results are returned or not. If no results, **0 Results** is displayed along with the timestamp.

On the Work Order Breakdown Report and the Work Order Item Report, users can use the breadcrumb to navigate back to any subwork order in the breakdown report or item in the item report, without having to relaunch a particular work order report.

Users and administrators must be in the appropriate user role or administrator role to access the respective reports functionality. Members of an administrator role that is Retention Managers, Records Manager, and Physical Records Manager can generate any available report. Members of specific user roles have access to only certain reports as listed in the roles and functional access tables.

Reports on the Records menu are associated to Retention Policy Services, Records Manager, and Physical Records Manager as follows:

Retention Policy Services Reports:

- Retention Report
- Retention Markup Report
- Close Folder Report
- Audit Trail Report
- Retention Notification Report
- Retention Markup Review Report

Records Manager Reports:

- Declassification Report (if Department of Defense functionality is available, meaning that the Department of Defense standard and classified DAR files are installed)
- Working Paper Report

Physical Records Manager Reports:

- Physical Record Report
- Library Request Report

Follow this link “[Retention Policy Services reports](#)” on page 247 to run a Retention Policy Services report.

Follow this link “[Records Manager Reports](#)” on page 440 to run a Records Manager report.

Follow this link “[Physical Records Manager reports](#)” on page 524 to run a Physical Records Manager report.

To view job reports, use Documentum Administrator, refer to *Viewing Job Reports* in the *OpenText Documentum Content Management - Administrator User Guide (EDCAC-UGD)*. To run a job, refer to “[Records Manager jobs](#)” on page 445.

All of the reports have various filters to search the data and filter the results that matter to you.

3.5 Records Dashboard

3.5.1 Dashboard overview

The Records Dashboard is used to review the current status of the system (including several system reports). To view Records Dashboard, users must be a member of Retention Policy Services Retention Manager role. It consists of the following components:

- **Home:** Provides the option to quickly navigate to the job results for compliance check and overdue disposition, configuration objects, and reports. For more information, see “[About Home Page](#)” on page 88.
- **Policy:** Displays reports and charts that provide information about the number of items having a particular retention policy applied. For more information, see “[About Retention Policy Usages](#)” on page 89.
- **Markup:** Displays reports and charts that provide information about the number of items having a particular retention markup applied. For more information, see “[About Retention Markup Usages](#)” on page 89.
- **Items Overdue:** Provides reports and charts listing all those contacts who have charged out one or more physical items that are overdue for return. For more information, see “[Physical Items Overdue for Return](#)” on page 90.

The work order report can be accessed to view the items overdue for disposition and to identify all the non-compliant objects present in the Records-Managed docbases, which do not conform to the Retention Policy Services Retention policies/markup implemented on them.

3.5.2 About Home Page

Users can quickly navigate to the job results for compliance check and overdue disposition, configuration objects, and reports from the **Home** page. The Home page includes:

- **Compliance Check Job Result:** Displays the last three results from the compliance check job report (which includes the workorder number, items that were processed, successful (compliant), failed (non-compliant), and the completion date and time). For more information about the compliance check of objects, see “[Compliance Check of objects](#)” on page 90.
- **Overdue Disposition Job Result:** Displays results of the last three executions of the overdue disposition job (which includes the workorder number, items that were processed, successful, failed, warned, and the completion date and time).
- **System Configuration**
 - Retention Policy Services Configuration. For more information on the configuration objects, see “[Retention Policy Services configuration](#)” on page 119.

- Workorder Configuration
 - Workorder Operations Configuration. For more information on the workorder configuration and workorder operations configuration, see “[About the work order framework configuration object and each of the work order operation configuration objects](#)” on page 37.
 - Records Manager Configuration. For more information on the configuration objects, see “[Overview of Records Manager](#)” on page 311.
 - Physical Records Manager Configuration. For more information on the configuration objects, see “[Introduction](#)” on page 467.
- **Reports**
 - Work Order Report. For more information, see “[Work order report overview](#)” on page 51
 - Retention Report. For more information, see “[Retention report overview](#)” on page 248
 - Retention Markup Report, For more information, see “[Running the retention markup report](#)” on page 257
 - Physical Record Report, For more information, see “[Running a physical record report](#)” on page 524
 - Library Request Report, For more information, see “[Running a library request report](#)” on page 530

3.5.3 About Retention Policy Usages

The table and bar chart in the **Policy** component of the Records Dashboard provide information about the number of items that have retention policy applied. If the policy name is very long, then the table displays only the first 50 characters of the policy, and the tool tip displays the full name of the policy. The bar chart displays the first 15 characters. (applies to the bar chart tool tip also). Data in the table can be sorted in ascending order or descending order by clicking on the column headings **Retention Policy** and **Number of items**.

3.5.4 About Retention Markup Usages

The table and bar chart in the **Markup** component of the Records Dashboard provide information about the number of items that have retention markup applied. If the item name is very long, then the table displays only the first 50 characters of the item, and the tool tip displays the full name of the item. The bar chart displays the first 15 characters. (applies to the bar chart tool tip also). Data in the table can be sorted in ascending order or descending order by clicking on the column headings **Retention Markup** and **Number of items**.



Note: The number of items displayed in the Policy and Markup reports are those that have either directly applied or inherited retention policies or markups on them.

3.5.5 Physical Items Overdue for Return

The table and bar chart in the **Items Overdue** component in the Records Dashboard provide list of all those contacts who have one or more physical items overdue for return. If the item name is very long, then the table displays only the first 50 characters of the item, and the tool tip displays the full name of the item. The bar chart displays the first 15 characters. (applies to the bar chart tool tip also).

In the **Items Overdue Information** table, you can click on each contact name to obtain the detailed reports about the physical items overdue for that contact. The detailed report includes the location (current shipping address), the age (number of days/months/years overdue), recall date (if the item was recalled), and Barcode (if available). Physical items that are marked as lost are also displayed in the detailed report. Click on the breadcrumb to go back to the previous page.

3.5.6 Compliance Check of objects

Compliance Check job (that is, dmc_rps_ComplianceCheckJob) is a feature to identify the non-compliant items present in the repository.

The compliance check job considers an item as non-compliant if:

- The item has not inherited all the expected Retention Policy Services retainers from its parent folders
- The item has inherited one or more Retention Policy Services retainers, although it is not expected to inherit those retainers from any of its parent folders
- The item has not inherited all the expected Retention Policy Services retention markups from its parent folders
- The item has inherited one or more Retention Policy Services retention markups, although it is not expected to inherit those markups from any of its parent folders

The compliance check job scans only those items in the repository that satisfies the filter criteria selected in Records Check Configuration options when the job is executed. The results of execution of compliance check job can be obtained from Work Order Report. In the Work Order Report page, you can configure different filter settings (such as setting the 'Operation' filter to Compliance Checker) and then click **Report** to get the results of all runs of compliance check job.

If the completion status for a particular run of compliance check job listed in the work order report results is SUCCEEDED, it indicates that all the items scanned by compliance check job are compliant. But if the completion status is PARTIALLY_SUCCEEDED or FAILED, then it indicates that one or more items scanned for compliance are non-compliant.

For more details about the items processed by compliance check job during a particular run, open the 'Work Order Item Report' by selecting the **View Items** link for the corresponding row listed in the work order report results. The Work Order Item Report provides item-wise results of compliance checks executed by the

Compliance Check job. If the result displayed for an item listed in the Work Order Item report is SUCCESS, then it indicates that the item is compliant. But if the result displayed for an item is FAILURE, then it indicates that the item is non-compliant. The Result Messages column explains why an item is marked as non-compliant.

In the Work Order Item Report, you have the option to view only the non-compliant items, by setting the configuration options in COMPLIANCE_CHECKER Work Order Operation Configuration object. If the compliance check job is invoked with the 'Enable to Suppress Successful Work Order Results' checkbox selected in the properties page of COMPLIANCE_CHECKER Work Order Operation Configuration object, then the Work Order Item report will display only the non-compliant items. But, if the compliance check job is invoked without selecting this checkbox, then the Work Order Item Report will list all the items processed by the compliance check job, including the compliant and non-compliant items. For information about work order configuration object, see ["About the work order framework configuration object and each of the work order operation configuration objects" on page 37](#).

Regardless of whether this option is enabled during the execution of compliance check job, the complete results of compliance checks executed on all the items scanned by the job are available in the xml output associated with respective work orders that processed those items.

Chapter 4

Retention Policy Services

Retention Policy Services provides enhanced retention capabilities for electronic and physical record-keeping systems.

4.1 Introduction



Note: To avoid potential problems and unnecessary troubleshooting, make sure 1) that you are in the correct Retention Policy Services role for the operation you are attempting and 2) that the instance of the Records Client you are working on, is approved for Privileged DFC. Each instance of the Records Client must be Privileged DFC approved for any of the records products, Retention Policy Services, Records Manager, and Records Manager Commonwealth Edition, to work properly. To determine which Retention Policy Services role an administrator or end user has to be a member of for specific operations, refer to “[Retention Policy Services roles and functional access](#)” on page 108.

4.1.1 Determining which Retention Policy Services version you are accessing

From the File menu, you can determine which Retention Policy Services version you are connected to.

To determine which Retention Policy Services version you are accessing:

1. Click File > About Retention Policy Services.
2. After you view the information, click Close.

4.1.2 Administration components

Retention Policy Services consists of the following components. Components preceded by an asterisk are the administration components that appear under Retention Policy Services in the navigation pane. Functionality associated with all other components is available to both end users and administrators.

- *Base dates
- *Contacts
- *Authorities
- *Global conditions
- *Conditions

- *Retention policies
- *Disposition run bundles (although displayed when Department of Defense dars are installed, it can be turned on without Department of Defense dars for other purposes)
- *Retention markups
- Qualification Manager
- Promotion Manager
- Disposition Manager
- Retention report
- Close folder report
- Retention markup report
- Retention notification report
- Retention markup review report
- Audit trail report

4.1.3 About privileged clients and accessing repositories



Caution

Each instance of the Records Client application must be registered and approved for privilege. If OpenText™ Documentum™ Content Management Foundation Java API is registered, ensure that it has been approved. If a member in any of the records product roles logs in to a Records Client application that is not registered and approved for privilege, none of the records administration nodes (Retention Policy Services, Records Manager, Records Manager Commonwealth Edition, Physical Records Manager) or menu items will be available. Records functionality in the Documentum Webtop client is also disabled if the Documentum Webtop client is not registered and approved for privilege. Attempts to log in to a Records Client application which is not registered and approved for privilege will result in an error message being posted to the message log. No error message however is posted to the Documentum Webtop message log.

Administrators can use Documentum Administrator to make sure the Approved setting of the clients for those users not expected to create administrative components is set to *No*. Administrators can change this setting from the Properties of privileged clients listed in the content pane. The session listener also checks for Privileged DFC and provides a dialog to administrators immediately after they log in to Retention Policy Services, Records Manager, or Physical Records Manager on the Records Client.

The use of Privileged DFC is pervasive throughout the general Records application stack for all categories of operations. As such, it is a mandatory

requirement that the OpenText Documentum Content Management (CM) Foundation Java API instance that is being used to carry out the business functions, has been approved for privilege. Operations that require Privileged DFC are listed by category in Appendix B.

Why privileged clients are necessary

Privileged clients are necessary for use cases where business logic has to grant additional powers temporarily that are only needed for a brief period of time during certain operations. A classic example is when a user creates an object in a retained folder. The new object requires a retainer to be applied but a normal user is not expected to require the ability to apply retention directly to objects. An administrator has decreed that objects put into a folder (going into the future) must adhere to policies that they have decided. The end user's documents merely inherit this intent.

What determines the need for a privileged client

The Records Client for example, must be privileged if it is used to create or import objects into policy managed folders. Administrative components cannot be created unless the client is approved for privilege. You will need to use Documentum Administrator to list and approve the Foundation Java API instance for the desired client. You will also notice in the list, that the Foundation Java API instance for the Documentum CM Server may already be approved, as its Foundation Java API instance is pre-approved. Make sure to approve it however if it is not already approved. Administrators have to think long and hard about potentially giving a client extra capabilities that they normally do not have.

The Foundation Java API instance on the Documentum CM Server and the Application server for Records Client must be approved.

The Documentum Administrator user interface, as shown in [Figure 4-1](#), illustrates a listing of clients that have their Foundation Java API instance approved for privilege.

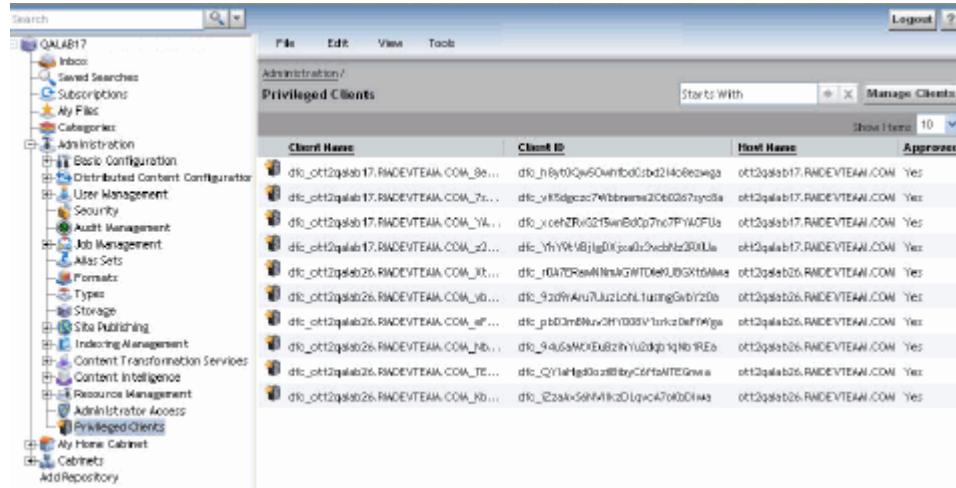


Figure 4-1: Approved clients listed on Documentum Administrator

The privileged clients listed are marked Yes under the Approved column if they have been approved. If you are having any difficulties trying to identify your client, refer to “[How to identify your Privileged DFC instance from other instances on the same host](#)” on page 715. The Documentum CM Server and Application servers listed in this example are all approved. If you do not see the Documentum CM Server or Application server listed in the Privileged Clients content pane for which you want to approve their Foundation Java API instances, click the Manage Clients button and add the desired clients to the Privileged Clients list from resulting locator screen. Their Approved status remains No until you right-click the client listed in the content pane and select Approve. For complete details, refer to Documentum Administrator documentation.

4.1.4 Setting up Retention Policy Services

4.1.4.1 Configuration options

The application configuration options for Retention Policy Services are described in “[Retention Policy Services configuration](#)” on page 119.

4.1.4.2 User preferences and column preferences

Use Preferences to make the Records Client user interface appear according to your personal needs.

To personalize your column preferences for certain features, refer to “[Setting column preferences](#)” on page 77.

Preferences provides the following tabs you can select from to customize your view of Retention Policy Services in the Records Client user interface.

To change your Preferences:

1. Click **Tools > Preferences**.

The **Preferences** screen appears exposing the following tabs:

- General
- Columns
- Virtual Documents
- Repositories
- Search
- Formats

2. Click the applicable tab for which you want to change the preferences.

Radio buttons, checkboxes, drop-down lists, as well as links such as edit links and locator boxes are provided as needed to facilitate your changes.

3. Apply your changes as needed in the applicable tabs.
4. Click **OK** to accept (save) the changes, or click **Cancel** to exit Preferences and ignore your changes.

4.2 Retention Policy Services administration

4.2.1 About Retention Policy Services functionality

Retention Policy Services is intended primarily to manage object retention in a OpenText Documentum CM repository. Using Retention Policy Services you can create retention policies and apply them to objects in a OpenText Documentum CM repository to control their aging and disposition within a lifecycle. A retention policy can have one or more phases plus a final phase to define a lifecycle. Retention Policy Services also includes capabilities to apply retention markups when necessary. Applying a hold for example, to halt the aging process until legal matters are resolved.

A retention policy determines the length of time an object (specifically a sysobject or sysobject subtype) is kept in a repository, according to operational, legal, regulatory, fiscal or internal requirements. Examples of objects include cabinets, folders and documents. An object remains in a repository for the duration of its applied retention policy. An object that is controlled by a retention policy cannot be deleted, nor can the original content be modified as we disable the check-in as same version feature. However, new versions can be created. Retention Policy Services provides the ability to create, edit, delete, remove or apply retention policies, as well as retention markups, create reports, and perform audits and searches. Retention Policy Services allows you to apply multiple retention policies to a single object or to apply a single retention policy to multiple objects.

4.2.2 Retention Policy Services



Note: Each records product is role based and therefore all users and administrators must be in the correct role for the expected functionality to work properly. It is equally important that each instance of the Records Client, which hosts each of the records products, is registered for Privileged DFC.

4.2.2.1 Overview of Retention Policy Services

4.2.2.1.1 Retention policies and lifecycles

A retention policy defines the template that contains all of the rules concerning aging. Use a retention policy to protect documents from deletion and to force them to undergo aging in a controlled manner.

Retention Policies are used to place a lifecycle on a document, to ensure that the document is protected and kept for a prescribed amount of time. Once the retention policy is applied, the end user can no longer delete as the document is now being managed in accordance with the lifecycle/retention policies.

A retention policy template is made up of a lifecycle that defines the phases in the policy. Six default retention policy lifecycles are supplied with Retention Policy Services to save you the task of lifecycle creation.

- 1 Phase + Final
- 2 Phase + final
- 3 Phase + final
- 4 Phase + final
- 5 Phase + final
- 6 Phase + final



Note: A lifecycle supporting a retention policy must not be deleted or renamed.

The defined stages or states of a retention policy are called phases. The Final phase is required in all retention policy lifecycles. Phases 1 through 6 are respectively labeled as follows. Each phase in the six Phase + final for example are named in this sequence:

- Active
- Semi-Active
- Semi-Dormant
- Dormant
- Inactive_1
- Inactive_2

There are seven standard disposition strategies (options) to choose from when creating retention policies; two extra NARA strategies if Records Manager and the Department of Defense Standard dar are installed:

- Unknown
- Review
- Export All, Destroy All
- Destroy All
- Export All
- Export All, Destroy Content
- Destroy Content
- NARA transfer, Destroy content
- NARA transfer, Destroy all



Note: The NARA transfer strategies are Department of Defense specific and only appear if you have installed the Standard Department of Defense dar (RM-DoD5015v3-Standard-Record.dar). Although the Department of Defense dars are optional, the Standard dar is mandatory for declaring Department of Defense formal records whereas the Classified dar is optional, required only if it is necessary to declare Department of Defense classified formal records.

[“Creating a retention policy” on page 156](#) describes the disposition strategies.

4.2.2.1.2 About retainers, lifecycle actions, and disposition actions

Lifecycle actions such as Email Notifications can be triggered on phase exit or phase entry when the retainer of an object is promoted. Regardless of the retention strategy specified for a retention policy, lifecycle actions work on retainers. Although the tendency is to think that it is the object under retention that ages and moves from one phase to the next, it is actually the retainer. Also, although disposition actions are performed only in the final phase, the object can only be disposed of when its retainer is in the final phase. In either case, it is technically the retainer and not the object it retains that ages and gets promoted.

4.2.2.1.3 About retainers and retention dates

[“Updating the estimated disposition date” on page 104](#)

Important points and advice regarding other sources for retention are included.

Although cascading of retention in a file plan is controlled by the retention strategy setting, the retention strategy, regardless of its setting, has no effect when retention is applied directly to a non-container object. A retainer is spawned and gets directly attached to the document, regardless of the retention strategy setting, if retention is directly applied to the document in a folder. Retention, however, when applied directly to a container object, folder for example, relies on the retention strategy

setting to determine whether content inherit their own retainers to age individually or age against one commonly shared retainer.

One or more retainers are created as a result when a retention policy is applied to an object. Objects in a folder for example, can end up aging individually with their own individual retainers or all together against one shared retainer based on the option selected for the Retention Strategy, Individual or Linked. Child objects in a container object typically inherit retention, linked or individual, from the parent unless, retention is applied directly to the content instead of the container. (Applying retention directly to) If an individual or linked type of policy is applied directly to a non-containing object, a direct retainer is applied. This setting takes effect only when retention is applied to container objects, to determine the inheritance strategy for aging the content.

Retention policies are phased based and each phase has a qualification date that is the earliest date on which the retainer can be promoted to the next phase. The qualification date is a calculated value that can include the duration of the phase and a cut-off period added to an entry date. The qualification date in the final phase is the earliest date where Disposition can be invoked. The qualification date is calculated upon phase entry; calculated whenever a retainer is created and recalculated whenever promotion to the next phase occurs. The qualification date however, is not calculated if one or more conditions specified for a phase are not met. The value for the Qualification Date attribute is set on the retainer not on the retained object. Each phase can have chronological or conditional or mixed aging. Chronological aging occurs immediately whereas conditional aging does not occur until an event (condition) has been fulfilled.

The qualification date is recalculated after each promotion of the retainer.

Qualification dates are calculated (against the retainer) and recalculated according to the following triggers:

- When the retainer is created as the result of applying retention to the object (chronological and mixed).
- When the retainer is suspended. When you remove a suspend relationship then the qualification date is then calculated based on the retention policy.
- When the retainer is re-qualified. If a policy phase duration is updated, then the administrator can use the qualification manager to requalify all objects that had been previously qualified.
- When the retainer is promoted (chronological and mixed).
- When an event date is fulfilled or modified (for a retainer) (chronological and mixed).

Qualification dates are NOT calculated for the following triggers:

- If the event date on the properties of a retainer is modified. All attributes are read-only unless an event is specified on the retention policy referenced by the retainer.

- It does not automatically requalify if a phase duration is changed, however it can be done automatically. This includes changes to the duration, cutoff values, and the event-based mixed mode settings.

These are the dates that can be seen when viewing a retainer, and that administrators need to know about:

- Entry Date
- Event Date
- Global Event Date
- Qualification Date
- Projected Disposition Date
- Application Date

Retention can be applied to an object from any of three sources:

- Retention Policy Services
- EMC Centera
- Documentum CM Server

Retention Policy Services retention is explained by this guide and follows its own particular process (qualification, promotion, and disposition) providing advanced GUIs for management.

Centera retention is a hardware solution for a file storage location. Centera retention can co-exist with Retention Policy Services retention, with different results depending on the mode setting for Centera. The following list itemizes the consequences when both Retention Policy Services and Centera retention are applied to the same object, depending on the mode Centera is set to:

- If Centera mode is set to Basic Edition:

Centera has no retention capability in this mode and therefore cannot cause a conflict with Retention Policy Services retention.

- If Centera mode is set to Governance Edition:

Centera retention if present takes effect. Retention Policy Services retention can also take effect and is independent. If Retention Policy Services wishes to destroy an object that also has Centera retention on it, it can do so using privileged delete or by the Disposition Manager when the force delete flag is checked. Retention Policy Services can effectively shorten the Centera retention.



Note: The capabilities definition in the Centera profile requires the upper case D for privileged delete to be set. A privileged delete or force delete from Retention Policy Services cannot be completed without this setting.

- If Centera mode is set to Compliance Edition Plus:

Centera retention applied in this mode is very strict. Retention Policy Services can only extend Centera retention. For example, If Centera has 5 years and Retention Policy Services has 1, you will not be able to destroy the object until 5 years. Privileged delete or an attempt to dispose with force delete have no effect in this mode.

Documentum CM Server retention has base capability provided by OpenText Documentum CM that prevents documents from being deleted. There is no GUI for applying Documentum CM Server retention and it can only be applied by using . This capability is very basic and does not have any of the advanced features of Retention Policy Services.



Note: *We strongly recommend not to use Retention Policy Services and Documentum CM Server retention on the same repository.*

Retention Policy Services does not manage retainers that are created through the Documentum CM Server API. It is recommended instead that the Retention Policy Services public API provided is used to create Retention Policy Services retainers programmatically if necessary.

The default retention value configured from Documentum Administrator on the content address store, dm_ca_store, is enforced at the storage level by Centera. Retention enforcement, if Retention Policy Services and Centera retention are applied, are out of sync whereby the Retention Policy Services retention policy, for example, positions a document for disposition processing at the software level but is prevented from being processed at the hardware level by Centera. Retention Policy Services has no knowledge of Documentum Administrator configured retention which is the default retention otherwise called Storage Based Retention (SBR).

Attribute values on an object for retention

- If customers are using Retention Policy Services, they should not set the i_retain_until field as Retention Policy Services will set it when it is appropriate.
- Setting the Retain Until (i_retain_until) by itself, without Centera applied and configured properly, does nothing. The i_retain_until field is calculated by the Documentum CM Server and passed onto storage aware devices. Retention Policy Services simply calls on the Documentum CM Server to execute its business logic to populate the field. This means that the i_retain_until date is set and controlled by the Documentum CM Server based on input from Retention Policy Services.

During the application of retention, directly or indirectly, when the retention is non-event based or the Repository has no Centera file stores, future date values for the applied retention (retainer) projected_disposition_date will be propagated to the i_retain_until date of the retained item, where those items do not already have a later date. Under certain circumstances, such as during a move inside Documentum Webtop based applications, past date values of the projected_disposition_date of the applied retention will not be propagated to the retained item.

- If Centera is configured to use the value from the `i_retain_until` attribute, setting the attribute will cause the object to be protected until that date. If Compliance Edition Plus mode is enabled there is no way to delete the object any sooner than the `i_retain_until` date. That date can only be set farther into the future once set.
- If Retention Policy Services is installed, a base date rule can be specified for a particular object type to use a date attribute on the object which Retention Policy Services will use to calculate the retention date on the retainer.

The retention date could be used or set as that date for the retention calculation. *Never set the `i_retain_until` date, as Documentum CM Server will automatically set or populate that date when it is prompted by Retention Policy Services.*

`a_retention_date` is explicitly reserved for use by Retention Policy Services, and is the field that should be used/viewed for any estimation disposition calculations. The following table differentiates the Retain Until date (`i_retain_until`) and the Estimated Disposition Date (`a_retention_date`):

Table 4-1: Retain until versus estimated disposition dates

	Retain Until Date (<code>i_retain_until</code>)	Estimated Disposition Date (<code>a_retention_date</code>)
When retention is applied	Set only if the retention policy is chronological or if all events on all phases are set at time of application. If the date calculated is not in the future, this value may not be set. Note, the value will not be set if the operation that causes retention to be applied is in a transaction. For example, moving an object into a retained folder using clipboard operations uses a transaction and the <code>i_retain_until</code> date will not be set. If re-qualification is done, the date will be pushed.	Is always set and is estimated based on the duration of all phases and of all retention policies. The value is set even if the operation causing retention to be applied is in a transaction.
Intended use	Meant for retention aware storage, such as Centera, that uses the date to guarantee that content is not destroyed until that date.	Is meant as a guide to indicate when an item could go through final disposition (if multiple policies are applied then it's the furthest date of all policies applied). Basically, an estimation on when an object may be up for disposition. The estimated date does take into consideration whether single or multiple retentions are applied.
Can the date be moved to an earlier date	No. In many cases an earlier date due to re-qualification will be ignored.	Yes

	Retain Until Date (i_retain_until)	Estimated Disposition Date (a_retention_date)
When all retention is removed	Cleared	Cleared
Auto-calculated	Yes	Yes

4.2.2.1.3.1 Updating the estimated disposition date

Retainer objects (dmc_rps_retaner) have an attribute called projected_disposition_date. This date can be affected in a number of ways:

- Application of retention.
- Removal of retention (the date will go away along with the retainer object).
- Promotion of a retainer. This includes supersede.
- Removing the last suspend record relation of a retained object if it results in the qualification of the retainer of the object.
- Setting the global event date of a retainer.
- Setting the phase event date of a retainer.
- Roll over to another retention as a result of disposition.
- Qualification of a retainer.
- Re-qualification of a retainer.
- Disposition of the children contained in a folder that is under structural linked retention. This causes a reset on the a_retention_date of the folder.
- Create two formal records. Make a suspend relationship between the two. Apply a conditional retention to the child. Set the event date to sometime in the future. No calculation should take place for estimated disposition date. Remove the suspend relation. Calculation for estimated disposition date should take place.
- Apply a conditional retention to a record. Apply a suspend relation to the record. Set event date. Should not get the date for Estimated disposition since it is suspended. Remove suspend record relation from a formal record.

There is an attribute on dm_sysobject called a_retention_date. a_retention_date of a sysobject will be managed and set by Records Manager based on a calculation of the latest of projected_disposition_date of all retainers protecting that object.

For cases involving application, removal and rollover of retentions, since the process of applying, removing and rollover of retention deals with one object at a time, there will not be a specific work order processing the evaluation and update of a_retention_date of dm_sys_object based on projected_disposition_date of retainers protecting the object.

For cases involving promotion, event date update, qualification and re-qualification, since the process of updating the a_retention_date may encounter a large number of

sys objects protected by the same retainer whose projected_disposition_date has changed, there will be a work order processor with operation name 'UPDATE_RETENTION_DATE'.

In cases of promotion, even date update, qualification and requalification, our implementation shall process the root object of the retainer outside a work order and rout a work order only if there are child objects affected by the changes to the retainer of the root object.

When considering possibility of child objects potentially affected by changes to projected_disposition_date of a retainer, we must examine dm_folder subtypes as well as VDMs, snapshots and Formal records.

From the UI, the a_retention_date of a sysobject will appear under the label Estimated Disposition.

4.2.2.1.4 Retention policy strategy

Retention policies are applied using one of two retention strategies: linked or individual. Objects in the folder age together with the folder if the retention policy applied to the folder is linked. Each object in the folder ages independently with their own separate retainers if the retention policy applied to the folder is individual. The folder itself is non-aging in this case.

All the objects age at the same rate, according to either the configured base date of the folder (for chronological aging) or the event date of the folder (for conditional aging). If you use the individual retention strategy and apply a retention policy to a folder containing objects, each object ages according to the configured base date of the object (for chronological aging) or the event date of the object (for conditional aging). A base date is mapped to a document/folder type using a base date utility. Each document or folder type (for example, dm_document) is mapped to a base date value.

Retention is applied to an object either through direct application of a retention policy or by inheritance through retention cascade, refer to "["Retention cascade"](#) on page 196" for additional details. Retention policies are applied to specific objects or documents, but cannot be applied to renditions of an object under retention. If you wish to protect renditions with the parent retention policy so that they also cannot be deleted, then use the Parent Rendition Rule in the retention policy and set it to All Renditions.



Note: Any policy that is directly applied to an object moves with the object whereas, any policy that is inherited is stripped from the object if it is moved to a new location. The new folder can have a different retention policy applied to it or none. Although Retention Managers can move retained documents from one folder to another, there are also three non-administrative move roles with specific move capability users can be put into when necessary:

- Move to Unretained Folder (dmc_rps_move_unretain_folder)
- Move to Any Retained Folder (dmc_rps_move_any_retain_folder)

- Move to Same Retained Folder (dmc_rps_move_same_retain_folder)

4.2.2.1.5 Retention markups

Sometimes special circumstances, such as a court order or an investigation, make it necessary to prevent disposition, which involves the destruction or final transfer of objects. There are five retention markups designated as follows:

- Hold: stops destruction of the objects. It prevents all retainers applied to the object from being eligible for disposition.
-  **Note:** When Hold is applied directly to the document, the document is not seen in the Disposition Manager page. If a child of a folder is under Hold, then the folder cannot be disposed.
- Freeze: stops the promotion of an object from one phase to the next phase. It prevents the retainers applied to the object from qualifying for promotion to the next phase in the retention lifecycle. It does not however prevent disposition of an object if it has already been promoted to the final phase.
 - Review: sends a notification (either an email or an inbox) to a named contact following a time period that you select.
 - Permanent: stops destruction of objects. Permanent is identical to a hold. The object is retained permanently unless this retention markup is revoked.
 - Vital: is a marker that can be used to designate which records are critical to the day-to-day operation of the business. It does not prevent disposition.



Note: Only the Hold and Permanent retention markups prevent an item from being disposed (destroyed or transferred). Hold or Permanent markups also prevent privilege deletes. Privileged Delete provides administrative ability (not for end users) to select an object under retention and delete it from any phase; before it can be disposed. Freeze only stops promotion. Review and Vital do not prevent promotion or disposition.

When an object is placed on hold, using the retention markup feature, the object can reach the final disposition phase, but will not be displayed within Disposition Manager as they cannot be destroyed or transferred. A hold prevents removing the retainer from the object (document or folder) and also prevents a privileged delete. The hold must be removed before such operations can occur. While holds prevent an object from being destroyed or transferred, they do not prevent an object from phase promotion. None of the date calculations are affected when an object is placed on hold. Single and multiple holds can be applied to an object. When holds are removed the object then becomes eligible for disposition.

Retention markups are applied at either the document or folder level. If **Cascades to Sub-folders** is checked, then any subfolders also get a markup. If unchecked, then only the documents contained in the parent folder receive the markup. There is only one markup in either case (cascading or not) and all items are related to this markup via inheritance. **Cascades To Sub-Folders** is deselected by default when you create a retention markup. For further details, refer to “[Retention markups](#)” on page 239.

4.2.2.1.6 Retention Policy Services navigation

You can access Retention Policy Services functions using the following navigation methods:

- In the navigation pane, select the Retention Policy Services node to access the following administration nodes:
 - Base Dates
 - Contacts
 - Authorities
 - Conditions
 - Global Conditions
 - Retention Policies
 - Retention Markups
- You can select the following Records menu options:
 - Declare Formal Record

You can only select this menu option if Records Manager is enabled, not if only Retention Policy Services is enabled.
 - Create Record Relationship
 - Qualification Manager
 - Promotion Manager
 - Disposition Manager
 - Reports
 - Apply Retention Policy
 - Apply Retention Markup
 - Privileged Delete

4.2.2.1.7 Virtual documents

Retention Policy Services provides functionality so that you can apply a retention policy to a virtual document. Retention Policy Services has an option called the virtual document retention rule that can protect the root only or the root and children with the retention policy. Refer to “[Virtual document retention rules](#)” on page 133 for more information on this topic.

4.2.2.2 Retention Policy Services roles and functional access

The records products are role based and therefore functional access is limited by the role a user is a member of. Members of the Retention Policy Services Retention Manager role for example, can access all Retention Policy Services functionality whereas members of other Retention Policy Services roles have varying degrees of access.

Role Administrator: administers and modifies role membership. There is no Retention Policy Services function access for this role. The only capability provided for this role is to modify role membership.

Retention Policy Services Retention Manager: an individual or group in this role is responsible for the creation, maintenance and application of retention policies. The Retention Manager is the only user with sufficient permissions to perform disposition, apply a permanent markup, and perform a privileged delete, which provides the ability to delete an object before its retention policy is completed. Retention Policy Services Retention managers can remove retention policies or unlink items from a retained folder and cause the inherited retention to be removed (or reset aging). Retention managers are granted permission to see the metadata on every item in the repository regardless of the ACL on the item. The Retention Manager has all the rights of the Compliance Officer, Power User and Contributor, as well as the overriding rights of disposition and privileged delete.



Note: The Retention Policy Services Retention Manager (dmc_rps_retentmanager) role should not be confused with the dm_retention_manager role which grants different privileges for items under retention. Retention Managers in the context of the records products implies Retention Policy Services Retention Managers.

Compliance Officer: an individual or group in this role has the ability to apply, edit and remove holds. Typically, the Compliance Officer is part of the organizational group that is aware of impending or ongoing investigations and must ensure that information is not prematurely destroyed or accidentally removed from the system. The Compliance Officer does not, however, have any disposition rights. Compliance officers (because they are members of the Retention Policy Services contributor role) can have retention applied through inheritance by linking into a retained folder.

Power User: an individual or group in this role has the ability to assign retention directly to an object, as well as the basic permissions of the Contributor, such as putting an object into a folder that has a retention policy applied. The Power User also has the ability to perform limited functionality within the retention policies, including the ability to apply event dates. Power Users do not have the ability to apply holds or invoke dispositions and cannot change conditions. Power users (because they are members of the Retention Policy Services contributor role) can have retention applied through inheritance by linking into a retained folder.

Contributor: an individual or group in this role has the ability to move objects into a folder that has a retention policy applied to it. A Contributor may not be aware that the folder has retention applied to it, or that by moving objects into a folder with

retention applied, they are applying retention to an object. A member that is only in the Retention Policy Services Contributor role cannot move items out of a retained folder.

Notes

- You cannot link into a retained folder (causing retention to be inherited) unless you are in the Retention Policy Services Contributor role. Most users should be made members of that role.
- Internal roles, considered atomic roles, for the system must never be modified or deleted. Customers must ignore and avoid touching internal roles.

Internal roles specific to Retention Policy Services are prefixed with dmc_rps_i.

Internal roles specific to Records Manager are prefixed with dmc_rm_i.

Internal roles specific to Physical Records Manager are prefixed with dmc_prm_i.

Internal roles specific to Records Manager Commonwealth Edition are prefixed with dmc_rmc_i.

To search and list roles, and to determine their descriptions, navigate to Administration > User Management > Roles. Enter search criteria based on the role name and click the search arrow.

[“ACL names and roles” on page 110](#) provides the access control list (ACL) names and corresponding Retention Policy Services roles and rights. The numbers in parentheses represent the ranking of the rights from 1-7, where 7 represents the permission with the most rights.

Table 4-2: Access permissions list

Access Permission (permit name)	Ranking
None	1
Browse	2
Read	3
Relate	4
Version	5
Write	6
Delete	7

Table 4-3: ACL names and roles

Object ACL name	Retention Policy Services roles/rightsThe numbers in parentheses are required to set rights in a repository or through a dar.					
	Retention manager	Compliance officer	Power user	Contributor	Work Order Administra tor	Work Order User
rps_system_config_acl	delete (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
rps_retentionpolicy_acl	delete+ (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
rps_condition_acl	delete+ (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
rps_retained_acl	delete+ (7)	relate+ (4)	write+ (6)	relate+ (4)	browse (2)	browse (2)
rps_event_acl	delete+ (7)	relate (4)	write+ (6)	relate (4)	browse (2)	browse (2)
rps_authority_acl	delete+ (7)	browse (2)	write+ (6)	browse (2)	browse (2)	browse (2)
rps_retention_markup_acl	delete+ (7)	delete+ (7)	browse (2)	browse (2)	browse (2)	browse (2)
rps_contact_acl	delete+ (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
rps_basedate_acl	delete+ (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
*dmc_rps_childstrategy_acl	delete (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
*dmc_rps_disposition_method_acl	delete (7)	browse (2)	browse (2)	browse (2)	browse (2)	browse (2)
dmc_rps_work_order_acl	delete+ (7)	none+ (1)	none+ (1)	none+ (1)	delete (7)	none+ (1)
*dmc_rps_work_order_config_acl	delete (7)	browse (2)	browse (2)	browse (2)	delete (7)	browse (2)
*dmc_rps_work_order_host_fdr_acl	delete (7)	browse (2)	browse (2)	browse (2)	delete (7)	browse (2)



Note: + denotes the ability of a role or group to create an object of this type.

* denotes an object that cannot be manipulated.

"[Roles in Retention Policy Services and functional access](#)" on page 111 provides a list of function access names and their corresponding Retention Policy Services roles.

Table 4-4: Roles in Retention Policy Services and functional access

Functions in Retention Policy Services	Retention Policy Services role attribute
Retention Manager (RM)	dmc_rps_retentionmanager
Power User (PU)	dmc_rps_poweruser
Compliance Officer (CO)	dmc_rps_complianceofficer
Vital Records Administrator (VRA)	dmc_rps_vitalrecordsadministrator
Contributor (CONT)	dmc_rps_contributor
Disposition Configurator	dmc_rps_disp_configurator
Work Order Administrator	dmc_rps_work_order_admin
Work Order User	dmc_rps_work_order_user
Role Administrator (RA)	dmc_rps_roleadministrator
Role Architect	dmc_rps_rolearchitect
Owner Delete	dmc_rps_ownerdelete
Close Folder	dmc_rps_close_folder
Re-open Foder	dmc_rps_reopen folder
Move to Unretained Folder	dmc_rps_move_unretain_folder
Move to Any Retained Folder	dmc_rps_move_any_retain_folder
Move to Same Retained Folder	dmc_rps_move_same_retain_folder
<p>Note: The Move to Unretained Folder, Move to Any Retained Folder, and Move to Same Retained Folder concerns moving a retained object, that is currently inheriting its retention, to another location where: 1) The target location does not have a retention policy associated with it 2) The target location has any retention policy associated to it 3) The target location has the same retention policy as the original source location. In all cases, when the object is moved, the original inherited policies are removed.</p>	
All Retention Policy Services roles require that the user has at least Contributor client capability.	

Table 4-5: Roles in Retention Policy Services and functional access

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Retention Policy Services administration actions						
Create/Modify/Delete Base Dates	Yes	No	No	No	No	No
Create/Modify/Delete Contacts	Yes	No	No	No	No	No
Create/Modify/Delete Authorities	Yes	No	No	No	No	No
Create/Modify/Delete Conditions	Yes	No	No	No	No	No
Create/Modify/Delete Retention Policies	Yes	No	No	No	No	No
Create/Modify/Delete Retention Markups  Note: CO role cannot create, delete, apply, or remove permanents.	Yes	No	*Yes	Yes (vital and review only)	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Create/Modify/Delete Addresses  Note: Physical Records Manager Inventor y Managers can also affect addresse s if they have Link permissi ons on the folder.	Yes	No	No	No	No	No
Link into Retention Policy or Retention Markup managed folders	Yes	Yes	Yes	Yes	Yes	No
Apply Retention Directly  Note: PU role can do all, except folders.	Yes	*Yes, see side note	No	No	No	No
Apply Retention via Inheritance	Yes	Yes	Yes	No	Yes	No
Remove Retention	Yes	No	No	No	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Apply/Remove Retention Markups	Yes  Note: CO role cannot create, delete, apply, or remove permanents. This operation implies applying a retention markup directly to the selected object or removing it directly from the selected object.	No	*Yes, see side note.	Yes (review only)	No	No
Validate Authorities	Yes	Yes	No	No	No	No
Qualification	Yes	No	No	No	No	No
Promote to Next Phase	Yes	Yes	No	No	No	No
Disposition	Yes	No	No	No	No	No
Privileged Delete	Yes	No	No	No	No	No
View Retention List	Yes	Yes	Yes	Yes	no	no
View Retention Markup List	Yes	No	Yes	Yes	no	no

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
*Apply/ Remove Condition to Phase	Yes	No	No	No	No	No
Apply/Remove Authority to Phase	Yes	No	No	No	No	No
Apply/Remove Action to Phase	Yes	No	No	No	No	No
Apply/Remove Contact to Retention Markup	Yes	No	Yes	Yes	No	No
Apply/Remove Contact to Event	Yes	Yes	No	No	No	No
Apply Remove Contact to Authority	Yes	Yes	No	No	No	No
Apply Remove Contact to Action	Yes	Yes	No	No	No	No
Retention Markup Reports	Yes	No	Yes	Yes	No	No
Audit Reports	Yes	Yes	No	No	No	No
Retention Reports	Yes	Yes	No	No	No	No
Notification Reports (Administrative)	Yes	no	No	No	No	No
Notification Reports (User)	Yes	Yes	Yes	Yes	Yes	No
Retention Markup Review Report (Administrative)	Yes	No	No	No	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Retention Markup Review Report (User)	Yes	Yes	Yes	Yes	Yes	No
Modify Aggregate Role Membership	No	No	No	No	No	Yes
Modify Atomic Role Membership	No	No	No	No	No	No
**Move to Unretained Folder	Yes	No	No	No	No	No
**Move to Any Retained Folder	Yes	No	No	No	No	No
**Move to Same Retained Folder	Yes	No	No	No	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Close Folder  Note: The Retention Manager and the Power User roles are added to the Close Folder and to the Re-open Folder roles during installation. Only members in Retention Manager and Power User roles can close/re-open/revert a folder.	Yes	Yes	No	No	No	No
Re-open Folder	Yes	Yes	No	No	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
Revert Folder  Note: Members in the respective close and re-open folder role can undo their action if they did it accidentally, as long as they remain in that role. Only Retention Managers and Power Users can otherwise perform any of these actions.	Yes	Yes	No	No	No	No

Retention Policy Services Functions	Records Manager role	PU role	CO role	VRA role	CONT role	RA role
*Applies only if the retention policy is not referenced (in use).						
** Regardless of which move to operation is performed, when a retained object with inherited retention is moved, the original inherited policies are removed. The 3 operations are defined as follows:						
<ul style="list-style-type: none"> • Move to Unretained Folder implies that the target location does not have a retention policy associated with it. • Move to Any Retained Folder implies that the target location has any retention policy associated with it. • Move to Same Retained Folder implies that the target location has the same retention policy as the original source location. 						



Note: Users who are to be members of the Contributor role should be added to a group before they are added to the Contributor role. This approach allows for efficient management of members in the Contributor role.

4.2.2.3 Retention Policy Services configuration

4.2.2.3.1 Records check configuration option settings

The filter criteria to identify the objects to be scanned during execution of Compliance Check job can be specified in Records Check Configuration object. Only Retention Policy Services Retention Manager and the user owning Records Check Configuration object can edit the values set for different fields of this object.

To set any of the records check options:

1. Navigate to Cabinets > System > Applications > RpsConfig > RPS Configuration or from the Records dashboard Home page, click RPS Configuration.
Set the filter in the upper right corner to Show All Objects and Versions.
The **Records Check Configuration**, **RPS Application Configuration**, and **RPS Disposition Configuration** options are displayed.
2. Select **Records Check Configuration** in the content pane and click View > Properties > Info or right-click to select Properties.
The Properties screen appears displaying the Info tab. By default, the **Properties: Info** page displays the attributes for **Disposition Overdue Scan Configurations** and the link to **Show Disposition Overdue Scan Configurations**.
3. Change the value for the attribute settings as applicable. The attributes for the Records Check Configuration are described in “Disposition Job Filters Configuration” on page 130 and “Records check configuration attribute: Compliance scan” on page 121.

Table 4-6: Records check configuration attribute: Disposition overdue scan

Attribute	Description
Grace Overdue Period (Days)	<p>This attribute provides a time period for a physical records manager/authorized user to collect, destroy, and acknowledge destruction of physical items due for disposition (marked for destruction), without the item being registered as overdue on disposition.</p> <p>The default value is 5 days, allowing the destroying user/disposing user, 5 days to process the items before they are marked as overdue.</p> <p>A Grace Period of 0 days indicates physical items not destroyed immediately will be identified as overdue.</p>
Grace Waiting Period (Days)	<p>This Grace Waiting Period provides a window/buffer after the items have been transferred to NARA before they are registered as being overdue for disposition (the NARA acknowledgement has not been received or the system has not been updated to indicate the receipt).</p> <p>For Disposition Strategies that include NARA Transfer, subsequent actions may not be executed until receipt of acknowledgement from NARA is recognized in the repository.</p> <p>The default value is 5 days, allowing the destroying user/disposing user, 5 days to process the items before they are marked as waiting.</p> <p>A Grace Period of 0 days indicates items not destroyed immediately will be identified as overdue.</p>
Enable Disposition Overdue Scan of Full Repository	The complete repository can be scanned by selecting this checkbox.
Folder Paths for Disposition Overdue Scan	<p>Click the Add link to select the folder paths that need to be scanned. However, folders in the system cabinet will not be scanned.</p> <p>Click the Remove link to remove the selected folder paths.</p>

Table 4-7: Records check configuration attribute: Compliance scan

Attribute	Description
Enable Compliance Scan of Full Repository	The complete repository can be scanned by selecting this checkbox.
Folder Paths for Compliance Scan	Click the Add link to select the folder paths that need to be scanned. However, folders in the system cabinet and their contents will not be scanned. Click the Remove link to remove the selected folder paths.

4. Click **OK** to accept and to close the **Properties** screen.

4.2.2.3.2 System configuration options settings

To set any of the system configuration options:

1. Navigate to **Cabinets > System > Applications > RpsConfig > RPS Configuration** or, from the Records dashboard Home page, click **RPS Configuration**.
Set the filter in the upper right corner to **Show All Objects and Versions**.
The **Records Check Configuration**, **RPS Application Configuration**, and **RPS Disposition Configuration** options are displayed.
2. Select *Retention Policy Services Application Configuration* in the content pane and click **View > Properties > Info** or right-click to select **Properties**.
The **Properties** screen appears displaying the **Info** tab.
3. Configure the settings to support the reporting needs of the organization.
Attributes for the Retention Policy Services System Configuration options are described in [“Retention Policy Services System Configuration options” on page 122](#).

Table 4-8: Retention Policy Services System Configuration options

Options	Description
Cascades To Containers	This is the default value on the interface when creating a new retention markup. If not checked, by default markups applied to a folder will not be applied to sub folders but will be applied to any non-containers in the folder. When checked, if applied to a container, all sub folders (recursively) will inherit the markup. However, when creating a markup, the administrator can change the default value for the markup. Changing this value will have no effect on existing retention markups (each markup defines what setting it will use).
Disposition Workflows	This is the list of available disposition workflows for routing for approval. By default, this value is not set. If multiple versions of the workflow template exist, make sure that this id refers to the CURRENT version of the workflow.
Export Address	The default export address for any physical objects that do not have any export location specified.
Maximum Number of Notifications Sent	Used by the retention notification report to limit the number of notifications sent.
Query Batch Size	An engineering setting that should not be changed. Used to limit the number of returned items in internal queries.
Query cache check interval	An engineering setting that should not be changed. Used for optimization and the value is in seconds.
Unlink on Dispose	If selected, allows a user to unlink the object they want to dispose of when a second retainer prevents it from being destroyed. The user can therefore see that the object linked to the folder they want to dispose from has disappeared, though in reality it has not been destroyed as it is still under inherited retention by the other folder.

Options	Description
Monthly Limit Days	Used only if Department of Defense dars are installed. When importing using an XML file that uses the Department of Defense schema, this value is used for the mapping for translating a Department of Defense folder that has a vital record review and update cycle period defined. If the value in the VitalRecordReviewandUpdateCyclePeriod is less than or equal to this value, the system will map this to a monthly review.
Quarterly Limit Days	Used only if Department of Defense dars are installed. Used in the mapping for translating a Department of Defense folder that has a vital record review and update cycle period defined. If the value in the VitalRecordReviewandUpdateCyclePeriod is greater than the monthly limit and less than or equal to this value, the system will map this to a quarterly review.
Semi-Annually Limit Days	Used only if Department of Defense dars are installed. Used in the mapping for translating a Department of Defense folder that has a vital record review and update cycle period defined. If the value in the VitalRecordReviewandUpdateCyclePeriod is greater than the quarterly limit and less than or equal to this value, the system will map this to a semi-annual review. Otherwise, if the value is greater than this value, it will be mapped to an annual review period.
Enable Mandatory Justification Field	The checkbox is deselected by default to allow creating, modifying or deleting retention policies without mandatory justification. The Reason for creating policy on the Confirmation Retention Policy Creation page displayed when you click Finish to create the retention policy is displayed as a mandatory field when this option is selected. An asterisk is added when selected or is removed when deselected.

Options	Description
Lock Timeout Threshold	The records product, Retention Policy Services and Records Manager, can now perform policy operations on policy managed objects that are checked out to other users, without breaking the lock. If the duration between the time the object was checked out and the time the operation is performed is short, a concurrency issue may occur. This value, in seconds, represents the amount of time that must elapse before the operation can be performed. The default value is 10 seconds and should be sufficient for most situations. If the time has not elapsed, the system will signal a retry of the operation. See the Retry Limit for further details.
Retry Limit	Normally if a lock was just applied to a document, waiting the interval is sufficient and then the system can save the object. However, in the rare case that an automated process is continually locking and unlocking the document, the retry limit specifies how many times we wait for the condition to resolve. The default value is 1 and if the retry limit is reached, the system will break the lock and perform the policy operation.

- Click **OK** to accept changes and close the **Properties** screen.

4.2.2.3.3 Disposition configuration option settings

Only members of the Disposition Configuration Administrator role (dmc_rps_disp_configurator) can manage (edit) the Disposition Configuration object. In addition, only these members can define and change members from this role.

The Disposition Run Bundles feature is enabled by default (automatically), for Department of Defense purposes, when the Department of Defense Standard dar (RM-DoD5015v3-Standard-Record.dar) is installed. Although disposition run bundle functionality can be manually enabled, for general usage, the Disposition Run Bundles node will not be displayed unless, the Department of Defense Standard dar is installed. To create/generate a disposition run bundle, refer to “[Disposition run bundles](#)” on page 729.

To set any of the disposition configuration options:

- Navigate to **Cabinets > System > Applications > RpsConfig > RPS Configuration** or, from the Records dashboard Home page, click **RPS Configuration**.

Set the filter in the upper right corner to **Show All Objects and Versions**.

The **Records Check Configuration**, **RPS Application Configuration**, and **RPS Disposition Configuration** options are displayed.

2. Select **RPS Disposition Configuration** in the content pane and click **View > Properties** or right-click to select **Properties**. Members of only the **dmc_rps_disp_configurator** role can manage (edit) the disposition configuration object. Also, only the members or owner of the **dmc_rps_disp_configurator** role can add/remove the members from this role. The **Properties** screen appears displaying the **Info** tab.
3. Change the value for the attribute settings as applicable. The attributes for the Retention Policy Services disposition configuration are described in “[Retention Policy Services Disposition Configuration attributes](#)” on page 125.

Table 4-9: Retention Policy Services Disposition Configuration attributes

Attribute	Description
Enable Disposition Run Bundle	Select or deselect the checkbox as necessary. If it is already enabled, it means that the Department of Defense Standard dar (RM-DoD5015v3-Standard-Record.dar) is installed, which automatically enables this option. Although it is disabled (deselected) when the Department of Defense Standard dar is NOT installed, you can always enable it manually for general usage. The Disposition Run Bundles node however, will NOT be displayed for general usage unless the Department of Defense Standard dar is installed.
Disposition Log Path	You can specify a value (used for disposition runs) that do not use the work order framework. This path can be a local path or network UNC path in windows or Linux. If this path is not valid or empty, the log file will go to the original path that is dfc.data.dir/logs/RPS/.

Attribute	Description
Allow only authorized export paths	<p>If this checkbox is selected:</p> <ul style="list-style-type: none"> The Authorized Export Paths field lets you enter multiple export paths. The Default Export Location field cannot be edited. <p>If checkbox is not selected:</p> <ul style="list-style-type: none"> The Authorized Export Paths field is not visible. The Default Export Location field can be edited to provide the value for the default export location.
Authorized Export Paths	Enables to add multiple export paths. The export paths must be valid UNC-formatted network location resolvable from Application Server, Documentum CM Server, and any Records Queue Manager host.
Default Export Location	<p>This is a network location for disposition runs that perform an export or transfer action.</p> <p>This is a read-only field if the Allow only authorized export paths checkbox is selected. The first entry in the Authorized Export Paths is set as the default export location.</p> <p>If this checkbox is not selected, then the field can be edited.</p> <p>For more information about export location, see "More about export location" on page 127.</p>
Disposition Strategy Override	The value specified is the disposition strategy used for objects being disposed with Unknown specified for their disposition strategy.
Rollover Policy  Note: For Linked and Individual	The value specified is the retention policy used for objects with the Unknown strategy being resolved to a strategy that requires a rollover.

- Click **OK** to accept and to close the **Properties** screen.

4.2.2.3.3.1 More about export location

The Export location is a network location where files should be exported for either the export or the transfer disposition strategies (contains Export Content or Export All OR NARA Transfer). The value for the export location should represent a universally accessible network location to which all the Application server, Documentum CM Server, and Records Queue Manager machines can write.

An example of a network location for Windows is given as follows: \\<ip address or machine name>\<shared location>. The value specified is used by the *Disposition Job* and the Disposition Manager.



Note: Overwriting the value for the Export Location however, may cause disposable items to not dispose if the path is restricted or does not exist. Make sure the path exists and is not restricted. The machine that processes a disposition operation is not necessarily the Application server. For example, if the machine (Records Queue Manager) that processes a disposition operation has an export action (or transfer action) and does not have an access to the path specified by the Export Location, then disposition fails.

During each disposition run, a new directory gets created in the configured export location to ensure that each disposition operation does not overwrite any existing files.

The directory name is in the following format: <username of the retention manager performing the operation>_<date + time> of the operation. For example, if the export location selected is \\xx.xx.xx.xx\share, then a directory named **retmgr1_11172014120822** gets created under \\xx.xx.xx.xx\share.

4.2.2.3.4 Qualification job filters configuration option settings

This qualification job filter criteria addresses the performance and work order timeouts for a large number of objects.

To set qualification job filter options:

1. Navigate to Cabinets > System > Applications > RpsConfig > RPS Configuration or from the Records dashboard Home page, click **RPS Configuration**.

Set the filter to **Show All Objects and Versions**.

The **Disposition Job Filters Configuration**, **Promotion Job Filters Configuration**, and **Qualification Job Filters Configuration** options are displayed.

2. Select **Qualification Job Filters Configuration** in the content pane and click **View > Properties > Info** or right-click to select **Properties**.

The **Properties** screen appears displaying the **Info** tab. By default, the **Properties: Info** page displays the attributes for **Qualification Job Filters Configuration**.

3. Change the value for the attribute settings as applicable. The following table provides attributes for the Qualification Job Filters Configuration:

Table 4-10: Qualification Job Filters Configuration

Attribute	Description
In Folder	This attribute enables users to select multiple folders. Objects from sub folders will also be considered if you select Include Sub Folders checkbox. The folder contents will be used for qualification.
Type	User can select multiple types. Only objects of these types will be considered for qualification.
Retention Policy	User can select multiple retention policies.
Authority	User can select multiple authorities.
Phase	User can select multiple phases. The job picks only those retainers whose status matches with the selected phases.
Allow Re-Qualification	If this option is selected, already qualified retainers will be picked by the job and re-qualify.
Qualification Date	To Date selected should be later than From Date. Retainers whose qualification dates are within this date range will be considered by the qualification job.
Event Date	To Date selected should be later than From Date. Retainers whose event dates are within this date range will be considered by the qualification job.

4. Click **OK** to accept and to close the **Properties** screen.

4.2.2.3.5 Promotion job filters configuration option settings

This promotion job filter criteria addresses the performance and work order timeouts for a large number of objects.

To set promotion job filter options:

1. Navigate to **Cabinets > System > Applications > RpsConfig > RPS Configuration** or from the Records dashboard Home page, click **RPS Configuration**.

Set the filter to **Show All Objects and Versions**.

The **Disposition Job Filters Configuration**, **Promotion Job Filters Configuration**, and **Qualification Job Filters Configuration** options are displayed.

2. Select **Promotion Job Filters Configuration** in the content pane and click **View > Properties > Info** or right-click to select **Properties**.

The **Properties** screen appears displaying the **Info** tab. By default, the **Properties: Info** page displays the attributes for **Promotion Job Filters Configuration**.

3. Change the value for the attribute settings as applicable. The following table provides attributes for the Promotion Job Filters Configuration:

Table 4-11: Promotion Job Filters Configuration

Attribute	Description
In Folder	This attribute enables users to select multiple folders. Objects from sub folders will also be considered if you select Include Sub Folders checkbox. The folder contents will be used for promotion.
Type	User can select multiple types. Only objects of these types will be considered for promotion.
Retention Policy	User can select multiple retention policies.
Authority	User can select multiple authorities.
Phase	User can select multiple phases. The job picks only those retainers whose status matches with the selected phases.
Qualification Date	To Date selected should be later than From Date. Retainers whose promotion dates are within this date range will be considered by the promotion job.
Event Date	To Date selected should be later than From Date. Retainers whose event dates are within this date range will be considered by the promotion job.

4. Click **OK** to accept and close the **Properties** screen.

4.2.2.3.6 Disposition job filters configuration option settings

This disposition job filter criteria addresses the performance and work order timeouts for a large number of objects.

To set disposition job filter options:

1. Navigate to **Cabinets > System > Applications > RpsConfig > RPS Configuration** or from the Records dashboard Home page, click **RPS Configuration**.

Set the filter to **Show All Objects and Versions**.

The **Disposition Job Filters Configuration**, **Promotion Job Filters Configuration**, and **Qualification Job Filters Configuration** options are displayed.

2. Select **Disposition Job Filters Configuration** in the content pane and click **View > Properties > Info** or right-click to select **Properties**.

The **Properties** screen appears displaying the **Info** tab. By default, the **Properties: Info** page displays the attributes for **Disposition Job Filters Configuration**.

3. Change the value for the attribute settings as applicable. The following table provides attributes for the Disposition Job Filters Configuration:

Table 4-12: Disposition Job Filters Configuration

Attribute	Description
In Folder	This attribute enables users to select multiple folders. The folder contents will be used for disposition.
Retention Policy	User can select multiple retention policies.
Qualification Date	To Date selected should be later than From Date. Retainers whose disposition dates are within this date range will be considered by the disposition job.

4. Click **OK** to accept and close the **Properties** screen.

4.2.2.4 Work order notifications

Work order notifications are optional and can be configured from the Work Order Operations Configuration object, on the Notifications tab, for any supported records operation. Notifications are intended to notify recipients when the processing of a collection of work orders is completed. That is, when processing of the master work order or any of its subwork orders is completed, regardless of the **Completion Status**, *Succeeded*, *Partially Succeeded*, or *Failed*. E-mail or Inbox notification can be configured against one or more recipients, the owner of the work order or other users. Notification can be sent to only the work order owner or to other users or both. The work order owner is the person who made the request against a particular operation. The Delivery Method, E-mail or Inbox notification, as well as the Sending Threshold, which is the notification trigger, can be set differently or similarly for the owner and the other recipients. Notifications, in the case of a work order recovery, may not go to the original person who created the work order, if someone else is recovering the item. For further details about work order configuration objects, refer to “[Work orders](#)” on page 33.



Note: The work order notifications tab is only visible to users who are members of the `dmc_rps_work_order_admin` role. This role also accounts for those users who are members of the `dmc_rps_retentionmanager` role. Recipients of work order notifications must have Read permission

To configure a work order Inbox or E-mail notification:

- A **Notification Base URL** is not required for Inbox notifications therefore, if no e-mail notifications are required, proceed to step 2. Otherwise, navigate to **Cabinets > System > Applications > RpsConfig > Workorder Configuration** or, from the Records dashboard Home page, click **Workorder Configuration** to configure the **Notification Base URL**.

The *Work Order Framework configuration object* is displayed. If **No items found** is displayed, set the filter in the upper right corner to **Show All Objects and Versions**.

The **Notification Base URL** must be configured if any users or groups will be recipients of e-mail notifications. E-mail recipients are given a link to the work order whereas Inbox notifications include the work order as an attachment. The **Notification Base URL** specified pertains to all of the *Work Order Operation Configuration* objects that have *E-mail* selected for the **Delivery Method**.

Follow these substeps to specify a value for the **Notification Base URL**:

- On the **Workorder Configuration** page, right-click the *Work Order Framework configuration object* and select **Properties**.
- Type the value that represents the location of your Records application using the following format:

`<protocol>://<application_server_IP_address>:<port>/<application_name>`

For example, `http://x.x.x.x:8080/records` where, `x.x.x.x` represents the actual or desired IP address.



Note: Do not add a trailing slash to the entry. The **Notification Base URL** is added to the e-mail as a link when it is sent and has the Work Order Report appended to it. For example, `http://x.x.x.x:8080/records/component/workorderreport?objectid=080035678300755b`.

The link is live for e-mail recipients who have HTML enabled e-mail. The link otherwise, if it is not live, must be copied and pasted into a browser to access the Work Order Report. The Work Order Report automatically displays the work order for which notification was sent. The recipient can then right-click the work order to view the results (View Results) or to view the inputs (View Inputs).

- Click **OK**.
- Navigate to **Cabinets > System > Applications > RpsConfig > Workorder Operations Configuration** or, from the Records dashboard Home page, click **Workorder Operations Configuration**.
If **No items found** is displayed, set the filter in the upper right corner to **Show All Objects and Versions**.
A configuration object is listed for each supported operation.
 - Right-click the desired operation for which you want to configure notifications and select **Properties**.

4. Select the **Notifications** tab. The *APPLY_REMOVE_MARKUP* operation is selected as an example.
5. Select the checkbox for **Send Owner Notifications** if owner notifications are required or otherwise, proceed to step 6. The screen refreshes to display the owner **Notification Details** pane for setting the **Delivery Method** and the **Sending Threshold**.



Note: The **Notification Details** pane is displayed when you select the checkbox for **Send Owner Notifications** and when you click **Add** under **Other Notifications**.

Follow these substeps to configure owner notifications:

- a. Select a value for the desired **Delivery Method**, either *E-mail Notification* or *Inbox Notification*.
 - b. Select a value for the desired **Sending Threshold**, to trigger notification delivery, on either *Failure*, *Partial Success*, or *All Results*. Only failed work orders are targeted if *Failure* is selected. Failed and partially succeeded work orders are targeted if *Partial Success* is selected. Failed, partially succeeded, and succeeded work orders are targeted if *All Results* is selected.
 - c. Click **OK** to finish the configuration or proceed to step 6 to include notifications against other users, which are recipients other than the work order owner.
6. To include other recipients for the notification, click **Add** under **Other Notifications**. The screen refreshes to display the other **Notifications** page.

Follow these steps to configure recipients for other notifications:

- a. On the **Notifications** page, type a value for the **Notification Name**, select the desired values for the **Notification Details**, and then click **Add**. Set the desired value for the **Delivery Method** and for the **Sending Threshold**, as described in Step 5.

A file is created with this name after you finish adding the desired recipients from the **Choose a user/group** locator page.
 - b. Click **OK** on the **Notifications** page. The **Notifications** page is refreshed and returns you to the **Notification** tab. The value specified for the **Notification Name**, according to substep a), is now listed as a file on the **Notifications** tab, under that **Notification Name**.
 - c. Repeat step 6 and these substeps if you want to create more recipient sets.
7. Click **OK** on the **Notification** tab to finish the configuration. Notifications can be set up similarly against any other work order supported operation. If necessary, repeat this procedure to configure notifications for other supported work order operations.

Note the following details about opening a work order notification and accessing the work order. Recipients, once they open the notification can then

see the work order Id and view it against any work order right-click menu option: **View Input**, **View Results**, **View Breakdown**, and **View Items**.



Note: The work order in an Inbox notification is added as an attachment, under **Attachments**, where you can right-click it directly to access the work order menu options. E-mail notifications however, include a link as the attachment to the work order. Unless the user is the person who initiated the request that results in the creation of a work order, or the recipient is a member of the dmc_rps_work_order_user group, the work order will not be accessible whether it is an Inbox or Email notification. Recipients of Inbox notifications who do not have sufficient work order permissions will see **No Attachments Found**. Recipients of E-mail notifications who do not have sufficient work order permissions will have the link but no access. The work order is accessible in E-mail or Inbox notifications for recipients who are:

- Super users
- Browse all users such as Records Managers and Retention Managers
- Power users and compliance officers, but only if Retention Policy Services is the only application installed
- Work order administrators
- Work order owners

All recipients, regardless of the permissions or delivery method, will see the completion message.

4.2.2.5 Virtual document retention rules

The virtual document retention rule is a retention policy attribute, set to either retain only the parent document (or root) or both the parent and child documents. Retention Policy Services support of virtual documents provides a means for nesting or associating documents and enhanced management of electronic data such as email. You can include one or more attachments with a virtual document and you can also apply a retention policy to a virtual document. For further details about virtual documents, refer to “[Virtual documents](#)” on page 671.



Note: Although you can add an attachment to a virtual document while it is under retention, you will be forced to check in the virtual document as a minor or major version. The new version will not be retained unless it is in a folder under retention.

A virtual document with an attachment cannot be converted to a simple document while it is under retention. The retention must be removed first.

The **Virtual Document Retention** rule has the following two values you can select from:

- **Retain Root Only**

- **Retain Root and Children**

You must choose **Retain Root Only** or **Retain Root and Children**.

If the rule is set to **Retain Root Only**, only the parent is retained.

If the rule is set to **Retain Root and Children**, the parent and attachments are all retained.

4.2.2.6 **Linking a record**

You can only link records in an open folder or a reopened folder. You must open the folder first, if it was closed, in order to link a record in there. You may link a record stored in one policy managed folder to another policy managed folder if the record has to be regulated by more than one policy managed folder. Records in linked instances inherit policies from all folders.

You can link a record from one policy managed folder to another policy managed folder, in the same file plan or to another policy managed folder in another file plan, only if the policy managed folder selected is in an open state. Linking a record to a policy managed folder that has been closed (Records > Close Folder) is not permitted. For further details about link levels and containment policies, refer to About containment policies.

To link a record to an open policy managed folder:

1. Navigate to a records location and select one or more records.
2. Select **Edit > Add To Clipboard**.
3. Navigate to the managed folder you want to link the records to and make sure that it is in an open (or re-opened) state.
4. Select **Edit > Link here**.

To monitor the processing status of a work order or to recover items that could not be processed in the work order, use the Work Order Report. A request is performed by a work order when the confirmation message at the bottom of the UI indicates that the request was sent to a work order.

4.2.2.7 **Moving retained objects (unlinking objects from a retained folder)**

The Move Retained Objects functionality makes it possible for non-Retention Managers to relocate retained records to another folder within the same file plan or to a different plan. Only system objects (dm_sysobject) that are not folders or light weight sysobjects are supported for this release. Retention Managers however, can move any retained object including folder types and light weight sysobjects. The two diagrams at the end of this section, [Figure 4-2](#) and [Figure 4-3](#), illustrate the Move Retained Objects functionality.

Moving a retained object implies moving any typical record that is not a container type object. Only those users who are in the Records Manager role can move

cabinets, folders, boxes, and so on. Records, meaning both typical records (electronic or physical documents) and formal records for example, can be moved.

Although Retention Managers are able to move such retained objects, there are also three roles with varying move capabilities available to users with fewer privileges. This feature enhancement is role based and therefore is enabled by adding the appropriate users or user groups to the Move Retained Object roles. If there are no members in the roles, then only Retention Managers are allowed to move retained objects. For example, if you want to allow Contributors and Power Users to move documents into subfolders within a Retention Cascade (this means that retention is being inherited down a folder hierarchy and you are moving the retained object within this folder hierarchy), the users or user groups who are members of the *dmc_rps_contributor* role and *dmc_rps_poweruser* role must also be added to the new role, in this case, the *dmc_rps_move_same_retain_folder* role. The move functionality and its corresponding new roles are described in the paragraphs that follow.

Records can be relocated from folders under retention to other folders, with or without retention depending on which Move Retained Object role the user is a member of. Each of the 3 roles are conditional and therefore restrict the user to the same retained folder, any retained folder, or to any unretained folder.

There are three roles with various degrees of relocation capability that allows less privileged users to move retained objects (these roles do not allow objects to be moved from folders that have a hold or permanent retention markup). The following three roles do not give permission to move folders from retained folders. The only role that can move items from the retained folders is the Retention Policy Services retention manager role:

- *dmc_rps_move_unretain_folder*

This role grants its members the privileges to remove inherited retainers. For example, to unlink a retained object from a folder with one or more retention policies and link it to another folder without a retention policy.

Members of this role are by default also members of the *dmc_rps_move_any_retain_folder* role and therefore, inherits its privileges.

This is the most powerful of the three roles.

- *dmc_rps_move_any_retain_folder*

This role grants its members the privileges to remove an inherited retainer, only if it is replaced by another retainer. It allows its members to move retained objects between two folders only if the destination folder is retained.

Members of this role are by default also members of the *dmc_rps_move_same_retain_folder* role and therefore, inherits its privileges.

- *dmc_rps_move_same_retain_folder*

This role grants its members privileges to move retained objects if and only if the destination folder has at least the same set of inherited retention policies as the source folder.

The *dmc_rps_retentionmanager* role is by default a member of this role.

This is the most restrictive of the three roles.



Note: It is recommended that you create a group, add the users that are allowed to relocate retained objects to this group, and then add the group to the appropriate role. In addition, this group MUST be a member of the dmc_rps_contributor role in order to be able to apply retention (by inheritance) to the object.

This feature enhancement applies to only objects with Retention Policy Services retainers. It does not handle retainers created by Centera for example.



Note: You cannot link or move a record to a folder that has a Terminal Retainer as such folders are marked for destruction and will be removed (if all of its content is ready for destruction) when the Terminal Disposition Job runs. For further details regarding terminal retainers, refer to the disposition strategies and the Disposition state diagram in the “[Retention policy overview](#)” on page 146. To determine which folders have a terminal retainer, use the Retention Report and select the filter labeled Retained Objects with Terminal Retention. To run a retention report, refer to “[Running the retention report](#)” on page 247.

Moving a retained object affects its inherited retention policy whereby it can either add or remove retention policy depending on the destination folder. Documents with retention policy applied directly will remain on the item when the object is moved. Only inherited retention policy can be added or removed:

- If a retention policy exists on the source folder but not on the destination folder, the retention policy will be removed.
- If a retention policy exists on the destination folder but not on the source folder, the retention policy from the destination folder will be inherited.
- If a retention policy exists on both source and destination folders, the retention policy will remain on the object.



Note: Retention manager should be careful when moving an item from a retained or held folder as the protection could be removed. There is no warning or confirmation about removing the inherited policies or markups.

The operation can be done using core OpenText Documentum CM functionality, such as:

- Drag and Drop
- Add to Clipboard and Move Here

To monitor the processing status of a work order or to recover items that could not be processed in the work order, use the Work Order Report. A request is performed by a work order when the confirmation message at the bottom of the UI indicates that the request was sent to a work order. Requests that involve processing a large number of objects are typically sent or delegated to a work order.



Note: Users, regardless of the role they are in, are prevented from moving documents to a closed folder or to a folder that has a terminal retainer.

Inherited retainers are always removed from the record when it is unlinked from a retained folder. The record as a result could end up with or without retainers depending on whether the destination folder has retention or not. The record will inherit new retainers if the destination folder has retention, or nothing if it has no retention. Retainers that are directly applied to the object are unaffected by the move operation and will remain on the object.

Moving Records to a Closed Folder

Moving retained records to a retained folder that is in the Closed state is prevented. Users who are members of the appropriate roles are able to move retained records from one retained folder to another retained folder in the same file plan or another file plan, only if the retained folder is in an open or re-open state or if there is no Terminal Retainer on the folder.

Moving Records from Folders Under Linked Retention

Records that age with the retainer on the folder according to the Linked retention strategy, are removed and replaced by retainers associated with the destination folder. The record assumes the state of the retainers on the new folder location. This applies to both cases where the source and target folders have the same or different retention policies.

Moving Records from Folders Under Individual Retention

Records that age individually with their own retainers, independently of the folder, according to the Individual retention strategy, are removed and replaced by retainers associated with the destination folder, even if the retention policies are the same. The new retainer is reset to the initial phase of the retention policy lifecycle. Retainer aging is reset. This applies to both cases where the source and target folder have the same or different retention policies.

Moving Checked Out Records

Users in any role, including Retention Managers, will be prevented from moving retained records that are checked out.

Moving Records with Retention Markup (Holds or Permanents)

This feature does not affect existing retention markup functionality.

Only Retention Managers can move retained documents that inherit the Hold or Permanent markups from its parent folder.

Moving a retained object affects its inherited retention markups whereby it can either add or remove retention markups depending on the destination folder. Documents with retention markups applied directly will remain on the item when the object is moved. Only inherited retention markups can be added or removed:

- If a retention markup exists on the source folder but not on the destination folder, the retention markup will be removed.
- If a retention markup exists on the destination folder but not on the source folder, the retention markup from the destination folder will be inherited.
- If a retention markup exists on both source and destination folders, the retention markup will remain on the object.



Note: Retention manager should be careful when moving an item from a retained or held folder as the protection could be removed. There is no warning or confirmation about removing the inherited policies or markups.

Moving Formal Records

Users in the appropriate role can move formal records from one file plan with a retention policy to another file plan with the same retention policy or different retention policy. Records Manager policies (containment, naming, and security) governing the destination file plan must also be satisfied before the move can be completed successfully. Users are prevented from moving a retained formal record to a file plan that is not managed by a retention policy, if the Records Manager system configuration setting for mandatory retention on a managed folder is enabled.

Moving Records with Security Policies

Moving records from a security policies managed folder to a folder that does not have any security policies are only allowed for and Privileged Records Users. When Records Manager is enabled, users in the appropriate role are able to move retained records that are managed by security policies, only if all the security policy criteria are met. Users must also be added to the appropriate Records Manager Security roles (dmc_rps_security_user and/or dmc_rps_security_officer) to successfully move records with security restrictions. Refer to “[Security policies](#)” on page 390 to ensure that these users are also added to the appropriate Records Manager Security roles in order to move documents, with security restrictions, successfully.

Moving Physical Records

Users in the appropriate role are able to move physical documents, created using Physical Records Manager. Physical containing objects, for example, Boxes, Bays, Bins, Shelves, and so on, are not supported by this feature. Retention managers however, are always able to move these items when necessary.

Auditing

Existing system audit events, dm_link and dm_unlink are used to log the relocation of retained objects. The audit logs for these events capture the name and object Id of the document and target folder. In addition, the Retention Policy Services audit events, dmc_rps_apply_retention_policy and dmc_rps_remove_retention_policy are used to log the retention policies that are added or removed due to the relocation. The audit logs for these two events capture the name and object Id of the retention policy involved. One audit log is created for each retention policy.

Figure 4-2 and **Figure 4-3** illustrate move actions within the same file plan and between file plans.

Figure 4-2 illustrates moving documents to a destination folder that has at least the same set of inherited retention policies on the same file plan and the user is a member of only the `dmc_rps_move_to_same_retain_folder` role.

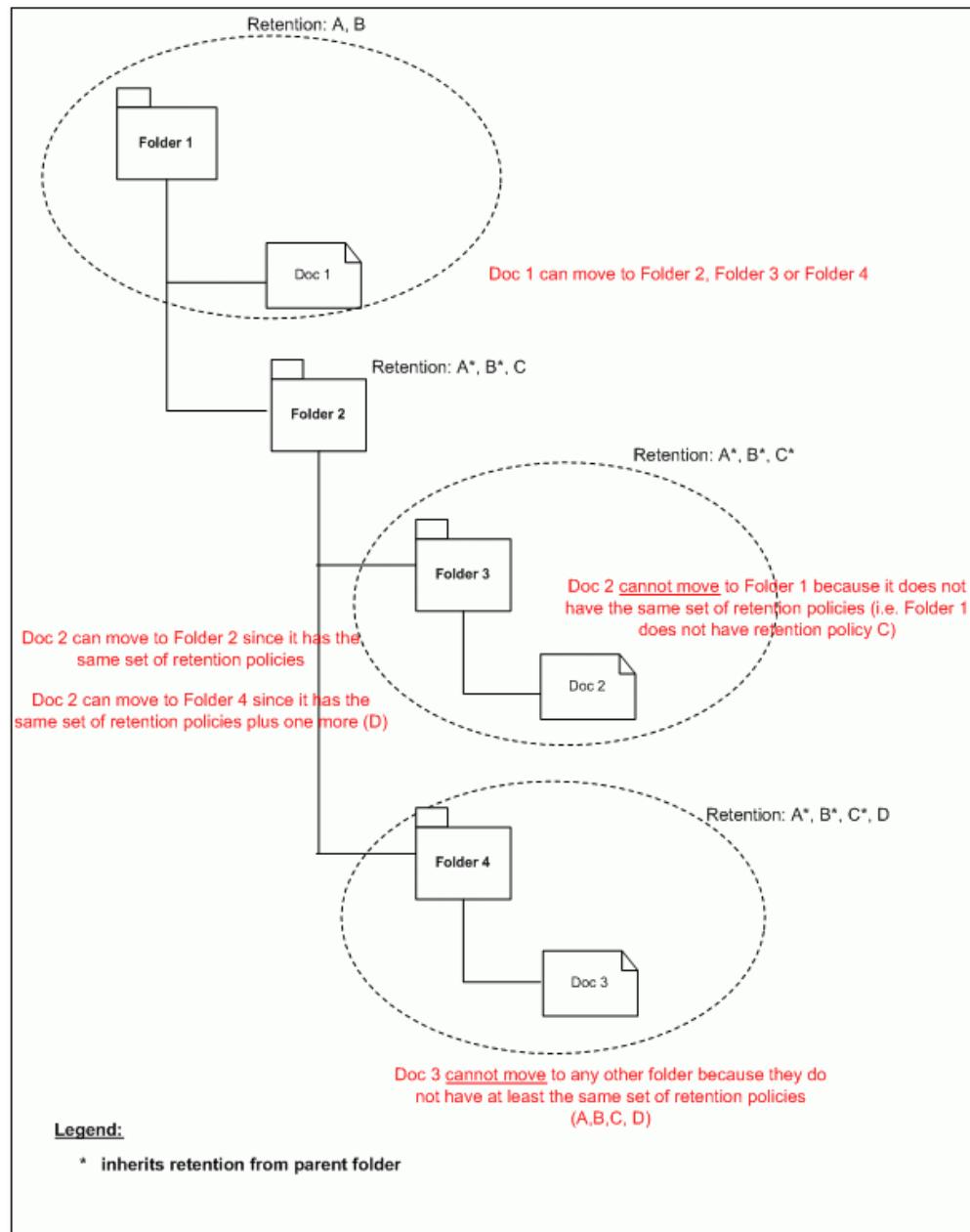


Figure 4-2: Moving documents in the same file plan

Figure 4-3 illustrates moving documents to a destination folder in a different plan that has at least the same set of inherited retention policies and the user is a member of only the dmc_rps_move_to_same_retain_folder role.

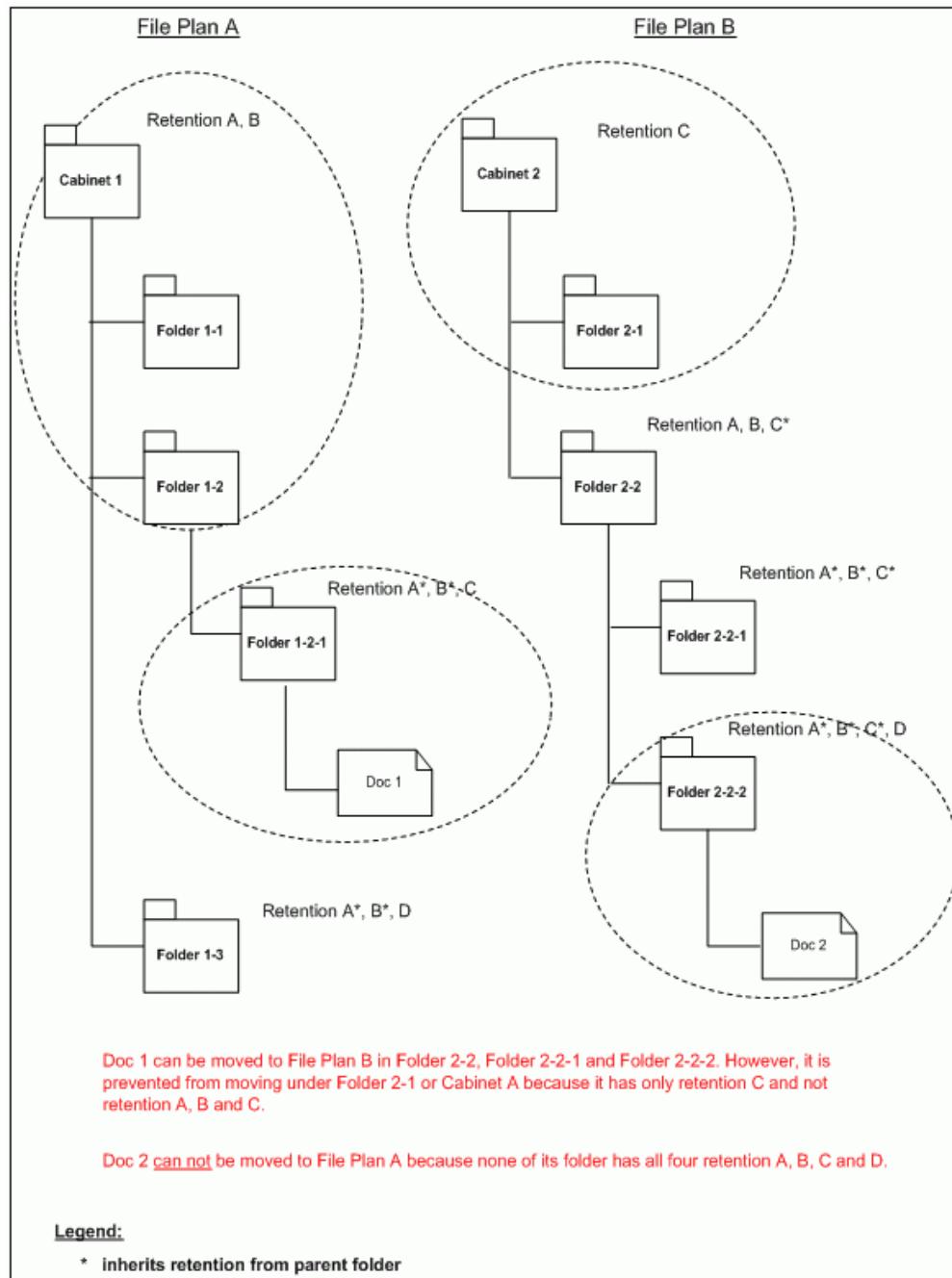


Figure 4-3: Moving documents between file plans

4.2.2.8 Close folder operations

4.2.2.8.1 Overview

The Close Folder feature is used to close or re-open a folder to prevent linking objects (folders and documents) into it when closed and to allow linking when re-opened. Although nothing can be added (linked to the folder, created within the folder, or imported into the folder) to the folder while it is closed, existing content can be copied and versioned. If however a closed folder is policy managed, copying or versioning of any content would be blocked. A checked out document from a closed folder cannot be checked in if a records policy was applied after the document was checked out.

If the folder is retained and is closed, checking content back in is prevented. If however, the folder is not retained and is closed, checkout and checkin is not prevented. Any container object type, normal or physical cabinets and folders, formal or not, including physical boxes, can be closed.

Reports and search utilities:

- Use the Close Folder Report to generate a list of folders, to act on or to simply determine which are re-opened or closed. The report can show a list of opened folders as well. All folders by default are deemed opened on creation. To run a Close Folder Report, refer to ["Running the close folder report" on page 267](#).
- Use the Audit Trail Report to report the details of audit events performed against Retention Policy Services governed folders. To run an Audit Trail Report against close folder actions, refer to ["Running the audit trail report" on page 272](#).
- Advanced Search on the Records Client is also available to search close folder objects. To run an advanced search against close folder objects, refer to ["Retention Policy Services searching" on page 246](#).

Folders are open by default when they are created and therefore can be re-opened, when necessary, after they have been closed. The open state occurs only once whereas subsequent state changes against close and re-open operations can occur multiple times. An open folder has no Retention Policy Services metadata and is therefore not governed by Retention Policy Services. A folder is Retention Policy Services governed only after it has been closed or re-opened.

A user can always revert closing or re-opening a folder, as long as that user who brought the folder to the current state is still in that role. For example, a user in the close folder role (dmc_rps_close_folder) who mistakenly closes an open or a re-opened folder, can revert the operation. A user in the re-open folder role (dmc_rps_reopen_folder) who mistakenly re-opens a closed folder, can revert the operation.

Reverting means that the folder is returned from the current state to the previous state, as if a state change never occurred. After the revert, all closed metadata is set to the metadata of the state the folder reverts to. When reverting to an opened state, the close folder aspect and Retention Policy Services metadata are removed from the folder.

If a folder is closed due to a retention policy phase action, Power Users are not able to see the Revert From closed state menu option, whereas Retention Manager can. Members in either role can see the Re-open Folder menu. Power Users and Retention Managers are in the closed folder and re-open folder roles and therefore can see both Re-open Folder and Revert from Closed State menu options when a folder is closed.

An audit trail is generated for every close, re-open, or revert operation performed. The audit events must be registered first before they can be picked up by the Audit Trail Report. The three audit events associated with the close folder feature are:

- dmc_rps_close_folder. This audit event tracks the:
 - user who closed the folder
 - date the folder was closed
 - reason for closing the folder
- dmc_rps_reopen_folder. This audit event tracks the:
 - user who re-opened the folder
 - date the folder was re-opened
 - reason for re-opening the folder
- dmc_rps_revert_folder_state. This audit event tracks the:
 - user who reverted the folder from its current state
 - date the folder reverted from its current state
 - reason for reverting the folder from its current state
 - previous state a folder returns to as a result of reverting
 - current state from which the folder is reverted

Although there are three events associated with the close folder feature there are only two customer-facing roles. The actions each of these roles can perform are compared in “[Roles and functional access for close folder actions](#)” on page 142.

Table 4-13: Roles and functional access for close folder actions

Action	dmc_rps_close_folder	dmc_rps_reopen_folder
Close folder	Yes	No
Re-open folder	No	Yes

Action	dmc_rps_close_folder	dmc_rps_reopen_folder
Revert from current state	Yes - only if it is the same user, the person who brought the folder to the current state, and - only if the current state is closed	Yes - only if it is the same user, the person who brought the folder to the current state, and - only if the current state is re-opened
Modify the reason attribute	Yes - only if the folder is in a closed state	Yes - only if the folder is in a re-opened state

There are a few ways that folders can be closed or re-opened:

- Manually, using the Close/Re-open folder menu options or using the Close Folder Report or the Retention Report.
All 3 actions, close, re-open, and revert, are all available on the Close Folder Report.
- Automatically, if the Close Folder or the Open Folder action option is selected for a given phase change of a retention policy and this policy is applied to a folder and the phase change occurs. You can opt to close or re-open a folder when entering a specific phase (upon phase entry) or exiting a specific phase (upon phase exit).



Note: The Open Folder action implies re-open but for internal reasons, is labeled Open Folder.

Close and open folder actions, if you are working with Records Manager Commonwealth Edition, are ignored by Commonwealth files and Commonwealth file parts.

The standard property pages of a OpenText Documentum CM container, viewed from the Records Client, includes a tab for **Close Folder Info**. The Close Folder Info tab is available only in the Records Client. The Documentum WebTop client however does not display this tab. You can select the **Properties** of a closed or re-opened container to view the details and if necessary edit the **Reason**. All other parameters are read-only. Only those users in the corresponding role however can edit the entry for the **Reason**. For example, only users in the dmc_rps_close_folder role can change the **Reason** for the state change when the folder is in a closed state. Similarly, only users in the dmc_rps_reopen_folder role can change the **Reason** for the state change when the folder is in a re-opened state.

The **Close Folder Info** tab displays the following message if the folder was never closed: **This object does not have any close folder attributes**. It is the message displayed for folders in their initial open state, for folders that are not Retention Policy Services governed. Close folder details are available only after a folder is closed, that is for folders in the closed or re-opened states, not the open state. The Close Folder Info tab displays the following details only if the folder was closed:

- Current State
The state that the folder is currently in.
- Reason
The reason for changing to the current state.
- State Change User
The name of the user who brought the folder to its current state.
- State Change Date
The date on which the user brought the folder to its current state.
- Date Folder Was First Closed
The date on which the folder was closed for the first time.
The value for this date is identical to the date value for the State Change Date, only when you look at the Properties of the folder after it has been closed for the first time. The values are never the same on subsequent state changes.

4.2.2.8.2 Closing a folder

This procedure provides steps to close a folder from the Close Folder menu option. The Close/Re-open Report and the Retention Report can also be used to close or to re-open folders.

To close a folder:

1. Navigate to an open container (cabinet, folder, or physical object container), select it in the content pane and click **Records > Close Folder**, or right-click it in the content pane and select **Retention > Close Folder**.
The **Close Folder** option is displayed only when an open folder is selected.
2. The **Close Folder Confirmation** screen is displayed and you can optionally type a reason, up to 255 characters long. No close folder metadata is displayed when the folder is being closed for the first time. Close folder metadata is displayed, only if the folder was closed at least once.
3. Click **Yes** on the **Close Folder Confirmation** screen to complete the process.
A successfully closed message is displayed at the bottom of the content pane.

4.2.2.8.3 Re-opening a folder

This procedure provides steps to re-open a folder from the Re-open Folder menu option. The Close/Re-open Report and the Retention Report can also be used to close or to re-open folders.

To re-open a folder:

1. Navigate to a closed container (cabinet, folder, or physical object container), select it in the content pane and click **Records > Re-open Folder**, or right-click it in the content pane and select **Retention > Re-open Folder**.
The **Re-open Folder** option is displayed only when a closed folder is selected.
2. The **Re-open Folder Confirmation** screen is displayed. Although the **Reason for Change State** is optional, the number of characters permitted is 255. Although no re-open folder metadata is displayed if the folder is being re-opened for the first time, close folder metadata however, will be displayed.
3. Click **Yes** on the **Re-open Folder Confirmation** screen to complete the process.
A successfully opened message is displayed at the bottom of the content pane.

4.2.2.8.4 Revert a folder from a closed or re-opened state

This procedure is intended to undo a close folder or re-open folder operation that was made by mistake. It is applicable only to that user who made the mistake, and only while that user remains in the same role. Examples are provided in the Overview. No other user can revert a folder that you closed or re-opened inadvertently. Only Retention Managers can revert a close folder action that is performed by the system.

To revert a folder from a closed or re-opened state:

1. Navigate to a closed or re-opened folder. The appropriate menu option is displayed depending on the state of the folder selected.
If the folder is closed, click **Records > Revert From closed State**. If the folder is re-opened, click **Records > Revert From re-opened State**.
2. Click **Yes** on the resulting confirmation screen, **Revert to Prior State Confirmation**, to complete the process. You can click **Yes** to the default settings or modify the **Reason for Revert**, if necessary. A link is also available to copy into the text box, the reason defined for the current state. Up to 255 characters are permitted for the reason.

A successfully reverted message is displayed at the bottom of the content pane.

4.2.2.9 Retention policies

This section includes the following topics:

4.2.2.9.1 Retention policy overview

This section includes the following topics:

4.2.2.9.1.1 In general

A retention policy is used to retain one or more objects according to conditional and/or chronological aging using lifecycles. You can create retention policies so that retention is based on a mixed mode setting to allow for chronological and conditional aging, instead of just one or the other.

A retention policy is the template object with the rules around how an object is managed according to a records lifecycle defined for the policy. The records lifecycle associated to a retention policy includes phases, durations and what happens at the end. Although the number of phases defined for a records lifecycle can vary, all records lifecycles have a final phase for disposition. Retainers are instances of retention policies and are spawned whenever a retention policy is applied. All retainers point to the policies that spawned them whether the policy was applied directly or inherited.

A retention policy determines the length of time an object is kept in a repository. The Properties of a retention policy include tabs for Info, Phases, Justifications, and History. The History tab includes details only if you have configured auditing for the retention policies. You can determine from its History tab, details about its creation and modifications. All metadata settings against a retention policy and its phases can be determined from the Info and Phases tabs.

Also, for details regarding records interoperability, refer to “[Records Interoperability with Content Intelligent Services \(CIS\)](#)” on page 31.

4.2.2.9.1.2 About retention policy lifecycles and retainers

A retention policy is defined with a lifecycle that moves an object through various phases of its life to the final phase for disposition treatment. Treatment, destruction of content and metadata along with export instructions if any, is based on the disposition strategy setting. A retention policy can be applied numerous times to different objects in a repository or file plan. A retainer is spawned each time a retention policy is applied to an object and therefore always references the retention policy. Although a retention policy cannot be deleted while it is referenced, it can be modified, though changes would affect only future objects to which it is applied. Only one retainer or multiple retainers are spawned depending on the retention strategy setting of the policy; one if set to linked or multiple if set to individual. This means objects in a cascade path, that is objects down a folder structure age together against one retainer or individually with their own retainers. A valid authority is mandatory for each phase to start the aging process of the retainer. The retainer stops aging if the phase entered is missing a valid authority. Aging resumes only when an administrator adds a valid authority by going to the properties of the

retention policy. Disabling the retention policy does not affect existing retainers and removes it from the list of available retention policies to choose from. Further details are provided in the following paragraphs.

Lifecycles determine the period of time an object (sysobjects and their subtypes) is retained in a repository according to operational, legal, regulatory, fiscal or internal requirements. A retention policy is defined by phases whereby each phase can have a duration. All of the phases together determine the period of time an object will age.

A retainer is spawned when a retention policy is applied directly to an object or when the object inherits the policy. It is the retainer that guards the object and each retainer spawned points to its respective retention policy. A retention policy can therefore have multiple retainers referencing it.

All objects that are under retention are protected from potential or inadvertent deletion. Only Records Managers can delete an object before it reaches disposition.

Retention policies when applied to a particular folder within a file structure, or file plan, cascade down the structure below the point of application. Retainers are created for each folder and their contents depending on the retention strategy specified, linked or individual. Though all objects are retained regardless of the retention strategy that is selected, child non-containing objects in a linked strategy share the retainer on the parent object and age with the parent object; the documents for example, would age with the folder. In an individual strategy however, separate retainers are created for each object, any time a new one is created or added; the documents for example would age separately.

Any folder-based object that has an individual retention policy applied to it will not have a qualification date and will not show up in promotion manager or disposition manager. Individual retention policies on folders do not age but rather propagate retention to its children. Physical boxes and physical folders show up only if a linked retention policy is applied. This applies to any folder-based object.

Aging can occur immediately, and/or can start based on an event. The mixed mode option on any phase can be used to trigger aging chronologically based on a based date or conditionally based on an event(s). All aging is dependent on a valid authority being present for the particular retention phase. Although an authority is optional, retainers will not start to age if a valid authority is not added to the phase.



Note: All of the attributes that cannot be changed once the policy is in use, are grayed out.

Disposition of the content and metadata of the object in the final phase, is determined by one of the following actions chosen for the Disposition Strategy: The disposition of a document or record in the final phase only, is based on one of the following options for the disposition strategy: The following are the options for the Disposition Strategy affecting only the Final phase of the retention policy:

- Unknown
- Review

- Export all, Destroy all
- Destroy all
- Export all
- Export all, Destroy content
- Destroy content
- NARA transfer, Destroy content
- NARA transfer, Destroy all



Note: NARA only appears if the Department of Defense Standard dar is installed. Objects in disposition that were NARA transferred display more details if the objects are Department of Defense Standard formal records, Department of Defense Classified formal records, or formal folders. Only limited details are displayed in disposition, for all other objects that are NARA transferred.

These options, except Unknown and Review, ensure that the objects are either destroyed, copied, or transferred to a new external directory.

Unknown allows the objects to reach the end of the retention policy but will not perform disposition until the retention policy final action has been updated to one of the other disposition strategies. Review; Export All; Export All, Destroy Content; and Destroy Content must specify a rollover retention policy as these are non-terminating and will NOT destroy both content and metadata. Rollover does not need to be specified for Export All, Destroy All and Destroy All as these are terminating and will destroy all content and metadata. Destruction methods include:

- Dispose
- Privileged delete

Dispose removes an object from the repository when the object reaches the Final phase for disposition. Privileged delete provides the ability to delete an object before it reaches the disposition phase. Digital shredding is available for file store storage areas. Digital shredding is a process that removes objects in shredding-enabled storage areas and renders them irretrievable. For information on digital shredding, refer to *OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS-GGD)*.

For a description of the Disposition Strategies, refer to “[Disposition strategy descriptions](#)” on page 149. The actions that can or cannot be taken are identified in “[Disposition strategy actions](#)” on page 150. The Unknown and the Review strategies are not listed in the actions table as they are not associated with any strategy actions. The NARA transfer strategies are also not listed as they too are special cases which require confirmation of transferred items.



Note: Records, returned in search results, that had only its content destroyed does not mean that the user has a permissions or browser problem.

Table 4-14: Disposition strategy descriptions

Disposition strategy	Rollover required	Description
Unknown	NA Must be resolved to another strategy.	Is a special case for which an override disposition strategy must be specified when disposition is performed. Unknown allows the objects to reach the final phase of retention but will not perform disposition until the retention policy final action has been updated to one of the other disposition strategies. A rollover must also be specified if the override selected is non-terminating. Overrides are used exclusively for Unknown.
Review	Yes	Object should be reviewed and when disposition is run will rollover to another retention policy.
Export all, Destroy all	No	Places a copy of the document and a copy of its associated metadata in a location on the Application server, then destroys the source document, both its content and metadata.
Destroy all	No	Destroys both content and metadata of the source document.
Export all	Yes	Places a copy of the document and a copy of its associated metadata in a location on the Application server, without destroying the source document.
Export all, Destroy content	No	Places a copy of both the content and its associated metadata in a location on the Application server, destroying the content of the source document but not its associated metadata.
Destroy content	Yes	Destroys the content of the source document but not its metadata.
NARA Transfer, Destroy content	Yes	This is the same as the export strategy. The difference is that the data that is exported is in XML format that complies to the Department of Defense/NARA schema and that the export process needs to be confirmed. Metadata in the original location however is not destroyed.
		 Note: Records Manager raises an alert or warning, a popup message, that all PDF records to be transferred or accessioned to NARA must include embedded fonts.

Disposition strategy	Rollover required	Description
NARA Transfer, Destroy all	No	<p>Same as NARA Transfer, Destroy content but also destroys the metadata.</p> <p>This operation is also called NARA Accession, the act of transferring physical custody of documentary material to an archival institution. In this case specifically for the National Archives and Records Administration (NARA) regulations.</p>

Table 4-15: Disposition strategy actions

Disposition strategy	Retention Policy Services Only Actions					Additional Actions with Physical Records Manager				
	Export content	Export metadata	Destroy content	Destroy metadata	Physical Object Marked for Export	Physical Object Marked Shipped	Physical Object Exported	Physical Object Marked for Destruction	Physical Object Destroyed	
Export all, Destroy all	Yes	Yes	Yes	Yes	Yes	Yes	Yes	n/a	n/a	
Destroy all	No	No	Yes	Yes	No	No	No	Yes	Yes	
Export all	Yes	Yes	No	No	Yes	Yes	Yes	No	No	
Export all, Destroy content	Yes	Yes	Yes	No	Yes	Yes	Yes	n/a	n/a	
Destroy content	No	No	Yes	No	No	No	No	Yes	Yes	



Note: The four core Retention Policy Services actions are export content, export metadata, destroy content, and destroy metadata. Five additional actions are included if Physical Records Manager is installed. If Physical Records Manager is installed, keep in mind that any physical object that is exported will not be followed by a destructive action as indicated with n/a, meaning not applicable

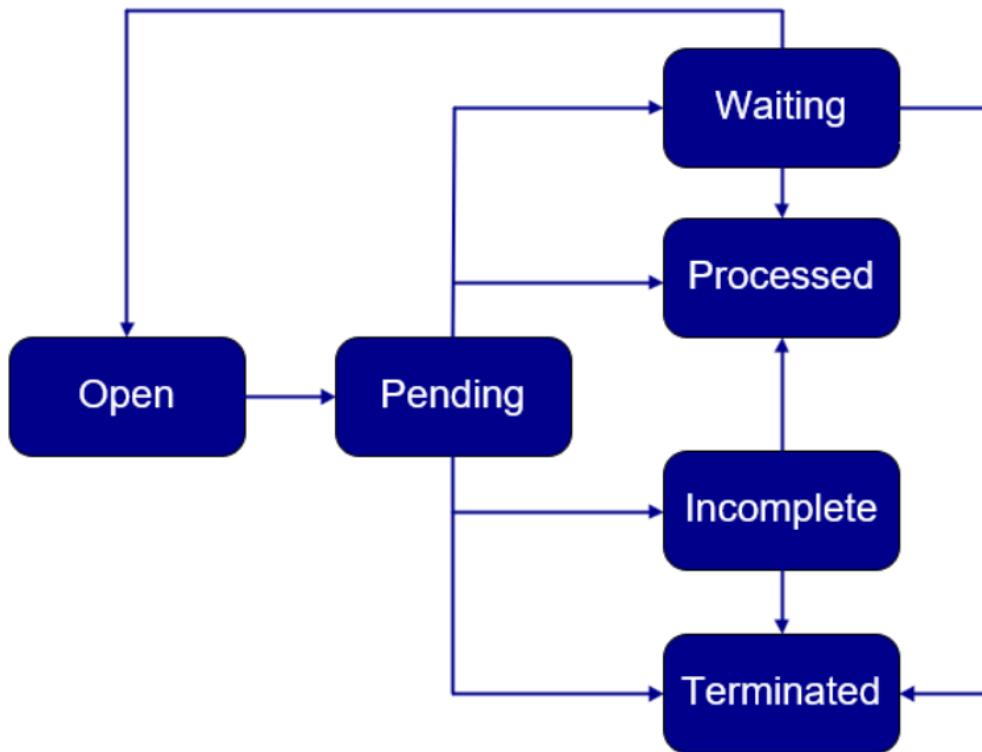
or no action, as shown for Export all/Destroy all and for Export all/Destroy content.

A sixth Physical Records Manager action Marked for Contained Objects Destruction is not included in the table as it is a special instance of Physical Object Marked for Destruction. Although a container and its contents can be destroyed through the disposition process (or otherwise), a structural container cannot. Only the contents of a structural container can be destroyed. Therefore, Marked for Contained Objects Destruction is used (instead of Physical Object Marked for Destruction) to mark only structural containers that are run through disposition. To learn more about structural retention and structural containers, refer to “[Retention policy overview](#)” on page 146 and “[Creating a retention policy](#)” on page 156.

Status on the disposition strategies is tagged using one of six labels when you view applied retention.

- Open: no disposition action has been taken yet.
- Pending: disposition is invoked (but not yet started; it will be initiated once all the retainers on the object are set to Pending and all its specified disposition actions can be executed).
- Incomplete: disposition processing on the object is not completed. This is not necessarily an error condition. For example, when disposing physical objects, someone has to perform a manual action on the objects and then inform the system that it has been done (for example, marking for destruction, confirming that the items have been destroyed).
- Processed: disposition processing on the object is completed. Processed only appears if the retention policy does not destroy the object. This means that a rollover to a new retention policy has occurred.
- Terminated: disposition was invoked using a destructive strategy on the object but destruction of the object is delayed. It is marked to be destroyed but is protected by another retention policy until it can perform disposition.
- Waiting: disposition was invoked and partially finished but could not continue processing until further user action is taken such as transfer confirmation or rejection.

[Figure 4-4](#) illustrates the possible states for an object under disposition in the final phase of a retention policy.

**Figure 4-4: Disposition state diagram**

You can determine the status from Records > Reports > Retention Report. To obtain a report on the Disposition Status of objects being retained, refer to “[Running the retention report](#)” on page 247.



Note: Terminated is the disposition status assigned to a destructive retainer when its disposition action to destroy the object/metadata is prevented by other conditions/retainers that are present on the same object. Destructive retainers are associated with terminating disposition actions while nondestructive retainers are associated with non-terminating disposition actions. Destructive retainers are associated with two possible destructive actions that destroy metadata, Destroy All and Export All, Destroy All, refer to the table in the “[Overview of disposition](#)” on page 222 for further clarification about the various disposition actions. Only those retainers that specify one of these two actions can be marked Terminated when disposition is invoked, whether manually or automatically. Take for example a document linked to multiple folders, two folders for example, one with a retention policy that specifies a destructive action and the other with a retention policy that specifies a nondestructive action. If disposition is invoked against the destructive retainer, the document is then unlinked from that folder and the retainer is marked Terminated. A terminated retainer is usually accompanied by the attachment of a terminal retainer which ensures that the object will be

eventually destroyed if the other retainers do not do it (if the other retainers are removed for example). The dmc_rps_TerminalDispositionJob when run will then destroy the document, assuming that no other retainer is holding it up. It should also be noted that the document will NOT be unlinked from a folder if it still has an unprocessed retention that is inherited from the same folder or if it is the only folder the document is linked to.

Once a terminal retainer is applied to a folder, no other objects can be linked to that folder. This affects all users including Retention Managers.

To better understand the disposition process as it relates to a *simple object* or a *complex object*, refer to “[Disposition Manager](#)” on page 222.

During the creation of a retention policy, you have the option of specifying the immutability selection. Applying retention to an object makes the content immutable regardless of this option. This option is for metadata immutability! This selection of the immutability is specific to the application of the retention policy and does not modify or change any pre-existing application of immutability. The Make Parent Metadata Immutable field provides two choices: No and Yes. When you select No, the original immutability settings are not changed by the application of the retention policy. When the administrator selects Yes, the immutability setting is applied by the retention policy and as such, certain property fields (metadata) cannot be altered.

During the creation of a retention policy, you can select whether to protect the renditions from deletion. The Parent Rendition Rule provides two options to choose from: All Renditions and Primary Format Only. If you select All Renditions, the retention policy extends itself to protect all renditions and the primary document from deletion. If you select Primary Format Only, only the primary document is protected from deletion, the renditions can be deleted as the retention policy does not extend itself to protect renditions of the primary document.

The Virtual Document Retention Rule allows you to retain only the root of the virtual document or the root of the virtual document and its child documents by selecting either Retain Root Only or Retain Root and Children.

Similarly, the Snapshot Retention Rule allows you to retain only the root of the snapshot or the root of the snapshot and its child documents by selecting either Retain Root Only or Retain Root and Children. Snapshots are created when formal records are declared using the Records Manager product.

The Make VDM/Snapshot Children Metadata Immutable is extended only to the child docs of a retained VDM or snapshot. Snapshot metadata and all of the children metadata is immutable if this is turned on.

Similarly, the VDM/Snapshot Children Rendition Rule is extended only to the child docs of a retained VDM or snapshot. If all renditions is selected it means that all of the renditions on the snapshot are protected along with all renditions on every child in the snapshot.

The defined stages of a retention policy are phases. The attributes that can be specified for each phase are:

- Phase Name
- Duration
- Cut-off period
- Conditions
- Authorities
- Action Name

4.2.2.9.1.3 About qualification date calculation



Note: The qualification date for each phase is calculated as follows. This is how retainers start to age, once the qualification date is calculated:
Chronological: Base Entry Date + Cut-off + Phase duration = Qualification date for the phase
Conditional: Event Date + Cut-off + Phase duration = Qualification date for the phase.

When using mixed aging, the calculation model can vary. For further details refer to the Mixed mode matrix table in “[Creating a retention policy on page 156](#)”.

The cut-off period is involved in the calculation of the qualification date that is calculated for each phase. Cut-off takes the initial date (base date mapping if chronological) or the Event date if conditional for the phase and rounds up the value. The duration of the phase is normally added to this rounded up value to determine the qualification date. For example:

An administrator creates a base date mapping that maps Last Review Date to dm_document. A document has the last review date set to February 2, 2009. A retention policy is created with the first phase set to: Cut-off Annually, on Month: 1, Day: 1, and the phase duration is set to 5 years, a valid authority is added, and there are no conditions specified. Retention is then applied to this document. The initial date is February 2nd, 2009 and this date has to be rounded-up according to the specified cut-off value. The rule states to round up to the first month and the first day of the year. The new date then becomes January 1st, 2010. To this the duration is added and the qualification date is January 1st, 2015. This means that the object cannot be promoted into the next phase until this date has been reached. For this example, settings on the Phases tab are set.

[Figure 4-5](#) shows how the document is processed according to the settings used for this example:

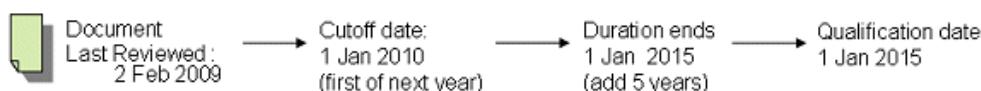


Figure 4-5: Processing results

4.2.2.9.1.4 About the Justifications tab

The Justifications tab provides details about:

- The reason for creating a retention policy. For further details refer to “[Creating a retention policy](#)” on page 156.
- The reason for modifying a retention policy. For further details refer to “[Viewing/modifying a retention policy, applied retention, or retainer properties](#)” on page 184.
- The reason for deleting a retention policy is carried in the audits. For further details refer to “[Deleting a retention policy](#)” on page 198.

Creation and modification dates along with the user are also listed on top of each reason displayed. Users are required to enter a mandatory reason for the justification each time they create, modify, or delete a retention policy.

4.2.2.9.1.5 About the History tab

The History tab captures the creation date of the retention policy and all of the changes that were made to it over its life based on registered audit events. It can be used to determine the dates on which changes were made and to compare current settings to previous settings. Audit trails cannot be captured unless the respective audit events have been registered first. The following audit events, which are also listed in the Retention Policy Services audit events table, must be registered against the object type dmc_rps_retention_policy to view anything in the History tab:

- dm_save
- dmc_rps_create_retention_policy
- dmc_rps_save_retention_policy
- dmc_rps_update_phase_rel
- dmc_rps_add_action_rel
- dmc_rps_update_action_rel

For a complete list of Retention Policy Services audit events and a description of the information stored in the strings of an audit event, refer to “[Retention Policy Services audit events](#)” on page 281. To register (enable) an audit event, refer to “[Enabling auditing](#)” on page 80.

Warning messages will be displayed if any of the Retention Policy Services audit events, that must be registered, are not registered. If no audit trails have been logged for a selected date range, a message will also be displayed to let you know.

The History tab consists of 3 major sections (panes) and are used and interpreted as follows:

- Audit Selection

This section shows the creation information associated with the selected policy and allows you to query against a specific date range to determine if any audit

trails were logged. If any changes were made within the date range specified, the dates on which those changes were made would be reported in the list box for the Select Audit Date. You can then select a specific audit date of interest from the list box and then refer to the Retention Policy and Phases sections to see which attributes changed or did not change, by comparing the entries in the Current Value field with those in the Previous Value field. The most recent audit, for any date range, is always displayed by default at the top of the list box.

- **Retention Policy**

When you select a date from the list box in the Audit Selection section, refer to this section for any changes to the attributes of the retention policy. This pertains to the attributes on the Info tab of the selected policy.

- **Phases**

When you select a date from the list box in the Audit Selection section, refer to this section for any changes to the attributes on the phases of the retention policy. This pertains to the attributes on the Phases tab of the selected policy.

The History tab is useful to determine dates of creation and modification and to compare previous values to current values. The Audit Trail Report however, can be used to determine further details against the following audit events:

- dmc_rps_create_retention_policy
- dmc_rps_destroy_retention_policy

There is no audit event to report on against retention policies that are modified. Use the History tab instead to obtain details about any modifications.

4.2.2.9.2 Creating a retention policy

Instructions in this section are intended to create new policies from scratch whereas, instructions in “[Copying, exporting, and importing retention policies](#)” on page 173 are intended to create new policies from existing policies.

Confirmation may or may not be mandatory for each retention policy that is created, modified, or deleted. Mandatory confirmation however, can be turned off when necessary on the rps_docbase_config file. The attribute that controls this setting is labeled Enable Mandatory Justification Field. For further details to turn this setting on or off, refer to “[System configuration options settings](#)” on page 121.

Retention policies can be created to be driven in chronological mode, conditional mode, or mixed mode to use both chronological and conditional modes.

Retainers do not start to age unless a valid authority is added to the retention policy.

To create a retention policy:

1. Navigate to **Retention Policy Services > Retention Policies** and select **File > New > Retention Policy**.

The **New Retention Policy** screen is displayed.

2. Type a unique name for the **Name**.
3. Select a **Lifecycle** from the list box. Six lifecycles are available out-of-the-box:
 - 1 Phase + Final
 - 2 Phases + Final
 - 3 Phases + Final
 - 4 Phases + Final
 - 5 Phases + Final
 - 6 Phases + Final
4. Click **Next** to accept entries and to display the **Info** tab.



Note: Additional information or attributes are displayed on the properties of a retention policy; to compare, refer to “[To view or modify the properties of a retention policy](#)” on page 184. The properties of a retainer spawned against a retention policy is mostly read-only; to compare, refer to “[To view or modify the properties of a retainer](#)” on page 188.

5. Enter values for all the mandatory attributes, described in “[Attribute values described on the Info tab](#)” on page 157, and for any optional attributes as needed.

Mandatory attributes are identified with an asterisk.



Note: Half of the mandatory attributes are already populated according to auto-default values. Though you can change the auto-default values if necessary, you do have to specify a value for those mandatory attributes which indicate *Please Select*.

Table 4-16: Attribute values described on the Info tab

Attribute	Description
Name	The value in this field is auto-populated according to the value you provided on the Create tab.
Description	Describe its usage, why or what it is needed for, whether it cascades or not, and so forth. A short description is recommended, in particular to benefit imported policies. The Import Policy page includes a Description column. Therefore the shorter the description, the better it will fit into the column.

Attribute	Description
Referenced	<p>A retention policy referenced by any of its retainers cannot be deleted until all retainers stop aging and go away or are deleted. The name of the retention policy can be changed only when it has no retainers referencing it. The default value in this field is set to <i>False</i> and remains <i>False</i> until at least one retainer is spawned. All new retention policies indicate <i>False</i> until the policy is applied to at least one object. Each retainer spawned when a retention policy is applied to an object references its retention policy.</p> <p>The default value automatically changes to <i>True</i> once the policy is referenced by a retainer.</p>
Enabled	<p>This checkbox controls the applicability of the retention policy, whether it can be applied to an object or not. It is selected, set to <i>True</i>, by default so that it can be applied immediately after it is created. Administrators can disable it to prevent further usage when necessary. A policy cannot be modified once it is in use (referenced), that is once it is applied to an object, unless it is disabled. Existing objects already referencing the policy are not affected when it is disabled.</p> <p>Usage of this checkbox depending on intent, might be for example, to disable the policy to commission a newer version. In this case, you can disable the policy to decommission the current version and modify a copy of it to create the newer version. The new version or copy can then be commissioned or enabled when necessary. Using the current version as a base copy for only a few modifications prevents unnecessary effort and possible mistakes. The need to reenter everything from scratch to create a newer version of the same policy can be avoided.</p> <p> Note: Disable the policy when making a copy of it, to prevent anyone from applying it while it is being modified, unless there is a reason to use both the old version and the new version. For complete details about copying retention policies, refer to “Copying, exporting, and importing retention policies” on page 173.</p>

Attribute	Description
Supersede On New Version	<p>Selecting the checkbox for this option means retainers on all versions, except the Current version, of the object created as a result of check-ins are promoted directly to the Final Phase, while the retainer on the <i>Current version</i> object continues to age normally.</p> <p>If you apply a supersede retention policy to an object and then version it and the current version is not retained the old version is not superseded - it will become superseded when the current version is retained (it can be retained by any policy and does not have to be a policy with supersede on it).</p> <p>Retainers on all versions, including the Current version of the object, will age normally if this option is not selected.</p> <p>If you use a <i>linked</i> retention policy with the <i>supersede checkbox enabled</i> and you apply the policy to a <i>folder</i>, the supersede functionality will NOT work as folders cannot be versioned in OpenText Documentum CM. The supersede functionality should only be used with retention policies that have Individual selected for the retention strategy.</p> <p> Note: Supersede functionality associated with this check box is completely different from supersede functionality in record relations. Retention supersede occurs when a newer version of an object causes the older version to go directly to the disposition phase whereas the objects in a supersede record relation are not related at all.</p>
Metadata Immutable	<p>When selected, makes metadata immutable. Applied retention on a folder with this option selected prevents folder linking or unlinking. The folder cannot be moved (unlinked) from its existing location or linked to another folder. This setting however does not affect the documents inside the folder and therefore any of the documents contained can be moved, unlinked or linked (assuming sufficient permissions).</p>
Cascade To Subfolders	<p>Controls whether the retention policy can cascade (propagate) from the point of application, that is from the parent folder to its sub folders (or children). All sub folders, when the checkbox is selected, inherit retention from the parent folder. Deselecting the checkbox prevents cascading.</p>

Attribute	Description
Cascade To Subcategories	<p>This option is displayed only if Content Intelligent Services (CIS) is enabled and when Cascade to Subfolders is selected. This option is not available when Cascade To Subfolders is deselected. This option, though similar to Cascade To Subfolders, is used in conjunction with taxonomies. A retention policy that is applied to a category, of a taxonomy, when the checkbox is selected, will cascade to all sub categories. Deselecting the checkbox prevents cascading.</p>
Structural Retention Type	<p>A container object that is under structural retention makes it a fixed container object that cannot be deleted or destroyed when it is up for disposition. A container object selected within a file plan for example, remains a non-structural container, meaning that it can be deleted or destroyed upon disposition, unless this option is selected. If selected, only the contained items, once they reach disposition in the final phase, would be disposed. Once the container object is emptied as a result of disposition, the retainer is reset and any new items added would start to age all over again beginning in phase 1.</p> <p>Resets the retainer on the folder or category after a disposition run that disposes the contained items. Only the contained items are disposed of, not the folder or category itself, and retention aging starts all over again based on a new entry date. For example, assume an initial entry date of 2000. Linked retention applied to the container retains the content for 5 years and disposes the contents in 2005. The retainer on the container is reset to start aging based on the new entry date, 2005. The container however, is also destroyed if this option is turned off (deselected).</p> <p>This option can be set only when the value for the Retention Strategy is set to <i>Linked</i> and if the value for the Disposition Strategy does not require a rollover. This option is not available (is grayed) if the Retention Strategy is set to <i>Individual</i>.</p> <p>Disposition strategies that do not require rollover include:</p> <ul style="list-style-type: none"> • <i>Export all, Destroy all</i> • <i>Destroy all</i> • <i>NARA transfer, Destroy all</i>

Attribute	Description
*Retention Strategy	<p>The setting for this will determine whether each object within a folder structure is associated to its own retainer object or whether the parent (folder) object and child object(s) share a common retainer. Child objects will age with the parent folder in a <i>Linked</i> strategy or independently in an <i>Individual</i> strategy.</p> <p>All the documents in a folder, when the <i>Linked</i> strategy is used, would age together according to the folder retainer. The documents would otherwise age separately if the <i>Individual</i> strategy is used.</p>
*Disposition Strategy	<p>The Disposition Strategy selected determines the action that will be taken for the retained object when it is processed in the final phase by Disposition Manager. There are several disposition strategies to select from, described in the “Retention policy overview” on page 146.</p> <p> Note: The folder itself when an individual strategy is applied to it, does not age.</p>

Attribute	Description
<p>*Rollover Retention Policy</p>	<p>This option can be set only if the Disposition Strategy specifies a non-terminating value. This option is not available (grayed) if the Disposition Strategy is set to:</p> <ul style="list-style-type: none"> • <i>Unknown</i> • <i>Destroy all</i> • <i>Export all, Destroy all</i> • <i>NARA Transfer, Destroy all</i> <p>Rollovers are mandatory if you create a retention policy that is non-terminating. Though optional, this field is Read-Only depending on the value selected for the Disposition Strategy. A retention policy will rollover to another retention policy if the Disposition Strategy selected is non-terminating. Export All, for example, is non-terminating whereas Destroy All is terminating.</p> <p>Select Retention Policy becomes selectable only when a non-terminating Disposition Strategy has been selected.</p> <p>A non-terminating retention policy is one whose disposition strategy leaves behind the metadata and/or the metadata and the content.</p> <p> Note: When rollover occurs, triggered through disposition, the rollover retention policy will only be applied to the set of objects that are single retainer managed. So when a linked retention policy does a rollover only the folder and the contained documents managed and aged through a single retainer will have the rollover policy applied to them. Any subfolders, which are managed and aged through separate retainers, will only have the rollover policy applied to them when their retainer has been triggered for rollover (disposition).</p> <p>Although rollover retention policies no longer cascade into child folders, existing rolled over retentions are grandfathered with the original inheritance pattern.</p>
<p>*Make Parent Metadata Immutable</p>	<p>This field has an auto-default value already specified which you can change as needed.</p> <p> Note: Regardless of the option settings the content is always immutable when retained.</p> <p><i>No</i> means the original immutability setting on the object, whether mutable or immutable prior to the application of a retention policy, will be honored.</p> <p><i>Yes</i> means the metadata for the object under retention can NOT be edited, regardless of whether the object metadata was immutable or not before the retention policy was applied.</p>

Attribute	Description
*Parent Rendition Rule	<p>This field has an auto-default value already specified which you can change as needed.</p> <p><i>Primary format only</i> means only the object to which retention was applied will be protected from deletion and retained.</p> <p><i>All Renditions</i> means the original object and any renditions will be retained. A Word document for example and its PDF rendition.</p>
*Virtual Document Retention Rule	<p>A virtual document and its attachment(s) are retained if <i>Retain Root and Children</i> is selected. Only the virtual document parent, and not the child attachments, is retained if <i>Retain Root Only</i> is selected.</p>
*Snapshot Rendition Rule	<p>A snapshot and its attachment(s) are retained if <i>Retain Root and Children</i> is selected. Only the snapshot parent, and not the child attachments, is retained if <i>Retain Root Only</i> is selected.</p> <p>Snapshots are created when a formal record is declared.</p>
*Make VDM/Snapshot Children Metadata Immutable	<p>This field has an auto-default value already specified which you can change as needed.</p> <p>The immutability rule is extended to the child documents in a snapshot.</p> <p><i>No</i> means the original immutability setting on the child object in a snapshot, whether mutable or immutable prior to the application of a retention policy, will be honored.</p> <p>The metadata for the snapshot itself is also immutable if this is turned on. <i>Yes</i> means the metadata for the child object in a snapshot under retention can NOT be edited, regardless of whether the child object metadata was immutable or not before the retention policy was applied.</p> <p> Note: The snapshot itself is not affected by this setting. If you want the snapshot to also be immutable then set the option for Make Parent Metadata Immutable.</p>
*VDM/Snapshot Children Rendition Rule	<p>This field has an auto-default value already specified which you can change as needed.</p> <p>Renditions on the snapshot are also retained if this is turned on. Renditions of the child documents that are in a snapshot are retained if the extended rendition rule says <i>All Renditions</i>. Only the child documents, not their renditions if any, are retained if <i>Primary format only</i> is selected.</p>

Attribute	Description
 Note: The following additional options are displayed, between the above attribute and the one below, on the properties of retention policies that have been either copied or imported. The Creation Method , Source Policy Name , and Source Repository are displayed on copied policies. Imported By and Exported By are additionally displayed on imported policies. These are not displayed during the normal creation of a retention policy, using this procedure. For additional details regarding copying or exporting and importing retention policies, refer to “ Copying, exporting, and importing retention policies ” on page 173.	
Global Conditions	<p>A global condition causes the object to go to the last phase if it is fulfilled. This special type of condition is outside of the phases of the retention policy. A global condition will override a standard condition if any are added to the Phases tab. For more information on global conditions, refer to “Global conditions” on page 209.</p> <p> Note: A global condition can be added during the creation of a retention policy or from its properties when it is not in use (not applied). Although a global condition cannot be added to the properties of a retention policy while it is in use, a global authority can. Retainers spawned from a retention policy when it is applied to an object start to age only when a valid global authority is added. A valid authority, whether one is being added for a global condition or a phase condition, can be added during the creation of the retention policy or from its properties. The Global Event Date or the phase Event Date however, can be added only after the retention policy has been applied to an object, that is from the properties of the retainer. To add a global authority or phase authority, refer to “To view or modify the properties of a retainer” on page 188. If multiple global conditions are added, the one with the latest date specified is used. Global Conditions are called Global Events on the properties of a retainer and similarly, phase Conditions are called Events.</p>
Global Authorities	<p>All phases in a retention policy require an authority present for aging to occur. If a particular phase does not have an authority, aging for that phase cannot be calculated and objects can only be promoted to that phase and no further until an authority is added. The retainers will start the aging process only when a valid authority is added.</p>

- Click **Next** to accept your values or the default values on the **Info** tab and to display the **Phases** tab. The most prominent phase is the phase being viewed.

 **Note:** The **Final** phase, when it is selected, displays the **Requires Approval** option between the **Phase Name** and the **Duration**. Approval will be required for disposition if it is selected. To better understand the

phase settings and the mixed mode rules, refer to “[About the final phase and the mixed mode settings](#)” on page 165.

7. Click the phase for which you want to change the default values and then click **Finish** when you are satisfied with the entries for each phase.

The **Confirm Retention Policy Creation** screen displays for confirmation, **Are you sure you want to create the retention policy?**

8. Click **OK** to complete the process or **Cancel** to back out if necessary.

The **Reason for creating policy** text however, may or may not be mandatory for confirmation depending on the setting in the Retention Policy Services Application Configuration file. If the red asterisk is displayed it means that the attribute labeled **Enable Mandatory Justification Field** on the configuration file is selected. For further details, refer to “[System configuration options settings](#)” on page 121. A reason must be provided when it is mandatory. A warning is otherwise displayed if you confirm without an entry, reminding you that **The Justification field is mandatory**. A warning against the text entered will also be displayed, in red, if it exceeds 255 characters.

4.2.2.9.2.1 About the final phase and the mixed mode settings

The **Final** phase is selected in the following example, to show you the **Requires Approval** attribute. Conditions cannot be added or removed if the retention policy is in use.

The **Phase Name** identifies the phase affected by the values entered. The mandatory **Phase Name** must not be left blank. You can change it for any phase by clicking the phase icon or its name below the icon. It cannot be changed however, once the policy is in use.

The **Requires Approval** attribute is displayed on the **Final** phase only. Selecting the checkbox for this attribute ensures the record is reviewed and approved before disposition is performed. If set to false, disposition will not require an approval before proceeding.

The phase **Duration** specified in terms of Days, Months, and Years, determines the length of time the aging process will last for once it is triggered based on an event fulfilled for conditional aging or a date fulfilled for chronological aging.

The **Cut-off period** is optional. The cut-off period affects the qualification date rounding it up to the interval specified *Monthly*, *Quarterly*, *Semi-annually*, or *Annually*. Any object that qualifies after the cut-off date will not be qualified until the next cut-off period. Any object that cannot be qualified by the cut-off date will only be qualified for the next cut-off period. All objects that are retained can be rounded up to a specific value. For example, fiscal records can start aging for the appropriate fiscal year. A retainer will not start aging however, unless a value for the **Authority** is added. These entries can be provided anytime from the Properties of the retention policy.

The cut-off or rounding up is used with events and without them, the event date that is entered is rounded up.



Note: The rules for mixed mode settings, provide flexibility to start the aging process based on the rule combination selected when a condition is added to a retention policy. The effects on qualification date calculations and aging, for the different combinations that can be selected, are described in the Mixed mode matrix table that follows.

The mixed mode rule is enabled only if at least one condition is specified. The mixed mode rule indicates how aging is calculated:

- Serial: is the default and means that when the events are fulfilled, use that date, apply the cutoff period, and then add the duration. If there is more than one event fulfilled, event selection rule defines which event to use (either the earliest or latest). Duration is added to the event fulfillment date for only this rule, if the policy is Conditional.
- Early Parallel: This setting allows for a calculation where two paths are evaluated, the Chronological path, and the Conditional path. When the two paths are evaluated, the qualification date becomes the shorter of the two paths.
- Late Parallel: The same as Early Parallel except the later of the two dates is used for the qualification date.

For both parallel options, the Conditional path does not add duration to the event dates.

The Event Fulfillment Rule is used to determine whether all events are mandatory or optional or if any single event is sufficient. [“Mixed mode matrix” on page 167](#) describes the aging behavior based on the combination selected for the Mixed mode Rule and the Event Fulfillment Rule.

Table 4-17: Mixed mode matrix

	All events are mandatory	All events are optional	Any one event is mandatory
Serial	<p>This is the original behavior that was only available in previous releases. Aging does not start until all events are fulfilled.</p> <p>Qualification date is calculated as follows:</p> <ul style="list-style-type: none"> • Take the event date (defined by selection rule of either earliest or latest) • Apply the cutoff (if specified) • Add the duration 	<p>Aging continues chronologically unless an event occurs to trigger recalculation. When the first event is fulfilled, the event date will be used instead of the entry date. If subsequent events are fulfilled, the event selection rule determines whether to use the earliest or latest date.</p>	<p>Aging does not start unless at least one event is fulfilled. When the event is fulfilled, cutoff is applied and then duration is added. If subsequent events are fulfilled, the event selection rule determines whether to use the earliest or latest date.</p>

	All events are mandatory	All events are optional	Any one event is mandatory
Early Parallel	<p>This combination means that aging does not start until all events are fulfilled. Qualification date is calculated as follows:</p> <ul style="list-style-type: none"> After all the events occur:- Apply cutoff to event date to determine the Conditional Path. Apply the cutoff to the starting date, add duration, to determine the Chronological Path. Choose the earlier of dates between the Conditional Path versus the Chronological Path. 	<p>If no events are fulfilled, aging continues chronologically. However, when an event is fulfilled, two different paths are evaluated:</p> <ul style="list-style-type: none"> Chronological Conditional: Use this combination when you want to normally chronologically age a certain period but have an exception event that moves up qualification date. <p>If the event is not fulfilled, apply the cutoff to the starting date and add the durationIf at least one event is fulfilled:</p> <ul style="list-style-type: none"> Apply cutoff to event date to determine the Conditional Path. Apply the cutoff to the starting date, add duration, to determine the Chronological Path. Choose the earlier of dates between the Conditional Path versus the Chronological Path. 	<p>This combination is similar to the early parallel, all events are optional except that aging calculations cannot be started until at least one event is fulfilled.</p> <p>Qualification date is calculated as follows:</p> <ul style="list-style-type: none"> After at least one event occurs, apply cutoff to event date to determine the Conditional Path. Apply the cutoff to the starting date, add duration, to determine the Chronological Path. Choose the earlier of dates between the Conditional Path versus the Chronological Path.

	All events are mandatory	All events are optional	Any one event is mandatory
Late Parallel	Similar to the above combination except the later of the two paths is used.	Similar to the above combination except the later of the two paths is used. This combination is useful if you want to use an event to push out the qualification date.	Similar to the above combination except the later of the two paths is used.

For our example, use the following settings on the retention policy as a base.

Assume the base date is Jan 1, 2010. Settings in our example for the mixed mode rule and the event fulfillment rule will be varied. For simplicity, the event selection rule will not vary and will be set to the latest event date. If you want to try this example yourself, apply retention to an object and then use the qualification manager to requalify (make sure to select the checkbox for Allow re-qualification before clicking Search) after making the changes to the phase. Make sure you add a valid authority to every phase.

"Retention policy changes and effect on objects that already have the policy applied" on page 169 describes various changes that could be made to a retention policy that has already been applied, and what happens to existing objects that have that retention policy applied.

Table 4-18: Retention policy changes and effect on objects that already have the policy applied

Action	Description	Next step to put change into effect
Add valid authority assuming there were no valid authorities on the current phase of the retention policy.	Changes will only go in effect for new applications of the retention policy. This includes documents that are linked into folders with individual retention or folders that are linked into folders with linked retention.	In the Qualification Manager, perform a search and qualify. The alternate method is to run the qualification job. To update the previously qualified objects, the Re-qualify option from the Qualification Manager needs to be run.
Remove all valid authorities from the current phase of the retention policy.	Changes will only go in effect for new applications of the retention policy. This includes documents that are linked into folders with individual retention or folders that are linked into folders with linked retention.	In the Qualification Manager, click the allow re-qualify checkbox, perform a search, and qualify.

Action	Description	Next step to put change into effect
Change duration or cut-off on the current phase of the retention policy.	Changes will only go in effect for new applications of the retention policy. This includes documents that are linked into folders with individual retention or folders that are linked into folders with linked retention.	In the Qualification Manager, click the allow re-qualify checkbox, perform a search, and qualify.
Change duration or cut-off on a subsequent or future phase of the retention policy.	When objects are promoted into the next phase the new values will be used to calculate the qualification date.	No manual action required.
Change the mixed mode setting of the retention policy.	Changes will only go in effect for new applications of the retention policy. This includes documents that are linked into folders with individual retention or folders that are linked into folders with linked retention.	In the Qualification Manager, click the allow re-qualify checkbox, perform a search, and qualify.

After the change is made, if an event date is set or cleared, Retention Policy Services will automatically try to requalify.



Note: If an event date is set or cleared programmatically, through IAPI or Webservices, Retention Policy Services will automatically try to qualify or unqualify.

Example 1, “Determining qualification date example when no event date set” on page 171: no event date is set.

Table 4-19: Determining qualification date example when no event date set

	All events are mandatory	All events are optional	Any one event is mandatory
Serial	(none - not all events fulfilled)	Event Does not happen, only one path Duration Path Entry Date: Jan 1, 2010 Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Qualification Date: Sept 15, 2013	(none - need one event fulfilled)
Early Parallel	(none - not all events fulfilled)	Event does not happen, only one path Duration Path Entry Date: Jan 1, 2010 Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Qualification Date: Sept 15, 2013	(none - need one event fulfilled)
Late Parallel	(none - not all events fulfilled)	Event does not happen, only one path Duration Path Date: Sept 15, 2013 Qualification Date: Sept 15, 2013	(none - need one event fulfilled)

Example 2, “Determining qualification date example when 1 of 2 event dates set” on page 172: set End of Employment event to May 1, 2010. Only one of the 2 event dates is set.

Table 4-20: Determining qualification date example when 1 of 2 event dates set

	All events are mandatory	All events are optional	Any one event is mandatory
Serial	(none - not all events fulfilled)	Event date: May 1, 2010 Apply cutoff: Sept 15, 2010 Add duration 3 years = Qualification Date: Sep 15, 2013	Event date: May 1, 2010 Apply cutoff: Sept 15, 2010 Add duration 3 years = Qualification Date: Sep 15, 2013
Early Parallel	(none - not all events fulfilled)	Duration Path Entry Date: Jan 1, 2010 Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Event path Event Date: May 1, 2010 Apply Cutoff: Sept 15, 2010 Earliest of two paths: Event Path: Sept 15, 2010 Qualification Date: Sept 15, 2010	Duration Path Entry Date: Jan 1, 2010 Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Event path Event Date: May 1, 2010 Apply Cutoff: Sept 15, 2010 Earliest of two paths: Event Path: Sept 15, 2010 Qualification Date: Sept 15, 2010
Late Parallel	(none - not all events fulfilled)	Latest of two paths: Duration Path: Sept 15, 2013 Qualification Date: Sept 15, 2013	Latest of two paths: Duration Path: Sept 15, 2013 Qualification Date: Sept 15, 2013

Example 3, “Determining qualification date example when 2 event dates set” on page 172: set Employee Retirement date to Nov 15, 2010.

Table 4-21: Determining qualification date example when 2 event dates set

	All events are mandatory	All events are optional	Any one event is mandatory
Serial	Latest event date: Nov 15, 2010 Apply cutoff: Sept 15, 2011 Add Duration: 3 years = Qualification Date: Sep 15, 2014	Latest event date: Nov 15, 2010 Apply cutoff: Sept 15, 2011 Add Duration: 3 years = Qualification Date: Sep 15, 2014	Latest event date: Nov 15, 2010 Apply cutoff: Sept 15, 2011 Add Duration: 3 years = Qualification Date: Sep 15, 2014

	All events are mandatory	All events are optional	Any one event is mandatory
Early Parallel	Duration Path Entry Date: Jan 1, 2010Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Event path Event Date: Nov 15, 2010Apply Cutoff: Sept 15, 2011 Earliest of two paths: Event Path: Sept 15, 2011	Duration Path Entry Date: Jan 1, 2010Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Event path Event Date: Nov 15, 2010Apply Cutoff: Sept 15, 2011 Earliest of two paths: Event Path: Sept 15, 2011	Duration Path Entry Date: Jan 1, 2010Apply cutoff: Sept 15, 2010 Add Duration: 3 years Duration Path Date: Sept 15, 2013 Event path Event Date: Nov 15, 2010Apply Cutoff: Sept 15, 2011 Earliest of two paths: Event Path: Sept 15, 2011
Late Parallel	Latest of two paths: Duration Path: Sept 15, 2013	Latest of two paths: Duration Path: Sept 15, 2013	Latest of two paths: Duration Path: Sept 15, 2013



Note: When you add an authority to a phase, you are prompted to add them to all phases.

Optionally, you can add an Action Name, to specify a means of communicating with or notifying the Authority if an authority is specified. The entries for the Action Name are entered on the Action Relation screen that is displayed when you click Add. A contact must be added if the option for Action Type is set to *Notification*. Contacts however, is not displayed for the other two action types when selected, that is for *Folder Operation* and for *Record relation*. A *Close Folder* or *Open Folder* action can be selected for folder operations. The *Record relation* type is used exclusively with the Suspend relationship type and a configured action resumes aging on the child. You can trigger any action based on the value for the Execution Rule so that notification for example, is sent upon Phase Entry or Phase Exit by the means specified *Email notification* or *Inbox notification*.

4.2.2.9.3 Copying, exporting, and importing retention policies

4.2.2.9.3.1 Overview

This feature can be used to facilitate the decommissioning and commissioning of retention policies. The copy created from a retention policy targeted for retirement for example, can be easily modified and put into service when it becomes necessary. This feature includes functionality to copy locally on the same repository or to copy between repositories. All metadata of the retention policy is copied. Its administrative components and relationship objects however, are not copied. Only IDs or references, in the metadata of the policy, that point to those objects are copied. All of the objects referenced in the original will also be referenced by its copy, unless one of the policies is modified.

The ability to copy a retention policy makes it possible to create a new version from an existing policy without having to start one from scratch. Only the entries against those attributes that would need their values edited would have to be modified.

Copy Policy, **Export Policy**, and **Import Policy** features allow members added to the Retention Manager role to copy retention policies. **Copy Policy** is used to copy locally, within the same repository. **Export Policy** and **Import Policy** are both used to create copies in other repositories. **Export Policy** is used instead of **Copy Policy** to create XML copies for import to other repositories. These features are selectable from the File menu or upon right-clicking a retention policy. Either approach supports single-select and multi-select capability. Content in strings 1-5 of the following audit events are described in “[Retention Policy Services audit events](#)” on page 281:

- dmc_rps_copied_policy
- dmc_rps_copy_policy_failure
- dmc_rps_rename_policy
- dmc_rps_export_policy
- dmc_rps_export_policy_failure
- dmc_rps_import_policy
- dmc_rps_import_policy_failure

Retention policies that are duplicates, resulting from dump and load or that are replicas for example, are not eligible for copying. An error message is displayed when an attempt is made to copy, export, or import retention policies under the following conditions:

- Copy Policy and Export Policy is prevented against a retention policy that is a duplicate or if any one of its ancillary objects associated to it that is a duplicate, authors or contacts for example.
- Import Policy is prevented against a retention policy if it or any of its ancillary objects are associated to an existing object in the target repository with the same name.

Copy Retention Policy Features:

- All metadata is copied to a new policy, in the same repository
- The new policy is given a generated name, in the same repository
 - The first copy is named Copy of <source policy name>
 - The second copy and every copy afterwards, are named Copy (#) of <source policy name>
- An audit trail is generated on a successful or failed copy
- New fields are displayed on properties page of copied policy
- New fields are displayed in the content pane

- The name of an existing policy can be changed only if it is not referenced

Use the **Copy Policy** menu option, to create copies of retention policies on the local repository.

Export Retention Policy Features

- Metadata of the retention policy is exported to a file in a user designated directory
- Metadata on the ancillary objects added to a retention policy is also exported. Ancillary objects include:
 - Contacts
 - Authorities
 - Conditions
 - Global Conditions
 - Rollover, that is the retention policy selected for rollover
- Metadata is exported in XML format
- Users can export multiple retention policies into a single XML file
- Generated file name of
Retention_policies_<docbase>>_yyyy_mm_dd_hh_mi_ss.xml
- Can use a text editor or an XML viewer, Internet Explorer for example, to view the results
- Only one instance of an ancillary object is exported when multiple retention policies are selected that reference the same ancillary object

Use the **Export Policy** menu option, to export copies of retention policies to other repositories. This operation generates an XML file to represent the retention policies to be copied.

Import Retention Policy Features

- Retention Managers can select one or more xml files (exported policies) to import.
- Retention Managers can choose which of the exported policies to import.
- Retention Managers can view the details of any policy and analyze its metadata.
- Retention Managers can change the name of a policy before they import it.
- Retention Managers can see, based on visual indicators, if any issues exist before importing. Warnings:
 -  Retention policy with same name exists in the repository or in the XML files
 -  Ancillary object with same name exists in the repository or in the XML files

The name of the objects being imported must be unique for the type of being created in the repository.

- Evaluate button that can be clicked to re-evaluate and clear warnings after name changes are completed to resolve duplicate naming.
- After import, an import log is created which contains the details of the import.
 - This is a localized file
 - Created in import users home cabinet
- New fields in the content pane when retention policies are listed identify imported policies.
- New fields in retention policy properties displays import related information.

Use the Import Policy menu option to create retention policies in other repositories. This operation consumes the XML file exported.

An XML file is created each time the Export Policy action is performed. Retention Managers performing import Import Policy can then select from a list of XML files and then target the specific retention policies for import.

All retention policies on the exported XML file listed on the resulting Import Policy screen, are selected by default and are also enabled by default. Retention Managers can deselect any of these checkboxes to prevent importing a retention policy or to disable it. The initial values are read from the source file, where the policy is defined. Although a retention policy can be disabled to prevent it from being applied, it should also be disabled if a modified version of its copy is going to be used instead. The impact of enabling or disabling a policy is further described for Enabled in the table within the instructions used to create a retention policy.

Any retention policy listed that has a red warning will fail import if a retention policy on the target repository has the same name. The name must be edited so that it is unique. The new name you provide can be edited directly and can then be evaluated for uniqueness before clicking Import.

The red warning disappears, if the new name provided is unique. Although the red warning may disappear, a yellow warning may appear in its place if any ancillary objects of the retention policy exist in the target repository with the same name. A warning against an ancillary object does not prevent the retention policy from being imported, only red warnings against the retention policy prevent it from being imported. Ancillary objects that are uniquely named are recreated on the target repository; ancillary objects that already exist are otherwise used.

The details of any retention policy listed can be displayed, when you click the blue information icon between the checkbox and new policy name. A plus sign displayed in the upper right corner of an icon indicates the object will be created in the repository. If you expand Phases, you can see that an Active phase and a Final will be created, with the details listed, as their icons have a plus sign. Although no conditions are specified for this policy, a NARA authority will be created for the Authorities.

The details of any exported policy, if multiple exported policies are selected for import, can be examined and then deselected so that it is not imported.



Note: The **Cascade Rule Name** is displayed only if the retention policy being imported, has the **Retention Strategy** set to *Linked* with a **Linked Strategy Type** of *Nonstructural*. Nonstructural implies that the **Structural Retention Type**, on the Properties Info tab of the retention policy, is deselected.

Once the user has selected all the polices they wish to import, they can click the Import button to start creating the new retention policies in the repository.

A message is displayed at the bottom of the content pane, to let you know when the import process has completed. The message also includes the name of the resulting log file that is stored in your home folder in the repository.

The log file created, when import finishes, contains the following information to help you resolve possible issues:

- The name and Id of each object created.
- The name and Id of an existing object that was associated with the retention policy.
- The name and reason why an object failed to be created.

Two summary sections, at the end of the log file, provide the following details:

- A summary of the entire import process includes a count of:
 - How many selected retention policies were imported.
 - How many objects in total were created.
 - How many objects in total failed to be created.
 - How many objects that existed in the repository were associated with the retention policy.
- A summary for each object type includes a count of:
 - How many of that type were created.
 - How many of that type failed to be created.
 - How many of that type existed in the repository and were associated with the retention policy.

The following read-only attributes are displayed on the Properties of only those retention policies that have been copied or imported:

- Creation Method
- Source Policy Name
- Source Repository
- Imported By

- Exported By

Only the first 3 are displayed on copied policies. All 5 are displayed on imported policies.

Retention policies listed in the content pane, can be differentiated by the Creation Method column. Possible values include:

- *Imported*: means that the retention policy was created based on a retention policy that was exported from one repository and imported into another repository.
- *Copied*: means that the retention policy was created from a copy of an existing retention policy on the same repository.
- If no value is displayed, means that the retention policy was created explicitly, **File > New > Retention Policy**.

The names of the retention policies used to create copies are displayed in the Source Policy Name column. The default name of retention policies on the XML file can be changed from a text editor before it is imported, or from its Properties after it is imported.

4.2.2.9.3.2 Copying locally

The copy retention policy locally feature, Copy Policy, allows a user to make an identical copy of an existing retention policy in the same repository.

Although a retention policy can be disabled to prevent it from being applied, it should also be disabled if a modified version of its copy is going to be used instead. Though generally it should be disabled if the original is going to be decommissioned, it really depends on the intent. The intent depends on which versions to keep or put into service, only the original or only the copy or both.

Any retention policy, regardless of its state is a candidate to be copied. All fields from the original policy are copied identically and existing relations on the source retention policy are recreated on the target policy. The only exception is the retention policy name, due to uniqueness constraints on the name of the copied policy which is auto generated by the system. Refer to “[Copy policy naming pattern](#)” on page 179 for the new name pattern. After the copy has been created, the administrator is able to modify both the name and any other field of the new copied policy just as if it was a newly created policy. All retention policy names in the repository must be unique. The Name field of a retention policy can be edited if the policy is not referenced (is not applied to any object and as a result has not spawned a retainer).



Note: Although all fields are copied identically, none of the objects referenced in the retention policy are copied. For example, actions, conditions, global conditions, authorities, and contacts referenced by the policy. Both the original and the copy will reference the same objects, unless the reference in one of the policies is modified. For example, although the original and the copy can point to the same authority, either or both can be modified to point to different authorities. Modifying the object being referenced however, does not affect

referencing in either policy. For example, the original and the copy that point to the same authority would continue to do so even if the authority is modified.

The following ancillary objects referenced by a retention policy is gathered from the source retention policy and then recreated and associated with the new policy:

- Phases and its attributes (duration, phase name, cut-off)
 - Phase authorities
 - Phase conditions
 - Phase actions
- Retention policy authorities
- Global Conditions
- Global Authority

4.2.2.9.3.3 Copy policy naming pattern

When a retention policy is copied, the new retention policy name will have Copy of pre-pended to its name. If a second copy is created from the original and the first copy has not been renamed, then the pattern Copy (2) of will be pre-pended to the name, a third copy will have Copy (3) of, and so on.

Copying a copy however takes on a different naming pattern such that Copy of is pre-pended each time a copy of a copy is created. For example, if you create a copy from the first copy you will get Copy of Copy of pre-pended, creating a third copy of a copy results in Copy of Copy of Copy of, and so on.

Users can also change the name of the policy after it has been copied, assuming no one has applied the copied policy.

4.2.2.9.3.4 Copying between repositories

The export and import features, Export Policy and Import Policy, allow Retention Managers to select one or more retention policies in a repository and copy those policies to another repository.

Although a retention policy can be disabled to prevent it from being applied, it should also be disabled if a modified version of its copy is going to be used instead. Though generally it should be disabled if the original is going to be decommissioned, it really depends on the intent. The intent depends on which versions to keep or put into service, only the original or only the copy or both.

The selected policies when exported, are written to disk in a single XML document and can then be imported into the target repository. Similar to local copy, any retention policy regardless of its state is a candidate for copying between repositories. The process of writing the selected retention policies to disk is referred to as export. The process of recreating those policies in the target repository is referred to as import.

Import will fail if the target repository has a retention policy with a name that matches the name in the Import Policy definition. All retention policies, copied or not, must have a unique name.

The following ancillary objects referenced by a retention policy is gathered from the source retention policy and then recreated and associated with the new policy:

- Phases and its attributes (duration, phase name, cut-off)
 - Phase authorities
 - Phase conditions
 - Phase actions
- Retention policy authorities
- Global Conditions
- Global Authority

4.2.2.9.3.5 Retention policy file definition naming pattern

The XML file generated as a result of the export process is named according to the following pattern:

```
Retention_policies_<repository_name>_<date/time stamp>.xml
```

Where <repository_name> is the name of the repository the retention policies were exported from. And, where <date/time stamp>, with a pattern of yyyyymmddhhmiss, is the date and time the export was initiated.

4.2.2.9.3.6 Contact import rules

Contact import rules are meant for special cases and are automatically enforced during import. A contact associated to an internal OpenText Documentum CM user, who is not on the target repository or the target repository has an identically named user, is handled in the following manner:

- If the contact in the export file exists in the target repository, it will be referenced and a warning will be logged.
- If the contact in the export file is an external one and does not exist in the target repository, an external contact will be created automatically and referenced.
- If the contact in the export file is an internal contact (associated to a user) and does not exist in the target repository, an external contact (not associated to a user) will be created instead, then referenced, and a warning will be logged.
When someone sees this warning they can modify the properties of the contact and associate it with an existing OpenText Documentum CM user.

4.2.2.9.3.7 Copy policy instructions

This procedure is intended to create copies of retention policies in the same repository.

To copy a retention policy within the same repository:

1. Navigate to **Retention Policy Services > Retention Policies**.
2. Select a retention policy displayed in the content pane and select **File > Copy Policy** or right-click the policy and select **Copy Policy**.

A success message is displayed at the bottom of the content pane when the copy is ready. For example, **Successfully copied selected retention policy(ies)**.

The new copy is displayed in the content pane with the same name but is prefixed with *Copy of*. For example, *Copy of Retention_Policy1*

Additional copies (if the first copied policy has not been renamed), if more than one copy is created from the original (not from a copy of the original), are identified as *Copy (2) of Retention_Policy1*, *Copy (3) of Retention_Policy1*, and so on.

Otherwise, *Copy of* is added each time a copy is created from the copy. For example, *Copy of Copy of Retention_Policy1* Although there are 2 copies it implies 1 copy was created from the copy. *Copy of Copy of Copy of Retention_Policy1* implies 2 copies were created from the copy.

4.2.2.9.3.8 Export policy instructions

This procedure is the first step to create copies of retention policies in other repositories. To create copies in other repositories the retention policy must be exported first and then imported according to the import instructions that follow these instructions.

The attribute settings of a retention policy can be viewed on the Properties page, or on the XML file against an exported policy. The Retention Policy Details page can be viewed when the XML file is being imported.

To export a retention policy from a repository:

1. Navigate to **Retention Policy Services > Retention Policies**.
2. Select one or more retention policies displayed in the content pane and select **File > Export Policy** or right-click a selected policy and select **Export Policy**.



Note: If more than one retention policy has to be exported, export them together instead of individually.

Retention policies that have a retention policy specified for rollover are also exported and listed for import. For example, if two retention policies were exported whereby one has a rollover selected, you would see three retention policies listed on the **Import Policy** screen.

3. Select a folder location from the **Select Folder** screen displayed and click **OK**.

The resulting XML file, if export is successful, is exported to the location selected. A message appears at the bottom of the UI confirming whether the export succeeded or failed. The message, if the export is successful, confirms the export location and also displays the name of the file. Success messages are displayed as follows: **All of the selected policies were exported into <path to the selected location\xml_filename>**. The message scrolls to the left when you hover the mouse cursor over it.



Note: If the transfer mode, which affects both downloading and uploading of files, on the Application server is set to http, instead of UCF, make sure to close the export window before attempting to export another retention policy.

Also, unlike UCF transfer mode, http transfer mode displays details about the XML file.

4.2.2.9.3.9 Import policy instructions

These instructions are meant for retention policies that have been exported from one repository and need to be imported into another repository. The XML file produced as a result of the export policy instructions must be available for importing. Retention policies and their ancillary objects are recreated from the XML file on the target repository if the names of the retention policies are unique. A red warning is displayed against a retention policy if it has a name that already exists on the target repository. A yellow warning is displayed against a retention policy if any of its ancillary objects have a name that already exists on the target repository. Retention policies with a red warning are prevented from import, unless the name is changed to one that is unique. An Evaluate button is available to test for uniqueness. A yellow warning against a retention policy will not prevent it from being imported, and will therefore be ignored. The ancillary object on the target repository is used instead.

To import a retention policy into another repository:

1. Navigate to **Retention Policy Services > Retention Policies**.
2. Select **File > Import Policy**.
3. On the **Upload Policy Definition Files** screen, click **Add Files**.
4. On the **Select Files** screen, select the XML file that you want to import and click **OK**.
5. On the **Upload Policy Definition Files** screen, click **Finish** to continue the upload against the XML files selected.

If you select more than 1 XML file to import/upload, click **Continue** on the resulting **Confirm** screen. The **Confirm** screen is otherwise not displayed if you are importing from a single XML file.



Note: If two retention policies were exported whereby one has a rollover selected, you would see three retention policies listed on the **Import Policy** screen.

The transfer mode setting on the Application server if set to UCF displays the screen differently than if it is set to http. In UCF mode, you click Add Files to browse whereas in http mode you click Browse directly for each file you want to add.

6. On the **Import Policy** screen if there are no warnings displayed, click **Import**. You can deselect the checkbox next to a retention policy if you do not want to import it. Deselecting the **Enable on Import** checkbox disables the policy. And, you can click **Import** even if there are warnings. However, only those retention policies that have no warnings or that have a yellow warning diamond shaped symbol are imported. Retention policies with the red warning octagon shaped symbol are prevented.

A green success message is displayed below the content pane which also identifies the location of the log file that is generated as a result. For example, **2 of 3 retention policies were successfully imported. See complete results in generated log /Administrator/Import Retention Policies Log (090019a780003e69)**. The message scrolls to the left, to let you read the entire message, when you position your cursor over it.

If you want to resolve the red warnings, follow these substeps and then click **Import**:

- a. Click the text field under the **New Policy Name** header against a retention policy that has a red warning.
- b. Edit the name to make it unique.
- c. Click **Evaluate** to make sure that the new value for the name is unique. The red warning is cleared if the new name for a retention policy is indeed unique.

A yellow warning replaces the red warning if the retention policy also has any ancillary objects with names that exist in the target repository. The yellow warning however, is ignored to allow association with the ancillary object that exists in the target repository. Log files can be referenced to determine if the association is based on the existing ancillary object or the one that was created upon import. Ancillary objects are created if they have no warnings.

4.2.2.9.4 Viewing/modifying a retention policy, applied retention, or retainer properties

This section includes the following topics:

- “To view or modify the properties of a retention policy” on page 184
- “To view applied retention” on page 187
- “To view or modify the properties of a retainer” on page 188

4.2.2.9.4.1 To view or modify the properties of a retention policy

Any attribute on the Properties page of a retention policy can be modified if it has not yet been applied to an object. The top of the Info tab on the properties of a retention policy indicates whether it is in use or not; the Policy In Use field indicates either Yes or No. Most attributes, after a policy is applied, are read-only with the exception of the checkbox used to enable or disable the policy and features used to add a global authority or a phase authority as well as an action name. The Properties page of a retention policy displays the Justification tab which is not displayed against the properties of any retainers spawned from it.



Note: Although changes to the Duration or Cut-off Period can be made after a retention policy is applied, existing retainers are grandfathered against the entries prior to the changes. The qualification date for objects that are qualified going forward, is calculated based on the new values entered.

Keep in mind that a retention policy acts as a template and is therefore referenced by one or more retainers depending on the number of objects it has been applied to. There is a properties page associated with the retention policy and a properties page associated with each retainer that is spawned when the policy is applied. Although the properties associated with the retention policy can be modified, the properties of a retainer are read-only except for the Event Date. The Event Date can only be modified if a condition (event) or global condition (global event) has been added to the retention policy. All of the attributes on the properties of a retainer are read-only unless the retention policy referenced has an event specified.

1. Navigate to the **Retention Policy Services** administration node.
2. Right-click a retention policy displayed in the content pane and select **Properties**.

For a description of the attributes, refer to “[Creating a retention policy](#)” on page 156. It includes a description of all the attributes that can be displayed on the **Properties** of a retention policy. Retention policies that are copied or imported however, display additional read-only information at the top of the **Properties** page. The same information is displayed at the top of the page regardless of the tab that is selected. The following read-only attributes are not displayed against the properties of retention policies that are created from scratch, using **File > New > Retention Policy** menu option:

- **Creation Method**

- **Source Policy Name**
- **Source Repository**
- **Imported By**
- **Exported By**

Imported By and **Exported By** are not displayed if the value for the **Creation Method** indicates that it was *Copied*.

Changes can be made to the properties of a retention policy when it is not in use, meaning not applied to an object, or in other words when it is not referenced by any retainers. Also note that a retention policy that is not referenced by any retainers is considered to be in use (referenced) if it specifies a rollover retention policy. Although most of the attributes are read-only when the policy is in use, it is always possible to:

- Disable or enable the policy when necessary.
- Change the Disposition Strategy.
- Add or remove a Global Conditions and Global Authorities.
- Change the Duration and Cut-off Period.
- Add or remove Authorities.
- Add or remove Action Name.

Note the details displayed at the top of the page for copied policies.

The name of a copied policy is prefixed with Copy of.

Properties: Info

Info Phases Justifications History

 Copy of KW_CascadeToBoth Type: dmc_rps_retention_policy Policy In Use: No Creation Method: Copied	Source Policy Name: KW_CascadeToBoth Source Repository: ESX14SQL_RM_D67SP2
Name: <input type="text" value="Copy of KW_CascadeToBoth"/> Description: <input type="text"/>	

Figure 4-6: Retention policy properties page - copied policy

Note the additional details displayed for imported policies.

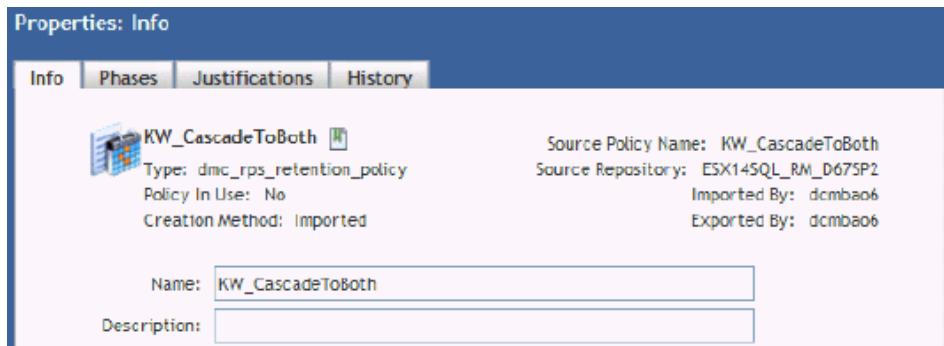


Figure 4-7: Retention policy properties page - imported policy

3. Click **OK** or **Cancel** if you are only viewing the properties. Otherwise, click **OK** to accept any modifications or **Cancel** to back out. If you click **OK** to accept any modifications, the **Confirm Retention Policy Modification** screen is displayed asking for confirmation, **Are you sure you want to modify the retention policy?**

 **Note:** Although the **Reason for modifying policy** in this example is mandatory, the **Enable Mandatory Justification Field** setting on the **RPS Application Configuration** object can be changed to make it optional. For further details to turn this setting on or off, refer to “[System configuration options settings](#)” on page 121.

4. Click **OK** to confirm and complete the process or **Cancel** to back out if necessary.

The reason for modifying however, may or may not be mandatory for confirmation depending on the setting in the Retention Policy Services Application Configuration file. If the red asterisk is displayed it means that the attribute labeled **Enable Mandatory Justification Field** on the configuration file is selected. For further details, refer to “[System configuration options settings](#)” on page 121. Text must be provided when it is mandatory. The previous reason can be copied if necessary so you do not have to retype it. A warning is otherwise displayed if you confirm without an entry, reminding you that **The reason field is mandatory**. A warning against the text entered will also be displayed, in red, if it exceeds 255 characters.

The **Phases** and **Justification** tabs are displayed.

The **Justifications** tab displays the **Creation** and **Last Modification** dates along with the users and their reasons for the justification. Details for the **Last Modification** represent the most recent modification since its creation. The **Justification** for the **Last Modification** always indicates *No previous justification entered* if there were no modifications. The **Date** and **User** details are otherwise the same as the **Creation** if there were no modifications. For further details, refer to About the Justifications tab in the “[Retention policy overview](#)” on page 146.

4.2.2.9.4.2 To view applied retention

The retainers that are applied to an object are displayed when you view the applied retention against the selected object. View applied retention to determine which retention policy, or policies, are applied to a retained object. Multiple retention policies are applied to the object if more than one retainer is listed. To view the properties of a retainer, refer to “[To view or modify the properties of a retainer](#)” on page 188.

1. Navigate to a retained object.
2. Right-click the object and select **View > Applied Retention**. The **Applied Retention** page is displayed and may list more than one retainer, depending on the number of retention policies that are applied to the object. All retainers spawned when a retention policy is applied to an object are assigned a unique ID number.



Note: The **Applied Retention** menu option is not displayed if the object is not under any retention.

The following default attributes are displayed when you view an applied retention:

- Name
- Current Phase
- Entry Date
- Event Date
- Global Event Date
- Qualification Date
- Disposition Status
- Projected Disposition Date
- Inherited
- Rollover
- Rollover Parent

4.2.2.9.4.3 To view or modify the properties of a retainer

The properties of a retainer can be displayed from the **Applied Retention** page. Most of the values displayed are read-only. Only the event dates and authorities can be modified. Only users with dmc_rps_contributor role can modify all the properties for the objects under retention.

1. Navigate to a retained object.
2. Right-click the object and select **View > Applied Retention**.

The Applied Retention option is not available if the selected object has no retention applied.



Note: Although you can navigate directly to a retained object to view applied retention, applied retention can also be viewed against objects listed in a report or in any of the managers (qualification, promotion, or disposition).

3. On the **Applied Retention** page, right-click the retainer listed and click **Properties**.

The retainer **Properties** page is displayed. The retainer ID is displayed at the top of the page. The following table describes the attributes above the **Policy Details**:

Attribute	Description
Type	The value displayed for this object type is always dmc_rps_retainer.
Policy Name	The name of the retention policy from which the retainer was spawned.
Description	This field is the same as the description specified for the retention policy.
Current Phase	The phase of the lifecycle the retainer is currently in. The lifecycle selected for a retention policy is applied to the retainer spawned when the policy is applied to an object.
Application Date	The date and time at which the retention policy was applied to the object. However, if the retainer is shared the value is when the folder was put under retention (the primary object under retention), not the documents.
Aging Details	

Attribute	Description
Base Date	The value for the base data is only important for chronological retention policies when they are applied. If there is no base date mapping for the item's object type, then the creation date is used. Note that for linked policies, the base date is relative to the folder.
Entry Date	The date the retainer entered the current phase.
Qualification Date	The date that the retainer is eligible to either be promoted or disposed. This date can be empty if the item could not qualify or if it was disqualified. To determine how the qualification date is calculated, refer to "About qualification date calculation" on page 154.
Projected Disposition Date	The earliest possible date based on phase duration that an item could be eligible for disposition. This calculation ignores events and cutoff and is meant only as a guide. It is also possible that the item could be disposed earlier than this date if global conditions are used or if supersede is used (either based on version or a record relation).
Structural Details	
This pane is displayed only if the retention policy is structural.	
Completed Disposition On	The date disposition was last completed. This date is meant for structural retention so that a retention manager can see when the last cycle completed. This date can be empty (if disposition was never done).
Number of Resets	This field pertains to structural retention only. This is the number of times the folder has been reset as a result of disposition. If this value is non-zero, then the last reset date is the "Completed Disposition On" attribute.
Supersede Details	
This pane is displayed only if the retention policy has Supersede On New Version selected.	
Date Superseded	The date and time at which objects other than the <i>Current</i> version are promoted directly to the final phase.
Phase Superseded	The name of the phase that the retainer was in before the supersede occurred.

Attribute	Description
Approval Details	
This pane is displayed only if disposition approval is required.	
Approval Status	The possible values displayed could be: Approved, Submitted for Approval, and Rejected.
Approval Date	The date and time on which it was approved. The value is blank if no approval is provided.
Hide/Show Policy Details	
Attributes in this pane are hidden by default and are described in “ Creating a retention policy ” on page 156.	

4. Optionally, if the retention policy referenced by the retainer has a phase condition or global condition specified, the phase **Event Date** or the **Global Event Date**, or both, can be added when you click **Edit** against a global event on the **Info** tab or against an event on the **Phases** tab.

The respective **Edit Event** and **Edit Global Event** pages have the same attributes. Although the **Name** and the **Condition Description** fields are read-only, the rest can be edited.



Note: If an event date is set or cleared programmatically, through IAPI or Webservices, Retention Policy Services will automatically try to qualify or unqualify the retainer.

4.2.2.9.5 Enabling or disabling a retention policy

Disabling a retention policy removes the retention policy from the list of available retention policies that can be applied to objects (documents or folders). Note that disabling a retention policy, however, does not affect the objects that were associated to the retention policy before it was disabled.

To enable or disable a retention policy:

The procedure to enable or disable a retention policy is like the procedure for viewing a retention policy. Any policy that is disabled cannot be applied until it is enabled.

1. Navigate to **Retention Policy Services**.
2. Right-click a retention policy displayed in the content pane and select **Properties**.
3. Select the **Enabled** checkbox, on the **Info** tab, to enable the retention policy or deselect the checkbox to disable it.
4. Click **OK**.

4.2.2.9.6 Applying a retention policy or viewing a list of retention policies

After a retention policy has been applied, the Referenced field from the info tab of the properties of the retention policy reads True, and the following operations cannot be performed:

- Deletion of a retention policy
- Addition or removal of conditions on any phase of the retention policy
- Changes to the child strategy, immutability rule or rendition rule

After a retention policy has been applied, you can change the following retention policy items:

- Removal of authorities from any phase
- Modification of the duration of a phase
- Changes to the disposition strategy
- Cut-off period or disable it

If a corrupted Retention Policy is the first in the list box, the UI will move to the next one until it finds one that initializes properly or can find no more policies to try. The UI will move to the next one, meaning from whichever UI a retention policy can be applied from. If a corrupt one is selected manually a message will be posted indicating that there is a problem with that selection. A properly initialized selection must be made before the application can be committed (it will not be possible to select 'Next' or 'Ok').

To apply a retention policy:



Note: It is recommended that you avoid applying both linked and individual retention policies to a folder, as any subfolders that inherit the individual retention will not be displayed in Disposition Manager.

The lock status on a document that is checked out from a folder to which retention is being either applied or removed, remains unchanged.

To avoid conflicting behavior, do not apply both a Linked Structural retention policy type and a Linked Non-Structural retention policy type to the same folder (container object). The conflicting behavior is that one retainer is meant to destroy the folder while the other is meant to reset the folder. Promoting a linked non-structural policy through to disposition would result in a terminal retainer on the folder after all its children have been destroyed. Since the terminal retainer is there, no more objects can be moved into the folder. Promoting a linked structural policy through to disposition would reset the folder.

1. Navigate to the object (cabinet, folder, or file) to which you want to apply a retention policy.
2. Right-click the desired object displayed in the content pane and select **Retention > Apply Retention Policy**.

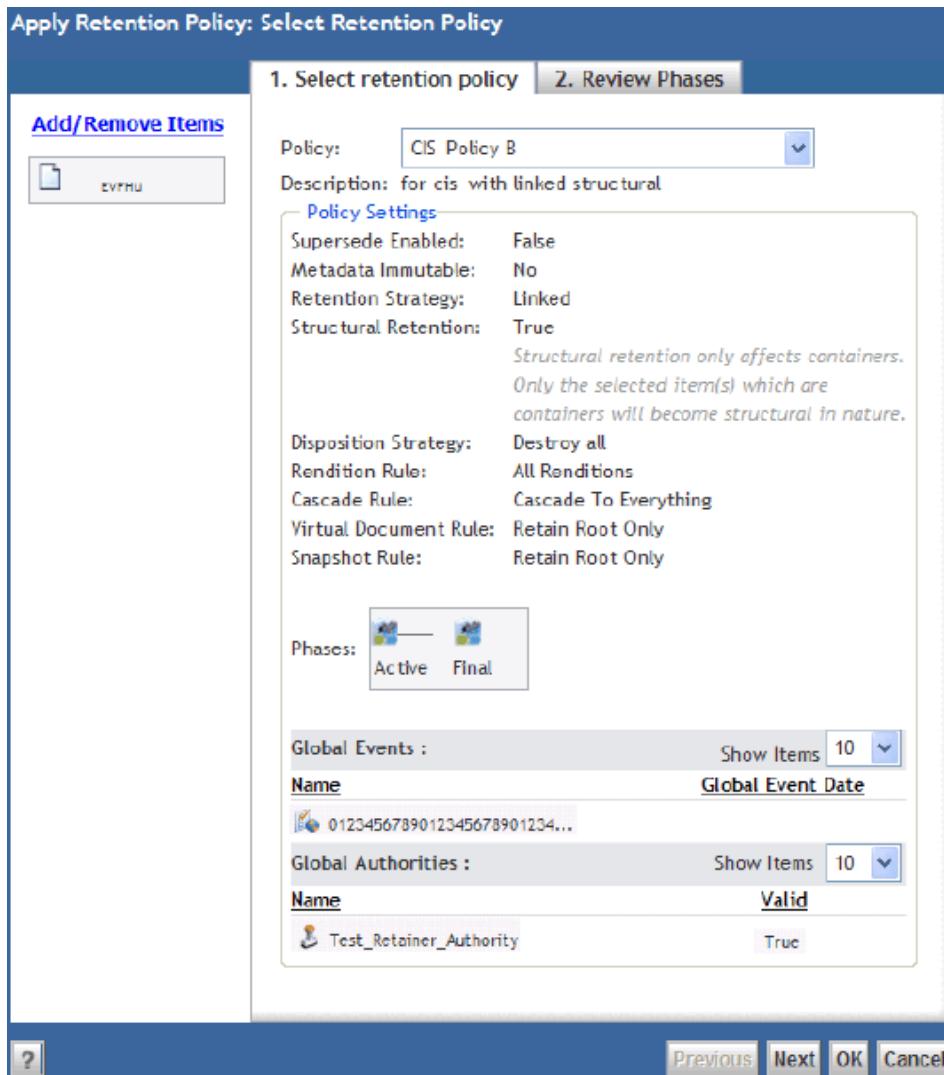


Figure 4-8: Apply retention policy page

The attributes on the **Apply Retention Policy** page are described in the following table (for further descriptions, refer to “[Creating a retention policy](#)” on page 156):

Attribute	Description
Add/Remove Items	Displays the object selected for retention application. Click this option if you want to add more objects or to remove objects.
Policy	Control used to select the desired retention policy that is to be applied to the selected object listed under Add/Remove Items .

Attribute	Description
Description	The value specified for the Description of the selected policy.
Supersede Enabled	Indicates <i>True</i> or <i>False</i> depending on whether the checkbox for Supersede On New Version on the selected policy is selected or not.
Metadata Immutable (against the policy)	Indicates <i>Yes</i> or <i>No</i> depending on whether the checkbox for Metadata Immutable on the selected policy is selected or not.
Retention Strategy	Shows the value, <i>Linked</i> or <i>Individual</i> , selected for the Retention Strategy on the selected policy.
Structural Retention	This attribute is displayed against the selected policy only when the checkbox for the Structural Retention Type on the selected policy is selected (checked) and the Retention Strategy is set to <i>Linked</i> . If the object selected for retention is something other than a container object, a message is displayed warning that a container object must be selected. The warning states: <i>Structural retention only affects containers. Only the selected item(s) which are containers will become structural in nature.</i>
Disposition Strategy	Shows the value selected for the Disposition Strategy on the selected policy.
Rendition Rule (against the policy)	Shows the value selected for the Rendition Rule on the selected policy.
Cascade Rule	Shows the value selected for the Cascade Rule on the selected policy.
Virtual Document Rule	Shows the value selected for the Virtual Document Retention on the selected policy.
Snapshot Rule	Shows the value selected for the Snapshot Retention on the selected policy.
Metadata Immutable (against the VDM)	Indicates <i>Yes</i> or <i>No</i> depending on whether the checkbox for Metadata Immutable on the selected policy is selected or not.
Rendition Rule (against the VDM)	Shows the value selected for the Rendition Rule on the selected policy.
Phases	Depicts the number of phases against the Lifecycle selected on the selected policy.

Attribute	Description
Global Events	Shows the Global Conditions if specified and the Global Event Date if specified.
Global Authorities	Shows the Global Authorities if specified and whether it is valid or not.

3. Select a **Retention Policy** from the list box and click **Next**.

4. Click **OK** to apply the retention policy.

A message at the bottom of the screen is displayed indicating whether the requested items were successfully processed locally (immediately) or not, or were successfully delegated or not to the Work Order Framework for asynchronous processing. The message is displayed whether the policy is being applied or removed or for whatever operation that is supported. Any spawning of a partitioned work order, from a master or reference work order, that times out or experiences a problem that prevents it from being successfully created, becomes a candidate for recovery. The master work order as a result, when displayed in the Work Order Report is identified with a completion status of either Partially Succeeded or Failed. Recovering the master work order recovers all the work orders spawned from it that could not be successfully processed.

5. Optionally, if the message at the bottom of the UI indicates that the request was processed by a work order, run the **Work Order Report** against the *Process Records Policy* operation, to see the master work order and details. To see the subwork orders, if any, spawned by a master work order, run the **Work Order Breakdown Report**. To see the items that were processed by the work orders, run the **Work Order Item Report**. For instructions to run any of these reports, refer to “Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report” on page 51. For a work order introduction, refer to “Work orders” on page 33.

To view a list of retention policies:

1. Navigate to **Retention Policy Services** and click the plus sign to expand and display its components.
2. Click **Retention Policies**.

A list of retention policies is displayed. Retention Policies are listed under the following column headings:

Table 4-22: Column headings described for retention policy listings

Column Heading	Description
Name	The name of the retention policy.
Description	Information that describes the retention policy.

Column Heading	Description
Retainer Lifecycle	The lifecycle selected for the retention policy when it was created. There are several possible lifecycle values that could be displayed: <i>1Phase + Final</i> , <i>2 Phases + Final</i> , and so on up to 6 phases. All retainers spawned from a retention policy when applied to an object have the same lifecycle.
Retention Strategy	The retention strategy selected for the retention policy when it was created. The two possible values that could be displayed are: <i>Linked</i> or <i>Individual</i> .
Disposition Strategy	The disposition strategy selected for the retention policy when it was created. Disposition strategies are listed and described in “About retention policy lifecycles and retainers” on page 146.
Cascade to Subfolders	If the value displayed is <i>True</i> , means that retention can cascade from the parent folder to its subfolders.
Cascade to Subcategories	If the value displayed is <i>True</i> , means that retention can cascade from the parent category to its subcategories.
Structural Retention Type	If the value displayed is <i>True</i> , means that aging, on the folder or the category against which disposition is run, is reset to start the aging process over again after the content is gone.
Enabled	If the value displayed is <i>True</i> , means that the retention policy can be applied to an object.
Created	Displays the date on which the retention policy was created.
Creation Method	Indicates the method that was used to create the retention policy. The possible values that can be displayed are: <i>Copied</i> or <i>Imported</i> . If no value is displayed, it means that the retention policy was explicitly created from scratch, File > New > Retention Policy.
Source Policy Name	The original retention policy that was copied or that was used to export a retention policy for import to another repository.

 **Note:** The value assigned against an attribute listed in the column heading are the same for all retainers spawned from a retention policy when it is applied (whether directly or by inheritance) to an object. It is the aging among the retainers spawned from a retention policy that is different.

4.2.2.9.6.1 Retention cascade

Retainers are always inherited throughout the entire folder structure in a cascading manner. If the parent object is a containing object to which a linked retention has been applied, each subfolder will also get its very own instance of linked retention. Non-container objects that are in a folder are linked to their parent. With individual style retention, each subfolder will be non-aging and will give its children a unique retainer.

Retention cascade will occur as a result of the following:

- Direct application of retention to a container
- Moving an object into a container under retention
- Creating objects in a container under retention
- Importing objects into a container under retention
- Linking objects into a container under retention
- Copying objects into a container under retention
- Dragging and dropping objects into a container under retention

Cascading actions when Retention Policy Services operations are performed such as applying/removing retention, privilege delete and applying holds are affected differently. When applying (or removing) retention to a root container object (folder and/or cabinet), retention is applied to or removed from every item in the cascaded tree (folders, sub folders, and all contained documents for example). Retention markups will also be inherited if the option Cascades to Sub-folders is selected. Cascades To Sub-Folders is deselected by default when you create a retention markup. Holds are applied one level deep to documents only, if the default setting is used. When performing a privileged delete on a root container object, the container and its contents are deleted. A privileged delete performed against an empty container however, cabinet or folder, is ignored. For instructions to perform a privileged delete, refer to ["Performing a privileged delete" on page 199](#).

Removing retention from the root parent container which contains other containers will result in retention being removed from all containers and objects in the retention cascade.



Note: Retention inherited by a subcontainer from its parent cannot be removed. However, if retention is removed from the parent container, retention is removed from the subcontainer.

4.2.2.9.7 Removing an applied retention policy

Removing an applied retention policy implies that you are removing instances of the retainer created by the retention policy. It is not the retention policy that will be removed but rather the retainers created by the retention policy. A retainer that is removed is essentially deleted. Only members of the Retention Manager role can remove a retainer. If you wish to delete a retention policy, refer to “[Deleting a retention policy](#)” on page 198.



Note: Removing retention (or any record policy) from the parent object can result in orphaned objects if for any reason all of the children could not be successfully processed. The Application server for example, if it crashes might not have processed all of the children or if one of the objects is unexpectedly moved before it is processed. Orphaned objects that result as a consequence of a move or server failure must be processed separately. If a message is displayed with a list of orphaned objects, run the Orphaned Record Policy Remover.

Use **Records > Reports > Retention Report** to remove the retainer associated with a particular retention policy. Alternatively, you can navigate to the object and select **View > Applied Retentions** to remove an applied retainer.

To remove a retainer using the retention report:

1. Click **Records > Reports > Retention Report**.
2. Click **Report**.
Objects that have a retention policy are listed in the lower half of the **Retention Report** screen.
3. Right-click the object from which you want to remove the retainer and select **Remove Retention**. The **Delete** option, if the object has retention, can only be used to delete the object after retention has been removed.
4. Click **Yes** on the confirmation screen to complete the process or click **No** to back out or abort.

Inherited retainers cannot be removed from the child and the action must be performed on the parent. You cannot complete the process if the selected object has an inherited retainer. Click **OK** in those instances to abort the process.

A message at the bottom of the screen is displayed indicating whether the requested items were successfully processed locally (immediately) or not, or were successfully delegated or not to the Work Order Framework for asynchronous processing. Any partition of a master work order or of a reference work order that cannot be partitioned due to a time-out, as can be determined from the Work Order Report, can be recovered using the Work Order Report.

5. Optionally, if the message at the bottom of the UI indicates that the request was processed by a work order, run the **Work Order Report** against the *Process Records Policy* operation, to see the master work order and details. To see the subwork orders, if any, spawned by a master work order, run the **Work Order**

Breakdown Report. To see the items that were processed by the work orders, run the **Work Order Item Report**. For instructions to run any of these reports, refer to “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51. For a work order introduction, refer to “[Work orders](#)” on page 33.

4.2.2.9.8 Deleting a retention policy

A retention policy can be deleted only when there are no retainers referencing it. Therefore, all retainers must be removed from those objects they retain before the policy can be deleted.



Note: If necessary, refer to “[Removing an applied retention policy](#)” on page 197, to ensure that all retainers associated with a particular retention policy are removed.

The lifecycle selected for a retention policy must not be deleted or renamed.

A reason may or may not be mandatory for each retention policy that is created, modified, or deleted. Mandatory confirmation however, can be turned off when necessary on the rps_docbase_config file. The attribute that controls this setting is labeled Enable Mandatory Justification Field. For further details to turn this setting on or off, refer to “[System configuration options settings](#)” on page 121.

To delete a retention policy:

1. Determine if there are any retainers referencing the retention policy to be deleted and remove the retainers from those objects. If there are retainers to remove, refer to “[Removing an applied retention policy](#)” on page 197, then navigate to **Retention Policy Services > Retention Policies**.

A retention policy cannot be deleted if any of the retainers it has spawned are still active (aging). If you cannot wait for the retainers to stop aging and go away automatically, you will have to remove them manually.

2. Right-click one or more retention policies and select **Delete**.

The confirmation page is displays asking for confirmation **Are you sure you want to delete the retention policy?**



Note: The **Reason for deleting policy** and the text box is not displayed if the dmc_rps_destroy_retention_policy audit event is not registered.

Deletion can be completed without providing an entry for the reason if it is optional. At least one character must be provided if the reason is mandatory.

The reason for deleting may or may not be mandatory depending on the setting in the Retention Policy Services Application Configuration file. If the red asterisk is displayed it means that the attribute labeled **Enable Mandatory Justification Field** on the configuration file is selected. For further details, refer to “[System configuration options settings](#)” on page 121. A reason must be provided when it is mandatory. A warning is otherwise displayed if you

confirm without an entry, reminding you that **The Reason field is mandatory**. A warning against the text entered will also be displayed, in red, if it exceeds 255 characters.

If only one retention policy is selected for deletion, **OK** and **Cancel** buttons are displayed. If multiple policies are selected, **Previous**, **Next**, **Finish**, and **Cancel** buttons are displayed instead. The top of the page lets you know which policy is being addressed, Policy 1 of 2 for example. Use **Next** to enter a unique reason for each of the justifications or **Finish** to assign the same reason to the remaining policies. Use **Previous** to return to entries already provided.

Also, any retention policy that cannot be deleted among multiple policies selected will be listed with a new question. For example, **The following retention policies are in use and will not be deleted: Do you still want to delete the remainder?**

4.2.2.9.9 Performing a privileged delete

Privileged Delete provides users with the ability to select an object at any time. Only users with the Retention Manager role can perform the privileged delete procedure. Use this procedure to perform a privileged delete.



Caution

Performing a privileged delete does not delete the retention policy. Performing a privileged delete results in the deletion of objects before their retention policy duration has elapsed.



Note: A privileged delete will not be executed when it is performed against an empty container, cabinet or folder. A privileged delete performed against a container, cabinet or folder, that has content will delete everything in the container and the container as well.

To perform a privileged delete:

1. Navigate to the object to which you want to perform a privileged delete.
2. Right-click the object that you want to perform a privileged delete on and select **Records > Privileged Delete**.
3. Type a justification in the **Justification** field.
4. Click **OK**.
The **Privileged delete confirmation** screen is displayed with a message asking if you want to delete the object.
5. Click **Continue**.
A message is displayed stating the object was deleted successfully.
6. Click **OK**.
A confirmation message is displayed in the task bar at the bottom right of the content pane.

The object is deleted. If you perform a privileged delete on a folder, the immediate objects under the folder that inherited retention from the folder are also deleted. The parent folder is never deleted.

4.2.2.9.10 Linking objects to a retained folder

You can now link objects to a retained folder using work order processor. Linking the objects to a retained folder will apply the retention policy on all the objects. Instead of applying policies directly on the documents, the retainers associated with the linked folder will be associated with the documents.

You can link the objects to a retained folder either by using a retention structure or without a retention structure. You need to use the internal public API `IRetentionLinkFolderService`, which is available as part of Records shared libraries to link or unlink the objects. Only members in Retention Manager role can link or unlink objects to a retained folder. [“Using API IRetentionLinkFolderService” on page 203](#) provides more details.

4.2.2.9.10.1 Linking objects without retention structure

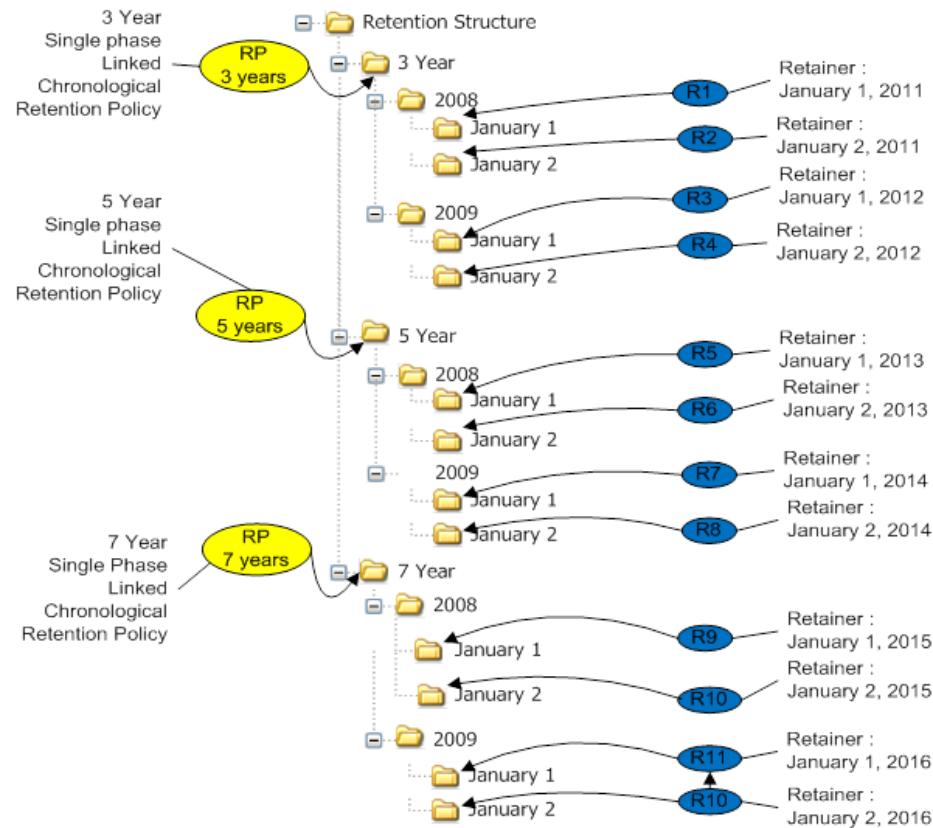
When you link objects with a retained folder without retention structure, the objects inherit the retainers of the retained folder. If the retention strategy for the retained folder is individual then linked objects would have individual retainers. If the retention strategy for the retained folder is linked then the linked objects would use the retainers of the retained folder.

4.2.2.9.10.2 Linking objects with retention structure

You can link objects to a retained folder using retention structure. Retention structure is a separate folder structure that uses the linked retention policies and is created separately from the structure that contains the documents that is used by applications to represent the documents to the users. The retention structure represents the retainers that are associated with the documents. The benefit of shared retainers is that you reduce the number of retainers to be processed and you can have one retainer for every date.

You can create two types of retention structure: Chronological or Conditional.

- Chronological retention structure creates folders and retainers for each day for the specified period. The retention structure is a hierarchy of folders that represent an individual date associated with a policy. The policy is the highest level of the hierarchy and each policy has its own date structure. Every year will have a maximum of 365 folders representing each day of the year, under each policy. A date on the folder will represent the date that the folder will age from. This will be used to associate the date of the document with its appropriate retainer.

**Figure 4-9: Example: Chronological retention structure**

- Conditional retention structure creates a folder structure similar to the Chronological retention structure, but it also includes folders for different events for each day. The retention structure is a hierarchy of folders that represent a date structure and the events of the policy under each date. All documents associated with a particular date and event will be associated to the folder. Each date will have the number of events that are created in the policy created under it automatically by the create retention structure.

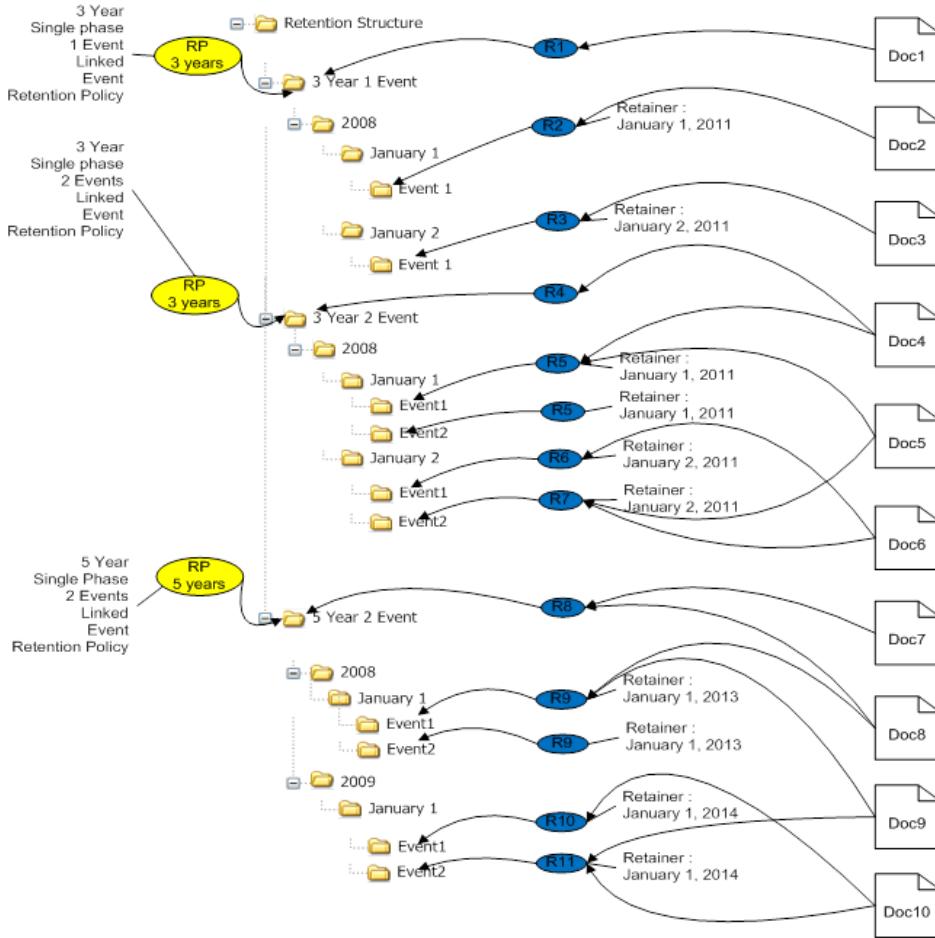


Figure 4-10: Example: Conditional retention structure

You can create and update the retention structure. Only members with the Retention Manager role can create and update retention structure. To create and update retention structure, use the `IRetentionStructureService` public interface. To update the retention structure, user must be a member of `dm_retention_mangers` group. You can create retention structure for one or for all linked retention policies. [“Using API IRetentionStructureService” on page 203](#) provides details to create and update retention structure.

You can also update the policy, year, month, and days folders in a retention structure using this interface. You can use this interface to remove any terminal retainers on the retention structure and update the disposition status of any retainers on these folders from terminated status to open.

4.2.2.9.10.3 Using API IRetentionLinkFolderService

The `IRetentionLinkFolderService` interface class provides the method to link or unlink object(s) to a retained folder. Using this interface class you can link or unlink objects to a retained folder using retention structure or without a retention structure. This interface class is available as a BOF module. The sample code to get the handle of this interface class:

```
IRetentionLinkFolderService linkFolderService = (IRetentionLinkFolderService)
DfClient.getLocalClient().newModule(dfSession.getDocbaseName(),
IRetentionLinkFolderService.class.getName(), dfSession.getSessionManager());
```

The parameter bean can be initialized as follows:

```
RetentionLinkFolderParamBean linkFolderParamBean = new RetentionLinkFolderParamBean();
linkFolderParamBean.setPolicyFolderId(folderId);
linkFolderParamBean.setObjectIds(objectIds);
linkFolderParamBean.setClearRetention(false);
linkFolderParamBean.setOperationMode(IRetentionLinkFolderParameters.OperationMode.LINK);
linkFolderService.link(linkFolderParamBean);
```

Each method in this interface class creates MASTER WORK ORDER operation `LINK_MOVE_FOLDER`. When using retention structure, the retention structure root folder should be associated with the LINKED RETENTION POLICY so that the linked object(s) inherit the same retainer.

This method returns ID of the master work order. It throws the following `DfException` exception if any runtime exception occurs:

```
com.documentum.fc.common.DfException
```

4.2.2.9.10.4 Using API IRetentionStructureService

This interface class provides methods for creating and updating retention structure. This interface class is available as a BOF module. The sample code to get an instance of this interface class:

```
IRetentionStructureService retStructureService = (IRetentionStructureService)
DfClient.getLocalClient().newModule(dfSession.getDocbaseName(),
IRetentionStructureService.class.getName(), dfSession.getSessionManager());
```

The parameter bean can be initialized as follows:

```
RetentionStructureCreateParamBean retStructureParamBean = new
RetentionStructureCreateParamBean();
```

To create retention structure:

```
retStructureService.create(retStructureParamBean);
```

`RetentionStructureCreateParamBean` has setter methods to pass required data to create a retention structure.

Setter methods	Description
<code>setRootFolderId(IDfId rootFolderId)</code>	Sets the root folder ID. In this folder retention structure is created. <code>rootFolderId</code> is a mandatory parameter.

Setter methods	Description
setACL(IDfACL aCL)	Sets ACL.
setCustomFolderBean(IRpsCustomFolderBean customFolderBean)	Sets custom folder bean. Folders in retention structure are of type custom folder.
setStartYear(int startYear), setEndYear(int endYear)	Sets start year and end year. Folders in retention structure are created for every date between the start year and end year.
setCreateForAllPolicies(boolean createForAllPolicies)	Sets boolean createForAllPolicies. If set to true , retention structure is created for all policies, else it is created for only one policy.
setPolicyId(IDfId policyId)	Sets PolicyId. It should be an ID of linked retention policy. Required if createForAllPolicies is set to false . Retention structure is created for the given policy ID.

To update retention structure:

```
retStructureService.update(retStructureParamBean);
```

RetentionStructureCreateParamBean has setter methods to pass required data to create a retention structure.

Setter methods	Description
setRootFolderId(IDfId rootFolderId)	Sets the root folder ID. In this folder retention structure is updated. rootFolderId is a mandatory parameter.
setIgnoreYearMonth(boolean ignoreYearMonth)	To set boolean ignoreYearMonth. If set to true , Policy, year, and month folders will be ignored. Only date folders will be updated. Else, policy, year, month, and date folders are updated.

4.2.2.10 Base dates

A base date is one of the variables used for the calculation of the qualification date against an object that is under chronological retention. The qualification date, which is used to start the aging process of a retainer, cannot be calculated without a base date value, unless a base date mapping has been created for the object type under retention. Only those object types that have a mapping to one of its date attributes, such as the creation date, modification date, or other, will have a base date value. The base date is used only when a new retainer is spawned (created), as a result of:

- Applying retention directly to an object.
- Inherited retention on a folder.
- Inherited retention, with individual retention strategy, on a document.

The base date is otherwise not used if directly applied retention is set to rollover or when structural retention is reset. If there is no base date mapping created for the object under retention, then the creation date (*r_creation_date*) of the object is used by default. If a date attribute, other than the creation date, is mapped but the value is null, then the creation date (*r_creation_date*) of the object is used.

Base date mappings apply only if the retained items have their own unique retainer. For example, if Linked retention is applied to a folder, any base date mapping for the documents are ignored. Only if the documents are inheriting Individual retention or the retention policy was directly applied will the base date mappings affect the qualification calculation. Folders only use the base date mapping if Linked retention is applied (it does not matter if it is directly applied or inherited).

If the item does not have a base date value assigned to it, or the base date value is not valid or configured (as the base date is not mandatory), the system searches for the best match. The system looks up the object type hierarchy to find the best base date mapping and stops when a base date mapping is found. If there is none defined, the system will use the creation date.

If a base date mapping is defined and if the attribute on the item is changed, the system will automatically recalculate the qualification date. If the field had a value and was cleared out, the creation date will be used.



Note: If the base date mapping is changed to a different field, existing retainers will need to be re-qualified manually (Qualification manager, requalify). However, if subsequently the new field was changed on an item, then an automatic re-qualification would be initiated.

To create a base date:

1. Navigate to **Retention Policy Services > Base Dates** and select **File > New > Base Date**.
2. Select an item from the **Object Type** list box.
3. Select an item from the **Attribute** list box. The attribute selected will represent the base date for the object type selected.

For example, if *Document* (*dm_document*) for the **Object Type** is mapped to the **Attribute** *Created* (*r_creation_date*), the base date will use the creation date of the document under retention. Once a mapping is created for a particular **Object Type**, that object type will no longer be displayed in its list box. The selectable **Attributes** include:

- *Accessed* (*r_access_date*)
- *Checkout Date* (*r_lock_date*)
- *Created* (*r_creation_date*)
- *Effective Date* (*a_effective_date*)
- *Expiration Date* (*a_expiration_date*)

- *Last Review Date (a_last_review_date)*
- *Modified (r_modify_date)*



Note: If a base date has not been created for the object type that is under retention, Retention Policy Services will search all of its super-types for a base date mapping. If none of the super types have a mapping to pick from, Retention Policy Services will then use the last disposition date of the object, if it has one. If nothing else, the creation date of the system object (dm_sysobject) will be used. Also note, although the retention date (Retained (a_retention_date)) was a selectable attribute, which it no longer is, any previously set base date entry that uses this attribute will be ignored when retention is applied or re-qualification in the first phase occurs.

The **Description** field is optional.

4. Click **Finish** to complete the process.

4.2.2.10.1 Deleting a base date mapping

All existing objects retained according to the base date selected for a retention policy will continue to age normally after the base date mapping is deleted. Any additional objects retained, after the base date mapping is deleted, will be retained according to the default base date mapping.

To delete a base date mapping:

1. In the navigation pane, select **Retention Policy Services > Base dates**.
2. Right-click the base date mapping you want to delete and click **Delete**.

4.2.2.11 Contacts

Contacts provide a master list that is used with the following items:

- Authorizers (for authorities)
- Approvers (for retention markups)
- Requestors (for retention markups)
- Contacts (for actions)

4.2.2.11.1 Creating a contact

Contacts provide an editable master list that you can access and use for authorizers, approvers, requestors, contacts (for events), and contacts (for actions). Use this procedure to create a contact.

To create a contact:

1. Navigate to **Retention Policy Services > Contacts** and select **File > New > Contact**.
2. Type a unique name in the **Name** field and click **Next**.
3. Enter values for the contact information using the respective Edit options. An entry for either the **Email** or **User** option is required. Everything else is optional for the **Phone**, **Address**, and **Description**.
4. Click **Finish** to accept the new contact.

4.2.2.11.2 Viewing or editing a contact

Use this procedure to view a contact.

To view or edit a contact:

1. Navigate to **Retention Policy Services > Contacts**.
2. Right-click the contact you want to view or edit displayed in the content pane and select **Properties**.
3. Click **OK** to close or accept any changes.

4.2.2.11.3 Deleting a contact

Use this procedure to delete a contact.

To delete a contact:

1. Navigate to **Retention Policy Services > Contacts**.
2. Right-click the contact you want to delete and select **File > Delete**.
3. Click **Yes** to confirm the deletion.

4.2.2.12 Authorities

An authority is a person or group that authorizes the promotion of objects from one phase of a retention policy to the next phase. You must also have an authority for the final phase, when the disposition of objects occurs.

Each phase of a retention policy must have at least one valid authority for the object to age. An authority is validated when you select the **Valid** checkbox. Multiple authorities can be applied to a single phase. The same authority or authorities can be used for all the phases of a retention policy. An authorizer is a person who is used as a reference or a contact to ensure that an authority is up to date. Authorizers are created with a master contact list. For information on contact lists, refer to ["Contacts" on page 206](#).

4.2.2.12.1 Creating an authority

Use this procedure to create an authority.

To create an authority:

1. Navigate to **Retention Policy Services > Authorities** and select **File > New Authority**.
2. Type a name in the mandatory **Name** field and click **Add** to add an authority now or click **Finish** to add the authority at a later time from the Properties of the authority.

If you add an authority now, you can also provide a description if desired. The authorities added are valid authorities if the checkbox for **Valid** is selected.

Retainers will not start the aging process unless the retention policy uses a valid authority.

3. Click **Finish**.

4.2.2.12.2 Viewing or editing an authority

Use this procedure to view an authority.

To view or edit an authority:

1. Navigate to **Retention Policy Services > Authorities**.
2. Right-click the authority you want to view or edit and select **Properties**.
You can add or remove authorities and make them valid authorities by selecting the checkbox or deselecting it to make them invalid.
3. Click **OK** to close or accept any changes.

4.2.2.12.3 Deleting an authority

Use this procedure to delete an authority.

To delete an authority:

1. Navigate to **Retention Policy Services > Authorities**.
2. Right-click the authority you want to delete and select **Delete**.
3. Click **Yes** to confirm delete or **No** to cancel delete.

4.2.2.13 Global conditions

Global conditions apply to the entire policy, as opposed to phase conditions that apply only to a given phase of a retention policy. Both can be specified for a retention policy.

A global condition ages across the entire retention policy, while a standard condition ages across a phase within the retention policy.

Global conditions may take precedence over phase conditions when both types are specified for a given retention policy. The global condition when fulfilled becomes the new qualification date. When the object is promoted, it goes directly to the final phase. When a global event is fulfilled, the object promotes to the final phase skipping the intermediary phases.

A retention policy could have one or more global conditions added to it in which case only the global condition with the longest date interval specified is acknowledged. For example, a global event that has March 23 specified is acknowledged while the global event that has March 22 specified is ignored.



1. A valid global authority must be specified on the retention policy so that its retainers can start the aging process, either when the retention policy is being created or anytime later through its Properties.
2. Though called a *global condition* on the retention policy, it is called a *global event* on the retainer. For standard conditions it is *condition* on the policy and *event* on the retainer.

Retainers will continue to age whether the global condition has a global authority specified for it or not, as long as a valid authority is added to each phase. The only thing that will not occur is that if the global event is fulfilled then nothing will happen. For example, this will not cause the item to be sent until the global authority is added.

4.2.2.13.1 Creating a global condition

Use this procedure to create a global condition. You can also create a standard condition if needed. To create a standard condition, refer to “[Conditions](#)” on page 211.

To add a global condition and authority, follow procedures used to create retention policies.

To create a global condition:

1. In the navigation pane, select **Retention Policy Services > Global Conditions**.
2. Select **File > New > Global Condition**.
The **New Global Condition** screen is displayed.
Only two of the three attributes displayed, **Name** and **Category** are mandatory and require values to create the global condition. The **Description** is optional.
3. Type a unique value for the mandatory **Name** attribute. The name could be based on the event that it is representing.
4. Either select a value or type a value for the **Category** according to the radio button you choose. The list box is displayed when the radio button for *Choose from existing categories* is selected. The list box is replaced to accommodate your typing for a new category when the radio button for *Specify a new category* is selected.
5. Click **Finish** to accept the values.

The new global condition is created and displayed in the content pane under Global Conditions.

4.2.2.13.2 Viewing or editing a global condition

Use the Properties of a global condition to view or edit.

To view or edit a global condition:

1. Navigate to **Retention Policy Services > Global Conditions**.
2. Right-click the global condition you want to view or edit displayed in the content pane and select **Properties**.
Use the **Info** tab to view the details or if necessary to change the entries.
3. Click **OK** to accept any changes or **Cancel** to ignore any changes.

4.2.2.13.3 Deleting a global condition

A global condition that is in use cannot be deleted.

To delete a global condition

1. Navigate to **Retention Policy Services > Global Conditions**.
2. Right-click the global condition you want to delete displayed in the content pane and select **Delete**.
3. Click **Continue** if the confirmation message displayed indicates that the selected global condition is in use, otherwise click **Yes** to complete the deletion process.

4.2.2.14 Conditions

A condition is a template for an event. One or more conditions can be added to a retention policy for a given phase. Once the policy is applied to an object then this becomes an event to which a date can be set. Once the date is set retainers start to age. Aging depends on the mixed mode rule you select on the Phases tab if you add one or more conditions when you create a retention policy. You can make the conditions:

- all optional (meaning that they may get fulfilled or they may not)
- all mandatory (meaning that all of them must be fulfilled if there is more than one)
- any one is mandatory (only one has to be fulfilled)

For more information about these rules, refer to “[Creating a retention policy](#)” on page 156.

4.2.2.14.1 Creating a condition

Use this procedure to create a phase condition. You can also create a global condition if needed. To create a global condition, refer to “[Global conditions](#)” on page 209.

To create a condition:

1. Navigate to **Retention Policy Services > Conditions** and select **File > New > Condition**.
The **New Condition** screen is displayed.
2. Enter values for the mandatory fields, the **Name** and **Category**, and click **Finish**.
Provide a description if necessary.
When applying a condition to a phase of the retention policy the conditions are grouped by category as a means to group them easily.
To select a category from existing categories, select a category from the list box when the radio button is selected for **Choose from existing categories**. If the

category you want to specify is not among the existing ones in the list box, select the radio button for **Specify a new category** and type a value in the text box; the screen refreshes to display a text box when this radio button is selected. The new category specified becomes available in the list box the next time it is used.

4.2.2.14.2 Viewing or editing a condition

You can view the details of the condition from its Properties screen and if necessary edit the existing entries.

To view or edit a condition:

1. Navigate to **Retention Policy Services > Conditions**.
2. Right-click the condition you want to view in the content pane and select **Properties**.
To set an event based on a condition, apply the policy, view the retainer, then add an event date to fulfill the condition.
3. Click **Cancel** or **OK** when you are done viewing. Otherwise, click **OK** to accept any changes.

4.2.2.14.3 Deleting a condition

Use this procedure to delete a condition.



Caution

You cannot delete a condition if it is referenced by a retention policy.

To delete a condition:

1. Navigate to **Retention Policy Services > Conditions**.
2. Right-click the condition you want to delete in the content pane and select **Delete**.
3. Click **Yes** to confirm the delete or **No** to cancel the delete.

4.2.2.15 Disposition run bundles

The Disposition Run Bundles node is displayed only when the Records Manager DoD Standard dar file (RM-DoD5015v3-Standard-Record.dar) is installed. For further details, refer to “[About disposition run bundles](#)” on page 314, as described under Records Manager.

4.2.2.16 Qualification, promotion, and disposition

About the Work Order Framework and the Monitoring and Recovery of Work Orders

The Work Order Framework is intended to process a large number of objects asynchronously, in a more efficient, scalable, and recoverable manner. An operation, qualifying a folder with millions of objects for example, is delegated to the framework if a UI message is displayed at the bottom of the screen that references a work order. The Work Order Report can be used for monitoring progress of a work order and when necessary, to recover a work order that fails to process. For further details about work orders and the framework, refer to “[Work orders](#)” on page 33. The Work order overview also includes the following link to the work order report: “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51.

Objects under retention are administered by the Qualification Manager, Promotion Manager, and Disposition Manager. Qualification Manager is used primarily if you want to requalify retained objects. For example, you changed the duration of a phase and would like the existing object to reflect this change. The system (Retention Policy Services) will automatically attempt to determine a qualification date the moment retention is applied to an object. A missing authority or the first phase being conditional are two reasons why the date could not be calculated automatically. An object cannot be promoted unless it qualifies for promotion from one phase to the next. In other words, the qualification date must be older or equal to the current date on the server when the promotion is attempted. Also, the authority field must be populated with a valid authority in order for an object to age.

Procedures that follow, provide information for manually running the Qualification Manager, the Promotion Manager, and the Disposition Manager. Objects that qualify for promotion can then be promoted to the next phase using promotion manager. Disposition manager can then be used to dispose objects when they reach the final phase. They can also be disposed of automatically by the disposition job according to its scheduling.



Note: Objects can also be qualified automatically, promoted automatically, and disposed of automatically, if you run the respective Qualification Manager, Promotion Manager, or Disposition Manager as a job. It is not necessary to run Qualification Manager in situations where objects are automatically qualified. When an object has been disqualified or is unqualified, the qualification job running in the background does not automatically requalify the object; you must manually run the Qualification Manager against the object that has retention applied to it, and select the checkbox next to Allow Re-qualification. For example, if you change the duration date in the retention policy and would like all previous object(s) to take the new value you would have to run the Qualification Manager to requalify those objects. For more information on running jobs, refer to “[Retention Policy Services jobs](#)” on page 273.

4.2.2.16.1 Qualification Manager

Qualification Manager is used to manually qualify or requalify objects for a qualification date. Only those objects under retention that have a qualification date are eligible for promotion. Qualification Manager can be run at any time against objects that could not be pre-qualified or against objects which need to be re-qualified. Objects that can be qualified when retention is applied, are automatically qualified (pre-qualified) by Retention Policy Services. If Retention Policy Services cannot prequalify an object, it can be manually qualified after a valid phase or global authority is added. You can run Qualification Manager after a valid authority is added to qualify an object immediately or wait for the qualification job to run. Objects with a cleared qualification date are eligible for re-qualification. The qualification date is cleared or removed if a setting against the duration or cut-off period is modified or if an object is disqualified from Promotion Manager.



Notes

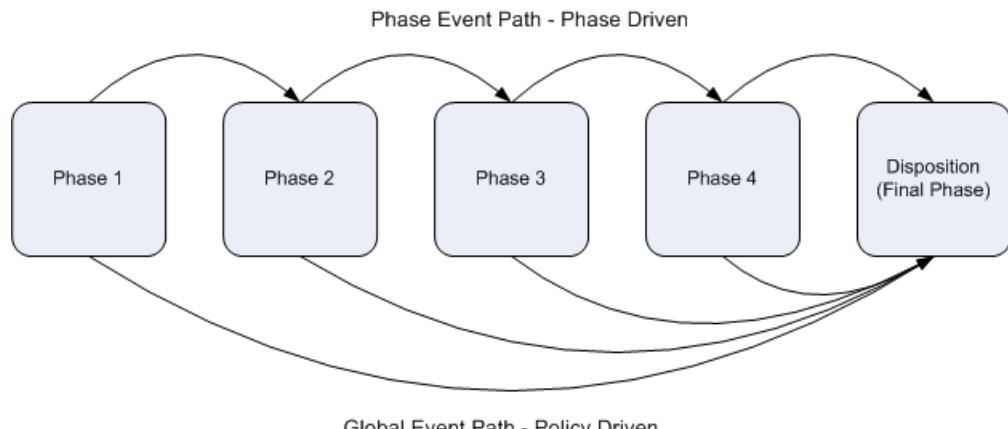
- Objects that already have the retention policy applied will continue to use the old qualification date (they are grandfathered). They will continue to age against the current qualification date unless they are re-qualified. If retention is applied to a folder, any new documents that are created or linked in the folder will either inherit the qualification date (for linked retention) or age individually and use the new values from the retention policy. Folders that are created or linked into retained folders will age individually for linked retention as well and will use the new values from the retention policy (folders that inherit individual retention do not age). Basically, spawning of new retainers use the new qualification date whereas, existing retainers continue to age against the old qualification date. The qualification date on objects with grandfathered retainers can only be cleared from Promotion Manager by being disqualified.
- If an event date is set or cleared programmatically, through IAPI or Webservices, Retention Policy Services will automatically try to qualify or unqualify the retainer.

Calculation of the qualification date is based on one of two paths, fulfillment of a phase event or fulfillment of a global event, if both phase and global conditions are specified on the retention policy. Fulfillment of a global event takes precedence over any phase events and promotes the object (technically, its retainer) directly to the final phase, skipping any intermediary phases. The calculation, if multiple global events are attached, is based on the one which occurs earliest.

Event Paths Used to Qualify Objects for Promotion

Object Under Conditional Retention with Both Phase Conditions and Global Conditions Specified

A phase event moves the object (retainer) to the next phase, upon promotion, once the event is set (fulfilled).



A global event moves the object (retainer) directly to the final phase, upon promotion, once the event is set.

In either case, the object must be qualified for a qualification date, once an event is set, before it can be promoted.

The path taken is based on the earliest specified event and only if a valid phase or global authority is specified.

Each phase must have a valid phase authority to move an object from one phase to the next.

Only one valid global authority is required to move an object from any phase to final.

Consider Phase 2 for example:
 Phase Event Path: includes one for Feb 15, 2015
 Global Event Path: includes two: one for Feb 10, 2010
 and one for Jan 1, 2013

The qualification date is set against the earliest date on either path, in this example Feb 10, 2010.

If the phase path has no eligible date (conditional with a missing date), then the earliest of the global event dates is used to calculate the qualification date.

Figure 4-11: Possible qualification paths

The following table further describes the path:

Table 4-23: Comparison of the Phase and Global paths for setting the qualification date

Path	Eligibility	Multiple event dates	Phase actions run
Phase	At least one valid authority on the phase (Phases tab)	All event dates must be set for a qualification, assuming mixed mode is not used.	- leaving the current phase - entering the next phase

Path	Eligibility	Multiple event dates	Phase actions run
Global	At least one valid authority on the retention policy (Info tab)	Only one event date needs to be set.	Leaving the current - enter the final (actions for intermediate phases are not run)

Objects are no longer displayed, removed from the list, once they have been qualified.

Pre-qualified or qualified objects have a qualification date present when viewing the retainer. You may not need to use Qualification Manager if the objects you need to promote have already been automatically pre-qualified. Use Qualification Manager when the duration of a phase in the retention policy or the cut-off period has been changed and you wish to requalify existing items to use the new values. If the item has been disqualified, use the qualification manager to requalify it.

Qualification allows the items to age within the phase. It can also be used to see what objects have already been qualified, as objects that can be qualified are automatically pre-qualified. Objects are automatically pre-qualified if a value can be calculated for the qualification date and only if at least one valid authority has been specified on the retention policy for the current phase. When a phase transition occurs, the entry date into the new phase is the date that promotion occurred. If the new phase is chronological, this is used in the calculation of the qualification date (the phase duration and any cut-off is added).

Only those objects that can be qualified will be gathered and displayed according to the search criteria you enter into the filter options provided. Qualification Manager only needs to be run under special circumstances as everything is pre-qualified.

You can either perform a customized search based on your search criteria to qualify one or more of the objects you select in the results list returned or you can qualify all objects in the repository that can be qualified. Objects that can be qualified for promotion are those that have completed the aging process for the phase that they are in.

Objects that have already been qualified can be gathered and displayed for viewing purposes using the qualification date. The from and to fields can be used to gather objects according to a specific date or range.



Note: A valid phase or global authority must be specified before a Qualification Date can be calculated.

Qualification dates are shown in the Promotion Manager.

Promotion Manager and Disposition Manager can be used to disqualify an object and reset/clear the Qualification date.

To run Qualification Manager:

1. Select **Records > Qualification Manager**.
2. Click **Search** to obtain results according to the default settings or change the filter settings to create your own custom search and then click **Search**. The filters for Qualification Manager are described as follows:

Table 4-24: Qualification manager filter descriptions

Filter Name	Description
In Folder	Allows targeting one or more specific folder locations within the repository, / Temp for example and all of its subfolders if desired. All folders are searched if nothing is selected.
Include Sub-folders	Subfolders of any selected folders are also searched when this checkbox is selected.
Retention Policy	Selecting one or more specific retention policies returns only those objects with retainers that reference the policies selected.
Phase	Represents the phase of a retention policy. A specific phase of the retention policies selected can also be selected to further narrow the results.
Event Date	Represents the event date setting on the Phases tab of a retention policy. Used to calculate the qualification date of objects under conditional retention. All objects with an event date within the date range selected are reported. The event date is a retainer attribute. The event date can be specified to return a list of objects that are retained according to a condition or global condition. The date can be entered to return a list of objects spanning a particular range or for a specific date if you specify the same date value for both the From and To fields. The Qualification Date , also described in this table below, can also be used similarly to return results spanning a particular range or for a specific date.

Filter Name	Description
Cascade Rule	<p>Used to filter retention policies that have Cascade To Subfolders setting selected or Cascade To Subcategories setting selected or both selected or neither selected, for the Cascade Rule. List box options here are: <i>All, Cascade To Everything, Cascade To Subcategories, Cascade To Subfolders, and Do Not Cascade.</i></p> <p> Note: The Cascade To Folder or The Cascade To Subcategories settings on a retention policy are identified on the Retention Policy Details page as the Cascade Rule Name when you view the details of an exported retention policy during the import process.</p>
Type	<p>The objects reported can be filtered against one or more object types. Select dm_folder for example, if you want to qualify or requalify only folder objects.</p> <p> Note: Results returned against the selected Type include all subtypes. If Select Type is clicked and one or more types is selected, then the results returned will be not be just for the type only, but for all of their descendant sub-types as well. For example, if dm_sysobject is selected, then not only will objects that are explicitly dm_sysobjects be returned, but so will all objects that are based on any type that is ultimately a sysobject. To elaborate, if dm_sysobject is selected, then also selecting dm_document or dmc_prm_physical_document would be redundant. In the former case, dm_document is extended from dm_sysobject. In the latter case, dmc_prm_physical_document is extended from dm_document which is, as mentioned, extended from dm_sysobject.</p>
Authority	<p>Represents the authority setting of a retention policy. Filters objects with retention against one or more authorities, whether the authority on the retention policy is valid or not.</p>

Filter Name	Description
Allow Re-qualification	When selected, reports on all objects under retention which can be qualified. Normally the report excludes objects that already have a qualification date but with this option, the objects can have their qualification date recalculated based on the current values of the retention policy. Use this option after making changes to a retention policy if you want the changes to update existing applications of the retention policy. Note: if the retention policy Event fulfillment rule is changed to be more restrictive, the item may no longer be able to qualify and will not show up in the report if this option is selected. If the intent was for this object to no longer have a qualification date, use the promotion manager to disqualify the item.
Qualification Date	Calculated setting on the retainer of a retention policy. The earliest date on which an object (retainer on the object) can be promoted to the next phase or disposed of in the final phase. All objects with a qualification date within the date range selected are reported.
Retention Strategy	Represents the Retention Strategy setting of a retention policy. <i>All</i> is the default setting which reports both Linked and Individual types. <i>Linked</i> for shared retention or <i>Individual</i> for independent retention. Linked retention means only one retainer is spawned when a retention policy is applied to a container object, a folder for example, whereby the contents age against the retainer on the folder (children do not have retainers and therefore age with the parent retainer). Individual retention means multiple retainers are spawned, when retention is applied to the folder, whereby all contents inherit their own retainers to age independently of the folder (children inherit retainers from the parent and age individually).

Results are returned under the following default column headings:

Table 4-25: Qualification manager default column headings

Column Heading	Description
Name	Name of the object that can be qualified.

Column Heading	Description
Version	Indicates the Version Label value on the properties of the object.
Retention Policy	Name of the retention policy that retains the object.
Phase	Indicates the phase in which the object can be qualified. This corresponds to the value displayed for the Current Phase on the retainer that retains the object. Values displayed under this heading, as well as under the entry, event, and qualification dates below, can be verified when you right-click one of the entries and select Properties. The properties displayed is based on the applied retention.
Entry Date	Indicates the Entry Date value on the properties of the object.
Event Date	Indicates the Event Date value on the properties of the object.
Qualification Date	Indicates the Qualification Date value on the properties of the object.

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

You can also right-click a work order in the results, select **Properties** and make changes if necessary.

3. You can either click **Search** according to the default filter settings to search and list all objects in the repository that can be qualified for promotion, or change the filter settings to customize the search so that only those objects you want to see are listed. All objects that can be qualified will be qualified if you click **Qualify All**.

Filters can be set for a more selective search if you want to avoid qualifying all objects that can be qualified in the repository. For example, you can search one or more folders and if necessary include their subfolders, and/or search for objects that can be qualified according to a particular retention policy, object type, or authority. You can also narrow the search to a particular phase.

Allow re-qualification can be selected to permit recalculation of the qualification date for objects that have previously been qualified. You may want to requalify the object if there is any change to the duration and/or cut-off on the retention policy used to retain the object.

The event date can be specified to return a list of objects that are retained according to a condition or global condition. The date can be entered to return a list of objects spanning a particular range or for a specific date if you specify the same date value for both the **From** and **To** fields. The qualification date can also be used similarly to return results spanning a particular range or for a specific

date (you would need to enter the same date value in both fields for a specific date).

4. Select one or more of the objects displayed in the content pane and click **Qualify** to complete the process. The action option is available/selectable only when at least one object is selected.
5. Optionally, to see a detailed report of the *Qualification* operation, run the **Work Order Report**, to see the master work order and details. To see the subwork orders, if any, spawned by a master work order, run the **Work Order Breakdown Report**. To see the items that were processed by the work orders, run the **Work Order Item Report**. For instructions to run any of these reports, refer to “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51. For a work order introduction, refer to “[Work orders](#)” on page 33.

4.2.2.16.2 Promotion Manager

The Promotion Manager is used to promote objects under retention whose qualification date for a particular phase has elapsed. It can also be used to disqualify any of the objects returned in the search list and it can also be used to apply a retention markup whenever one is needed. The promotion job promotes objects to the next phase if the current date is equal to or greater than the qualification date.

Use the Filters provided to perform a customized search to list qualified objects for promotion then take the desired action on the objects you select from the list.

To run Promotion Manager:



Note: Any container object that has an individual retention policy applied to it will not have a qualification date and will not show up in promotion manager or qualification manager. Individual retention policies on folders do not age but rather propagate retention to its children. Container objects, such as folders, physical folders or boxes, categories, and so on, show up only if a linked retention policy is applied.

Objects under conditional retention cannot be promoted (or processed for disposition), unless the qualification date is now (matches the current date) or is in the past.

1. Select **Records > Promotion Manager**.
Options to **Disqualify**, **Promote**, and **Apply Retention Markup** are displayed only after a search is performed with at least one item found.
2. You can either click **Search** according to the default filter settings to search and list all objects in the repository that are qualified for promotion, or change the filter settings to customize the search so that only those objects you want to promote are listed.

Refer to “Qualification manager filter descriptions” on page 217 Qualification manager filter descriptions as the filters for both Qualification and Promotion Managers are the same.

3. Select one or more of the objects displayed in the content pane and click the desired action option to complete the process. The action options are available/selectable only when at least one object is selected.
4. Click **Yes** on the confirmation screen displayed to continue and complete the process if you choose to **Promote** the selected objects.

Select a retention markup from the locator displayed if you choose to **Apply Retention Markup**. A text box for **Reason for applying markup** is included. You will need to click **OK** to accept the selected retention markup then click **Yes** on the confirmation screen displayed to continue and complete the process.

No confirmation is required if you choose to **Disqualify** the selected objects.

5. Optionally, to see a detailed report of the *Promotion* operation, run the **Work Order Report**, to see the master work order and details. To see the subwork orders, if any, spawned by a master work order, run the **Work Order Breakdown Report**. To see the items that were processed by the work orders, run the **Work Order Item Report**. For instructions to run any of these reports, refer to “Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report” on page 51. For a work order introduction, refer to “Work orders” on page 33.

4.2.2.17 Disposition Manager

4.2.2.17.1 Overview of disposition



Note: Run the dmc_rps_DMCleanJob whenever you are finished running disposition. It should also be configured to run automatically on a predetermined schedule to account for cleanup after disposition runs that are performed by the Disposition Job. To run the dmc_rps_DMCleanJob, refer to “Retention Policy Services jobs” on page 273. Cleanup is meant to free up physical space on the disk after disposition runs that destroy all or destroy content.

4.2.2.18 About the disposition job, strategies, actions, export and transfer locations

Disposition Manager is used to perform disposition actions on one or more objects that are under retention in the final phase of their lifecycle. You can only run a disposition action on objects whose qualification date has elapsed in comparison to the current date. The disposition process destroys and/or transfers content and/or metadata according to the disposition strategy specified. The object selected is considered destroyed only when both its content and metadata are destroyed. Some of the disposition strategies are nondestructive (non-terminating) in which case the object will roll over to another retention policy, based on the retention policy specified for the rollover, that finally destroys both its content and metadata.

The disposition strategies, specified in a retention policy, include:

- Unknown
- Review
- Export all, Destroy all
- Destroy all
- Export all
- Export all, Destroy content
- Destroy content
- NARA transfer, Destroy content
- NARA transfer, Destroy all

To select multiple disposition strategies while querying for the items in the Disposition Manager UI, you can click on the **Select Disposition Strategy** link against the **Disposition Strategy** field.

If retention manager wants to know the items that are required for disposition (items that cannot be processed because there are no defined export location), the retention manager can select export specific disposition strategies and can query for the items.

The disposition job for only the Unknown strategy must be properly configured for it to run successfully. Refer to the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)* to configure the disposition job to run successfully against objects with an Unknown disposition strategy.



Note: The disposition strategies provided out-of-the-box and their associated actions are described in “[Retention policy overview](#)” on page 146. Both NARA options are only present if the Department of Defense Standard dar is installed. Objects in disposition that were NARA transferred display more details if the objects are Department of Defense Standard formal records, Department of Defense Classified formal records, or formal folders. Only limited details are displayed in disposition, for all other objects that are NARA transferred.

Disposition Manager takes the appropriate actions according to the Disposition Strategy selected for the applicable retention policy. Each disposition strategy is associated with a combination of one or more, up to four possible actions. Export all, Destroy all performs all of the actions, as previously shown in “[Disposition strategy actions](#)” on page 150, whereas Unknown and Review have no actions to perform.

Disposition strategies that are terminating specify Destroy all. For example: Destroy all, Export all, Destroy all, and NARA transfer, Destroy all. Both content and metadata are removed. A non-terminating strategy is one that leaves the content or the metadata behind. A rollover must be specified for retention policies that are non-terminating. An override and rollover must be specified for disposition if the retention policy is set to Unknown, unless the override selected is set to Destroy all.

Export actions are performed immediately when disposition is run, regardless of the number of retainers associated to a particular object. Destructive actions however, when more than one retainer is associated to the object, will not be taken until all retainers are in the final phase ready for disposition.



Note: The following factors affect disposition:

- Objects on hold will not qualify for disposition. An object under hold does not appear in the Disposition Manager Report. You can run the Retention Markup Report to see objects currently under a retention markup.
- To perform disposition on an object with Unknown, you must change the strategy by selecting the override value from the pull-down menu.
If you want to export, the export location must be a valid network (UNC) path.
- If the disposition strategy selected for a retention policy includes a transfer strategy, the Disposition job will not work unless the Java Method Server and Records Queue Manager server are running on a Windows machine.

4.2.2.19 About disposition status

Actions associated with a particular retainer are tagged with one of six possible disposition status labels:

- Open: no disposition action has been taken yet.
- Pending: disposition is invoked (but not yet started; it will be initiated once all the retainers on the object are set to Pending and all its specified disposition actions can be executed).
- Incomplete: disposition processing on the object is not completed. This is not necessarily an error condition. For example, when disposing physical objects, someone has to perform a manual action on the objects and then inform the system that it has been done (for example, marking for destruction, confirming that the items have been destroyed).
- Processed: disposition processing on the object is completed. Processed only appears if the retention policy does not destroy the object. This means that a rollover to a new retention policy has occurred.
- Terminated: disposition was invoked using a destructive strategy on the object but destruction of the object is delayed. It is marked to be destroyed but is protected by another retention policy until it can perform disposition.
- Waiting: disposition was invoked and partially finished but could not continue processing until further user action is taken such as transfer confirmation or rejection.



Note: Exceptions encountered in disposition processing are placed or captured in an XML work order report, displayed when you right-click a work order and select the menu option View Results. You can right-click a work order listed in the results of a Work Order Report or a Work Order Breakdown

Report or when it is attached to a work order Inbox or E-mail notification. For further details, refer to [Appendix D, XML Report examples against View Input and View Results](#) on page 763.

4.2.2.20 Disposition on a simple object

A simple object has no children. For example, a normal document, a spreadsheet, and a physical document. When disposition is started for an object, all eligible retention information (stored internally on retainers) will be processed. If there are Pending or Incomplete retainers on the object, they will be included in the processing. Based on the selected objects from the Disposition Manager, the disposition actions to execute will be resolved according to disposition rules.

Non-destructive actions, which include all export actions, will *always* be executed. Destructive actions will only be executed if all considered retainers *agree* and, if there is no Open retainer on the object.

If all actions on the retainer are executed, it will be marked as Processed. This will always be the status for a retainer that has only non-destructive actions, *unless an error occurred*.

If not all actions on the retainer are executed, it will be marked as Incomplete. This will also be the status if any error occurred during processing.

If none of the actions on the retainer are executed, it will be marked as Pending. This will always be the status for a retainer that has only destructive actions and with still an open retainer on the object.

4.2.2.21 Disposition on a complex object

A complex object has children. Retention Policy Services understands the following types of complex objects (and subtypes):

- A virtual document
- A formal record
- A snapshot
- A folder or cabinet

For the object itself, it will follow the same rules as that of a simple object. It will propagate disposition to its children (in the case of virtual documents and snapshots/formal records only if the retention policy is set for this, to retain root and children) but will not be held up by a child that is a member of another complex object or that has a direct retainer on it. Hence, if a disposition action cannot be legitimately executed on a child, even if it is called for in the root, it will not affect the status of the root itself.

However, if the action is to be executed on a child and results in an error, and it is an action that is called for on the root as well, then it will cause an Incomplete status on the root's retainers that call for that failed disposition action.

To obtain a Disposition Status, refer to “[Running the retention report](#)” on page 247.

4.2.2.22 About disposition rules

There are two rules Disposition Manager follows to determine disposition against an object retained by more than one retainer: one rule for destructive actions and one rule for non-destructive actions. Destructive actions are executed only if each retainer specifies the same destructive actions; destructive actions in each retainer must agree. An export action will be executed if it is a specified action in any of the disposition strategies applied to the object; export actions in each retainer are executed without agreement.

4.2.2.23 Disposition processing behavior when multiple retainers are applied to an object

For example, running Disposition Manager against an object with three retention policies applied.

Assume three retainer objects are applied to an object:

1. Destroy all (DA), terminating
Actions include: destroy content, destroy metadata
2. Export all, Destroy content (EA-DC), non-terminating
Actions include: export content, export metadata, destroy content, keep metadata
3. Export all (EA), non-terminating
Actions include: export content, export metadata

Run 1: During the disposition run, assuming that all of the retainers have reached the disposition phase and can be processed: retainers 1, 2, and 3 are gathered, their disposition strategies are determined, and all actions that can be executed are executed. In this run all export actions are executed (unlike destructive actions which require agreement across all retainers gathered, export actions require no agreement and are always executed in a run). Therefore, retainer 3 is given a disposition status of Processed, 2 is Incomplete, and 1 is Pending. No destructive actions are performed until all three retainers agree; all three retainers must specify Destroy content or Destroy metadata or both. Because retainer 3 is Processed and is non-terminating, it is rolled over to another retention policy, which we will name retainer 4, and assume it specifies Destroy content for the disposition strategy. The object is now being retained by retainers 1, 2, and 4.

Run 2: Now the disposition run gathers retainers 1, 2, and 4, determines their disposition strategies, and executes all actions that can be executed. In this run all export actions and Destroy content are executed, metadata remains in the system. Now, retainer 4 is given a disposition status of Processed, 2 is Processed, and 1 goes to Incomplete. Retainers 4 and 2 now rollover as they are Processed and non-terminating. Assume retainer 4 rolls over to retainer 6 specifying a disposition

strategy of Export All, Destroy all and retainer 2 rolls over to retainer 5 specifying a disposition strategy of Destroy all.

Run 3: Now the disposition run gathers retainers 1, 5, and 6, determines their disposition strategies, and executes all actions that can be executed. In this run all export actions and all destructive actions are executed. All retainers are now processed and the object under retention is destroyed, both its content and metadata.

4.2.2.24 About terminal retention

Terminal retention is a mechanism to indicate that an object went through disposition but could not be destroyed for some reason. For example, a document is linked into two different folders that apply linked retention. When disposition is run on one of the folders, the system would like to destroy the object but cannot because the second folder is still protecting the document. If the Unlink On Dispose setting (on the Retention Policy Services Configuration object) is enabled, the system will unlink the document from the folder (allowing the first folder to finish disposition) and a terminal retainer is applied. The reason for the terminal retainer is that if the other retention is removed, because disposition was already run, the document should be deleted. The terminal retention job will search for documents that have terminal retention applied but no longer have Retention Policy Services retention applied.

Folders that have terminal retainers will not allow any items to be created or linked into the folder (similar to close folder functionality). The reasoning is that the folder should be destroyed so that the system prevents new items from being put into the folder.

If the disposition process is to destroy the folder that has any children, then a terminal retainer will be applied to the folder to prevent additional items from being put into the folder (as the folder is supposed to be destroyed). Children may still be in the folder if:

- Documents are under hold.
- Documents that could not be deleted (for example a file-storage policy such as Centera in Compliance Plus mode may block the destroy).
- Folders that are not eligible for disposition (or were not selected).
- Folders that do not have retention (because the retention policy specified is not configured to cascade to the folder (or the category)).

Terminal retainers are not applied if the retention is structural because by definition, structural retention does not destroy the folder so we do not want to put a terminal retainer on it.

For disposition strategies such as Export All, Destroy all or NARA Transfer, Destroy all, a terminal retainer is only applied if all of the other steps could be done. For example, if the Export location is not writable, a terminal retainer will not be applied to the folder (using linked retention).

4.2.2.25 About structural retention

Structural retention provides the ability to apply retention to a folder so that when disposition is run, only the contents of the folder are destroyed. If the folder contains subfolders, each must go through disposition separately and will not be destroyed. Structural retention can only be defined for retention policies that use the Linked Retention strategy and for disposition strategies that do not require a rollover. Retention policy that use an Unknown disposition strategy cannot specify structural retention.

When a structurally retained folder is disposed successfully, the retention resets and the retainer state changes to the first phase (and aging begins again).

4.2.2.26 About disposing physical objects

For details, refer to “[Disposition of physical objects](#)” on page 509.

4.2.2.27 About disposition workflows

Disposition workflows are used to route objects, documents for example, for approval so you can manually dispose of them, if they require approval but have not yet been approved. Once approved, the disposition job will automatically dispose of them as well. Approval for disposition is required. Documents can then be processed either manually or by the job.



Note: The set of objects gathered in a disposition workflow is referred to as the Disposition Bundle. A Disposition Bundle can be thought of as the disposition approval bundle and has nothing to do with Disposition Run Bundles.

The following audit events are available for disposition bundles:

- dmc_rps_disposition_approved
- dmc_rps_disposition_rejected
- dmc_rps_submitted_for_approval

The audit trails however are created only if the desired audit event is enabled from Documentum Administrator.

You are prevented from disposing of a document when you select the Dispose option against a document that requires approval in the Final phase but has not yet been approved. The disposition job also honors this in that it will skip all items that need approval. A document in the Final phase would require approval, before it can be disposed of using the Dispose option, if its retention policy has the Requires Approval attribute selected. You can tell which documents require approval using Disposition Manager to Search and list documents eligible for disposition in the Final phase. The documents listed would show *true* or *false* in the Approval Required column. The document must be routed for approval, using the Route for Approval option (see procedure below), before it can be disposed of if its Approval Required field indicates *true* and its Approval Status field is *blank*. You can also use

Route for Approval even if this option is not set on the retention policy when you want to do a one-off!

There are four values that can be displayed for the Approval Status:

- Blank, when nothing is displayed
- Submitted for Approval
- Rejected
- Approved

The Properties of the retainer applied to a document also includes information about the Approval Required, Approval Status, and Approved Date attributes. To view or modify the properties of a retainer that is applied to an object, refer to “[To view or modify the properties of a retainer](#)” on page 188.

4.2.2.28 To route a document for approval (start a workflow for review and approval)

If *true* appears, in the Approval Required column, then this step is mandatory. If not you are free to do this if you want one or more items to go through approval, even if the policy does not state it. The policy only forces approval to be mandatory once objects get to the disposition phase.

The workflow template allows a reviewer to choose one of two options:

- One for everyone that approves, ready for disposition.
- One for a rejected review.

The implication is that if someone rejects the review a records manager will want to restart the approval process after the issue is resolved.

1. In Disposition Manager, perform a **Search** according to the desired filter option settings or default settings to list the document of interest, the document you want to dispose of but has not yet been approved.
2. Select the document you want to dispose of, but has not yet been approved, when the search results are returned and click **Route for Approval**.

The **Start Disposition Workflow** screen is displayed from which you can choose a predefined workflow.

The application creates a disposition approval package that can be approved or rejected. The entire package for example, all of the records in the package can be approved or rejected.

3. Select the preferred workflow from the list displayed and click **OK**.
The document selected should be the one listed as an attachment in the resulting **Start Workflow** screen.
4. Click **Finish** to complete the process or click **Next** if you want to add any comments. Comments will appear with the task when notifications are sent to

the recipients Records Client Inbox. Comments when you add a comment can be displayed **For subsequent recipients** or **For next recipient(s) only**.

Recipients when they receive notification can double-click the notification in their Inbox to open it and review the attachment before they approve or reject the task.



Note: Once the workflow is started, each of the objects that have the primary retainer applied would show up in the Inbox task. So, if a linked retainer was applied to a box, the box would show up in the Inbox task (and not the contents of the box).

4.2.2.29 Running Disposition Manager

About disposition manager

Filters and columns in Disposition Manager include:

- List box to filter against the Disposition Strategy.
- Checkbox to filter against the disposition status of Waiting.
- Column headers at the top of the content pane:
 - Previous Receiving Organization
 - Export Location

Use Disposition Manager to query objects that are in the Final phase of their lifecycle where they are eligible (ready) for disposition. It is used to gather the eligible objects and then used to run (start) the disposition process. Information about a disposition run is contained in a disposition run bundle. Although disposition run bundle functionality was meant specifically for transfer runs only, that is for DoD NARA transfers, it can also be used for strategy runs. For further details about disposition run bundles, refer to “[About disposition run bundles](#)” on page 314. Disposition processing will not be performed against those documents/objects which have an applied retention policy with Requires Approval on the Phases tab selected for the Final phase. The document/object must be reviewed and approved before disposition, in such instances, can occur. The Requires Approval feature option is available/intended to prevent disposition processing from starting until a review process has been completed. For further details, refer to “[About disposition workflows](#)” on page 228, “[Creating a retention policy](#)” on page 156, “[Viewing/modifying a retention policy, applied retention, or retainer properties](#)” on page 184, and “[Applying a retention policy or viewing a list of retention policies](#)” on page 191.

Unlike the Qualification or Promotion Managers, you must log in to the Disposition Manager. Typical disposition actions include export to long-term storage, destruction, or preservation for archival purposes.



Note: Physical objects that undergo disposition are exported or transferred against the Home Location of the physical object instead of the Export Location specified in Disposition Manager. The Export Location on the address object

assigned for the Home Location on a physical object is used, to dispose physical objects, instead of the Export Location specified on Disposition Manager. If the physical object has no address, a default address can be configured on the Retention Policy Services Application Configuration object. A value for the Export Address on the configuration object should be manually set by the user if they want to have a default backup value. Disposition will first attempt to determine the value for the Export Address from the Home Address of the physical object in question, if it has a value specified. If not, disposition will then attempt to determine the value for the Export Address from the Retention Policy Services Application Configuration object. If the value cannot be determined in either case, an error message is displayed. The object being disposed is consequently added to the disposition log if a value cannot be determined.

Before Running Disposition Manager

Any folder-based object that has an individual retention policy applied to it will not have a qualification date and will not show up in Promotion Manager or Disposition Manager. Individual retention policies on folders do not age but rather propagate retention to its children. Physical boxes and physical folders show up only if a linked retention policy is applied. This applies to any folder-based object.

Reasons that may prevent disposition processing from completing (that is, when you click Dispose):

- Physical objects are not marked for destruction or export. Physical objects in disposition must be marked physically destroyed or marked exported first, then rerun disposition so that the process can complete.
- Waiting for a confirmation. Department of Defense records retained in retention policy managed folder with a NARA transfer disposition strategy, must be confirmed before disposition processing can continue.
- A document in a folder is under hold.



Note: The retainer on a folder that is under linked retention and is being NARA transferred, is marked as Incomplete if one or more documents have a hold or permanent retention markup applied. The document and the folder are not transferred and the retainer is marked as Incomplete so that it can be recovered from the master work order. The transfer run status remains IN_PROGRESS. Confirmation of the transfer as a result cannot be performed. The documents in the folder that do not have a hold or permanent markup are however transferred (exported). To successfully complete the transfer, follow instructions to remove the hold or permanent retention markup from the documents that have it and then follow recovery instructions. To remove a retention markup, refer to “[Removing a retention markup](#)” on page 246. To recover a failed disposition run, refer to “[To open a disposition run bundle and view the details, and when necessary to view the details of the work order and perform recovery actions](#)” on page 731. Although recovery can also be performed from the Work Order Report, It is

recommended to perform NARA transfer recovery from the disposition run bundle.

- The object is stored in a filestore that requires the force delete option (for example, some configurations of Centera) and the force delete option is not set.
- Items are still in the folder and prevent destruction for the following reasons:
 - Subfolders, if the folder contains any, were not selected. Folders displayed in disposition manger must be selected before they can be processed. Note, if the retention policy does not cascade to the subfolder, the subfolder will need to be manually deleted.
 - Subfolder is not eligible for disposition (is not in final phase, qualification date is not set, or qualification date is set but represents a date in the future).
 - Document could not be destroyed.
 - Another retention policy may be protecting the subfolder or the document. All applied retention policies must agree that the object can be destroyed.

A warning is displayed, in the Work Order Report, against items picked up for the Disposition operation that no longer exist. The warning is meant to identify items in a work order that are deleted unexpectedly before the work order framework gets around to actually processing them. If a Retention Manager for example, tries to dispose of a folder and someone privilege deletes it when disposition is about to process it, disposition issues the warning but does not affect processing of the parent folder.

Also note that a warning against any physical object that is run through disposition means that intervention is required to allow disposition processing to continue. For example, destruction of a physical object must be marked for destruction before it can be destroyed. Similarly, NARA transfers require confirmation before the actual transfer can proceed.

Reasons that can prevent objects from showing up in Disposition Manager:

- If the retainer is missing the qualification date or if it has a qualification date that is in the future. And, here are the reasons that can prevent the qualification date from being set:
 - No valid authority on final phase.
 - Unfulfilled event date on final phase.
 - Someone manually disqualified the object.
- If the object is checked out. Verify that the object is not checked out.
- If the object has a Hold or Permanent retention markup applied.

To run Disposition Manager:

1. Select **Records > Disposition Manager**.

Refer to “[Qualification manager filter descriptions](#)” on page 217 Qualification manager filter descriptions where the following filters are described:

- In Folder
- Retention Policy
- Disposition Strategy
- Cascade Rule
- Authority
- Retention Strategy
- Event Date
- Type
- Authority

The other filters on **Disposition Manager** are described as follows:

Table 4-26: Disposition manager filter descriptions

Filter Name	Description
Show (Open, Pending, Incomplete, Waiting)	Objects that are ready for disposition or are already undergoing disposition can be reported against one or more specific disposition processing states. The disposition processing states are described in “ About retention policy lifecycles and retainers ” on page 146. Although there are six possible states, objects in either the Processed or the Terminated states are not considered, as they have already been disposed.
The following options are displayed only when one or more results are reported. These options are not filters!	

Filter Name	Description
<ul style="list-style-type: none">• Unknown Disposition Strategy• Override• Rollover	<p>This option is meant to be used against only those objects that are reported with a Disposition Strategy of <i>Unknown</i>. It can otherwise be ignored. Unknowns are meant to be resolved only when they are up for disposition. If an <i>Unknown</i> is reported that you would like to resolve, select the desired value for the Override. The value you select will determine whether a rollover has to be specified. If the override selected is nondestructive, <i>Export all</i> for example, Select Retention Policy Rollover becomes selectable (underlined), signaling you to select a retention policy to roll over to. You can avoid rollovers by selecting a retention policy with a Disposition Strategy that destroys all, content and metadata. A rollover retention policy does not have to be selected if the value for the Override selected is destructive, destroys all.</p> <p>Also, make sure the retention policy selected for the Rollover is one that has a Retention Strategy that matches the original. If multiple unknowns are reported, avoid selecting more than one to specify an override unless, the value for the Retention Strategy is the same for each of the selected unknowns.</p>

Filter Name	Description
Export Location	<p>Path to a network location where objects are exported or NARA transferred.</p> <p>If the Allow only authorized export paths is enabled on the RPS Disposition Configuration object, then the Disposition Manager UI provides a dropdown list with the configured network paths that are configured on the RPS Disposition Configuration object. The default export directory on the RPS Disposition Configuration object is set as the default path in the drop down list.</p> <p>If the Allow only authorized export paths is not enabled on the RPS Disposition Configuration object, then the Disposition Manager UI will show the Export Location textbox pre-populated with the default export directory. You can change this path with any other valid network path before processing the disposition.</p> <p> Note: Since the disposition (export action if applicable) processing is performed through the Application server or Records Queue Manager, the network path should be resolvable from Application server or Records Queue Manager installed hosts.</p>
Force delete	<p>If the content is on a filestore that is retention aware, the filestore will prevent deletion until the date passed has been met. This option instructs the filestore to allow deletion of the content before that date. Note that Force Delete will not work if Centera is configured to run in the highest security mode (Compliance Plus).</p>

Using the Start With search field, you can search within the displayed results. Results are returned under the following default column headings:

Table 4-27: Disposition manager default column headings

Column Heading	Description
Name	Name of the retained object. The name may be repeated in the list if more than one retention application is eligible for disposition.
Version	Version of the retained object.

Column Heading	Description
Retention Policy	Name of the retention policy applied to the object.
Rollover Policy	If the disposition strategy requires a rollover policy, this is the name of the rollover policy (defined on the retention policy).
Qualification Date	The value for the Qualification Date on the retainer applied to the object. Each retainer that is eligible for disposition will have its own qualification. All retainers on an object must be selected to enable disposition to complete.
Approval Required	The value shown is <i>Yes</i> if the Requires Approval checkbox, in the final phase of the retention policy referenced by the object reported, is selected. <i>No</i> if it is not selected. Even if the final phase of the retention policy does not require approval, if the items are routed for approval, then Approval Required is automatically set to <i>Yes</i> .
Approval Status	The value for the Approval Status on the retainer only matters if approval is required. The possible values displayed could be: <i>Approved</i> , <i>Submitted for Approval</i> , and <i>Rejected</i> . The value is blank if approval is not required or if approval is required but the item has not been routed for approval yet.
Disposition Strategy	The value for the Disposition Strategy on the retention policy applied to the object.
Status	Disposition processing status. The possible states that can be reported in Disposition Manager are: Open , Pending , Incomplete , and Waiting . For additional details, refer to Show in the preceding table that describes the filters. If Incomplete is displayed, use the Work Order Report to recover or use the Disposition Run Bundles.

Column Heading	Description
Physical Status	If the object is physical, a status may be shown for the item. Possible values are blank, Physical Object Marked for Export, Physical Object Marked Shipped, Physical Object Marked for Destruction, Physical Object Marked Content for Destruction, Physical Object Marked Physically Destroyed, and Physical Object Marked Contents Destroyed.

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- Assembled From Id
- Cascade Rule
- Completed Disposition On
- Disposition Strategy Id
- Format
- Has Frozen Assembly
- Is Replica
- Is Virtual Document
- Link Count
- Linked Strategy Type
- Number of Resets
- Object Id
- Previous Receiving Organization
- Reference
- Retainer Id
- Retention Strategy
- Rollover Policy Id
- Type

To add, remove, or reorganize columns, refer to [“Setting column preferences” on page 77](#).

2. Click **Search** to obtain results according to the default settings or change the filter settings to create your own custom search and then click **Search**.



Note: Disposition Manager, regardless of what the filters are set to, reports only those objects in the final phase that have a qualification date.

Not all items shown in disposition may be eligible for disposition. For example, if a duration was specified in the final phase of the retention policy and the qualification date is in the future or if the items require disposition approval which has not been approved yet, disposition is not possible.

Action options to **Disqualify**, **Dispose**, or **Route for Approval** are displayed when at least one item is returned. You must also select at least one of the objects reported to make any of the actions available.

3. Select one or more of the objects listed and click the desired action:
 - **Disqualify** to clear the qualification date and prevent disposition.
 - **Dispose** to export, transfer, or destroy. A confirmation dialog is displayed when this action is selected to which you will have to answer *Yes* or *No* to continue or not.
 - **Route for Approval** to obtain signoff. The **Start Disposition Workflow** dialog box is displayed when this action is selected. You will not be able to select a disposition workflow if none are available. If necessary, follow instructions to create a disposition workflow and register it. For instructions, refer to How to register and configure a disposition workflow (based on the shipped sample workflow) in the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*. Once this is done, refer to the following instructions in “[To route a document for approval \(start a workflow for review and approval\)](#)” on page 229.

If destruction of a folder, under linked retention, during a disposition run is prevented because the folder is not empty, you can determine why using the **Work Order Item Report**. If however, work order functionality is disabled, refer to the audit trail logs to determine the reason why each of the remaining objects could not be processed. The reason is tied to each remaining object, not the folder. The only reason associated with the folder is the fact that it was not empty.

The following error is displayed when you click **Route for Approval** if the selected item(s) are currently routed for approval or are under disposition processing: **All of the selected items are either already in an approval workflow or disposition processing has already started.**



Note: Although it is possible to right-click a physical container object that is under normal Retention Policy Services retention and mark it for destruction, any physical container object that is under Retention Policy Services structural retention cannot be marked for destruction. Only the contained objects of a structurally retained physical container can be marked for destruction. Container objects that are structurally retained are meant to be permanent fixtures. Only the content in structural containers can be disposed. Although a structural container (that is container with structural retention) cannot be destroyed, it is however reset to restart the aging process. Any physical object that goes through disposition, whether

it is structurally retained or not, after it has been **Marked for Destruction** cannot be unmarked while it is under retention. For further details about structural retention, refer to About the Content Intelligent Services (CIS) integration with Retention Policy Services in “[Retention policy overview](#)” on page 146. The **Structural Retention Type** attribute setting is further described in “[Creating a retention policy](#)” on page 156.

Information about disposition runs is contained in disposition run bundles. For further details, refer to “[About disposition run bundles](#)” on page 314.

4. Optionally, to see a detailed report of the *Disposition* operation, run the **Work Order Report**, to see the master work order and details. To see the subwork orders, if any, spawned by a master work order, run the **Work Order Breakdown Report**. To see the items that were processed by the work orders, run the **Work Order Item Report**. For instructions to run any of these reports, refer to “[Running the Work Order Report, the Work Order Breakdown Report, or the Work Order Item Report](#)” on page 51. For a work order introduction, refer to “[Work orders](#)” on page 33.
5. Run the `dmc_rps_DMcleanJob` whenever you are finished running disposition. To run the `dmc_rps_DMcleanJob`, refer to “[Retention Policy Services jobs](#)” on page 273. Cleanup is meant to free up physical space on the disk after disposition runs that destroy all or destroy content.

4.2.2.30 Retention markups

A retention markup is applied to an object, a document or a folder, to either simply tag a document or documents in a folder or, to prevent any further action or processing against the document or documents in the folder. Retention markups can be created with various designations or combination of designations to prevent processing actions such as promoting the object if it is under retention or preventing it from being destroyed whether it is under retention or not. Some of the designations can be applied to an object with or without a retention policy. Up to 5 designations can be selected for a retention markup. All existing documents in the folder, or any new ones added, will inherit the markup once it is applied to the folder, whether the markup is set to cascade to subfolders or not. Documents in subfolders however will only inherit if cascading to subfolders is allowed. Cascades to Sub-folders is disabled by default, to prevent propagation to subfolders.

The 5 retention markup designations are described as follows:

- Hold

Protects a document, temporarily, from being destroyed whether the document is retained or not. Prevents deletion of the document when it is not retained. Otherwise, prevents destruction of the document when it is under retention in the final phase. Although a document in the final phase that is up for disposition will not be destroyed, all other nondestructive actions, such as transfers however, will be processed. Documents under Linked retention in the final phase are not

displayed for disposition, only documents under Individual retention which have retainers. Qualification and promotion processes continue normally. A hold is intended to suspend the destruction of a document only temporarily, until the investigation in a legal matter for example is over. A permanent markup should be used when it is necessary to preserve a document indefinitely.



Note: If you are using Centera, configure the system to accept Retention Policy Services hold (instructions are in Centera documentation).

The Centera cluster has to be configured to grant retention hold privilege. Retention Hold in Centera requires an advanced retention license and this is configured by the Centera administrator.

- Permanent

This designation is very similar to a hold in that objects cannot be deleted or destroyed. Applying a permanent markup means that the object should never be deleted or destroyed. Holds protect temporarily whereas permanents protect indefinitely. Permanent markups require a higher privilege to apply than holds. Only those members in the Retention Manager role can create and apply a permanent markup.

- Freeze

This designation prevents a document that is under retention from being promoted to the next phase. Promotion of the document is stopped. If the document is not under retention, applying this retention markup will do nothing. However, if the object is placed under retention at a later time then the markup will prevent promotion.

- Review

Applying this designation to an object, whether it is retained or not, indicates that the object is under review. Markup review notifications, or simply review notifications, are sent periodically according to the action name and review period specified.

Review notifications can be configured upon creating a retention markup, or re-configured from its properties, as an Email or an Inbox notification. A review notification has Retention Policy Services Review for the Subject to differentiate it from other notification types. Only 1 markup notification is generated, whether the markup created is applied to one or more objects.

- Vital

Applying this retention markup indicates that the object is a vital record. It is possible to search records that have been tagged with this designation. There is no other business logic.

A retention markup can be applied to objects that are either under retention or not. If the object is not under a retention policy, only a hold or a permanent markup can protect the object from deletion.

 **Warning**

Applying a vital, review, or freeze retention markup will not prevent the object from being deleted. In order to protect the object, either apply a hold or permanent or apply a retention policy.

None of the date calculations are affected when an object has a retention markup other than a freeze. The freeze affects the qualification date of the next phase after the freeze has been removed, if the freeze was applied when the qualification date was passed. If multiple holds or permanents are applied to an object, they must all be removed first for the disposition process to occur.

Members in the Retention Manager role can administer all retention markups. The Compliance Officer can also administer retention markups (create, apply, and remove), except the permanent.

A retention markup must be created before it can be applied to an object.

4.2.2.30.1 Creating a retention markup

To create a retention markup:

1. Navigate to **Retention Policy Services > Retention Markups** and select **File > New > Retention Markup**.
The **New Retention Markup** screen is displayed.
2. Enter a unique name and select one or more designations. All other fields are optional. Refer to the following table for a description of the attributes:

Table 4-28: Retention markup attributes

Attribute	Description
Name	Type a unique value to distinguish this markup from other existing markups.
Description	Provide additional information if necessary.
Enable	Is selected by default and means that this retention markup can be applied. If deselected, means that this retention markup will not be available for application. In other words, when you apply a retention markup you will not see this one listed in the locator when you click Select retention markup. The setting for this option can be changed only if this retention markup is not in use (not applied). A retention markup must be removed from all objects it is applied to before it or this option can be modified.

Attribute	Description
Cascade To Sub-folders	Is deselected by default to prevent the markup from being inherited by subfolders. Otherwise propagates to subfolders when selected.
Retention Markup Approved Date	This field can be used as necessary. It might be beneficial to indicate the date it was approved for usage for example.
Retention Markup Review Date	This field also can be used as necessary. It might be beneficial to review this markup from time to time. A new review time can be set each time it is reviewed.
Designations	Select one or more of the designations displayed.

 **Note:** Although you can create a retention markup by providing entries for only the mandatory fields, notifications will not be sent unless a contact is specified. The contact can be specified when the retention markup is created or from its properties after it has been created.

The **Review Properties** section is displayed only when **Review** is selected for **Designations**. The attributes in the **Review Properties** section are described in this table:

Table 4-29: Review properties attributes

Attribute	Description
Period	Review notifications are sent periodically, at intervals based on one of the following choices: <i>Monthly</i> , <i>Quarterly</i> , <i>Semi-Annually</i> , or <i>Annually</i> .
Month	This option is not displayed if the value for the Period is set to <i>Monthly</i> . Select the desired month if the period is set to <i>Quarterly</i> , <i>Semi-Annually</i> , or <i>Annually</i> . Its usage is described in the Note below this table.
Day	The day of the month, for the period selected, on which the notification will be sent.
Reason	Descriptive text.

Attribute	Description
Action Name	The means by which notification is sent. Notifications can be sent as either an <i>E-mail notification</i> or an <i>Inbox notification</i> . Email notifications are sent to the Inbox of the recipient's email application. Inbox notifications are otherwise sent to the recipient's Inbox on the Records Client application.
Notify	Recipient of the notification.

The values that can be selected for the **Month** and **Day** attributes vary depending on the value selected for the **Period**. **Month** is not displayed if the **Period** is set to *Monthly*. Only a specific day of the month 1-31 must be selected if the **Period** is set to *Monthly*. Both the **Month** and the **Day** attributes are displayed if any other value is selected for the **Period**.

When the **Period** is set to *Quarterly*, the **Month** allows you to select a value from 1-3. 1 represents the first month of each quarter, 2 represents the second month of each quarter, and 3 represents the third month of each quarter. The value for the **Day** selected 1-31 represents the day within the month.

When the **Period** is set to *Semi-Annually*, the **Month** allows you to select a value from 1-6. 1 represents the first month in each half of the year, 2 represents the second month, 3 represents the third month, and so on. The value for the **Day** selected 1-31 represents the day within the month.

When the **Period** is set to *Annually*, the **Month** allows you to select a value from 1-12. 1 represents the first month in each half of the year, 2 represents the second month, 3 represents the third month, and so on. The value for the **Day** selected 1-31 represents the day within the month.

Table 4-30: Quarterly cutoff mappings to months

Value Selected for Month	Corresponds To			
1	January	April	July	October
2	February	May	August	November
3	March	June	September	December

Table 4-31: Semi-Annually cutoff mappings to months

Value Selected for Month	Corresponds To	
1	January	July
2	February	August
3	March	September
4	April	October
5	May	November

6	June	December
---	------	----------

Table 4-32: Annually cutoff mappings to months

Value Selected for Month	Corresponds To
1	January
2	February
3	March
4	April
5	May
6	June
7	July
8	August
9	September
10	October
11	November
12	December

3. Optionally, you can enter values for the optional fields; the description, approved and review dates of the retention markup.

The selected retention markup(s) are enabled by default such that they are enforced immediately when applied. You cannot apply them if they are disabled. Select **Cascades to Children** if you want folders below the parent folder to inherit the retention markup.

4. Click **Finish** to create the new retention markup.

The **New Retention Markup** screen disappears and the new markup designation is listed under **Retention Markups**.

5. To verify that the selected markup was created, click **Retention Policy Services > Retention Markups**.

All retention markups are listed according to:

- **Name**
- **Description**
- **Designation**

4.2.2.30.2 Deleting a retention markup

A retention markup cannot be deleted if it is in use.

To delete a retention markup:

1. Navigate to **Retention Policy Services > Retention Markups** and right-click the retention markup in the content pane you want to delete. If necessary, press the Shift key to select a group of contiguous objects or the Ctrl key to select more than one object. The Shift key allows selecting a string of objects whereas the Ctrl key allows you to pick and choose objects.
2. Click **Delete** from the list box displayed.
3. Click **Yes** to confirm.

4.2.2.30.3 Applying a retention markup

Retention markups are enabled by default when they are created unless they are purposely disabled. Retention policies and retention markups cannot be applied if they are disabled.

To apply a retention markup:

1. Navigate to the document or folder object.
2. Right-click the document or folder object displayed in the content pane and select **Retention > Apply Retention Markup**. A text box, **Reason for applying markup** is available for describing the business reason for the application of the markup in question.
3. Select one or more of the retention markups needed on the locator screen and click **OK**. If necessary, press the Shift key or the Ctrl key to select more than one object. The Shift key allows selecting a string of objects whereas the Ctrl key allows you to pick and choose objects.



Note: When selecting a retention markup to apply directly to an item, any retention markup already directly applied to the item will not be available to be selected from the locator.

4. Click **Continue** to confirm the action.

4.2.2.30.4 Viewing an applied retention markup

This feature is used to see which retention markups are applied to a particular object.

To view an applied retention markup:

1. Navigate to the object that has the applied retention markups.
2. Right-click the object displayed in the content pane and select **View > Applied Retention Markups**.

4.2.2.30.5 Viewing usages of a retention markup

This feature is used to see a list of objects which are using a particular retention markup. The list displayed includes objects from all federated repositories.

To view the usages of a retention markup:

1. Navigate to **Retention Markups** under the Retention Policy Services node.
2. Right-click a retention markup displayed in the content pane and select **Retention Markup Usages**.

4.2.2.30.6 Removing a retention markup

To remove a retention markup:

1. Navigate to the object that has the retention markup so that it is displayed in the content pane.
2. Right-click the object displayed in the content pane and select **View > Applied Retention Markups**.
3. Select the retention markup item that has to be removed and click **Records > Remove Retention Markup**. You cannot remove multiple items at a time using this option.
4. Click **Continue** to confirm the action.

4.2.2.31 Retention Policy Services searching

Retention Policy Services items are searchable using Search located at the top of the Records Client user interface. Depending on the screen displayed Search is available most of the time.

To perform a simple search, type the characters you want searched in the Search box and click Search.



Note: You can verify or change the Default Search Location in the Preferences screen, by clicking Tools > Preferences and selecting the Search tab.

The search criteria in the Preferences screen automatically defaults to the Current repository only. You can change the default setting to one of the other two settings if needed; My Favorite Repositories or Others.

To perform an advanced search against formal records:

1. Click the arrow button for advanced search, next to the magnifying glass icon above the navigation pane.

The **Advanced** search option is displayed.

2. Click **Advanced**.

The **Advanced Search** screen is displayed displaying the **General** tab by default.

3. Click the **Formal Records** tab. The **Formal Records** tab is displayed only if Records Manager is installed.
4. Enter search criteria in the filters according to the combination you need to narrow the search results and click **Search**.

For example, you can simply click Search according to the default settings for a return of results which includes all the formal records that are of the Object Type selected. You can add a keyword to narrow the search to those records that contain the keyword(s) against the object type selected; the keyword(s) entered in the Contains box are highlighted in the results list. To further narrow, specify a property and/or series of one or more dates on which the record file was modified. You can also search for files of a size that falls within a particular range. You can search the default repository identified for the Locations or Edit the locations to add or remove repositories from the search. Additional criteria could also be included to return results against hidden objects and/or for all versions and/or recently modified properties. Ultimately, you can pick and choose any filter combination to fine-tune the search to the degree needed.

4.2.2.32 Retention Policy Services reports

There are six reports available with Retention Policy Services.

For a reports overview, refer to “[Records reporting](#)” on page 86.

4.2.2.32.1 Running the retention report

- “[Retention report overview](#)” on page 248
- “[To run the retention report](#)” on page 251

4.2.2.32.1.1 Retention report overview

The Estimated Disposition date on a retained object, and on the retention policy it references, indicates the date on which disposition can be run. A value for this attribute is specified only if the object is under retention. The Estimated Disposition date (`a_retention_date`) is obtained or calculated from the Projected Disposition Date (`projected_disposition_date`) of the retainer applied to the object. Retainer objects (`dmc_rps_retainer`) have the attribute Projected Disposition Date (`projected_disposition_date`). System objects (`dm_sysobjects`) have the attribute Estimated Disposition (`a_retention_date`). If multiple retainers are applied to the object, the value specified is then based on the retainer that retains the object the longest, or furthest into the future (latest date). In either case, it is a prediction of the date (or any date thereafter) on which disposition can be run.

The Projected Disposition Date on a retainer is based on the total duration of all the phases of the retainer. The calculation ignores:

- If there is a valid authority.
- Holds.
- Any suspensions due to record relations.
- Unfulfilled events (including global events which could fast track the aging).
- Cutoff, if defined on phases.

This Estimated Disposition date can be affected in a number of ways:

- Application of retention
- Removal of retention (the date will, of course, go away along with the retainer object)
- Promotion of a retainer. This includes supersede
- Setting global event date of a retainer
- Setting phase event date of a retainer
- Rollover to another retention as a result of disposition
- Qualification or Re-qualification of a retainer
- Disposition of a folder that is under structural linked retention. This causes a reset on the `a_retention_date` of the folder

For those instances listed that do not involve applying or removing retention, updating the retention date on a retainer could affect a large number of objects. If more than one object is affected by the date change, a work order will be created automatically and will revise the date if appropriate. The operation for this work order is called Evaluate Retention Date.

The projected disposition report is used to predict or get an idea of the number of objects that could be disposed of by a particular date into the future. The projected

disposition retainer date is based on the total duration of all the phases of the retainer. The calculation ignores:

- If there is a valid authority.
- Holds.
- Any suspensions due to record relations.
- Unfulfilled events (including global events which could fast track the aging).
- Cutoff, if defined on phases.

This projected disposition date is a rough estimate of the earliest disposition could be run. This projected disposition date or projected end of life date is also known as the Retention Date.

The report displays all items, that would be qualified for disposition, up to and including the **As-of-Date**. Filters on the report can be set in any combination to target:

- Any folder and its subfolders if necessary
- Any object type
- Only objects retained according to a specific retention policy
- Only objects retained according to a specific disposition strategy
- Only objects retained according to a specific condition, regardless of the phase or within a particular phase

Results can be returned to include only a count of the number involved or to include the list of objects along with the count.

About Retainers and Their Projected Disposition Date

Retainer objects (dmc_rps_retainer) have an attribute called the Projected Disposition Date (projected_disposition_date). There is an attribute on dm_sysobject called a_retention_date (Estimated Disposition), which is now a calculation of the latest of projected_disposition_date among all of the retainers protecting that object. This date can be affected in a number of ways:

- Application of retention
- Removal of retention (the date will, of course, go away along with the retainer object)
- Promotion of a retainer. This includes supersede
- Setting global event date of a retainer
- Setting phase event date of a retainer
- Rollover to another retention as a result of disposition
- Qualification or Re-qualification of a retainer

- Disposition of a folder that is under structural linked retention. This causes a reset on the a_retention_date of the folder

For those instances listed that do not involve applying or removing retention, updating the retention date on a retainer could affect a large number of objects. If more than one object is affected by the date change, a work order will be created automatically and will revise the date if appropriate. The operation for this work order is called Evaluate Retention Date.

Run a retention report to obtain information on retained objects; and, if necessary, to take user action against any one or more of the objects reported. Objects with terminal retention can also be reported using the advanced filters. User actions are exposed when at least one item is reported. The user actions in the header are:

- Export All To CSV
- Export Selections To CSV
- View Applied Retention
- View Applied Retention Markups
- Apply Retention Markup
- Close Folder
- Re-open Folder

Right clicking on a result, gives the context for the object (in previous versions of the product, the context was for the retainer). It is possible to view either the properties of the object or the retainer. This means that it now possible to double-click on documents to view their content or to double-click on folders to view its contents.

The Retention Manager and the Power User have rights to run the Retention Report.



Note: The **Perform Privileged Delete** is now available from the right-click context menu under **Retention > Perform Privileged Delete**. In previous versions of the product, this action was done from the header.

Use the filters as needed to narrow your query and create a customized report. If you select a Condition for example, you can target the phase in which an event was Fulfilled. Items reported can then be selected for further user action, Close Folder for example.

4.2.2.32.1.2 To run the retention report

1. Select **Records > Reports > Retention Report**. The Retention Report is displayed.

Additional filters after a folder is selected or a condition is selected are displayed.



Note: A count and timestamp is displayed in the upper left-hand corner when a query is submitted, that is when you click the **Report** button, or when a column is added or removed. It can be determined at a glance when the report was last generated. The count and the timestamp is updated each time the **Report** button is clicked. Although the count may not change, that is if filter settings remain the same, the timestamp will change. Even if the filter settings do remain the same the count could increase, if for example retention was applied or removed since the last reported time. Also, the plus sign (+) next to the count means that there are more results to page through. The actual count, if there is more than one page of results, can be determined when you go to the last page.

2. Either, click **Report** directly to obtain results against the default filter settings, or change the default filter settings to create your own customized report. A count and timestamp is displayed in the upper left-hand corner only if results are returned. The filters for this report are described as follows:



Note: Except for the event date, when specifying the filter Criteria for the Global event Date or Qualification Date, the result will not fetch those records which has null date.

Table 4-33: Retention report filter descriptions

Filter Name	Description
Retention Policy	Results can be narrowed to only those objects with retention against a specific retention policy. One or more retention policies can be selected. All objects with any retention are otherwise reported if nothing is selected.
Disposition Strategy	A specific disposition strategy can be selected to report only those objects under retention with the strategy specified.
Event Date	A date range can be specified to report objects under retention that have an event date within the range specified.

Filter Name	Description
Estimated Disposition	The latest date disposition can be performed against a retained object. If multiple retainers are applied, the value is based on the retainer that retains the object longest. The Estimated Disposition attribute is searchable from Advanced search. If you want to see results for this filter setting, select Column Preferences and add Estimated Disposition. The Estimated Disposition column is optional and is described in Appendix E, Optional attributes on page 765 .
In Folder	One or more folders within a file plan can be targeted for the report. All folders are searched if nothing is selected. The Include sub-folders filter is displayed only if a folder has been selected.
Type	Objects under retention that are reported can be limited to a specific object type, dm_sysobject for example.
Unfulfilled Event Dates	Objects under retention with event dates that have not been fulfilled are reported when this checkbox is selected.
Condition	Once a condition is selected, additional filters are displayed which can be set to return results on objects under retention that have the condition in any phase or in a current, past, or future phase. Any Phase is the default setting. Conditions on the objects reported can include only those with conditions that have been fulfilled. Leaving the Fulfilled checkbox deselected returns results on objects whether the condition is fulfilled or not.
<i>Filters under Show Advanced</i>	
Phase	Objects under retention can be reported against a particular phase of the lifecycle specified for a retention policy. One or more phases can be selected.
Authorities (All Phases)	The authority specified, valid or invalid, for a particular phase can also be used for further filtering. One or more authorities can be selected. Show me all of the retainers that have this authority specified.
Global Event Date	Objects under retention with global event dates occurring within the specified date range.

Filter Name	Description
Cascade Rule	Filters retained objects based on any cascade rule if set to <i>All</i> , or any other specific option: <i>Cascade To Everything</i> , <i>Cascade To Subcategories</i> , <i>Cascade To Subfolders</i> , <i>Do Not Cascade</i> .
Retention Strategy	Filters retained objects based on any retention strategy if set to <i>All</i> , or any other specific option, <i>Individual</i> or <i>Linked</i> .
Qualification Date	Objects under retention with qualification dates occurring within the specified date range.
Objects Under Terminal Retention Only	Only those objects with only a terminal retainer are reported when the checkbox is selected. This implies objects with no other retainers, only a terminal retainer. To obtain a report against objects that have regular retainers and a terminal retainer, select the checkbox for Retained Objects with Terminal Retention. Only one or the other can be selected.
Show Disposition Status	Objects under retention that undergo disposition in the final phase can be reported according to any one or combination of checkboxes selected for the possible values: Open , Terminated , Processed , Incomplete , Pending , and Waiting . All are selected by default.
Non-Aging Retentions Applied to Containers	Reports objects under retention that do not age, when the checkbox is selected. A non-aging retention applied to a container occurs only under ONE condition; when you apply an individual style of a retention policy to a folder. The folder becomes non-aging and will never appear in any of the managers, promotion, disposition, or qualification. It serves as a means to give retention to its children in an easy and practical way as anything linked into this type of folder automatically inherits a unique retainer.
Retention with Invalid Authority	Reports objects under retention that have an invalid authority specified for any of the phases. In other words, show me the retainers that do not have a valid authority for at least one phase.

Filter Name	Description
Retained Objects with Terminal Retention	Objects with a combination of a terminal retainer and one or more regular retainers are reported when the checkbox is selected. To obtain a report against objects that have only a terminal retainer, select Objects Under Terminal Retention Only. Only one or the other can be selected.

 **Note:** When an item has only terminal retainers left on it then the terminal disposition job (dmc_rps_TerminalDispositionJob) can destroy the object. If any other retainer is on the object then it will be ignored by the job. For example:

A document has two retention policies applied to it that both have Destroy All specified. When you run disposition against one of the policies, the object cannot be destroyed as there is another retainer on it. A terminal retainer is placed on the object as a result to tell the system that it should have been deleted but could not be because of another retention policy on the object. If you were now to remove the remaining policy on the object, it would no longer have any active retention - this is what the terminal retainer is for. The object should have been destroyed but is not due to an open retainer. If you remove the retainer it does not matter, once the job is run the item will be destroyed. Objects reported with terminal retainers will be destroyed when the terminal disposition job is run.

Using the Start With search field, you can search within the displayed results.

Results are returned under the following default column headings:

Table 4-34: Retention report default column headings

Column Heading	Description
Checked Out	The header for this column does not say Checked Out, the key icon is used instead. It is however spelled out in the Column Preferences. The key is displayed for any item that is checked out. Keep in mind that the reading is historical and therefore the item may well have been checked in recently.  Note: This column is displayed as the first column by default.
Name	The name of the object that is under retention.
Version	The version number of the object listed.

Column Heading	Description
Retention Policy	The name of the retention policy referenced by the object, or more specifically by the retainer on the object. It can be said that the object is one phase or another, though technically it is the retainer on the object that is actually in one phase or another.
Current Phase	The phase of the retention policy that the retainer is currently in.
Disposition Strategy	The disposition strategy selected for the applied retention policy. All retainers spawned from a particular retention policy have the same strategy. Possible values are listed and described in “Disposition strategy descriptions” on page 149 . The actions that can be taken for each of the strategies are further described in “Disposition strategy actions” on page 150 . These two tables are available in the “Retention policy overview” on page 146 .
Disposition Status	The disposition status of the retainer on the object. Possible values are listed and described in “Overview of disposition” on page 222 .
Entry Date	The date on which the retainer for this object was promoted to the next phase. It can also be thought of as the phase transition date or promotion date.
Event Date	The last date on which an event is triggered when the conditional aging method is used to calculate the qualification date of the object.
Global Event Date	The date on which a global event is triggered when the conditional aging method is used to calculate the qualification date of the object. When a global event is fulfilled, the object promotes to the final phase skipping the intermediary phases.

Column Heading	Description
Qualification Date	The date on which the retainer for an object qualifies for promotion or for disposition. A folder or document will be listed in the report for each retainer (retention policy application) applied. If the current phase is not the Final phase, the date is the earliest time that the retainer could be promoted. Otherwise, it is the earliest date that disposition could be run against the object.
Application Date	The date on which retention was applied to the object, whether directly or by inheritance.

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- All Events
- Assembled From Id
- Cascade Rule
- Completed Disposition On
- Current Events
- Estimated Disposition
- Format
- Fulfilled Events
- Future Events
- Has Frozen Assembly
- Container Aging
- Final Phase
- Is Replica
- Is Virtual Document
- Link Count
- Linked Strategy Type
- Number of Resets
- Past Events
- Phase Authorities
- Reference
- Retained Object Id

- Retainer Id
- Retention Strategy
- Retention Type
- Type

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

3. Optionally, you can select one or more reported items and click one of the following actions, if necessary, depending on which is available:
 - **Export All To CSV**
 - **Export Selections To CSV**
 - **View Applied Retention**
 - **View Applied Retention Markups**
 - **Apply Retention Markup**
 - **Close Folder**
 - **Re-open Folder**

Only those actions that can be used for the selected item are available (displayed in black). The availability of these actions is also reduced when multiple items are selected for processing. You cannot **View Applied Retention Markup** for example, if multiple items are selected. Close Folder and Re-open Folder actions are available (displayed in black instead of white) only when folder items are selected. These actions are not displayed at all if no folders are reported. To perform a **Privileged Delete**, select an item and then select **Records > Privileged Delete**. You can also right-click an item to select **Properties** and make changes if necessary.

You can remove a retainer from an item by right-clicking the item and selecting **Delete**. Deleting a retainer means you will have to confirm **Yes** to continue or **No** to cancel. (if you have Records Manager installed you see the tab).

4.2.2.32.2 Running the retention markup report

Run a retention markup report to obtain information on objects that have a retention markup applied; and, if necessary, to take action against any one or more of the objects reported. Although the retention markup report feature can be used to list only those objects you want to see, it can also be used to edit the properties or to determine the retention markup usages.

Filters include:

- Checkbox for the new fifth Vital retention markup designation.
- Textbox to Search by Markup Reason.

- Checkbox to Include objects that have Inherited Markups.

The Retention Manager, Compliance Officer, and the Power User have rights to run the Retention Markup Report.

To run the retention markup report:

1. Select **Records > Reports > Retention Markup Report**. The Retention Markup Report, and its advanced settings, is displayed.
The advanced settings are hidden by default.
2. Either, click **Report** directly to obtain results against the default filter settings, or change the default filter settings to create your own customized report. Results are displayed.

The filters for this report are described as follows:

Table 4-35: Retention markup report filter descriptions

Filter Name	Description
Retention Markup	Results can be narrowed to only those objects with the retention markup selected. One or more retention markups can be selected. All objects with any of the retention markups available in the Retention Markups administration node are otherwise reported if nothing is selected.
Search by Markup Reason	The value that was entered in the text box against the Reason for Applying Markup in the Apply Retention Markup page can also be used.
Marked Object Review Date	A date range can be specified to report all objects with Review designations that occur within the range selected.
Show Designations	Only those objects with the selected designations are reported. All of the designations are selected by default.
Include objects that have Inherited Markups	Results, unless this checkbox is selected, are returned against only those objects that have retention applied directly. Objects with both directly applied and inherited retention markups can be reported when this checkbox is selected. Objects with inherited retention markups are not reported by default. To determine if there are any objects with inherited retention markups, select this checkbox, deselect each checkbox in Show Designations, and leave all the other filter settings with the defaults.

Filter Name	Description
<i>Filters under Show Advanced</i>	
Requestor	Objects with retention markups can be reported based on one or more requestor names specified for the Contacts of a retention markup.
Markup Reviewed On	A date range selected for this field returns objects with retention markups that have a Retention Markup Review Date , entered on the Info tab, which falls within the range.
Approver	Objects with retention markups can be reported based on one or more approver names specified for the Contacts of a retention markup.

Results are returned under the following default column headings:

Table 4-36: Retention markup report default column headings

Column Heading	Description
Checked Out	The header for this column does not say Checked Out, the key icon is used instead. It is however spelled out in the Column Preferences. The key is displayed for any item that is checked out. Keep in mind that the reading is historical and therefore the item may well have been checked in recently.  Note: This column is displayed by default as the first column.
Name	The name of the object that has the applied retention markup.
Version	The version number of the object listed.
Retention Markup	The name of the retention markup applied to the object. A retention markup can have one or more of the 5 available designations selected: Hold, Freeze, Review, Permanent, and Vital. All of the column headings with these designations for example, could have an entry if they were all selected for the retention markup listed.
Hold	If the retention markup listed has the Hold designation selected, the value for this entry would be <i>Hold</i> .

Column Heading	Description
Freeze	If the retention markup listed has the Freeze designation selected, the value for this entry would be <i>Freeze</i> .
Review	If the retention markup listed has the Review designation selected, the value for this entry would be <i>Review</i> .
Permanent	If the retention markup listed has the Permanent designation selected, the value for this entry would be <i>Permanent</i> .
Vital	If the retention markup listed has the Vital designation selected, the value for this entry would be <i>Vital</i> .
Markup Reason	All markups applied to an object may include a reason, which would be displayed if it is the case.
Duration	The difference between the date applied for the retention markup and the current date. It will be displayed in the following format: year(s) month(s) day(s) hours(s).

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- Applied Markup Id
- Approved On
- Approvers
- Inherited
- Markup Id
- Object Id
- Requestors
- Review Date
- Reviewed On
- Type

To add, remove, or reorganize columns, refer to [“Setting column preferences” on page 77](#).

3. Optionally, you can select one or more reported items and click one of the following actions, if necessary, depending on which is available:
 - **Export All To CSV**
 - **Export Selections To CSV**

- **View Applied Retention Markup**
- **Remove Retention Markup**
- **Apply Retention Markup**

Only those actions that can be used for the selected item are available (displayed in black). The availability of these actions is also reduced when multiple items are selected for processing. You cannot **View Applied Retention Markup** for example, if multiple items are selected.

You can also right-click an item to select **Properties** and make changes if necessary.

4.2.2.32.3 Running the retention notification report

The retention notification report lists Retention Policy Services notifications, against those phases of a retention policy configured for notifications, that have not yet been acknowledged. Although users and administrators can use this report to acknowledge Retention Policy Services notifications, their views are different. Users can acknowledge only their Retention Policy Services notifications from the User view setting whereas, administrators can acknowledge any Retention Policy Services notification from the Administrator setting. Notifications on a retention policy are configured as part of the Phase Action name and are triggered upon phase transition. Phase transition means upon phase exit or entry, when the retainer of a retention policy is promoted. Retention Managers, Compliance Officers, Power Users, and Contributors have rights to run a Notification Report. The administrator view is meant for Retention Managers only.

You must be a OpenText Documentum CM user to receive and acknowledge Retention Policy Services notifications. Retention Policy Services notifications can be sent to the OpenText Documentum CM Inbox of contacts only within OpenText Documentum CM, or to an external contact that is not associated with a OpenText Documentum CM account.

Notifications are sent according to Jobs and Jobs scheduling determines when notifications are sent. There are two jobs that need to be configured for this, dmc_rps_NotificationGenerationJob and dmc_rps_NotificationJob. The retention notification report lists all notifications that were sent out by the notification job. Notifications are sent repeatedly, at pre-configured intervals, until the notification is acknowledged. The number of times a notification is sent, before it is acknowledged, is registered for the report under Number Sent.

To run the retention notification report:

1. Select **Records > Reports > Retention Notification Report**. The Retention Notification Report displayed for users or for administrators is displayed.
2. Click **Report** to obtain results against the default settings or change the filter settings to create your own custom report. Administrators have two additional filters: **Sent Maximum number of times** and **Ignore acknowledged items**. They also have an additional action which allows them to **Remove All Acknowledged** notifications when necessary.

The filters for this report are described as follows:

Table 4-37: Retention notification report filter descriptions

Filter Name	Description
Mode	Set this value to <i>User</i> if you are in an end user role or to <i>Administrator</i> if you are in an administrator role.
Notification Type	Results are obtained against either Email notifications or Inbox notifications or both if <i>All</i> is selected.
Retention Policy	Results are obtained against objects that received notification based on any retention policy if nothing is selected or against one or more if any is selected.
Phase	Results are obtained based on any phase if nothing is selected or on one or more phases.
Sent Date	The objects reported would be those that received a notification within the date range selected.
<i>Additional Filters Displayed When Mode is set to Administrator</i>	
Contacts	This filter is displayed only when the Mode is set to <i>Administrator</i> . Results are obtained based on any contact if nothing is selected or on one or more contacts. The contacts for a retention markup are added as Requesters and Approvers on the Contacts tab.
Sent maximum number of times	This filter is displayed only when the Mode is set to <i>Administrator</i> . If selected, lists those notifications that were sent the maximum number of times; notifications are sent until acknowledged, unless the maximum number of notifications is reached.
Ignore acknowledged items	This filter is displayed only when the Mode is set to <i>Administrator</i> . Administrators can choose to ignore notifications from being reported that were sent and acknowledged.

Results are returned under the following default column headings:

Table 4-38: Retention notification report default column headings

Column Heading	Description
Name	The name of the object that has the applied retention policy.

Column Heading	Description
Retention Policy	The name of the retention policy that retains the object. Notification settings are set on the Action Relation page displayed from the Phases tab when you click Add for the Action Name .
Sent Date	The date on which the most recent notification was sent.
Acknowledged By	The name of the entity that acknowledged the notification.
Sent To	The name of the entity to which the notification was sent.
Reason For Notification	This indicates phase entry or phase exit

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- Acknowledged By Me
- Action Name
- Assembled From Id
- Format
- Has Frozen Assembly
- Is Replica
- Is Virtual Document
- Link Count
- Notification Id
- Notification Type
- Number Sent
- Object Id
- Phase
- Reference
- Type
- Version

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

3. Optionally, you can select an item in the list returned and click **Remove** to remove it or right-click it to select its **Properties** and make changes if necessary.

4.2.2.32.4 Running the retention markup review report

The retention markup review report is used to report objects with the Review designation against which a notification has been generated or sent. This can help you identify documents that were repeatedly sent for review but are not yet acknowledged. Notification is sent only within the period specified for the review and only after both the notification generation and notification jobs are run.

Although a notification is created or prepared when the notification generation job is run, it is sent only when the notification job is run. Notifications are sent repeatedly until the recipient or an administrator acknowledges the notification.

The report screen displayed for user roles is different from the screen displayed for individuals in administrator roles which allows administrators to see all of the reviews. The user report shows reviews that are sent to you and that you can acknowledge. Although the user screen permits users to query reviews, the administrator screen permits increased querying capability. The Retention Manager, the Compliance Officer, the Power User, and the Contributor have the rights to run a retention markup review report. The administrator screen is only for retention managers.

Use this feature to obtain a status on documents routed for review by E-mail notification or by Inbox notification.

To run the retention markup review report:

1. Select **Records > Reports > Retention Markup Review Report**. The Retention Markup Review Report is displayed for users or administrators.
If you are an administrator, select the **Administrator** option from the list box.
2. Click **Report** to obtain results against the default settings or change the filter settings to create your own custom report. Administrators have an additional button which allows them to **Remove All Acknowledged** reviews when necessary.

The filters for this report are described as follows:

Table 4-39: Retention markup review report filter descriptions

Filter Name	Description
Mode	Set this value to <i>User</i> if you are in an end user role or to <i>Administrator</i> if you are in an administrator role.
Notification Type	Results are obtained against either email notifications or Inbox notifications or both if <i>All</i> is selected.
Retention Markup	Results are obtained against objects that received notification based on any retention policy if nothing is selected or against one or more if any is selected.

Filter Name	Description
Review Interval Period	Results are obtained regardless of a review interval if <i>All Periods</i> is selected or the results returned can be set against a specific setting: <i>Monthly</i> , <i>Quarterly</i> , <i>Semi-Annually</i> , or <i>Annually</i> .
<i>Additional Filters Displayed When Mode is set to Administrator</i>	
Contacts	This filter is displayed only when the Mode is set to <i>Administrator</i> . Results are obtained based on any contact if nothing is selected or on one or more contacts. The contacts for a retention markup are added as Requesters and Approvers on the Contacts tab.
Sent maximum number of times	This filter is displayed only when the Mode is set to <i>Administrator</i> . If selected, lists those notifications that were sent the maximum number of times; notifications are sent until acknowledged, unless the maximum number of notifications is reached.
Ignore acknowledged items	This filter is displayed only when the Mode is set to <i>Administrator</i> . Administrators can choose to ignore notifications from being reported that were sent and acknowledged.

Results are returned under the following default column headings:

Table 4-40: Retention markup review report default column headings

Column Heading	Description
Name	The name of the object that has the applied retention markup.
Review Reason	The information that is specified for the retention markup that was selected and applied to the object.
Retention Markup	The name of the retention markup that is applied to the object.

Column Heading	Description
Review Period	The value displayed could be: <i>Monthly</i> , <i>Quarterly</i> , <i>Semi-Annually</i> , or <i>Annually</i> . The value is set for the Period in the Review Properties section on the Create tab when a retention markup is created with Review selected for the Designations . This value cannot be changed from the properties of a retention markup once it has been applied.  Note: The Review Properties section is displayed for a retention markup only when Review is selected under Designations .
Month	The value displayed is an integer from 1-12 depending on the value selected for the Month in the Review Properties section for the Period selected. This attribute, on the Create tab, is not displayed if the value for the Period is set to <i>Monthly</i> . Refer to “ Creating a retention markup ” on page 241 for further details.  Note: The value 0 is displayed for the Month whenever the Review Period displays <i>Monthly</i> .
Day	The value displayed is an integer from 1-31 depending on the value selected for the Day in the Review Properties section for the Period selected.
Acknowledged By	The name of the entity that acknowledged the notification.
Sent To	The name of the entity to which the notification was sent. If nothing is displayed for the object selected, it means that the notification has been created by the notification generation job but has not yet be sent by the notification job.

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- Acknowledged By Me
- Action Name
- Assembled From Id
- Format
- Has Frozen Assembly
- Is Replica

- Is Virtual Document
- Link Count
- Notification Id
- Notification Type
- Number Sent
- Object Id
- Phase
- Reference
- Type
- Version

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

3. Optionally, you can select one or more reported items and click one of the following actions, if necessary, depending on which is available:
 - **Export All To CSV**
 - **Export Selections To CSV**
 - **Acknowledge**
 - **Remove**
 - **Remove All Acknowledged**

Only those actions that can be used for the selected item, are available (displayed in black).

You can also right-click an item to select **Properties** and make changes if necessary.

4.2.2.32.5 Running the close folder report

The Closed Folder Report reports folder objects and allows users to change the state from closed to re-opened, or from re-opened to closed or from opened to closed. Although folder objects in the Opened state are not Retention Policy Services governed, they too are reported but do not include details in the results returned other than to indicate a value for Current State, Created, and Object Id. Actions are also included to revert to the previous state and to specify a reason for the state change. Folders reported that are closed or reopened by anything other than the Retention Policy Services Close Folder feature are not actionable by the Close Folder Report. For further details about the Close Folder feature, refer to “[Close folder operations](#)” on page 141.

To run the close folder report:

1. Select **Records > Reports > Close Folder Report**. The **Close Folder Report** is displayed.
2. Click **Report** to obtain results against the default settings or change the filter settings to create your own custom report.

The filters for this report are described as follows:

Table 4-41: Close folder report filter descriptions

Filter Name	Description
Folder Type	Allows targeting a specific folder object type, dmc_prm_box for example, within the folder location specified for the In Folder filter. All sub-types of the folder object selected can also be included if desired, dmc_prm_box and all of its sub-types.
In Folder	Allows targeting one or more specific folder locations within the repository, / Temp for example and all of its subfolders if desired. All folders are searched if nothing is selected.
User	Results can be further narrowed against one or more specific users, that is against the Owner Name specified for a folder object.
Current State	Only Closed folder objects may be reported or only Re-opened folder objects may be reported or both if Any State is selected.
State Date	Reports only those folder objects that were either re-opened or closed within the date range specified. There is no filtering if Any Date is selected. For example, you can determine all of the folders that changed their state last week. A calendar is displayed, to facilitate specifying a date range, when Any Date is deselected.
Date First Closed	Reports only those folder objects that were closed for the first time within the date range specified. There is no filtering if Any Date is selected. For example, you can determine all folders that were closed for the first time last week. A calendar is displayed, to facilitate specifying a date range, when Any Date is deselected.

Filter Name	Description
State Change Reason	<p>All folder objects that have a reason specified and which match the entry will be reported. Other folders that have a partial match may also be reported. Each word or series of letters separated by a space is sufficient for a matching pattern. For example, <i>end of month</i> would return all folder objects that have <i>end of month</i> for the reason. Other folder objects could also be returned if any one word results in a match. Therefore, all folder objects that have <i>end</i> or <i>of</i> or <i>month</i> within their reason would also be reported. Also note:</p> <ul style="list-style-type: none"> - Entries are not case sensitive. - Multiple strings can also be entered. - The reason must have double quotes at both ends of the string to be treated as a single query or token. <p>For example: Missing double quotes warning: “end of month” “months end //You have an open double quote that is not closed by a matching double quote While, the valid entry is : “end of month” “months end” month end</p>

Results are returned under the following default column headings:

Table 4-42: Close folder report default column headings

Column Heading	Description
Folder Name	Name assigned to the folder object.
Current State	Indicates the current state that the folder is in. The possible values are: <i>Closed</i> , <i>Opened</i> , or <i>Re-opened</i> .
State Date	Indicates the date and time at which a folder object had its state changed. This information is displayed for only those folder objects that were either closed or re-opened. No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.
State Change User	Identifies the user responsible for the state change. No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.

Column Heading	Description
Date First Closed	Indicates the date and the time at which the folder object was closed. No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.
State Change Reason	Indicates the reason that was specified. No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.

The following columns are optional and are described in [Appendix E, Optional attributes on page 765](#):

- **Created**
- **Current State Number**

No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.

- **Object Id**
- **State Change User Id**

No value is displayed for any Opened folders or for any folder objects that were closed or re-opened using applications other than Retention Policy Services.

To add, remove, or reorganize columns, refer to [“Setting column preferences” on page 77](#).

3. Select one or more items, among the items returned, and perform the desired action displayed on the action bar. No actions are displayed unless there is at least one item returned in the results pane. Although all of the actions are displayed when at least one result is returned, none are available unless one or more of the results is selected. Only applicable actions are displayed depending on the current state of the items selected. Only the **Close Folder** action is available against folder objects that have a **Current State** of *Opened*. Actions are described as follows:

- **Export All To CSV**
- **Export Selections To CSV**
- **Close Folder**

Users in the dmc_rps_close_folder role can close a folder if they have Write permissions on the folder selected.

- **Re-open Folder**

Users in the dmc_rps_re-open_folder role can reopen a folder if they have Write permissions on the folder selected.

- **Revert From Re-opened State**

Only the same user who reopened the folder can revert it to its previous closed state.

- **Revert From Closed State**

Only the same user who closed the folder can revert it to its previous reopened state.

- **Set State Change Reason**

Users in the role that match the state of the folder selected can update the reason. The same reason can be propagated to all folders or a different reason can be provided for each folder, when multiple folders of the same state are selected.

Export Selected Rows to CSV is available on the **Tools** menu.

Actions on the action bar are not available if the user does not meet the following conditions:

- Is not in the appropriate role, and
- Does not have Write permissions on the selected folder, or
- If the selected folder was not closed or reopened by the Retention Policy Services close folder feature



Note: The Close Folder Report reports any folder that was closed or reopened, regardless of the product or feature that was used. Although Commonwealth files and file parts, that were closed or opened using Records Manager Commonwealth Edition, may be included among the folders reported, none can be actioned including their sub-types. A warning is displayed whether to continue or not against the rest of the items that are not Commonwealth items. For example, the warning displayed against Commonwealth files and file parts reads as follows: The following folders cannot be closed and also asks: Would you like to proceed with the rest?.

4. Click **Yes** on the confirmation dialog to continue the desired action or click **No** to back out. An entry for the reason, in all cases, is optional. If you want to provide a reason, enter it and then click **Yes**.

The prompt for confirmation varies depending on the action selected:

- **Are you sure you want to set state change reason for the following folder(s)**
- **Are you sure you want to close the following folder(s)**
- **Are you sure you want to re-open the following folder(s)**

- **Are you sure you want to revert the following folder(s) from re-opened state**
- **Are you sure you want to revert the following folder(s) from closed state**

4.2.2.32.6 Running the audit trail report

The Audit Trail Report reports audit trails against registered audit events, whether the object associated to the audit trail was deleted or not. It is used to view the details of the audit trails reported and if necessary to declare or capture the results in a formal record or to export the results to CSV. Results can be declared as individual formal records or as a single formal record. The Declare Formal Record action item, displayed when results are returned, is displayed only if Records Manager is installed. Although the Retention Manager and the Power User have rights to run the Audit Trail Report, Power Users however, cannot declare formal records.

Auditing must be enabled for the system to register any audit trails. To enable auditing, refer to “[Enabling auditing](#)” on page 80. Audit trails can be purged from the system only after they have been declared as a formal record and only if the dm_audit_policy schema is activated. To activate the dm_audit_policy schema, for archiving and purging, refer to “[Configuring the audit policy \(to prevent purging audits until archived\)](#)” on page 82. You can set it up this way as an option but out-of-the-box audits can be purged, regardless of whether they are declared as a formal record or not.

To run an audit trail report:

1. Select **Records > Reports > Audit Trail Report**. The **Audit Trail Report** is displayed by default.

To add, remove, or reorganize columns, refer to “[Setting column preferences](#)” on page 77.

Although you have to register the audit events in order to create audit trails, only those events that have occurred will appear in the list box for **By Event Name**. Results can be returned against all events or a specific event and similarly for the object type and the user. Any combination of filter settings can be made to customize, narrow or broaden, the report.

Specific objects can also be reported on based on the ID of an object or the audited object ID, that is typed into the text box.

2. Click **Report** to obtain results according to the default settings or change the filter settings to create your own custom report.

If you add a column for **Audited Object ID** and click **Report**, the ID returned in the results can be used by copying it into the text box, **Enter Object IDs**, and clicking **Report**. The audited object ID is 0900167c80000b7a. For example, is copied to the text box and reported.

Export All To CSV is displayed and selectable whether items are found or not. A CSV consists of results in comma-separated values.

Export Selections To CSV however, is displayed only when results are reported, and is selectable only when an item is selected.

Deselecting **Any Dates** for the **Time Period** adds/reveals an option for specifying a specific date or range of dates.

Declare Formal Record is displayed to only and only if Records Manager is installed. All of the results are included in one formal record when this action is taken and each audit entry is marked Archived. To complete the process for declaring a formal record, refer to “[Declaring electronic or physical documents as formal records](#)” on page 340.

A success message is displayed below the content pane when any of these actions are completed, for example, **Audit trail report created successfully in <the path indicated>**.

4.2.2.33 Retention Policy Services jobs

Jobs can automate certain processes and can be scheduled to work continuously. Job objects are available and executable on a user-defined schedule. Retention Policy Services jobs and their method arguments are described in “[Retention Policy Services jobs and method arguments descriptions](#)” on page 274.

 **Note:** All Retention Policy Services jobs depend on Privileged DFC and will not run if the Records Client is not registered and approved for privilege. For further details, refer to “[About privileged clients and accessing repositories](#)” on page 94.

Actions performed by Retention Policy Services jobs are described in the table below. You can find further details about a job, Last Run and Job Status for example, under Job Management (Administration > Job Management > Jobs) if you log in to Documentum Administrator.

Administrators can disable a job from its Properties to prevent it from running automatically. To enable or disable a job, right-click the job and select Properties. On the Properties screen for the State attribute select *Inactive* to disable or *Active* to enable.

Although a job may be disabled from running automatically, it can at any time be run manually. To run a job manually, if you cannot wait until it is run automatically, right-click the job and select Run.

 **Note:** If errors are displayed when a job is run and a patch was installed before the job was run, make sure that the Java Method Server (JMS) was restarted beforehand, before escalating or troubleshooting any further. The JMS must always be restarted after a patch is installed.

Objects that are processed by work orders when the qualification, promotion, and disposition jobs run, can be recovered, if they could not be successfully processed, using the Work Order Report.

Table 4-43: Retention Policy Services jobs and method arguments descriptions

Job name	Description	Method arguments	Default Value	Mandatory	Description
dmc_rps_DispositionJob	This job disposes of objects that have reached the final phase of the retention policy. The disposition job does not process retainers that have <i>Review</i> specified for the Disposition Strategy . Use Disposition Manager instead.	No arguments.	120 minutes		
dmc_rps_DM CleanJob	Multi-threaded job that is similar to the dm_DMclean. Deletes orphaned objects. Users are required to run this after disposition runs.	maxThreads	2		Maximum number of threads that can be spawned.
		destroysACLs	true		Deletes orphan ACLs if true.
		destroyAnnotations	true		Deletes orphan annotations if true.
		maxNo_of_batches	10		Represents the maximum number of batches that can be processed.

Job name	Description	Method arguments	Default Value	Mandatory	Description
		reportOnly	false		If true, content is not deleted but just a report is created with a list of orphaned objects ready to be destroyed.
dmc_rps_NotificationGenerationJob	Generates notification messages	No arguments.			

Job name	Description	Method arguments	Default Value	Mandatory	Description
dmc_rps_NotificationJob	<p>Dispatches messages generated automatically by the system (Notification Generation job). Notifications include:</p> <ul style="list-style-type: none"> • markup review notifications • retention policy notification • This notification job sends-inbox notifications, or • email notifications <p> Note: Both the dmc_rps_NotificationGeneratorJob and dmc_rps_NotificationJob must be run for markup review notification. Only the</p>	maximumNumberSent	5	Yes	The value you enter determines the number of times the notification job can be run for all notifications generated by the notification generation job. No notification is sent if the notification job is run more times than the number specified. If the value is changed to a smaller number, notifications will cease after the new value is met. For example, if the notification job is run when the value is set to 5 and you run it again after it is changed to 1, no more notifications will be sent when it is run again. If instead the value was changed from 5 to 2 only one more notification could be sent

Job name	Description	Method arguments	Default Value	Mandatory	Description
	dmc_rp_s_NotificationJob is necessary for Inbox and email notifications.				if it was run again.
		baseurl	http://mySite.myCompany.myDomain:myPort/myApp	No	The value you enter is the path to the Retention Policy Services login on the Application server, in the following format, http://mySite.myCompany.myDomain:myPort/myApp. For example, http://ottlab:8080/records.
		bulkEmailSend	false	Yes	This parameter determines whether one email is sent to a list of recipients or whether recipients are emailed individually. If set to <i>True</i> , recipients are added to a distribution list for one email. If set to <i>False</i> recipients are emailed individually.

Job name	Description	Method arguments	Default Value	Mandatory	Description
		message	ADMINISTRATOR the message field is optional. Please change this value.	No	<p>This is the parameter where you can include a message for the notification. For example, You have a notification. Please follow this link. Follow instructions in this section to set the baseurl and to enter a message for the notification.</p> <p>The entry for this field is not localized and is used for both Retention Policy Services Review and for Retention Policy Services Notification.</p>
dmc_rps_Pro motionJob	Promotes objects that qualify for promotion.	No arguments.			

Job name	Description	Method arguments	Default Value	Mandatory	Description
dmc_rps_QualificationJob	Qualifies objects that are eligible. Will only qualify objects that do not already have a qualification date (disqualified objects also). Re-qualification must be done manually using Qualification Manager.	No arguments.			
dmc_rps_TerminationDispositionJob	Destroys objects that were previously prevented from being destroyed because of other applied retention policies. Only when the other retention policy is removed, will the object be eligible to be destroyed by this job.	No arguments.			
dmc_rps_ComplianceCheckJob	This job checks the compliance of the objects.	No arguments	Inactive		
dmc_rps_ReportOverdueDispositionJob	This job identifies the items that are overdue for disposition.	No arguments	Inactive		



Note: The **dmc_rps_ComplianceCheckJob** and **dmc_rps_ReportOverdueDispositionJob** scan all the items present in the repository that satisfy the filter criteria defined in the Records Check Configuration object. For more information about the Records Check Configuration options, see “[Records check configuration option settings](#)” on page 119.

The **dmc_rps_TerminalDispositionJob** job should be set to *Active* and running by default. Log in to DA and look for the **dmc_rps_TerminalDispositionJob** after installing Retention Policy Services, to make sure it is set to *Active*. This is to prevent legal issues where an object that was supposed to be destroyed, is destroyed.

The Notification Generation Job creates or sets up review notifications for Review retention markups according to the notification period specified for each subsequent review, every 30 days for example or as necessary.

The Notification Job searches for notifications and sends out those notifications that meet the notification period. Both notification jobs must be running in order for notifications to be sent successfully.

A notification for an object under a Review retention markup will not be sent unless both the Notification Job and the Notification Generation Job are running. A phase retention notification will not be sent unless the Notification Job is running.

The Disposition Job calls the disposition method whereby, the disposition method defines two parameters, all of which are mandatory:

- The dispositionStrategyOverride is the strategy you want to resolve an Unknown strategy to. Valid choices include all disposition strategies except Unknown.
- The rolloverRetentionPolicy is used if the value of the disposition strategy override requires a rollover retention policy. Disposition strategies that require a rollover are:
 - Review
 - Export all
 - Export all, Destroy content
 - Destroy content
 - NARA Transfer content

For the Notification Job, make sure you edit the following parameters for automatic notification before you run a Notification Job. You need to do this only once unless you run the Notification Job from a different Application server. Although you need to do this only once, you can follow these instructions at any time to edit only the message text when necessary.

Follow these instructions to set the baseurl and the message text before you run a notification job:

1. Using Documentum Administrator, navigate to **Administration > Job Management > Jobs**.
2. Right-click *dmc_rps_NotificationJob* in the content pane and select **Properties**.
3. Select the **Method** tab.
4. Click **Edit** next to **Arguments**.
The **Method Arguments** screen is displayed.
5. Set the values for the following parameters:
 - -baseurl <url> (For example: -baseurl http://<server_name>:<port_number>/recordsclient)
 - -message <message> (For example: -message Notification text)
6. Click **OK** to accept changes in the **Method Arguments** screen.
7. Click **OK** to accept changes in the **Method** tab.

At scheduled intervals, the agent exec process examines the job objects in the repository and runs jobs that are ready for execution. Any user can create jobs.

For information about working with jobs in Documentum Administrator, refer to *Jobs, Methods, and Administration Methods* of the *OpenText Documentum Content Management - Administrator User Guide (EDCAC-UGD)*, which includes procedures for creating jobs. Also refer to “[Qualification, promotion, and disposition](#)” on page 213 for information about the **Qualification Manager**, **Promotion Manager** and **Disposition Manager**.

4.2.2.34 Retention Policy Services audit events

“[Audited events in Retention Policy Services](#)” on page 282 describes the information, in the audit trail object, that is stored in string_1 to string_5 of the audit trails for Retention Policy Services events. Only the strings that are populated are listed. Objects are also described for audit trails that pass one or more object IDs.

For an overview of auditing and the procedures to enable auditing, to activate the audit policy schema, to verify an auditing of an event, and to view and remove an audit refer to, “[Records auditing](#)” on page 78.



Note: Although up to 5 strings can be utilized by an event, only strings 1 and 2 are displayed in the results of an Audit Trail Report. Also, the content of one string may spill into the next string if it needs extra space.

Table 4-44: Audited events in Retention Policy Services

Retention Policy Services audit events (Application Code = dmc_rps)		
<p><i>Target Object Type: dm_sysobject</i> Check the Include all subtypes on the Register Audit screen when adding/selecting the various events for only this object type.</p>		
<i>Event name</i>	<i>Strings usage (200 characters/string)</i>	<i>Object ID</i>
dm_save		
dmc_rps_apply_retention_markup	string_1: name of retention markup string_2: indicates selected designation; <i>true</i> if selected, <i>false</i> if not. For example: isHold=true; isFreeze=false; isReview=false; isPermanent=false; isVital=false string_3: reason for markup (could be blank if no reason was entered)	ID1: object id of the retention markup
dmc_rps_apply_retention_policy	string_1: name of retention policy	ID1: object id of the retention policy
dmc_rps_delete_failure This event is generated when an object that has a retainer that is ready for disposition (with Destroy All strategy for example) but cannot be deleted.	string_1: reason for failure	n/a
dmc_rps_dispose_failure This event is generated when disposition of an object in final phase cannot be completed successfully.	string_2: indicates disposition status. For example: [DMC_RPS_INCOMPLETE_DISPOSITION] cannot dispose. Object 09008a6b80015d5 has no retainer ready for disposition.	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_dispose This event is generated when disposition is successfully completes.	<p>string_1: names of retention policies processed in the following pattern. If multiple policies were processed, the names are delimited by vertical bar. For example if 3 policies were processed: Destroy after 3 years Linked Export All Linked Structural Retention</p> <p>string_2: final disposition result. There are 5 possible values:</p> <ul style="list-style-type: none"> • DESTROYED Object was deleted. • ROLLED_OVER Rolled over to the new retention policy. • RESET When retention is reset due to structural retention. • UNKNOWN STATE • TERMINAL_RETAINER The terminal retainer applied to the object. <p>For example if the same 3 policies were processed the value could be: TERMINAL_RETAINER ROLLED_OVER RESET</p> <p>string_3: applicable action names. Example: Destroy - mark physical for destruction Destroy - mark physical as destroyed Destroy content destroy metadata.</p> <p>string_4: disposition strategy names. For our example, Destroy all Export all Destroy all</p>	ID1: formal object id

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_dispose_warning This event is generated when disposition becomes paused and is waiting for manual intervention before disposition can continue. For example, physical objects require confirmation (marking that the items have been physically destroyed) before continuing disposition processing. Similarly NARA transfers require confirming the transfer.	string_1: name of retention policy string_2: name of disposition action string_3-5: concatenation of failure reasons	
dmc_rps_dispose_reset_retention	string_1: name of retention policy string_2: name of phase reset to string_3: number of times the structural container has been reset (including this time) string_4: date on which disposition was completed string_5: previous completed disposition date (could be blank when it is the first time it is being reset)	ID1: object id of the retention policy ID2: object id of the phase being reset to ID3: object id of the retainer being reset

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_dispose_unlink This event is generated when an object under linked retention is linked into a folder and is unlinked due to a disposition action. The checkbox for Unlink on Dispose must be selected on the Retention Policy Services Application Configuration object for this event to occur. If the object is linked into 2 folders with linked retention and you dispose one folder, a terminal retainer is immediately attached to the object in the other folder. A remove event dmc_rps_remove_retention_policy is also generated immediately against the object that is unlinked. The dmc_rps_dispose_terminate event is generated only when the dmc_rps_TerminalDispositionJob is run.	string_1: indicates the object id of the object that is unlinked and the path to its location. string_2: name of retention policy	n/a
dmc_rps_dispose_terminate This event is generated when the dmc_rps_TerminalDispositionJob is run.	n/a	n/a
dmc_rps_attach_terminal_retention This event is generated when an object linked into more than one folder is unlinked from one of the folders. The terminal retainer is attached to ensure the object will be destroyed when retention on the other folder allows it.	string_1: name of retention policy	n/a
dmc_rps_privileged_delete This event is generated whenever an object under retention is deleted using privileged delete.	string_1: indicates the text provided for the Justification field. For example: [DMC_RM_PRIVILEGED_DELETE]testing. In this example testing was the entry for the Justification.	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_promote This event is generated whenever an object under retention is promoted. It is actually the retainer of the object under retention that is promoted.	string_1: name of retention policy and retainer id. For example: Vijay_LINK_080011b78000160d	ID1: id of promoted object
dmc_rps_remove_retention_markup	string_1: name of retention markup string_2: indicates selected designation; <i>true</i> if selected, <i>false</i> if not. For example: isHold=true; isFreeze=false; isReview=false; isPermanent=false; isVital=false string_3: reason for markup (could be blank if no reason was entered)	n/a
dmc_rps_remove_retention_policy	string_1: name of retention policy	ID1: object id of the retention policy
dmc_rps_global_promote Affects global conditions and is similar to dmc_rps_promote.	string_1: name of retention policy and retainer id. For example: Vijay_LINK_080011b78000160e	ID1: id of promoted object
dmc_rps_export_to_xml This event is generated when a schema is selected to recreate records from Records > Export to XML.	n/a	n/a
dmc_rps_supersede	string_1: name of retention policy	n/a
<i>Target Object Type:</i> <i>dmc_rps_retention_policy</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rps_add_action_rel The action relation in this usage implies record relation or notification.	string_1: name of the review notification string_2: contact list string_3: action type string_4: action name string_5: execution rule	n/a
dmc_rps_add_authority	n/a	n/a
dmc_rps_add_condition	n/a	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_remove_action_rel Generated when action relation is directly or indirectly removed (action on a review markup is changed). The action relation in this usage implies record relation or notification. Refer to alternate usage under Target Object Type: dmc_rps_retention_markup.	string_1: name of the review notification string_2: contact list	
dmc_rps_remove_authority	n/a	n/a
dmc_rps_remove_condition	n/a	n/a
dmc_rps_update_action_rel This event is generated when the value for the Action Name is changed on the phases tab of a retention policy. The action relation in this usage implies record relation or notification. Refer to alternate usage under Target Object Type: dmc_rps_retention_markup.	string_1-5: OLD_VALUE-NEW_VALUE pairs	n/a
dmc_rps_update_phase_rel This event is generated when a value on the phases tab of a retention policy is changed.	n/a	n/a
 Note: This is the event name for the dmc_rps_audit_phase object, which is a subtype of dm_audit trail. The attribute names associated to this object type are listed in “Attributes of the dmc_rps_audit_phase object” on page 292.		
dmc_rps_add_global_condition This event is generated when a global condition is added to a retention policy.	string_1: name of global condition	n/a
dmc_rps_remove_global_condition	string_1: name of global condition	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_add_global_authority This event is generated when a global authority is added to a retention policy.	string_1: name of global authority	n/a
dmc_rps_remove_global_authority	string_1: name of global authority	n/a
dmc_rps_save_retention_policy This event is created using the dmc_rps_audit_ret_policy object type. This event is meant as an extension of the dm_save system audit for the policy, storing information that dm_save audit event cannot.  Note: This is the event name for the dmc_rps_audit_ret_policy object, which is a sub-type of dm_audit trail. The attribute names associated to this object type are listed in “ Attributes of the dmc_rps_audit_rel_policy object ” on page 294.	n/a	
dmc_rps_create_retention_policy This event logs the creation of the retention policy which can then be viewed in the Audit Trail Report.	string_1: User who created the policy string_2: The name of the new policy string_3: Reason for creating the policy string_4: Date and time	n/a
dmc_rps_destroy_retention_policy	string_1: User who destroyed the policy string_2: The name of the policy destroyed string_3: Reason or justification for destroying the policy string_4: Date and time	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rps_copied_policy Audited against the newly created object, it tracks the information from the source policy	string_1: source policy name string_2: source docbase	ID1: source policy
dmc_rps_copy_policy_failure Audited against the source of the copy, it tracks what was going to be created.	String_1: new policy name String_2-5: reason for failure	
dmc_rps_rename_policy	String_1: old policy name String_2: new policy name	n/a
dmc_rps_export_policy Audited against the policy that was exported.	String_1: docbase name String_2: username of person doing the export	n/a
dmc_rps_export_policy_failure	String_1-5: reason for failure	n/a
dmc_rps_import_policy Audited against the new policy that was created, tracks what the policy was sourced from.	String_1: source policy name String_2: source repository	ID1: source policy
dmc_rps_import_policy_failure audited against the user doing the import, tracks what type of object was being created and the source file it came from.  Note: The <i>Target Object Type</i> for this is audit is <i>dm_user</i> , not <i>dmc_rps_retention_policy</i> .	String_1: name of configuration object String_2: type of configuration object String_3: source file String 4-5: reason for failure	n/a
<i>Target Object Type: dmc_rps_retention_markup</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rps_add_action_rel This audit is generated whenever the Review designation is added to a retention markup. Notification can be by email or inbox.	string_1: email or inbox notification string_2: name of the contacts, comma separated	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
Event name	Strings usage	Object ID
dmc_rps_update_action_rel This audit is generated whenever the information about the review notification is changed. The possible values that could change include the trigger period, trigger month, trigger day, contact list, and the review action.	<p>string_1 : comma separated list of the fields that changed with their old and new values. Only changed attributes are listed.</p> <p>For example: review_action: OLD_VALUE='Inbox notification' NEW_VALUE='E-mail notification',trigger_period: OLD_VALUE='Monthly' NEW_VALUE='Semi-Annually',trigger_month: OLD_VALUE='N/A' NEW_VALUE='2',trigger_day: OL</p> <p> Note: All five string fields may be used to display a list depending on the extent of the changes. Each string field can display up to 200 characters therefore, up to 1000 characters can be displayed.</p>	n/a
dmc_rps_remove_action_rel This audit is generated whenever the Review designation is removed from a retention markup.	string_1: email or inbox notification	
<i>Target Object Type: dmc_rps_retainer</i>		
Event name	Strings usage	Object ID
dmc_rps_disposition_approved This event is generated when an object in a disposition workflow is routed for approval and approved. Refer to “ About disposition workflows ” on page 228. See alternate usage under the Target Object Type: dmc_rps_disposition_bundle.	n/a	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rps_disposition_rejected This event is generated when an object in a disposition workflow is routed for approval and rejected. Refer to "About disposition workflows" on page 228. See alternate usage under the Target Object Type: dmc_rps_disposition_bundle.	n/a	n/a
dmc_rps_submitted_for_approval This event is generated when a disposition workflow is submitted containing objects for approval. Refer to "About disposition workflows" on page 228. See alternate usage under the Target Object Type: dmc_rps_disposition_bundle.	n/a	n/a
<i>Target Object Type: dmc_rps_disposition_bundle</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rps_disposition_approved This event is generated (only if the Department of Defense Standard dar is installed) when objects in final phase for disposition are confirmed for transfer. Refer to "Disposition run bundles" on page 729. See alternate usage under the Target Object Type: dmc_rps_retainer.	n/a	n/a

Retention Policy Services audit events (Application Code = dmc_rps)		
dmc_rps_disposition_rejected This event is generated (only if the Department of Defense Standard dar is installed) when objects in final phase for disposition are rejected for transfer. Refer to "Disposition run bundles" on page 729 . See alternate usage under the Target Object Type: dmc_rps_retainer.	n/a	n/a
dmc_rps_submitted_for_approval This event is generated (only if the Department of Defense Standard dar is installed) when a disposition run bundle has Action Required set to Yes. Refer to "Disposition run bundles" on page 729 . See alternate usage under the Target Object Type: dmc_rps_retainer.	n/a	n/a
<i>Target Object Type: dm_folder</i>		
Event name	Strings usage	Object ID
dmc_rps_reopen_folder	(user who re-opened the folder, date the folder was re-opened, reason for re-opening the folder)	n/a
dmc_rps_close_folder	(user who closed the folder, date the folder was closed, reason for closing the folder)	n/a
dmc_rps_revert_folder_state	(user who reverted the folder, date the folder was reverted, reason for reverting the folder)	n/a

Table 4-45: Attributes of the dmc_rps_audit_phase object

Attribute name	Description
action_audits (repeating ID)	List of audit ids of any action audit events generated during the creation or modification of a retention policy.

Attribute name	Description
action_contacts (repeating ID)	Corresponding list of any contact ids for the actions that had an audit event generated during the creation or modification of a retention policy.
authority_ids (repeating ID)	List of ids of any authorities on the phase at the time of creation or modification of a retention policy.
authority_names (repeating String – length 255)	List of names of any authorities on the phase at the time of creation or modification of a retention policy.
compound_audit_id (ID)	The compound audit identifier – the object id of the dm_save audit event generated during the creation or modification of a retention policy. As the property data is stored on many different audit, this id allows for the gather of these different audit to create a complete picture of the state of the policy at the time of a save.
condition_ids (repeating ID)	List of ids of any conditions on the phase at the time of creation/edit of a retention policy.
condition_names (repeating String – length 255)	List of names of any conditions on the phase at the time of creation/edit of a retention policy.
cutoff_duration (String –length 32)	The month and day portion of the cut-off duration. Month and day integrals are separated by a comma.
cutoff_period (String –length 32)	Cut-off period
event_fulfillment_rule (String – length 32)	Event Fulfillment Rule
event_selection_rule (String – length 32)	Event Selection Rule
mixed_aging_rule (String – length 32)	Mixed Aging Rule
phase_duration (String – length 32)	The year, month, and day of the phase duration. Integrals are separated by a comma.
phase_id (ID)	Phase ID
phase_name (String – length 32)	Phase Name

Table 4-46: Attributes of the dmc_rps_audit_rel_policy object

Attribute name	Description
compound_audit_id (ID)	The compound audit identifier – the object id of the dm_save audit event generated during the creation/edit of a retention policy. As the property data is stored on many different audit, this id allows for the gather of these different audit to create a complete picture of the state of the policy at the time of a save.
global_authority_ids (repeating ID)	List of ids of any global authorities on the phase at the time of creation/edit of a retention policy.
global_authority_names (repeating String – length 255)	List of names of any global authorities on the phase at the time of creation/edit of a retention policy.
global_condition_ids (repeating ID)	List of ids of any global conditions on the phase at the time of creation/edit of a retention policy.
global_condition_names (repeating String – length 255)	List of names of any global conditions on the phase at the time of creation/edit of a retention policy.

4.2.2.35 Retention Policy Services glossary

Active Phase

Usually the first phase of a retention policy, the active phase represents the amount of time an object is active before it becomes dormant or qualifies for promotion.

Authority

A person or group that authorizes the promotion of objects from one phase of a retention policy to the next phase, as well as the disposition of objects. The authority field must be populated and the authority must be validated in order for an object to age. Multiple authorities can be applied to a single object. The same authority or authorities can be used for all the phases of a retention policy.

Authorizer

A person who is used as a reference or a contact to ensure that an authority is up to date.

Base date Mapping

(A date attribute on an object that is used for the entry date in the qualification date calculation that) A mapping that is used to calculate the entry date for a retention policy phase that employs a chronological aging method. Each object type (for example, dm_document) is mapped to a base date value using the Retention Policy Services base date utility. The entry date is used to calculate the

qualification date employing the chronological aging method. If no base date value is mapped, the system uses an internal default, which is the creation date of the document.

Chronological Aging

One of two types of aging methods used in Retention Policy Services. The qualification date of an object using the chronological aging method is calculated by adding the entry date to the phase duration. See also conditional aging.

Condition

An event that must occur to initiate aging of a retention policy that employs the conditional aging method. Two conditional aging methods include the standard conditional aging method, originally introduced with Retention Policy Services, which is phase driven and now global conditions, introduced in D6, which is policy driven. The global condition, if an object is retained using both conditional aging methods, takes precedence over the standard condition and promotes the object to final phase. A single standard condition or multiple conditions can be applied to a single phase. If an object has multiple conditions applied, all the conditions must be met before the calculation of the retention policy begins.

See also global condition and conditional aging.

Conditional Aging

One of two types of aging methods used in Retention Policy Services. Conditional aging commences after a specific event has occurred. The qualification date, calculated for promoting an object from one phase to the next in the selected lifecycle of a retention policy that uses the conditional aging method, is calculated by adding the event date to the phase duration. See also, chronological aging.

Contact List

A master list that is used to populate fields relating to events, actions, retention markups, and authorities.

Cut-off Period

A date that is used in the calculation of a qualification date of an object for phase promotion or disposition. The cut-off period rounds off the sum of the phase duration plus either the entry date (for chronological aging) or the event date (for conditional aging). Cut-off values include Monthly, Quarterly, Semi-Annually, Annually or Disabled. The Monthly Cut-off Period selection allows you to specify the day (1-31); the Quarterly Cut-off Period selection allows you to specify the month of the quarter (1-3) and the day (1-31); the Annually Cut-off Period selection allows you to specify the month (1-12) and the day (1-31). Cut-off periods are needed before disposition or phase promotion instructions can be applied to an object.

Dispose

Dispose in relation to Retention Policy Services can imply any of three actions: export, transfer, or destroy.

Disposition

The act of disposing objects as determined through their appraisal. Typical Retention Policy Services disposition strategies include destroy, or export to another system. When an object is in the final disposition phase, it is removed from the system.

The act of disposing objects as determined through their appraisal. A disposition run, or disposition processing, is started when you click the Dispose option on the action bar of Disposition Manager, against any selected objects reported (listed). Dispose implies that the content and/or metadata of objects may be exported, transferred, or destroyed. The disposition strategy on the objects reported determines whether the objects will be exported, transferred, or destroyed.

Dormant Phase

A phase that represents the period of time an object must be dormant before it qualifies for promotion to the next phase.

Entry Date

A date that is used with the chronological aging method to calculate the qualification date of an object.

Event Date

A date that is used with the conditional aging method to calculate the qualification date of an object.

Freeze

A retention markup that applies a Freeze to a record under retention stops promotion of the record. Although retainers are prevented from qualifying objects for promotion, objects in final phase however are not prevented from disposition.

Global Condition

An object retained according to a global condition is policy driven and promoted regardless of the phase it is currently in, based on the event date when it is reached, directly to the final phase bypassing all remaining phases. Disposition, once the object is in the final phase, occurs based on the retention date calculated.

Hold

A retention markup that applies a Hold to a record under retention stops destruction of the record.

Non-container objects

Non-container objects are dm_sysobjects that do not extend dm_folder (which includes cabinets). Non-containers refer to any object whose type does not inherit from dm_folder. Containers include but are not limited to:

- Cabinets
- Volumes
- Part (again I suspect you are referring to Records Manager Commonwealth Edition)
- Formal Folders
- Folders

Containers do not include snapshots or VDMs (which are container-like in that they have children).

Phase

A defined state of an object within a retention policy. Each phase has a duration, a cut-off period, and authorities. A phase that uses conditional aging has conditions. The possible phases of a default retention policy are active, semi-active, semi-dormant and dormant. A retention policy must have a minimum of two phases, and a maximum of 30 phases. The final phase of a retention policy is the disposition phase, when objects are destroyed or transferred.

Promotion

Movement of objects from one phase of a retention policy to the next phase.

Qualification Date

The date on which an object qualifies for promotion or disposition.

Records Policies

Records policies include:

- Retention policies
- Containment
- Naming
- Security
- Derived security
- Restrictive markings
- Shared markings
- Security levels
- Attribute marking sets
- Attribute markings

Records Manager policies exclude retention policies.

Retention Markup

A function of Retention Policy Services that prevents an object from undergoing disposition. Retention markup provides a means of applying additional information to a retained object. Objects with a Hold or Permanent retention markup applied cannot be destroyed or transferred on schedule because of special circumstances, such as a court order or an investigation. Objects on Hold or Permanent cannot be deleted or transferred until the retention markup is removed. Hold and Permanent prevent disposition whereas Freeze prevents promotion. None of the date calculations are affected when an object has a retention markup applied. Single or multiple retention markups can be applied to objects.

Retention Policy

A policy that is defined in a retention policy lifecycle, which determines the period of time an object is retained in a repository according to operational, legal, regulatory, fiscal or internal requirements. A retention policy lifecycle consists of at least two phases, where each phase has a distinct duration. The final phase is the disposition phase.

Retention

The period of time an object must be kept according to operational, legal, regulatory, fiscal or internal requirements.

Transfer

The act or process of moving objects from one storage location to another.

Chapter 5

Records Manager

Records Manager is an integrated electronic record-keeping system (ERS) equipping organizations with capabilities to:

- Ingest/create large quantities of records
- Manage electronic records
- Safeguard and access vital records
- Relate records to relevant business content
- Cost-effectively archive or destroy records according to system-enforced administrative, regulatory, or legal requirements

Records can be described according to the business need of the customer. Customers decide which policies to associate to a document to make it a record.

5.1 Records Manager Introduction



Note: To avoid potential problems and unnecessary troubleshooting, make sure 1) that you are in the correct Records Manager role for the operation you are attempting and 2) that the instance of the Records Client you are working on, is approved for Privileged DFC. The Records Client must be approved for Privileged DFC. Any Foundation Java API client (for example, Documentum Webtop, Documentum Administrator, Web Services) that could be linking items into policy managed folders must be registered for privilege. To determine which Retention Policy Services role an administrator or end user has to be a member of for specific operations, refer to “[Records Manager roles and functional access](#)” on page 316.

5.1.1 Determining which Records Manager version you are accessing

From the File menu, you can determine which Records Client version you are connected to.

To determine which Records Manager version you are accessing:

1. Click **File > About Records Client**.
2. After you view the information, click **Close**.

5.1.2 Administration components

Records Manager consists of the following components:

- *Containment policies
- *Security policies
- *Derived security
- *Restrictive markings
- *Shared markings
- *Security levels
- *Attribute marking sets
- *Attribute markings
- *Classification guides (Department of Defense specific node, available only if Department of Defense dars are installed)
- *Naming policies
- *Record relation definitions
- *Classification subscription lists
- Record versioning
- Record declaration process
- Formal folder
- Formal cabinet
- Declassification report (Department of Defense specific node, available only if Department of Defense dars are installed)
- Working paper report
- File plan
- Search
- *Commonwealth Administration (Records Manager Commonwealth Edition specific, available only if RMC dars are installed)
 - *Functional thesaurus
 - *Series control

Components preceded by an asterisk are the administration components that appear under Records Manager in the navigation pane. Functionality associated with all other components is available to both end users and administrators.

5.1.3 About privileged clients and accessing repositories



Caution

The Records menu options associated to a particular product, Retention Policy Services or Records Manager, are available only when they are registered for Privileged DFC. Do not approve the Privileged Clients setting for those client instances that do not require Privileged DFC. Users who are not expected to create administrative components do not require their Records Client approved for Privileged DFC. Administrative components include all of the items associated to an administration node in the navigation pane. For example, all of the components under the Retention Policy Services node, Base Dates, Authorities, Global Conditions, and so on. Administrators can use Documentum Administrator to make sure that users have the correct setting. The Approved setting of the clients for those users not expected to create administrative components must be set to *No*. Administrators can change this setting from the Properties of a privileged client. The session listener also checks for Privileged DFC. It provides a dialog to administrators immediately after they log in to Retention Policy Services or Records Manager on the Records Client.

The use of Privileged DFC is pervasive throughout the general Records application stack for all categories of operations. As such, it is a mandatory requirement that the Foundation Java API instance that is being used to carry out the business operations, has been approved for privilege.

Why privileged clients are necessary

Privileged clients are necessary for use cases where business logic has to extend powers temporarily during certain operations. A classic example is when a user creates an object in a retained folder. Although the new object requires retention, the user is not expected to apply retention directly to objects. An administrator has decreed that objects put into a folder (going into the future) must adhere to the policies that are applied. Documents put into such a folder by an end user, whether it is linked or created directly within the folder, simply inherit the policy or policies.

What determines the need for a privileged client

The Records Client for example, must be privileged if it is used to create or import objects into policy managed folders. Administrative components cannot be created unless the client is approved for privilege. Use Documentum Administrator to list and approve the Foundation Java API instance for the desired client. Notice in the list that the Foundation Java API instance for the Documentum CM Server may already be approved, as its Foundation Java API instance is pre-approved. Make sure to approve it however if it is not already approved.

The Foundation Java API instance for the Documentum CM Server and on the Application server for the Records Client must be approved.

The Documentum Administrator user interface lists the clients that have their Foundation Java API instance approved for privilege. The privileged clients listed

are marked *Yes* under the Approved column, if they have been approved. The Documentum CM Server and Application servers listed in this example are all approved. Click Manage Clients if the Documentum CM Server or Application server are not listed and add them from the resulting locator screen. Their Approved status remains *No* until you right-click the client listed in the content pane and select Approve.

5.1.4 Setting up Records Manager

5.1.4.1 Policies

Configure Records Manager before you use it to declare formal records. Configuring Records Manager involves setting up a file plan (managed objects), creating policies and adding rules for containment. Although you can apply as many policies as necessary, there are three different Records Manager policy types to choose from; four if you count retention policies:

- Containment
- Security
- Naming
- Retention

Policies enforce business logic according to the rules specified for them.



Note: Retention policies are documented in “[Retention Policy Services](#)” on page 93.

It is recommended to turn off folder security as the security policy offers finer control over security. Turn folder security Off if you are using a security policy, as folder security is inherently less secure than the Records Manager security policy. There should be no problems however, using folder security turned On as it is less restrictive. In either case, users must be granted Write permissions on the folder to declare a record. With security policies in place, you can turn folder security Off, and control at a finer level the security of objects. Users only need Browse and Link to declare a record (along with Create on the specific record type).

5.1.4.2 About setting up a file plan and configuration options

There are five general actions for you to take when setting up your file plan:

1. Do some planning and determine the requirements for your file plan. For example, do your folders need extra metadata? Or, is it mandatory that the folders apply retention to objects declared formal records?
2. Create custom object types for your folders or cabinets, if you choose. Object types could include physical objects created using Physical Records Manager, which are representations of physical objects (real-world objects, boxes, folders (manilla folders); bay/bin/shelf and so on for example). Folders can also be

created for real-world folders. A physical folder for example, can also be included in the file plan.

3. Create the cabinets and folders to build the basic skeleton for your file plan. There are some choices to make, for example:

- whether to use formal folders or ordinary folders
- whether to turn mandatory retention On or Off

Formal records cannot be declared to an unmanaged folder; for example, a folder without any retention or a records policy. In addition, if mandatory retention option is turned on then retention must be applied to the managed folder in order to declare a formal record in it. For additional details and instructions, refer to [“Records Manager system configuration options settings” on page 373](#).

4. Apply the policies to the cabinets and folders.



Note: Security policy rules become more restrictive when you apply additional security policies to a particular cabinet or folder. Ensure that containment of a valid object is not denied when two or more policies are applied to the same container object. To learn more about policies, refer to [“Overview of records policies” on page 361](#).

5. Determine whether you want your file plan to include attribute inheritance, also called metadata inheritance. Attribute inheritance rules can be specified for a file plan so that objects added to or created in a folder inherit the value for the same attribute from the parent folder. For example, a rule specified for Authors means that an object added to or created in the folder will inherit the value for Authors from the parent. Rules can be specified for only those attributes that are common to the form fields of both the parent and child objects. Values are copied from the parent object to the child object for those rules that are defined. Deploying the rm.dar creates a table with the file name dmc_rm_attribute_copy_rule in the repository for defining the rules. You can edit the table by adding or removing attributes that define the rules. This table is populated with pre-defined rules when RM-DoD5015v3-Standard-Record.dar is installed. For further examples and details, refer to [“About attribute inheritance and the file plan” on page 306](#).

You can structure your file plan as needed. Managed objects are containers and/or documents that have one or more applied policies. Policies are inherited as they cascade down the file plan structure from the point of application. A policy applied directly to a cabinet is inherited by all of its contents, cascades to all folders and documents. A policy applied to a folder is inherited by its documents and cascades down the file plan to its subfolders and their documents from the point of direct application.

Inheritance of a policy (with some exceptions to retention policies listed in the note that follows) cascades from the cabinet or folder to which it is directly applied, down the branch to the subfolders and their contents, as shown in [Figure 5-1](#). If a branch consists of ten folders and the policy is applied to the fifth folder, only those folders

below the fifth will have the same policy applied indirectly as well as any subfolders off another branch below the fifth.



Note: 1) If the **Snapshot Retention Rule** of a retention policy is set to *Retain Root Only*, then only the parent, that is the formal record, is retained. Children objects of the record however, that is the original documents, can be deleted at any time. However, if it is set to *Retain Root and Children*, both the formal record and its children are retained.

2) If the **Retention Strategy** of a retention policy is set to *Individual*, then the retainers on the folders are non-aging though each item contained in each folder gets their own individual retainers that do age. Only the contents of the folders are displayed/listed in a retention report or when disposition is run, not the folders. However, if it is set to *Linked*, the content in the folder is linked to the folder and therefore ages with the folder. Sub folders also inherit unique retainers, not their contents. Only the folders are displayed/listed in a retention report or when disposition is run. When retention is applied to folder A for example, retention cascades to folder B which inherits a unique retainer of its own. Objects in folder A age with folder A. Objects in folder B age with folder B.

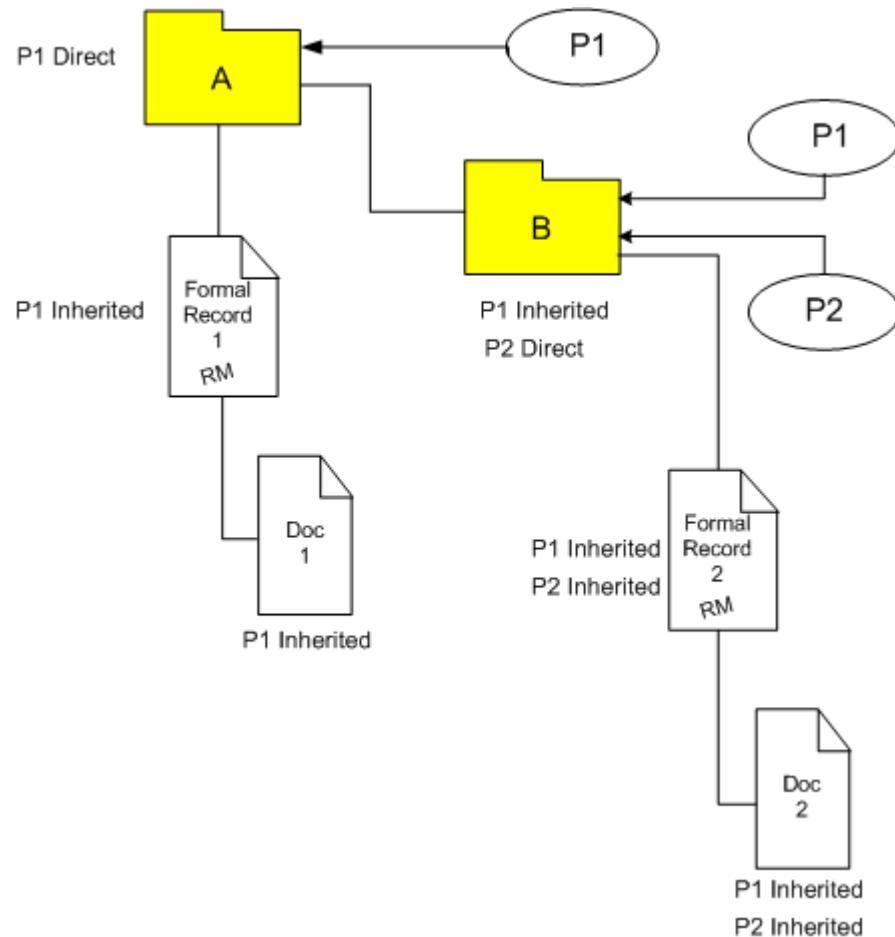


Figure 5-1: File plan example and policy inheritance

Folder A of the file plan illustrated in this example can be either a cabinet or folder; or instead, a formal cabinet or formal folder associated with a form and metadata. The cabinet or folder, formal or not, which has the first policy applied directly is considered the root of the file plan. All objects under Folder A inherit policy 1 (P1) automatically by cascading down the hierarchy. Policy 2 (P2) however is inherited by only those objects under Folder B.

The hierarchy structure of the file plan consists of:

- Root folder (cabinet or folder, formal or not)
 - Although you can apply any one or more policies, naming and containment policies are usually applied to the root folder.
- Sub folders directly linked to the root folder
 - Branching or classification for folders and records
- Folder

- Location for records
- Records

5.1.4.3 About attribute inheritance and the file plan

Attribute inheritance is controlled by the dmc_rm_attribute_copy_rule object in the repository, which is also called the inheritance table. It determines what attribute values can be copied from one form template to another. For example, the values for authors, keywords, and subject already specified on the form template for dmc_rm_formal_folder would be copied to the same fields on the form template loaded for the object that is filed to such a container. Authors, keywords, and subject as a result would be pre-populated on the form template that is loaded for the object being declared as a formal record. Formal records declared and filed to formal folders or to formal cabinets inherit common attribute values from the formal folder or formal cabinet as indicated in “[Default copy rules defined for Department of Defense formal records and folders](#)” on page 306 and “[Default copy rules defined for regular formal records and folders](#)” on page 307. Users declaring formal records can always change a pre-populated value loaded form template when necessary. To add rules to the inheritance table, that is if the dmc_rm_attribute_copy_rule object is in the repository, refer to “[Adding rules to the attribute inheritance table](#)” on page 307.

Editing entries in the table for the dmc_rm_attribute_copy_rule changes the default copy behavior. Each row in the table represents a rule. The rule according to row 1 for example, takes the values specified for authors, keywords, and subject from the parent type and populates the same attributes on the target object type. You can edit existing rules and also add rows to create new rules as necessary.



Note: The dmc_rm_attribute_copy_rule should not be confused with the construct copy rule that is associated with naming policies.

Table 5-1: Default copy rules defined for Department of Defense formal records and folders

Child type (target_object_type)	Inherited metadata (attribute_list)	Parent type (required_parent_type)
dmc_rm_dod5015v3_std_rec	authors, keywords, subject	dmc_rm_dod5015v3_folder
		dmc_rm_dod5015v3_cabinet
dmc_rm_dod5015v3_class_rec	authors, keywords, subject	dmc_rm_dod5015v3_folder
		dmc_rm_dod5015v3_cabinet
dmc_rm_dod5015v3_email_rec	keywords	dmc_rm_dod5015v3_folder
		dmc_rm_dod5015v3_cabinet
dmc_rm_dod5015v3_folder	authors, keywords, subject, category_description	dmc_rm_dod5015v3_folder

Table 5-2: Default copy rules defined for regular formal records and folders

Child type (target_object_type)	Inherited metadata (attribute_list)	Parent type (required_parent_type)
dmc_rm_formal_record	authors, keywords, subject	dmc_rm_formal_rec_folder dmc_rm_formal_rec_cabinet
dmc_rm_formal_folder	authors, keywords, subject	dmc_rm_formal_rec_folder dmc_rm_formal_rec_cabinet

Table entries in the dmc_rm_attribute_copy_rule object can be edited with the following constraints:

- Copying is intended only to populate the record fields in the form templates, so only the form template attributes should be used.
- System attributes and internal attributes (those that start with a_, i_, r_) and a special attribute, the category_identifier, cannot be copied.
- For formal folder types, apart from the types mentioned in table “[Default copy rules defined for regular formal records and folders](#)” on page 307, form templates of the parent and the child should be the same.

5.1.4.3.1 Adding rules to the attribute inheritance table

Using IAPI commands, set the target object types and the parent object types for the attributes you want to define. The following sample procedure defines the rules for formal records added to either a formal folder or a formal cabinet. You must repeat these steps for every target object type you want to affect. The attributes you want to affect can be different for each target object type but must be common to the parent folder or cabinet. If you wanted to include formal folders and affect the same attributes that were set for formal records, replace dmc_rm_formal_record in step 2 with dmc_rm_formal_folder:

To add a rule to the attribute inheritance table regarding formal records, folders, and cabinets:

1. API> create,c,dmc_rm_attribute_copy_rule
2. API> set,c,l,target_object_type
SET> dmc_rm_formal_record
3. API> append,c,l,attribute_list
SET> keywords
4. API> append,c,l,attribute_list
SET> subject
5. API> append,c,l,attribute_list
SET> authors

6. API> append,c,l,required_parent_type
SET> dmc_rm_formal_folder
7. API> append,c,l,required_parent_type
SET> dmc_rm_formal_cabinet
8. API> save,c,l

The following procedures define the rules for Department of Defense formal records added to either a Department of Defense formal folder or a Department of Defense formal cabinet.

**To add a rule to the attribute inheritance table for
dmc_rm_dod5015v3_std_rec:**

1. API> create,c,dmc_rm_attribute_copy_rule
2. API> set,c,l,target_object_type
SET> dmc_rm_dod5015v3_std_rec
3. API> append,c,l,attribute_list
SET> keywords
4. API> append,c,l,attribute_list
SET> subject
5. API> append,c,l,attribute_list
SET> authors
6. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_folder
7. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_cabinet
8. API> save,c,l

**To add a rule to the attribute inheritance table for
dmc_rm_dod5015v3_class_rec:**

1. API> create,c,dmc_rm_attribute_copy_rule
2. API> set,c,l,target_object_type
SET> dmc_rm_dod5015v3_class_rec
3. API> append,c,l,attribute_list
SET> keywords
4. API> append,c,l,attribute_list
SET> subject

5. API> append,c,l,attribute_list
SET> authors
6. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_folder
7. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_cabinet
8. API> save,c,l

To add a rule to the attribute inheritance table for dmc_rm_dod5015v3_email_rec:

1. API> create,c,dmc_rm_attribute_copy_rule
2. API> set,c,l,target_object_type
SET> dmc_rm_dod5015v3_email_rec
3. API> append,c,l,attribute_list
SET> keywords
4. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_folder
5. API> append,c,l,required_parent_type
SET> dmc_rm_dod5015v3_cabinet
6. API> save,c,l

To add a rule to the attribute inheritance table for dmc_rm_dod5015v3_folder:

1. API> create,c,dmc_rm_attribute_copy_rule
2. API> set,c,l,target_object_type
SET> dmc_rm_dod5015v3_folder
3. API> append,c,l,attribute_list
SET> keywords
4. API> append,c,l,attribute_list
SET> subject
5. API> append,c,l,attribute_list
SET> authors
6. API> append,c,l,attribute_list
SET> category_description
7. API> append,c,l,required_parent_type

```
SET> dmc_rm_dod5015v3_folder  
8. API> save,c,l
```

5.1.4.4 User preferences

Use Preferences to make the Records Client user interface appear according to your personal needs.

Preferences provides the following tabs you can select from to customize your view of Records Manager in the Records Client user interface.

To change your preferences:

1. Click **Tools > Preferences**.

The **Preferences** screen is displayed exposing the **General** tab. The **General** tab is first in line with the following tabs:

- General
- Columns
- Virtual Documents
- Repositories
- Search
- Formats

2. Click the applicable tab for which you want to change the preferences.

Radio buttons, checkboxes, drop-down lists (list box, list boxes), as well as links such as edit links and locator boxes are provided as needed to facilitate your changes.

3. Apply your changes as needed on the applicable tabs.
4. Click **OK** to accept (save) the changes, or click **Cancel** to exit **Preferences** and ignore your changes.

5.1.5 About customized email optional mappings

To provide customized email optional mappings in addition to existing out-of-the-box mappings, between the email source and email record, follow these steps:

1. Use *API* to add a customized attribute to a formal record object type.
2. Use *Forms Builder* to update the forms template, directly on the application repository, to show the customized attribute.
3. Use *Notepad* for example to update the email mapping transformation (xslt) file. To complete the update, check out the file, edit, save, and then check it in.

5.2 Records Manager administration

5.2.1 About Records Manager functionality

Records Manager is intended primarily to declare electronic or physical records into a compliant file plan within a OpenText Documentum CM repository.

Records Manager features include:

- Policy administration
- File plan creation
- Declaring records
- Reporting

For more information about Records Manager features, refer to “[Overview of Records Manager](#)” on page 311.

For information on an optional component of Records Manager called Records Manager Commonwealth Edition, refer to “[Commonwealth administration](#)” on page 446.

For Records Manager functionality specific to Department of Defense requirements, refer to [Appendix C, Records Manager and Department of Defense functionality](#) on page 723.

5.2.2 Records Manager



Note: Each records product is role based and therefore all users and administrators must be in the correct role for the expected functionality to work properly. It is equally important that each instance of the Records Client, which hosts each of the records products, is registered for Privileged DFC.

5.2.2.1 Overview of Records Manager

Records Manager is used to declare formal records and to create a file plan using various policies, such as security, containment, and naming, to control the filing of the records declared. Members added to the Records Manager role can create and apply policies to a folder to make it a suitable location to store formal records.

Avoid creating any policies that utilize the special characters listed below. Certain features like the quick search **Starts With** does not work if you use a special character to query. Creating a policy for example that is named beginning with % would not be reported in a query that starts with %. The following special characters must not be used when creating and naming administrative components:

- !
- @

- \$
- %
- (
-)
- ` (the accent character on the keyboard below tilde)
- +
- –
- -
- ,

As mentioned in the Preface, Records Manager can be used in combination with Retention Policy Services for a total records management solution. Install Retention Policy Services if you want to retain records in the file plan according to a specific lifecycle. Online help is available against these products, even if you have only one of them installed.

1. The `rm_docbase_config` configuration object (under Cabinets/System/Applications/RmConfig) governs whether retention is mandatory on a folder in order to declare a document as a formal record.

If you want to change the setting for mandatory retention on a folder, refer to [“Records Manager system configuration options settings” on page 373](#). The option for this setting is turned off (checkbox is deselected) by default so that a formal record can be declared without being retained. It is however normally turned on in regulated environments, especially those that have to conform to the Department of Defense requirements.

2. You may want to turn off folder security on each repository that Records Manager is installed on because records security can automatically set the ACL for documents in folders. Folder security is turned on by default. You must use DA to turn off folder security. Records Manager can work with or without folder security. The effects of turning folder security off are described in [“Functional access and permissions” on page 337](#).

You need Write on the document and Write on the folder to file formal records if folder security is turned on. You need Write on the document and only Browse on the folder to file formal records if folder security is turned off.

All policies, when directly applied to a folder, automatically cascade down the folder structure to its sub folders, by inheritance. All child folders and their contents inherit the policy from the parent folder.

The first objective is to create and configure a file plan as well as maintain it. You must be assigned to the role of Records Manager to create, configure, and maintain the file plan. The Records Manager file plan is basically a highly organized cabinet/folder structure. Your first step in setting up a file plan is to create the policies and then apply them to objects that become managed objects as a result. A managed object is an object that has at least one policy applied to it. You can have one

managed object that is your file plan and you can easily build the file plan simply by creating additional managed objects.

Although Records Manager supports creating record relationships and includes auditing and reporting capabilities, it has two major functional areas:

- File Plan Creation and Maintenance

The role of Records Manager is responsible for this functional area looking after:

- Creating and applying record policies
- Creating and applying retention policies
- Managing record security
- Creating the file plan structure
- Configuring the file plan
- Maintaining the file plan

- Formal Records

The role of **Records Contributor** is responsible for this functional area looking after:

- Declaring formal records
- Browsing formal records
- Searching formal records
- Viewing formal records
- Versioning formal records

A formal record is comprised of a snapshot that has associated metadata. Formal records must be declared manually into a file plan location where they are encapsulated within a structure (snapshot) that contains the original documents. The formal record type and the Department of Defense record types include:

- Formal record(dmc_rm_formal_record)

This record type is always available for declaring regular formal records and is not Department of Defense compliant. The form for this type requires that the RM-Default.dar is installed. It is mandatory that this dar file is installed, even if only Department of Defense records are going to be declared.

- Record DoD5015 V3 Standard(dmc_rm_dod5015v3_std_rec)

The form for this type requires that the RM-DoD5015v3-Standard-Record.dar is installed. All of the Department of Defense record types are optional and therefore the Department of Defense dars can be installed when Department of Defense functionality is required.

- Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)

The form for this type requires that the RM-DoD5015v3-Standard-Record.dar is installed. Both Department of Defense email records and Department of Defense standard records version 3 functionality rely on the same dar file.

- Record DoD5015 V3 Classified(dmc_rm_dod5015v3_class_rec)

The form for this type requires that the RM-DoD5015v3-Classified-Record.dar is installed.

The following Department of Defense record types are available for declaring Department of Defense Chapter 2 and Chapter 4 records. The dar files for these record types (version 2 Department of Defense type dars) do not have to be installed if the version 3 Department of Defense type dars are installed.

- Record DoD 5015 Ch2(rm_dod5015ch2record) (version 2 of standard records)

The form for this type requires that the RM-DoD5015-2.dar is installed.

- Email Record DoD 5015(rm_dod5015ch2email) (version 2 of email records)

The form for this type requires that the RM-DoD5015-2.dar is installed. Both Department of Defense email records and Department of Defense standard records version 2 functionality rely on the same dar file.

- Record DoD 5015 Ch4(rm_dod5015ch4record) (version 2 of classified records)

The form for this type requires that the RM-DoD5015-4.dar is installed.

5.2.2.2 About disposition run bundles

A disposition run bundle captures statistics when Disposition Manager, or the disposition job, is run to process items that are in the final phase of a retention policy. For instructions and further details regarding disposition run bundles, refer to [“Disposition run bundles” on page 729](#).

The Disposition Run Bundles node is displayed by default only when the Department of Defense Standard dar file (RM-DoD5015v3-Standard-Record.dar) is installed. Installation of the Standard dar causes the Enable Disposition Run Bundles configuration option on the Retention Policy Services Disposition Configuration object to be automatically set. Although this configuration option can be set manually, for general usage, without installing the Standard dar, the Disposition Run Bundles node will not be displayed. For instructions and further details regarding Retention Policy Services configuration options, refer to [“Retention Policy Services configuration” on page 119](#). Both the Retention Policy Services Application Configuration and the Retention Policy Services Disposition Configuration objects are located in the same folder. To enable or disable disposition run bundle functionality refer to [“Disposition configuration option settings” on page 124](#).

5.2.2.3 Roles and functional access

5.2.2.3.1 About roles and permissions

Functional access is determined by the end user role or administrator role a person is in. Each role is associated with a set of actions, some of which they may or may not be able to perform unless their Basic Permissions and Records Manager Application Specific Permissions are appropriately set. The person in the role for example, generally has access to all functionality but may not be able to take certain actions unless they have the appropriate permissions set on the object (cabinet, folder, or record). This means that a Records Manager may not be able to remove an object from a folder unless they have BROWSE for Basic Permissions and UNLINK on the folder. Though they can remove, they cannot edit unless they have WRITE permissions. Anyone added to a group however, regardless of their role and permissions, is granted the necessary permissions of the group.

Retention overrides any delete permission so that you cannot delete an object that is retained! Only members in the role can do this through an audited process.



Caution

Users in the retention manager role dm_retention_manager can delete objects under retention. It is recommended that administrators do not put users or groups directly in this role.



Notes

- Retention managers have BROWSE on all objects even if the ACL on the individual objects gives them no access. This is so that basic retention operations such as qualification, promotion, and disposition can be done.
- Once an object is put under retention, it will under normal circumstances go through a disposition process. The object will not go through a disposition process if retention is removed or if a privileged delete is done.
- Objects under retention can be versioned, only as minor or major as they cannot be overwritten.
- Objects under retention cannot be deleted.

Roles and functional access also vary according to the client type you are using. Anyone in the role for example has no access to administrative functionality using the Documentum Webtop client, regardless of any permissions. The differences, already covered, between the three available clients for records are fully described in the “[Overview of Records Manager](#)” on page 311.

5.2.2.3.2 Records Manager roles and functional access



Note: A group or user added to a security policy must also be added to the Records Manager Security User role when their permission is set to WRITE, DELETE, create, link, or unlink. A user for example, who is part of a security policy and is NOT in any of the out-of-the-box roles in the following list, have to be added to the Records Manager Security user role! The following roles are members of dmc_rm_security_user out-of-the-box in an Records Manager installation:

- Records Contributor (dmc_rm_recordscontributor)
- Records Manager Privileged User (dmc_rm_privilegeduser)
- Records Manager (dmc_rm_recordsmanager)
- Security Architect (dmc_rm_security_architect)
- Security Officer (dmc_rm_security_officer)

The Records Manager Security User role (dmc_rm_security_user) is to Records Security as the Retention Policy Services Contributor (dmc_rps_contributor) is to Retention Policies.

Unless a user is in the Security User role, they will not be able to move a document either into or out of a folder that has a security policy.

Administrators and Records Manager privileged users (those users whose privileges are escalated in order to perform privileged Records Manager operations) are already in this role out-of-the-box.

Records Manager Privileged Users:

- Can directly apply and remove Security Policies, Shared Markings, Restrictive Markings, Security Levels for non-container objects to which they have WRITE privileges through the Manage Record Security UI.
- Cannot apply and remove Security Policies, Shared Markings, Restrictive Markings, Security Levels for containers (folders, cabinets and their subtypes) through the Manage Record Security UI.

Regarding this bullet item and the one above it: although the Manage Record Security menu option is disabled (not available) if a Privileged User selects a dm_folder object type, it will be available if they select non-folder object types, dm_document object types for example.

- Make changes to items (including containers) that expose Security Levels or Attribute Markings through their Properties UI, in the same manner as an Records Manager Security User.
- Can cause all of these policies to be inherited in the same manner as an Records Manager Security User by linking documents or folders into Records Security managed folders or declaring Formal Records into Records Security managed folders.
- Can unlink documents from Records Security managed folders.

- Cannot unlink folders from Records Security managed folders. The error message if they attempted to do so would indicate that they have insufficient rights to perform the task.

“Roles in Records Manager and functional access” on page 317 describes and identifies the actions for each role in Records Manager. Retention Policy Services and Physical Records Manager actions and role associations are otherwise described in the respective Retention Policy Services or Physical Records Manager part of this guide. The top portion of the table that follows, also identifies Records Manager roles that are nested in Retention Policy Services roles. A Records Manager for example is equivalent to a Retention Manager or Physical Records Manager such that each can perform all the actions of the other.

Table 5-3: Roles in Records Manager and functional access

Role names	Role name as it appears in the UI	Role nested in the following Retention Policy Services role
Records Manager  Note: The Records Manager is included in all of the roles listed, except the Security Architect and the Form Designer roles.	dmc_rm_records_manager	Retention Manager (dmc_rps_retentionmanager). Also, both the and the Retention Manager roles are nested in the Physical Records Manager role.
Privileged Records User (PRU)	dmc_rm_privilegeduser	Power User (PU) (dmc_rps_poweruser)
Records Contributor (RC)	dmc_rm_recordscontributor	Contributor (dmc_rps_contributor). This role is also nested in the Form User role.
Security User (SU)	dmc_rm_security_user	Contributor (dmc_rps_contributor)
Security Architect (SA)	dmc_rm_security_architect	n/a

Role names	Role name as it appears in the UI	Role nested in the following Retention Policy Services role
Form Designer (members of this role are able to modify/ edit Records Manager form templates)	form_designer	<p>The install owner is added to the Form Designer role. No other roles are added to this role. The idea is that the administrator will want to add whoever is going to design forms into this role.</p> <p> Note: The install owner is also added to the records manager role to install the product and components.</p>
Form User (members of this role are able to use Records Manager form templates)	form_user	Members in Records Contributor and Privileged Records User roles are nested in the Form User role.
Classification Guides Administrator	dmc_rm_class_guide_admin	
Classification Subscription Lists Administrator	dmc_rm_csl_admin	
Record Relation Administrator	dmc_rm_record_rel_admin	
Declassification Report User	dmc_rm_declass_report_user	
Security Officer	dmc_rm_security_officer	
Classification Guides Administrator	dmc_rm_class_guide_admin	
Classification Subscription Lists Administrator	dmc_rm_csl_admin	
Record Relation Administrator	dmc_rm_record_rel_admin	
Declassification Report User	dmc_rm_declass_report_user	
<p>All Records Manager roles require that the user has at least Contributor client capability.</p> <p>Records Manager roles nested in the Retention Policy Services roles have access to both Records Manager and Retention Policy Services functions. Anyone that is a Records Manager for example, is also a Retention Manager. All functional access granted to the role of a Records Manager includes access granted to all the functions the Retention Manager has in Retention Policy Services. All functional access granted to the role of a Privileged User includes access granted to all the functions the Power User has in Retention Policy Services. All functional access granted to the role of a Records Contributor includes access granted to all the functions the Contributor has in Retention Policy Services.</p>		

Table 5-4: Roles in Records Manager and functional access

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
<i>Administration actions in Records Manager</i>					
Create/ Modify/ Delete Containment Policies	Yes				
Create/ Modify/ Delete Security Policies	Yes				
Create/ Modify/ Delete Restrictive Markings	Yes				
Create/ Modify/ Delete Shared Markings	Yes				
Create/ Modify/ Delete Security Levels	Yes				
Create/ Modify/ Delete Attribute Markings	Yes				
Create/ Modify/ Delete Attribute Marking Sets	Yes				
Create/ Modify/ Delete Naming Policies	Yes				

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Create/ Modify/ Delete Classification Guides	Yes				
View Derived Security Policies				Yes	Used to help debug applied security policies
View Classification Guides	Yes	Yes			
Create/ Modify/ Delete Formal Cabinet	Yes	Yes			User must have coordinator as client capability, user must also have privileges so that they can create a cabinet. Note: this applies to unretained formal cabinets

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Create/ Modify/ Delete Formal Folder	Yes	Yes	Yes		User must have coordinator as client capability, user must also have privileges so that they can create a folder  Note: This applies to unretained formal folders.
Apply Containment Policies	Yes				Apply Record Policies menu
Apply Naming Policies	Yes				Apply Record Policies menu
Apply Security Policies	Yes	*Yes			Manage Record Security menu *RM Privileged users can only apply to non-container objects.

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Apply Restrictive Markings	Yes	*Yes			Manage Record Security menu *RM Privileged users can only apply to non-container objects.
Apply Shared Markings	Yes	*Yes			Manage Record Security menu *RM Privileged users can only apply to non-container objects.
Apply Security Levels	Yes	Yes			Manage Record Security menu
View Applied Record Policies	Yes	Yes			Select View > Applied Record Policies menu. This applies to all policies.
Remove Attribute Markings	Yes	*Yes			Standard and classified records, or from their Properties page
Remove Containment Policies	Yes				Remove Record Policies menu
Remove Naming Policies	Yes				Remove Record Policies menu

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Remove Security Policies	Yes	Yes			Manage Record Security menu
Remove Restrictive Markings	Yes	Yes			Manage Record Security menu
Remove Shared Markings	Yes	Yes			Manage Record Security menu
Remove Security Levels	Yes	Yes			Manage Record Security menu
Undeclare Formal Records	Yes				Not allowed if the record is under retention
<i>Records actions available from the Documentum Webtop client</i>					

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Declare Formal Records  Note: Members of a role that allows them to declare also require Write permission on the object they are declaring.	Yes	Yes	Yes		Security and Containment policies can prevent this action depending on location and it should be noted that retained records cannot be deleted
Edit metadata of Formal Records	Yes	Yes	Yes		Need Write permission on the record

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Check-out Formal Records	Yes	Yes	Yes		<p>Need Version permission on the record</p> <p> Note: A formal record is comprised of the record itself and its components (the objects/documents) that are in it. You can version the record by itself or the record and its components. To do so you would need Version not only on the record, but also on all of its components.</p>

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Check-in Formal Records	Yes	Yes	Yes		Need Version permission on the record
View Formal Records	Yes	Yes	Yes		Need at least Browse permission on the record
View Formal Records Association	Yes	Yes	Yes		Need at least Browse permission on the record
View Content (Brava!)	Yes	Yes	Yes		To enable Brava! Viewer functionality, refer to Appendix B of the <i>OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)</i> .

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Create Records Relationship	Yes	Yes	Yes		The record relationship definitions provide an area, named Relationship Permissions, where you can select the users or groups that can create and remove (delete) the relationships. Members added to a record relationship definition must have Relate permissions, on both objects selected, to create the relationship. Members added to remove the relationship also need Relate permissions. The Record Relation Definitions is under the Records Manager node.
View Records Relationship	Yes	Yes	Yes		Need at least Browse permission on the record

Records Manager functions	Records Manager roles				Notes
	RM	PRU	RC	SA	
Remove Records Relationship	Yes	Yes	Yes		The record relationship definitions provide an area, named Relationship Permissions, where you can select the users or groups that can create and remove (delete) the relationships. Members added to a record relationship definition must have Relate permissions, on both objects selected, to create the relationship. Members added to remove the relationship also need Relate permissions.

5.2.2.3.3 Records Manager roles and functional access using Documentum Webtop

Documentum Webtop provides no administrative capability to Records Manager and Retention Policy Services. The Documentum Webtop client provides only end user functionality for declaring formal records, creating record relationships, and making library requests for physical objects. You cannot apply a retention policy directly in Documentum Webtop. You can only inherit one.



Note: You can use the Records Client to perform all of the records functions, even those that are simply user based, as it is role-based. There are some limitations however, if you use the Documentum Webtop client to do simple user functionality.

"Records Manager roles and records functional access using Documentum Webtop" on page 329 describes and identifies records actions that can be taken using Documentum Webtop.

Table 5-5: Records Manager roles and records functional access using Documentum Webtop

Records Manager roles in Documentum Webtop	Role name		
Records Manager	dmc_rm_records_manager		
Records Contributor (RC)	dmc_rm_recordscontributor		
All roles in Documentum Webtop have access to all functions except Delete.			
Records functions in Documentum Webtop	RC role	Any user	Notes
Declare Formal Records	Yes		Security and Containment policies can prevent depending on location
Edit Formal Records metadata	Yes		Need Write permission on the record
Check-out Formal Records	Yes	Yes	Need Version permission on the record
Check-in Formal Records	Yes	Yes	Need Version permission on the record
View Formal Records	Yes	Yes	Need at least Browse permission on the record (ACL)

Records functions in Documentum Webtop	RC role	Any user	Notes
Delete Formal Records			This function is disabled so that no one can delete a formal record. You cannot delete records from Documentum Webtop and only Records Managers can perform a Privileged Delete on a record if it is under retention. This action destroys the record and its contents completely. If you wish to recover the linked documents from the record, you can perform an undeclare formal records if the record is not retained.
View Formal Records Association	Yes	Yes	Need at least Browse permission on the record

Records functions in Documentum Webtop	RC role	Any user	Notes
Create Records Relationship	Yes	Yes	The record relationship definitions provide an area, named Relationship Permissions, where you can select the users or groups that can create and remove (delete) the relationships. Members added to a record relationship definition must have Relate permissions, on both objects selected, to create the relationship. Members added to remove the relationship also need Relate permissions.
View Records Relationship	Yes	Yes	Need at least Browse permission on the record

Records functions in Documentum Webtop	RC role	Any user	Notes
Remove Records Relationship	Yes	Yes	The record relationship definitions provide an area, named Relationship Permissions, where you can select the users or groups that can create and remove (delete) the relationships. Members added to a record relationship definition must have Relate permissions, on both objects selected, to create the relationship. Members added to remove the relationship also need Relate permissions.
Create Typical Records	Yes	Yes	

5.2.2.3.4 Records functionality that appears in Documentum Webtop

This section lists all records functionality, available on the Records Client, that end users can access on the Documentum Webtop client from the Records and the View menus:

- End users working with Documentum Webtop can access the following Records menu options:
 - Declare Formal Record
 - Create Record Relationship
 - Make Library Request
- End users working with Documentum Webtop can access the following View menu options:
 - My Library Requests
 - Formal Record Associations
 - Record Relationships

Follow these links to instructions for the desired functionality:

- “Declaring electronic or physical documents as formal records” on page 340
- “Viewing document record associations” on page 345
- “Creating and viewing record relationships” on page 345
- “Removing a record relationship” on page 348
- “Making a library request” on page 482
- “View/edit my library requests” on page 488

5.2.2.3.5 Documentum Webtop operations and Records Manager

Though objects can be removed from a closed folder, no object can be placed into a folder if it is closed. The open or closed folder status is governed by Retention Policy Services.

A security policy, containment policy, or a close folder operation can block an object from being filed or placed into a folder. The following operations could be affected:

- New (create)
- Import
- Copy
- Move
- Link

A security policy or containment policy can also block an object from being removed from a folder. The Move operation could be affected.

5.2.2.4 Records overview

A record consists of recorded information, regardless of medium or characteristics, made or received by an organization that is evidence of its operations, that has value requiring its retention for a specific period of time. Although records are ultimately defined according to the needs of your organization, OpenText Documentum CM defines records as either formal records or typical records. Formal records are created explicitly by filling out additional form metadata and assigning them to a formal file plan. The formal records are also subdivided into types that adhere to the Department of Defense standard and those that do not. Typical records are created by inheriting a policy when an object is dragged and dropped into any Records Manager or Retention Policy Services policy managed folder, or if the policy is applied directly to the object.

Although a document, virtual document, snapshot, or typical record can be exported, formal records cannot. The Export menu option is not available against formal records.

If your installation includes Records Manager, then the Records Client lets you create, relate, and search both formal and typical records.



Note: What determines if you can do the administrative functions or just plain user functions is the role that you are in! All functionality associated with the Records components, Retention Policy Services, Records Manager, Records Manager Commonwealth Edition, and Physical Records Manager, in the Records Client, are role-based, except for core OpenText Documentum CM functionality covered in part 5.

Documentum Webtop however, provides no administrative functionality for records; it has limited client functionality and does not have any administrative capabilities. The Records menu list box using the Documentum Webtop client includes only the following two options:

- Declare Formal Record
- Create Record Relationship

The Records menu is not displayed at all if Records Manager is not installed. The Documentum Webtop user must also be added to the Records Contributor role to declare formal records or typical records from Documentum Webtop

Many people think of records as objects that cannot be deleted without going through a special process (disposition). Records Manager does not mandate the use of retention to consider an object a record. The administrator is responsible for applying the appropriate policies to folders or cabinets.

A record is either a formal record or a typical record based on the method used to add it to a policy managed folder (also called policy enabled folder). Though a typical record cannot be declared, that is filed to a policy managed folder, a formal record is always and must be declared (filed) to a policy managed folder. Typical records are placed, linked, copied, or moved, to a policy managed folder. A policy managed folder has one or more policies applied to it consisting of Records Manager policies and/or Retention Policy Services policies. Although typical records can be placed into a policy managed folder they cannot be declared, as declare functionality is restricted to formal records.

A record is a typical record either, when the document has a policy applied directly to it (the case in which it is not placed into a policy managed folder), or when it is copied, moved, or linked to a policy managed folder.

A record is a formal record only when the document is declared to a policy managed folder using the menu option Declare as Formal Record. All declared records are formal records filed using a selected form and are differentiated by the form used to create them. Forms for declaring formal records are described in [“Declaring electronic or physical documents as formal records” on page 340](#).



Note: A record, formal or typical, inherits the policies from the container object, cabinet or folder it is contained in.

Though a record can mean different things to different people, there is a difference between linking a document into a policy managed folder versus declaring a document as a formal record into a file plan location. Both record types are

differentiated in “[Differences between a typical record and a formal record](#)” on page 335. “[Overview of Records Manager](#)” on page 311 also compares formal and typical records.

Table 5-6: Differences between a typical record and a formal record

Criteria	Typical record	Formal record
Means by which the record is created	<p>This record type is created <i>implicitly</i> when a document is placed, that is linked, copied, or moved to a policy managed folder. Users may be totally unaware that this has happened.</p> <p> Note: Applying a policy directly to a document also creates a typical record.</p>	<p>This record type is created <i>explicitly</i> by declaring the documents to be made a formal record using a menu item for which a form needs to be filled out. The source documents are not linked into the file plan, instead the formal record is. A formal record is a record construct with a form associated to it and components (the documents inside of it).</p> <p>A formal record is always declared, that is filed into a container object that has at least one policy applied to it.</p> <p>It is also possible to unlink or not to unlink the source documents when declaring. If unlinked they will appear to be only in the formal record. If not unlinked they will appear in the location where the documents were selected and in the formal record. The Unlink source documents checkbox can be selected or deselected on the Create tab when declaring.</p>
Additional dars	No additional dars need to be installed to create typical records.	The appropriate dars must be installed to declare the various formal record types.

Criteria	Typical record	Formal record
Metadata	<p>No new object is created, so the metadata is on the original object.</p>	<p>An assembly object (or snapshot) is created with a separate version tree and metadata which is different from the source documents that are linked into the formal record snapshot. A new snapshot is needed if you want to capture any changes to a document already in a snapshot.</p> <p>Note that the security can be set up differently for the source documents versus the formal record metadata.</p>
Viewing	<p>The original source document is what you will see when viewing.</p> <p>By default, the current version of the document is shown.</p>	<p>The view of the formal record is different and allows you to see the list of source documents that make up the formal record.</p> <p>When the formal record is created, the version of the source documents is fixed at the time of creation.</p>
Policies	<p>Inherits policies from folder.</p> <p>A policy can also be directly applied.</p>	<p>Formal records inherit policies from the folder and can only be created if a folder has a policy on it.</p> <p>Source documents inherit policies from the formal record (which includes the policies from the folder).</p>
Versioning	<p>There is only one object.</p>	<p>Because there are two different objects, a formal record and at least one source document, a new version can be created for the source document independent of the formal record.</p>

Criteria	Typical record	Formal record
When making a new version of the source document, does the new version inherit policies?	<p>Yes, all policies are applied if a new version of a source document is linked to a policy managed folder.</p> <p>No however, when a policy is applied directly to the document being versioned.</p>	<p>No, new versions of a source document do not inherit policies.</p> <p>The formal record will still point to the original version of the source document (even if that version is no longer current) as that is the record reference.</p> <p>Yes however, if you version the record itself and opt to version the source documents at the same time.</p>
<p> Note: A formal record version may be processed separately from the source document version contained by the formal record. If necessary, a document declared as a formal record can be versioned separately from the formal record it is filed to.</p> <p>Any version of a record that is linked to a managed folder is considered a managed object (i.e. record).</p> <p>Although both formal and typical record versioning is allowed, check in as same version however is disallowed only if the record is retained.</p> <p>Snapshots may be different from the source document versions because the first version of a document declared or in a formal record may not be version 1, however the snapshot <i>must</i> start at version 1. This is why a separate object is used to manage formal record versions.</p>		

5.2.2.4.1 Functional access and permissions

Users in the Records Contributor role (dmc_rm_recordscontributor) can perform the actions listed in “[Formal records contributor role](#)” on page 337.

Table 5-7: Formal records contributor role

Function	Members in Records Contributor Role	Any user	Notes
Declare Formal Records	Yes		<p>Need write on the original source document(s) in order to declare them as a formal record.</p> <p>Security and Containment policies can prevent filing depending on location</p>

Function	Members in Records Contributor Role	Any user	Notes
Edit Formal Records	Yes		Need Write permission on the record
Version Formal Records	Yes		Need Version permission on the record
Check out Formal Records	Yes	Yes	Need Version permission on the record
Check in Formal Records	Yes	Yes	Need Version permission on the record
View Formal Records	Yes	Yes	Need at least Browse permission on the record (ACL)
Delete Formal Records			This function is disabled so that no one can delete a formal record. Only Records Managers can perform a Privileged Delete on a record if it is under retention. This action destroys the record and its contents completely.
View Formal Records Association	Yes	Yes	Need at least Browse permission on the record
Create Records Relationship	Yes	Yes	Need Relate permission on both ends. Need Create permission on the record relation definition. Each definition has its own setting to control who can create this type of relation.
View Records Relationship	Yes	Yes	Need at least Browse permission on the record

Function	Members in Records Contributor Role	Any user	Notes
Remove Records Relationship	Yes	Yes	Need Relate permission on both ends. Need to add group to remove as part of the relation definition. Each definition has its own setting to control who can remove this type of relation.
Users must be in the dmc_rps_contributor role at minimum to apply retention through inheritance. Users must be in the dmc_rm_recordscontributor role to create formal records.			



Note: There is also the undeclare record option for record administrators only. If the formal record is not under retention, you can undeclare it, meaning that its parts become dissociated so that you can recover the documents.

Minimum permissions required for creating records are identified in “[Minimum permissions required to declare a record in a container object](#)” on page 339.

Table 5-8: Minimum permissions required to declare a record in a container object

Object	Permissions	Records Manager security
Source Document	WRITE	n/a
Folder with Folder Security	WRITE	LINK
Folder without Folder Security	BROWSE	LINK
Note: If record security is on the file plan then the user needs the Records Manager Create extended permission for the type of formal record they want to create.		

You only need WRITE on the source document but would need LINK on the folder if you are using an Records Manager Security policy. The containment policy on the folder, if used, would also need to accept the record type being created for the file plan location. For the record type, if the security policy is applied to the file plan, the record type must have CREATE permissions for that type of record. For more information on linking and unlinking objects from a Records managed folder, refer to the last note provided in “[Overview of security](#)” on page 390.

5.2.2.5 Declaring electronic or physical documents as formal records

Instructions in this section are intended to declare formal records. Formal records can be both Department of Defense formal record types and regular formal records which do not have to adhere to the metadata required by Department of Defense. Although you can use these instructions to declare any formal record type, the attributes on each of the respective forms are described separately. The attributes on the regular formal record form (dmc_rm_formal_record) are described in this section, that is the subsection that immediately follows the instructions for “[Entering values on the formal records form](#)” on page 344. The attributes on each of the three Department of Defense forms however are described in [Appendix C, Records Manager and Department of Defense functionality](#) on page 723. All four formal record form types are listed in the appendix.



Note: Formal records when they are being declared can also be related to another formal record using the Create Record Relationship button at the bottom of the form. It is available for your convenience to create record relationships as well when you declare a formal record. You do not have to follow one process to declare a formal record and then follow another process to create a record relationship. For further details about record relationships, refer to “[Record relations](#)” on page 405.

Users must select the appropriate form to declare a formal record. All records, except typical records, must be associated to a form and declared to a valid file plan location.

Declaring a physical or an electronic document as a formal record means that you are creating a snapshot of one or more source documents to capture all information, content and metadata, in a VDM at a particular point in time. To find out more about physical documents or physical objects in general, refer to “[Physical Records Manager](#)” on page 467. Newer versions of the same source documents can be declared again when needed, though the newer version of the original source document gets associated to the new formal record.

The steps provided to declare records can be used to declare electronic content, email content (if it is already in a OpenText Documentum CM repository), and physical content as formal records or as specialized formal records that adhere to Department of Defense standards.



Note: Email messages can be declared as Department of Defense Email Records only through Records Activator for Microsoft Outlook client. Records Activator prompts you to select file plan to save the email record while declaring it and also displays the Department of Defense Email Record form to allow you to enter the values for different fields of Department of Defense Email Record form. For more details regarding declaring of email record, refer, *OpenText Documentum Records Activator for Microsoft Outlook - User Guide (EDCRMCOOUT-UGD)* and “[Entering values on the Department of Defense email records form](#)” on page 743 .

To declare an email message as an email record through Records Activator for Microsoft Outlook, the 'shouldParseMsgFile' property must be set to true in mailapp.properties on the Application server where records (to which records activator is pointing) is deployed. If you select 'Include Attachments' while declaring an email message as an email record through Records Activator for Microsoft Outlook, but the attachment separation is disabled in mailapp.properties by setting 'shouldSeparateAttachments' to false, then you will receive a prompt asking if you want to declare only the email message as a record without including attachments. Depending upon the option selected on this prompt, either email message alone is declared as an email record without including its attachments or email record declaration operation is canceled.

The source email message, which is declared as an email record, is imported into the repository in its native outlook message format (.msg format) as an object of dm_email_message type or any of its subtypes. The object type of the source email message imported into the repository while declaring the email record is decided based on the value set for the 'Source Email Type For Filing Email Records' attribute in Records Manager Docbase Configuration object. The supported object type values for this attribute include dm_email_message and its subtypes. The default value for this attribute is dm_email_message. For more information on this attribute, see ["Records Manager system configuration options settings" on page 373](#).

To declare electronic or physical documents as formal records:

1. Navigate to the location of the document or email to be declared and select it in the content pane.

 **Note:** Although you can select more than one item and declare them individually or grouped according a particular record type, you cannot declare them as different record types. You would have to declare them independently to file each as a different record type.

2. Click **Records > Declare Formal Record.**

The screen displayed for multiple documents selected is slightly different from that displayed for one single record or individual records from the documents selected. It includes an optional field to make one record or individual records of the documents selected.

 **Note:** Optionally, you can change the default setting for **Declare selected documents as from Individual records to One record** if you have multiple documents selected.

3. Click **Select** next to the **File Plan** entry and select a valid file plan, a cabinet or a folder, from the locator screen displayed. The valid choices are managed container objects that have at least one policy applied to it.

 **Note:** If a Classification Subscription List (CSL) was created, users can select its icon in the Choose a folder locator screen to select a shortcut to the filing location. This saves users from having to find the desired

location each time a record is declared. For further details about classification subscription lists and to create them, refer to “Classification subscription lists” on page 414.

Valid cabinets and folders, when you select **All File Plan**, are highlighted to differentiate them from those that are not valid choices. Valid choices could also be buried in a container that is not valid. A valid folder for example could be buried in a cabinet that is not valid/managed. A folder might not be selectable for any of the reasons described in “Reasons why a folder cannot be selected” on page 342.

The **Unlink source documents** checkbox, in the default state, when deselected means that the document selected will remain visible and available in the location it was selected in and in the formal record. If selected, it means the document selected will no longer appear in that location and that it will be available only in the formal record.

Table 5-9: Reasons why a folder cannot be selected

Reason	Notes
Container is closed	By default, containers are open.
No policies are applied to the container.	Any one of the following policies is sufficient: <ul style="list-style-type: none">• Retention• Security• Containment• Naming• Any security marking (security level, shared marking, restrictive marking)
No retention policy applied and the system setting requires a retention policy	By default, a retention policy does not need to be applied. This setting can be changed on the Retention Policy Services configuration object. For further details about how to change the setting, refer to “Records Manager system configuration options settings” on page 373.
Security policy is applied and the Records Manager extended permission of Link is not granted on the folder.	



Note: A dm_folder that a login user owns does not show up in the **Mine** list of the file plan locator when its modify date is older than the time interval configured for the **Mine** list. The **Mine** list in the file plan locator contains all the objects of type dm_folder and/or its subtypes that the login user owns and that were modified by the login user in the last seven days from the current date. The time interval, seven days by default, is configured in the WDK component, MyObjectLocator.

4. Click **OK** to accept the location for the selected file plan.

The locator screen closes while the **Declare Formal Record** screen is refreshed displaying the selected file plan and some additional attributes. Additional attributes include the following:

- **Type**, mandatory
 - **Form Template**, mandatory
 - **Unlink source documents**, optional
 - **Show options**, optional
5. Select the formal record **Type** you want to declare.
- The value for the **Form Template** is automatically populated according to the value selected for the **Type**.
-  **Note:** Only the email record forms are displayed in the list box when email records are declared using Records Activator for Microsoft Outlook client.
6. Optionally, you can select the checkbox to **Unlink source documents** only if you want to allow anyone with *Unlink* privileges to remove the source documents from its original location after it has been declared a formal record.
 7. Optionally, you can subscribe to the selected folder in the file plan by clicking **Show options** and selecting the checkbox next to **Subscribe to this file**. A shortcut is added to the **Subscriptions** node to facilitate access for frequent access.
 8. Click **Continue** to fill out the form displayed according to the **Form Template** selected. Refer to “[Entering values on the formal records form](#)” on page 344 to enter values on the formal records form.
Or, refer to [Appendix C, Records Manager and Department of Defense functionality](#) on page 723 to enter values on the different Department of Defense forms if you are declaring Department of Defense formal records.
It is a clear indication that you are declaring multiple documents as **Individual records** when the top of the form indicates 1 of a number.
 9. Click **Finish** when you are done filling out the form. Clicking **Cancel** backs out the entire process.

5.2.2.5.1 Entering values on the formal records form

Refer to this section if you are declaring a document as a formal record according to the dmc_rm_formal_record form type. “[Attributes for formal records](#)” on page 344 describes each of the attributes on the form.

The **Next** button is displayed at the bottom of the form only when you select more than one item to be declared as Individual records. You do not have to click Next. You can click Finish to apply the same metadata to the remaining records. You only click Next if you want each individual record to have different metadata when filing.

All mandatory fields require entries to proceed with filing. Any field that is incorrectly addressed prevents the form from being processed. Unaccepted entries are clearly described in red text at the bottom of the form when processing is prevented. Make sure to provide entries for all the mandatory fields and that all the entries are valid.

Table 5-10: Attributes for formal records

Attribute (*) indicates mandatory attributes	Description
*Name	The name of the document is populated in this field automatically if a single document was selected for the record. If multiple documents were selected to be filed as a single record, Please Enter Record Name is displayed for this value.
Subject	Any value you type for this field is acceptable. The principal topic addressed in a document could be used.
Authors	The value you type for this field should identify the author of the document that is being declared a formal record. You can click Insert to insert another value and all inserted values are saved.  Note: Each field inserted is reorganized, after the form is saved, so that it appears under the field that had the radio button selected.

Attribute (*) indicates mandatory attributes	Description
Keywords	<p>The value you type for this field can be used to facilitate searching. The metadata on a form associated to a particular record can be used for keywords.</p> <p>You can click Insert to insert another value and all inserted values are saved.</p> <p> Note: Each field inserted is reorganized, after the form is saved, so that it appears under the field that had the radio button selected.</p>
Create Record Relationship	<p>Displays a page that allows you to choose the record relationship type. On this page there is also a locator that allows you to connect the record being declared to another as a child or as a parent using the selected relationship type. For further details about record relationships, refer to “Record relations” on page 405.</p>

5.2.2.6 Viewing document record associations

Use this feature to determine if a document is in a formal record or not. Each formal record declared against a particular document is called a formal record association. A document can be declared a formal record more than once if necessary.

To view formal record associations:

1. Navigate to a document in the file plan under **Cabinets**.
2. Right-click the document displayed in the content pane and click **View > Formal Record Associations**.

The screen refreshes to display all of the formal records that contain the object in question.

5.2.2.7 Creating and viewing record relationships

Creating a record relationship is an end user activity. However, before they can do this the administrator (Records Manager) has to set up the Record Relation Definitions. Record Relation Definitions provided out-of-the-box are described in the procedure below. To create Record Relation Definitions, refer to “[Create record relation definition](#)” on page 410.

The object selected in the content pane might not be eligible for a record relationship depending on the available record relation definitions in the Record Relation Definitions node. The Relation Name (relation type) used to define the rules against the parent and child objects can prevent a user from creating the relationship. The

objects selected for a relationship must match the rules. If the rule specifies that both the parent and the child have to be formal records, then anything else selected prevents the relationship from being created. Only those record relation definitions in the Record Relation Definitions node are available (filtered) in the list box, when you Create a Record Relationship, if the parent and child selected match the rules. Swapping the parent and the child in a record relationship could change filtering when they have different rules. The number of Record relation definitions in the list box for example could be more or less. The user must also be a member of the Creation Group Name selected for the Record Relation Definition being used. Only those record relation definitions appear in the list box that the user has been added to.

A record relation definition is required to create a record relationship. Administrators can verify and if necessary create the desired relation definition in the Record Relation Definitions node. Record relation definitions available out-of-the-box include:

- Cross-reference Relationship
- Email Attachment Record Relation Definition
- Supersede Relationship
- Supporting Relationship
- Suspend Relationship

Suspend and supersede relationships can be created only when the objects involved are under individual retention. To create a suspend or a supersede relationship between records in a file plan, the file plan must be under individual retention.

Usage of record relation definitions is not limited to formal records only, they can be used with typical records and even plain old documents that are not retained. “Record relationship valid object types” on page 346 lists the parent and child types that can participate in a record relation.

Table 5-11: Record relationship valid object types

Record relation	Parent	Child
Cross-reference Relationship	dm_sysobject	dm_sysobject
Email Attachment Record Relation Definition	dmc_rm_formal_record	dmc_rm_formal_record
Supersede Relationship	dm_document	dm_document
Supporting Relationship	dm_sysobject	dm_sysobject
Suspend Relationship	dm_document	dm_document



Note: Record relation definitions are described in the Overview, along with a list of instructions, in “Record relations” on page 405.

To create record relationships:

1. Navigate to a formal record, under **Cabinets** for example, and click it in the content pane.
2. Select **Records > Create Record Relationship**. The **Create a Record Relationship** screen appears.
3. Select **child** or **parent** to create the appropriate end of the relationship that you are interested in.



Note: Make sure the following 4 conditions are met before attempting to establish a Suspend relationship:

- The parent in a suspend record relationship must be under direct retention.
 - The child in a suspend record relationship must be under direct retention.
 - The parent object must be under a retention policy that has the trigger defined to release the suspension on a current or forthcoming phase, including rollover. At least one of the retainers or rollovers on the parent must have a remaining phase action (phase action that have not expired) with a suspension release trigger.
 - The record relation must not result in a cyclical relationship among the related objects, or in its relationship chain that will result in a suspension deadlock. The system will check to make sure the child is not the parent of any suspend relationship that might result in this parent being its either direct or indirect child.
4. Select the **Record relation definition** from the list box that represents the relationship type you want to create. The list box is empty if there are no record relation definitions or if none of the existing definitions have rules that match. You would have to create the desired record relation definition if it is not already available and then return to this procedure. If you are not in an administrator role, contact your records administrator.
 5. Click **Select** to locate the formal record to relate to.
 6. Click **OK** to complete the operation.

To view record relationships:

There are two ways to view record relationships: View > Record Relationships which users and administrators can utilize and View > Record Relationship Definition Usages which only administrators can utilize:

1. Navigate to one of the formal records involved in a record relationship.



Note: Administrators can also navigate to a record relation definition of interest, right-click it, and select **View > Record Relationship Definition Usages**.

2. Right-click the formal record displayed in the content pane and select **View > Record Relationships**.

The relation type is indicated under the **Definition Name**, along with the records selected for the **Parent** and the **Child**.

5.2.2.8 Removing a record relationship

Users and administrators must be able to view the parent and child to remove a record relationship. They also require Browse permissions and must be in the Removal Group Name, as listed in a record relation definition.

To remove a record relationship:

1. Navigate to a formal record and select it in the content pane.
2. Click **View > Record Relationships**.
3. Right-click the object listed and select **Records > Remove Record Relationship**.
If the record has multiple relationships, that is if more than one object is listed, right-click the desired object and then select **Records > Remove Record Relationship**.

5.2.2.9 Formal records, formal folders, and formal cabinets

About formal records

Formal records are associated with a form and metadata. You can declare multiple documents as one formal record or you can declare them as individual formal records. The option to Declare Formal Record is found in the Records menu. Forms are available out-of-the-box for the following formal record types:

- Formal records, default functionality
Using default functionality, emails can also be declared as formal records when they do not have to be Department of Defense compliant email records.
- Department of Defense classified records, optional functionality
- Department of Defense standard records, optional functionality
- Department of Defense email records, optional functionality



Note: A system configuration option (switch) can be set to force managed folders in a file plan to have retention on them in order to declare formal records. The system configuration option is turned Off by default to allow records to be declared without retention. Once turned On retention would be required before formal records could be declared successfully. “[Records Manager system configuration options settings](#)” on page 373 provides more details on this topic.

Formal records typically inherit the polices from the folder to which they are applied. Although it is possible to apply a policy directly to an object, most

administrators, such as the Records Manager, ensure that the correct policies are applied by putting them on a folder so that the policies are automatically applied by inheritance.

The Records Manager can choose any combination of policies to apply to a folder when creating a file plan. The applicable rules are based on the policies applied. Formal records can only be created in folders that have at least one policy applied.

There are two ways a Records Manager can control where formal records can be placed:

- Applying a containment policy to prevent various, unwanted, object types from being put into that folder.
- Applying a security policy where the Records Contributor needs CREATE permissions on the record object type and LINK permissions on the folder to link an object in that folder. UNLINK permissions on the folder is also required if it is necessary to remove an object from that folder.

Customers decide what policies they need associated to a document in order for it to constitute a formal record. Their needs may be as simple as associating a retention policy, or more complex such as associating a Retention Policy, a Security Policy, a Containment Policy, and a Naming Policy or any combination.

When an administrator applies either an Retention Policy Services retention policy, or any Records Manager policies, or any combination of both to a folder or cabinet, the folder or cabinet becomes a suitable location to store formal records. For more information and procedures used to declare formal records, refer to “[Declaring electronic or physical documents as formal records](#)” on page 340.

There are four formal record types, each associated to a form, that can be filed to a folder, formal folder, cabinet, or formal cabinet.

Formal record forms

- Formal Record (dmc_rm_formal_record)
- Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec)
- Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec)
- Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)

Formal folder types and associated forms

- Folder DoD 5015 V3 (dmc_rm_dod5015v3_folder)
- Formal Record Folder (dmc_rm_formal_rec_folder)

A formal folder has a *form* associated to it whereas a folder does not. For more information on this topic, refer to “[Creating a formal folder](#)” on page 434.

Formal cabinet types and associated forms

- Cabinet DoD 5015 V3 (dmc_rm_dod5015v3_cabinet)
- Formal Record Cabinet (dmc_rm_formal_rec_cabinet)

A formal cabinet also has a *form* associated to it whereas a cabinet does not. For more information on this topic, refer to “[Creating a formal cabinet](#)” on page 429.

5.2.2.10 Declare new version

Use the Declare New Version option on the Records menu to declare a new version of a formal record. This allows the user to update the formal record to show the current version of the child documents. As well, it is possible to add or remove documents that will be part of the new version of the formal record.

A new formal record version can be declared from an existing formal record if you have to include additional source documents or if the existing source document has to be modified.

Using this feature, users can:

- Add/remove source contents for the new formal record version.
- Revise metadata for the new formal record version.
- Cancel the formal record versioning operation at any stage.

Permissions for record contributors and the security policy applied to a target file plan must be set as follows:

- The folder in the new file plan location must have *Write* permissions for check-in to work, only if its folder security is turned on (folder_security is set to T). Write permission is otherwise not required if folder security is turned off (folder_security is set to F).
- The security policy applied to the new folder must also be configured such that:
 - Users have at least *Version* permission on the formal record (dmc_rm_formal_record or its subtypes).
 - Users have at least *Version* permission on the 'dmc_rm_formal_recstructure' in order to alter (checkout) the VDM to add/remove source contents. In the future, we may use privileged code to do this, but for now please make sure that it is the case.
 - Users have at least *Version* permission on the existing source contents in the formal record if checkout of both the formal record and the children is chosen. Otherwise, *Browse* permission on the source contents is sufficient.
 - Users have at least *Write* permission on the new source document to be added to the new formal record version.
 - The file plan, the existing location and new location, must be configured for the user to have *Unlink* and *Link* for the Records Manager Permissions.

A formal record version is processed separately from the source document version contained by the formal record. If necessary, a document declared as a formal record

can be versioned separately from the formal record it is associated with. Formal record versioning considerations:

- Check in as same version is never allowed for a record, formal or typical, that is under retention.
- Formal record versions are different from source document versions because the first version of a document to be a formal record may not be version 1, however the formal record version must start at version 1. This is why a separate object is used to manage formal record versions.



Note: Only Current versions can be declared as records. And, if you version a document that is part of a record, the new version will not be associated with the existing record. Also, checkout of a formal record will be problematic if a child of the formal record is versioned independently. To work around, modify the child documents as desired, check in all of the child documents, and then check in the formal record.

To declare a new formal record version:

1. Navigate to a formal record in the file plan.
2. Select a formal record in the content pane and click **Records > Declare New Version**, to check it out. The **Declare New Version** screen is displayed.
3. Click **Continue** if you want to version only the formal record, or select **Formal Record and all Contents** to version both the formal record and its source documents and then click **Continue**.
4. Click **Add** to add additional source documents as necessary or right-click the existing source document and select **Properties** to edit the metadata. Documents you want to add must be the Current version.



Note: In order to continue, there must be at least one document listed.

5. Click **Continue**. You can change the file plan location or keep the existing location, save as minor or major version, and add a version label and a description.
6. Click **Continue**. The Info tab is displayed.
7. Enter values against the mandatory attributes and then click **Finish**.

To confirm results, navigate to the location of the new record version to see the changes.



Note: If declaring a new version of a formal record is prevented, due to a naming, containment, or security policy for example, the error message displayed allows you to either continue by clicking OK or to back out of the operation by clicking Cancel. Although the original version selected for versioning seems to have disappeared (most clients display only current versions), it has not, and will continue to appear as though it did.

until the error is resolved. The reason for this is that OpenText Documentum CM by default displays only the current version of an object. Only current versions are displayed in the content pane unless you change the default filter setting from **Show Files and Folders** to **Show All Objects and Versions**. Although you can back out of the operation and restore the original to resolve the error, only the new version of the formal record is discarded, any children however are preserved. The original formal record is unaffected and will still point to the original versions of the source documents.

5.2.2.11 Working paper

5.2.2.11.1 Working paper overview

Working paper is a designation that can be assigned to a document in an repository. The working paper designation is a precursor to a Department of Defense formal record where each working paper has a security level associated to it as it contains national security information. This means that administrators can designate documents in the repository as working papers by assigning a security level until they are declared as formal records. The security level and the working paper designation are removed from the document once it is declared as a Department of Defense formal record.

Working papers can be deleted manually at any time but are purged automatically after 180 days by default. Documents once designated as working papers are destroyed by the working paper job, if they have not been declared as formal records after 180 days. The job is ignored however if the document is under retention or has a retention markup of hold or permanent applied that prevents its destruction.

Metadata is linked to the document once it is designated a working paper. Although you cannot designate formal records as working papers you can declare working papers as formal records. Documents can be designated as working papers only when it is not checked out or not part of a formal record. Physical objects cannot be designated as working papers.

A security level is applied to the working paper from the Properties of the document on the Working Paper tab. Records Manager (the system) attaches an aspect to the document to denote it as a working paper, if the checkbox is selected and a security level is assigned. If you deselect the checkbox, Records Manager removes the working paper aspect and the security level to make it a plain ordinary document once again. For more information about security levels, refer to ["About security policies" on page 364](#). To create security levels, refer to ["Creating security levels" on page 396](#). The desired security level must be created first if it is not already available. You cannot declare a working paper if no security levels are available to choose from. There is a flag in any security level that makes it World Selectable or not. If World Selectable is checked, it means that you do not have to be in the group and that you will see the security level.

Working papers can be deleted manually at any time or automatically after a certain period of time if the working paper job, dmc_rm_DestroyWorkingPaperJob, is

enabled. The job uses the designation date, that is the date you made it a working paper, as the initial value. A configuration option also allows you to specify how many days to keep them (located in Cabinets/System/Applications/RmConfig/RM DocbaseConfig). The default setting for the rm_docbase_config object is set to 180 days, which can be modified by changing the value of Working Paper Aging Period in the rm_docbase_config object.

The existing security level for a working paper can be changed whenever necessary from its Properties.

The following metadata on a working paper is entered and linked to the document:

- Working Paper Indicator
- Security Classification Level
- Designation Date (Read Only)
- Designator (Read Only)

This is the person who turned (designated) the document into a working paper, not necessarily the person who created the document.

Pre-conditions:

- The user has been authenticated into the repository.
- The user has the required access rights to write the files into the repository and write permissions on the document.
- The user is in the Record Contributor role.
- The document (dm_document) is not checked out.
- The document (dm_document) is not part of a formal record (dmc_formal_record_document) or a physical object.

5.2.2.11.2 Designating working papers

1. Navigate to a document in the repository.
2. Right-click the document in the content pane and click **Properties**.
3. Click the **Working Paper** tab.

Only the **Working Paper** checkbox is displayed. The screen refreshes displaying the other three attributes when the Working Paper checkbox is selected.

The checkbox is enabled if at least one global security level is available or if at least one non-global security level, you are a member of, is available.

4. Select a value for the **Security Level** from the list box.
5. Click **OK**.

Values against **Designation Date** and **Designator** are automatically entered when the screen closes. To see the value select its **Properties** again.

5.2.2.11.3 Canceling working paper designations

1. Navigate to a document in the repository that is a working paper.
2. Right-click the document in the content pane and click **Properties**.
3. Select the **Working Paper** tab.
4. Deselect the **Working Paper** checkbox and click **OK**.

5.2.2.11.4 Declaring working papers as formal records

1. Navigate to a document in the repository that is a working paper or, run the working paper report.
2. Select the document in the content pane and click **Records > Declare Formal Record**.
The security level is removed from the document and is no longer considered a working paper. The indicator as a result is removed and cannot be reset. The document in the formal record has two retainers, if the working paper was previously retained at the time that it was made into a formal record. One from the previous working paper and one from the location in the file plan to which it was associated, assuming that the folder has retention.
3. To complete the procedure, follow existing instructions for declaring formal records, refer to “[Declaring electronic or physical documents as formal records](#)” on page 340.

5.2.2.11.5 Running a working paper report

A working paper report lets you see what documents have been designated as a working paper. Security officers can run this report.

1. Select **Records > Reports > Working Paper Report**. The Working Paper Report appears.
2. Click **Report** according to default settings or change default settings to customize and narrow the number of results returned before clicking **Report**.
The screen refreshes if you deselect checkboxes, to reveal **From** and **To** fields to specify date ranges.

5.2.2.11.6 Searching for working papers in the repository

1. First click the black triangle next to the **Search** button and then from the submenu, click **Advanced**.

The **Advanced Search** screen is displayed displaying the **General** tab. The **General** tab must be selected for this step.

2. Select the **Locations** you want to search.
3. Select **dm_document** for the **Object Type**.
4. Select **Aspect Name** in the first field of **Properties**.
5. Select **=** or **Contains** in the second field of **Properties**.
6. Type **dmc_rm_working_paper** into the third field of **Properties**.
7. Click **OK**.

Options on the **Search Results** screen are available to **Restart**, **Edit**, and **Save**. You can for example edit the search criteria to restart the search and, if necessary, save the results.

5.2.2.11.7 Cleaning up working papers

Working papers can be cleaned up (purged from the system) by running the working paper job, **dmc_rm_DestroyWorkingPaperJob**. The working paper job is run from and configured in Documentum Administrator. It can be left to run automatically according to scheduled intervals once configured or it can be run manually at anytime, whether the state of the job is Active or Inactive. A job that is active runs automatically according to configured scheduling on its Job Properties screen. The job, run manually or automatically, ignores working paper objects that are retained or that have a Hold or Permanent retention markup. The job works with the value in the configuration setting for the Working Paper Aging Period. All working papers older than 180 days (default setting) are purged from the system automatically with the job.

To see the Job Properties screen for **dmc_rm_DestroyWorkingPaperJob**:

1. Navigate to **Administration > Job Management > Jobs**, using the Documentum Administrator client.
2. Scroll the list of job names to **dmc_rm_DestroyWorkingPaperJob**.
3. Right-click **dmc_rm_DestroyWorkingPaperJob** displayed in the content pane and select **Properties**. Job Properties appears.

Click **OK** to accept changes, or **Cancel** to close the screen or to ignore changes.

To manually run **dmc_rm_DestroyWorkingPaperJob**:

1. Navigate to **Administration > Job Management > Jobs**, using the Documentum Administrator client.

2. Scroll the list of job names to **dmc_rm_DestroyWorkingPaperJob**.
3. Right-click **dmc_rm_DestroyWorkingPaperJob** displayed in the content pane and select **Run**.

Display the **Job Properties** screen if you want to see the **Job Run History**. The job was successful if the value for the **Last Status** is *Completed*.

5.2.2.12 Derived security and attribute marking sets

The ability to view Derived security is scoped to the dmc_rm_security_architect role. By default, Records Managers are not members of this role. However, the install owner is added as a member.

5.2.2.12.1 Derived security

Derived security is the resulting ACL of merged ACLs when more than one security policy is applied to or inherited by the same object. Derived security is created when a second security policy is applied, resulting in derived security based on the combination of A and B for example. Enforcement of derived security is based on rules or permissions that are most restrictive. If a security policy specifies Read for John and another specifies Write for John and both are applied to the same folder, John gets Read, the most restrictive. A second permutation of derived security is created for example, when a third security policy is applied, based on the new combination A, B, and C.

Security policies include shared, restrictive, and attribute markings. The Derived Security node is Read-Only. You cannot select a menu option to create a new derived security policy. The Properties of derived security allows you to see merged ACLs.

The Security Policy object (dmc_rm_security_policy) is derived from dm_sysobject. A derived security policy like object is used to store rules that result from the application of multiple security policies to a managed object. Derived security policy objects have associated dm_acl objects assigned to the managed object. The derived security policy object records, in a repeating ID attribute, which security policies were merged to create it. Whenever one of these source security policies is changed the merged security policy must be recalculated.

The derived security policy is reused whenever the same combination of security policies is used on a managed object; it is otherwise removed from the system if it is no longer in use. A derived security policy is not in use when none of its associated dm_acl objects are in use:

- All restrictive markings and all shared markings are brought forward from all security policies that are merged.
- The highest (most restrictive) Security Level from across all of the merged Security Policies is brought forward.
- The basic permissions are merged independently.

For the Permissions section, a dm_acl is created for each type of object named in any of the security policies involved. The appropriate type or super-type dm_acl (in a security policy that does not have a specific reference to a type) from every involved security policy is considered when creating the new dm_acl for the object type. A user or group must be named in all of the source dm_acl's in order for them to be added to the derived dm_acl. The lowest level of permission that they have across all of the source dm_acl's is used as their level of permission in the derived dm_acl. For extended permissions, the user or group must have been granted the extended permission in all source dm_acl's for it to be added to the derived dm_acl.

The Access Restrictions section is similarly merged with the change that the lowest (most restrictive) restriction for a user or group has, in any of the source dm_acl's, is put in the derived dm_acl.

5.2.2.12.2 Attribute markings

Attribute markings can be used to provide an additional layer of security for controlling access to a formal record. They are like Restrictive Markings. The difference however, is how they are applied to the formal record. To apply an attribute marking, you would have to select them on the form when declaring a classified record. To apply a restrictive marking you would have to select a record in the content pane in order to apply the marking. Attribute markings have membership, and if more than one attribute marking is defined on the classified record, the user *must be in all* of the groups. Attribute markings for the Attribute Marking Sets named Project Name and Supplemental Marking on the classified record form, for example, must be created first, before an attribute marking can be selected from those sets when a classified record is declared. Items in the Available list for example would otherwise not be displayed. Attribute markings must be unique to each set. Project A for example, is unique to Project Name and must not be added to the Supplemental Marking set.

When an attribute marking is set, or removed, the change in security occurs once you click OK or Finish. In earlier versions, the change would not go into effect unless a policy had been applied (either inherited or directly applied to the object).

Membership is defined for each attribute individual marking that constitutes the set. Separate procedures however, must be followed to add members.

You can create an attribute marking set when you click File > New > Attribute Marking Set. Attribute markings can then be added using the Add button.



Note: Attribute markings protect access to the entire object. If you want to limit access to particular fields in the form, the Forms Builder can be used for this purpose.

The procedure used to delete an attribute marking is the same, refer to “[Deleting policies and attribute markings](#)” on page 384.

Attribute markings usage is not limited to Department of Defense standard or classified records. Formal records too can have attributes designated for marking. To

customize a record attribute so that a client of Records Manager can also have its own attributes for marking, refer to “[Attribute marking sets](#)” on page 358.

5.2.2.12.3 Attribute marking sets

Attribute marking sets contain one or more attribute markings that can be selected as needed for additional security when formal records are declared. Only those members of the selected attribute marking would have access to the formal record declared. *Supplemental Marking* and *Project Name* are the two valid attribute marking sets defined out-of-the-box for declaring Department of Defense records. They appear on the form with values that can be selected for either one.

How to set up custom attributes of a formal record to use attribute markings:



Note: These steps can be used to create your own custom version from scratch. The Department of Defense standard formal record for example, can be used as a guide. If the Department of Defense standard dar is installed, a subtype of formal record becomes available that has been configured to make use of two different attribute marking sets. Note that installation of the dar does not create the Supplemental or Project Name attribute marking sets. Therefore, steps 11-14 must be completed or else there will be no attribute markings to choose from on the form when declaring a standard record:

1. Use Composer to create a Create composer project.
2. Subtype Formal Record object type (dmc_rm_formal_record) or any of its 20.4 release subtypes and create your own custom type.
For example, assume creating a record type my_record and have it subtype dmc_rm_formal_record.
3. Add any number of repeating attributes that you would like to designate for marking.

For our example, lets assume that we want two attributes that cause attribute markings to be applied. Add one attribute, as shown in “[Example for marking attributes](#)” on page 358, called attribute_1 with its repeating value set to *True* and another called attribute_2 set to *False*.

Table 5-12: Example for marking attributes

Attribute name	Type	Size	Repeating	Notes
attribute_1	string	255	True	Multiple attribute markings can be applied based on this attribute.

Attribute name	Type	Size	Repeating	Notes
attribute_2	string	255	False	Only one attribute marking can be applied based on this attribute.

 **Note:** The Type and the Size must be string and 255 respectively.

- In the Composer project select the attributes that you would like to designate for marking and then add value assistance to them. The following query can be used for value assistance:

```
select object_name from dmc_rm_attribute_marking where r_object_id in (select attribute_marking_ids from dmc_rm_attribute_mark_set where object_name='<markup_set_object_name>') and is_enabled=1 order by 1
```

 **Note:** The value in the value assistance query, <markup_set_object_name> is the name assigned to the markup set that contains the markup attributes.

For example, “Setting up value assistance for the example” on page 359 shows how you would set it for our example (assuming that you use the following attribute marking sets):

Table 5-13: Setting up value assistance for the example

Attribute name	Attribute marking set	Value assistance
attribute_1	attribute_marking_set_1	Select object_name from dmc_rm_attribute_marking where r_object_id in (select attribute_marking_ids from dmc_rm_attribute_mark_set where object_name='attribute_marking_set_1') and is_enabled=1 order by 1
attribute_2	attribute_marking_set_2	Select object_name from dmc_rm_attribute_marking where r_object_id in (select attribute_marking_ids from dmc_rm_attribute_mark_set where object_name='attribute_marking_set_2') and is_enabled=1 order by 1

- In the post install script of your composer project, write a routine to create an instance of dmc_rm_attribute_mark_table. Then set the values for this object according to “Key attributes for enabling attribute markings” on page 360.

Table 5-14: Key attributes for enabling attribute markings

Attribute	Repeating	Notes
record_object_type	False	The formal record object type that will be instrumented for using attribute markings.
attribute_names	True	The names of attributes on the record type which when set will cause an attribute marking to be applied.

For our example, set the values as in “[Values for enabling attribute markings for the example](#)” on page 360.

Table 5-15: Values for enabling attribute markings for the example

Attribute	Value	Notes
record_object_type	my_record	
attribute_names	attribute_1 attribute_2	Both entries are added to the repeating attribute.

6. Install Forms Builder.
7. Using Documentum Webtop or Documentum Administrator, add the user who builds forms to the form_designer role.
8. Using Forms builder, create a form for you record (subtype of Formal Record). Make sure the attributes you are configuring are available on the form.
9. Using Composer, import the form into your Composer project and then create a dar for your project.
10. Using the dar Installer, install the dar in your repository.
11. Using the Records Client (log in as a Records Manager), create Attribute Marking Set(s) based on the attributes sets referred to in the value assistance (see step 4).
12. From each attribute marking set, create the Attribute Markings (attribute markings are groups that can have users). If this step is inadvertently skipped the attribute will have no values to choose from.
13. Navigate to the Attribute Markings node, find the attribute marking and double click it. Now add members (users or groups) to the attribute marking (these will be the only users and groups that can view the object once the attribute marking is applied (records managers can always see everything)).

14. Optionally, to test that this is working properly from the Records Client, create a formal record from the Records menu and choose your record type after selecting the file plan location. When the form is displayed, choose one or more of the attribute markings. After filing is completed, navigate to the formal record and choose Manage Record Security. Click the Attribute Marking tab and verify that each of the attribute markings that you chose are applied to the formal record.

Each attribute marking is associated to a single group. Membership in the group determines access to the formal record if this marking has been applied to the record. If several markings are applied, you must be a member of all attribute marking groups in order to access the record. Attribute Markings are an additional layer of security that governs access to the object. The security policy is still enforced and determines the user's permissions on the object.

Procedures for creating attribute marking sets, adding members, and viewing are all contained under [“Security policies” on page 390](#).

5.2.2.13 Records policies

5.2.2.13.1 Overview of records policies

Policies are created and applied to various objects, typically container objects, to enforce business logic. Various objects could include physical objects as well, created using Records Manager. One or more policies can be applied directly to an object, container or contained object, and can cascade down a folder structure by inheritance from the point of application. For further details about inheritance refer to [“About setting up a file plan and configuration options” on page 302](#). A note is also provided in that section that describes some exceptions when retention policies are applied to a file plan.

There are three records policies to choose from:

- Containment
- Security
- Naming

To learn about retention policies, refer to [“Retention Policy Services” on page 93](#). Although not listed, Derived Security, is also considered a policy. The policy framework when policies are applied:

- Allows multiple policies to be applied to the same object.
- Cascades each policy associated to an object to its lower-level objects.
- Handles conflicts when multiple policies of the same type are applied to or inherited by the same object.

Generally:

- More than one of the same policy type (different security policies for example but not the same one twice) can be applied to the same managed object plus managed objects can inherit multiple policies from more than one parent.
- Policies are hierarchical in nature, so that policies that are applied at an upper level are cascaded down the hierarchy tree and applied to every managed object.

A policy (not to be confused with a lifecycle) is a group of business logic. Retention Policy Services, for example, defines a retention policy that when applied prevents the document from being deleted unless done by a controlled process (disposition). Records policies are building blocks for a file plan:

- Containment policies define the structure of the file plan; what can be contained, what cannot be contained and how many levels and links are permitted within each of these objects.
- Security policies build additional capabilities on top of the existing OpenText Documentum CM security model.
- Naming policies are used to define the name, commonly referred to the file plan naming rules; what separator is to be used and what character is to be used as the delimiter between levels.



Note: The rules of a policy, or multiple policies, applied to a container object must be satisfied for containment. An object can be linked to a container object only when the object being linked satisfies or matches all the rules of all the retainers applied.

5.2.2.13.2 About policy usages and applied policies

This topic differentiates features, between Records Manager and Retention Policy Services, used to identify the objects that are governed by a policy and conversely, the policies that govern an object.

Use the Applied Record Policies feature to determine which records policies, if any, are applied to a particular object. Use the Applied Retention feature to determine which retention policies, if any, are applied to a particular object. These options when you select an object, that is policy managed or not, are available on the View menu or when you right-click the object.

Use the Record Policy Usages feature to determine which objects, if any, are governed by a particular record policy. Use the Retention Report feature to determine which objects, if any, are governed by a particular retention policy. The Record Policy Usages option, when you select a record policy, is also available on the View menu or when you right-click a record policy. The Retention Report option however, to view retention policy usages, is available on the Records menu.

5.2.2.13.3 About containment policies

A containment policy specifies rules for container objects such as cabinets and folders. The object placed in the container must meet all criteria of at least one rule to be accepted.

A containment policy applied to the parent container is inherited by its children. Each containment rule defines the object type (Child Type) that can be placed in the managed container (Parent Type), the allowable number of links the Child Type can have to another policy managed object, and the allowable number of levels of additional folders a folder object can contain.

Each containment policy can have more than one containment rule. Only those rules in a containment policy that are enabled will be evaluated. In the case where there are conflicting rules (same parent and child types but different link and level values) among the applied containment policies in a managed container, the most restrictive value is taken.

 **Note:** Containment policies grandfather existing objects meaning that if existing objects do not match the containment policy that is being applied, the policy comes into effect for future objects placed into the container.

A containment policy applied to a container must be *enabled* with the appropriate rule before an object can be evaluated for placement in the managed container. *Nothing can be put in a folder if the applied containment policy does not have any rules enabled.* Applying a containment policy to a cabinet of the dm_cabinet type that is composed of the following sample list of rules for example, means that you can create or add a container that matches the Parent Type specified. No other container types would be permitted, only those that are listed and enabled *True*. The objects that the parent container can contain is limited to the Child Type specified. Though you can specify only one Child Type per Parent Type added, you would need to add the same Parent Type again to associate the same container object to more than one Child Type. The dmc_rm_formal_rec_folder specified three times for the Parent Type, for example, can contain three different types of records specified for the Child Type.

Rules in the containment policies that are *most restrictive* are used where more than one containment policy specifies the same parent and child rule, but conflicting rules for the number of links and levels specified. For example, if the following two containment policies are enabled:

In policy A, a rule specifies: dm_folder for the parent, dm_folder for the child, and a restriction or limitation to 2 links and 5 levels.

In policy B, a rule specifies: dm_folder for the parent, dm_folder for the child, and a restriction or limitation to 1 link and 6 levels.

The applicable rule in this case uses: dm_folder, dm_folder, limited to 1 link and 5 levels.

 **Note:** If you specify 0 for the level when the parent and the child are of the same type it means you can add an unlimited number of levels. If the parent

and child types are different, 0 is specified by default, meaning not applicable, and no levels can be specified.

Containment policies that do not match for a specific rule are merged. For example, if containment policy A states that dm_documents are allowed in a folder, B states that dmc_rm_formal records are allowed in a folder, you get both, so folders can contain documents and other folders.

The link limit indicates the number of folders that can link to this object.

5.2.2.13.4 About security policies

Although a security policy defines the ACL that is being applied to the various objects defined in it, it also prevents the ownership of the managed object from being altered, or more specifically, prevents the Access Control List (ACL, object type is dm_acl) on the managed object from being directly manipulated.

Although a security policy applied alone to an object may be sufficient, you also have the option of applying additional layers of security (extended security) if needed. Restrictive markings, shared markings, and security levels act as a door; what you can do once you are in is determined by the ACL. In order to get past the door using restrictive markings, you have to be in all restrictive marking groups. In order to get past the door using shared markings, you only have to be in one shared marking group. Markings only look at group membership in the ACL (MACL). In order to get past the door using security levels, you only have to match or exceed the ranking specified. Further details are as follows:

- **Restrictive markings:** you must be a member of all groups listed in order to see the item. What you can do with the item is governed by the ACL. For example, an ACL that defines members in group A and group B, only those users that are members of both groups are provided access.

A user must be in *all* groups if more than one group is specified.

- **Shared markings:** you only need to be a member of one group to access the item - Again, the ACL determines what you can do with the item. For example, an ACL that defines members in group A and group B, all users in both groups are provided access.

A user must be in *at least one* group if more than one group is specified.

- **Security levels:** although similar to restrictive markings creates a hierarchy where group membership is automatically added to groups with a lower ranking.

A user must have a ranking *equal to or greater than* the value specified to access the object. A user must be a member of a particular security level to have access to the object. The security levels are ordered by a ranking that ranges from 0-99999. Security levels that have a higher ranking are considered members of security levels with lower rankings. Each security level must have a unique rank (number).

Members of a security level with a ranking greater than the ranking assigned to members of another security level are given access. For example: a security level named Secret is created with a ranking of 5000 and is applied to an object.

Anyone that is a member of this security level can access the object as well as anyone that is a member of another security level with a ranking equal to or greater than 5000. A member of a security level with a ranking that is less than 5000 is denied access to the object. If another security level is applied to the same object, the security level with the higher ranking is enforced. For example: another security level named Top Secret with a ranking of 10000 is applied; users with a ranking of 5000 are now denied access to the object, only users with a ranking equal to or greater than 10000 can access the object. Also, the security level specified supersedes the ACL of the security policy.

These additional layers extend security and override (trump) permissions defined in the ACL of the security policy they are associated with.



Note: Permissions defined by more than one security type applied to the same object will resolve to one permission set. If you apply two security policies to an object (or apply all security types, general permissions, Restrictive Markings, Shared Markings, Security Levels), the ACLs in each policy are combined to provide a new ACL enforcing the most restrictive rules. For example: security policy A specifies Delete and security policy B specifies Write, the new ACL will specify Write as it is more restrictive than Delete.

A security policy sets the access rights upon the policy managed objects to which it is applied. These access rights include:

- Changing ownership of the security policy managed object to the Records Manager system group.
- Removing the group permit or changing it to an appropriate Records Manager system group to allow for administration of managed objects.
- Removing world permit on the managed object means setting the default world permission to NONE (cannot search object, cannot find object).
- The dm_acl that is applied to the managed object.
- Linking objects into a policy managed dm_folder.

Basic Permissions are on a security policy-object type basis. When an object type is added to a security policy, the permissions for that object type are stored on a dm_acl object that is related to the security policy.

The basic permissions are values that can be assigned in the Permissions for Groups and Individuals: and the Restrictions for Groups and Individuals portion of the permission set.

All basic permissions are exposed, all extended permissions are exposed except for change permission and change owner.

The application-specific permissions of create, link child and unlink child have been added. These represent the rights of a user to link (add an object to a container) or unlink a child object (remove an object from a container) to an object of this type, or to create or add the objects of this type in policy controlled situations with this Security Policy applied to it (inherited or direct).

Providing additional layers of security

You need to create a security policy and any extended layer of security before you can apply it. *A group is created transparently when you create a restrictive marking, shared marking, or security level. The group however, is created without any members. You need to follow separate procedures to add members.*



Notes

- Normally, if a document is under a security policy or under a restrictive marking, shared marking, or security level, we ask users not to add anything to the objects permission directly but rather to add them in the security policy or to remove the groups that represent a shared marking, restrictive marking, or security level. No access is provided if you grant extended security without any members defined (added). You can verify if any members have been added when you click the Properties icon of an object and select the Permissions tab. None specified is an indication of no members defined.
- All extended security, restrictive, attribute, and shared markings, including security levels, can be defined as either global or non-global depending on the checkbox setting for the World Selectable attribute. Globally defined extended security levels for example, are available to everyone if the checkbox is selected in which case you (and anyone else) do not have to be added as a member. Non-globally defined security levels are available to members only, that is if the checkbox is not selected. Users will not see a security level if they are not a member of its security level group. World Selectable means that when applying a security level, shared marking, restrictive marking, and/or attribute marking that all of them are available to be applied to the object. If you apply a marking to which you are not a member of, the object will no longer be accessible once the screen is refreshed as the marking will take effect. If you want to change this behavior so that when applying a marking only those to which you are a member of the group are visible then deselect the option World Selectable.

Restrictive Markings and Attribute Markings

Use Restrictive Markings to extend security on the object to which it is applied. The person accessing the object to which the Restrictive Markings is applied must be a member of all groups if more than one group is specified.

The Restrictive Markings feature is similar to the Supplemental Markings feature in that users must be members of all groups if more than one group is specified. Attribute Markings are set from the metadata form for the Department of Defense Standard, Classified, and email record types. Restrictive Markings however, are available as yet another more *general* mechanism to control access that is not tied to the metadata of the object, as they are applied externally.

Restrictive markings are modeled as a controlled set of dm_group objects. Because the dm_group type itself cannot be subtyped, a dm_relation subtype (dmc_rm_group_suppmark_rel_type) is used to mark the dm_group objects as

having been defined as a restrictive marking. Such a group should be used for no other purposes in the repository.

Restrictive markings are used to indicate that the protected dm_sysobject cannot be accessed by anyone who is not a member of every restrictive marking.

The selected set of restrictive markings (dm_group) are put into the Required Groups section of every dm_acl associated with the restrictive marking.

Shared Markings

Use Shared Markings to extend security on the object to which it is applied. The person accessing the object to which a Shared Marking is applied must be a member of at least one group if more than one group is specified.

The Shared Markings feature is also a *general* mechanism (not specific to any Department of Defense requirements) somewhat like the Restrictive Marking but instead of the user being a member of all groups, the user must be a member of at least one group if more than one group is specified.

Shared markings are modeled as a controlled set of dm_group objects. Because the dm_group type itself cannot be subtyped, a dm_relation subtype (dmc_rm_group_sharedmark_rel_type) is used to mark the dm_group objects as having been defined as a shared marking. Such a group should be used for no other purposes in the repository.

Shared markings are used to indicate that the protected dm_sysobject cannot be accessed by anyone who is not a member of at least one of the groups added.

The selected set of shared markings (dm_group) are put into the Required Group Set section of every dm_acl associated with the shared marking.

Security Levels

Use Security Levels to extend security on the object to which it is applied. You must specify one ranking (one number), from 0-99999, for each Security Level created and you can create as many Security Levels as needed. Although you can apply different ones, the highest ranking number (most restrictive) is enforced. For example, you can create 3 Security Levels, one instance with a ranking of say 500 named Top Secret, another with 400 named Secret, and a third with 300 named Protected. All members subsequently added to these Security Levels are given access to the object to which they are applied. Users must be a member of the group that has an equal or higher security level than what is applied to the object. Security levels work with the level number. As long as you are in a group that has a higher level or equal level to the applied security level on the object, then you can access the object. If the user is member of a group that has a lower number than the security level that is applied to the object, access to that object is denied.

Security levels are modeled as a controlled set of dm_group objects. Because the dm_group type itself cannot be subtyped, a dm_relation subtype (dmc_rm_group_secllevel_rel_type) is used to mark the dm_group objects as having

been defined as a security level. Such a group should be used for no other purposes in the repository.

Security levels are used to indicate that the protected dm_sysobject cannot be accessed by anyone who is not a member of that security level or is a member of a lower security level.

Security levels with higher rankings are nested automatically in those with lower rankings.

The selected security level (dm_group) is put into the Required Groups section of every dm_acl associated with the security level.

5.2.2.13.5 About naming policies

Naming policies govern creation and naming of folders that constitute a file plan and they also filter placement of objects in the folders according to a specific naming pattern. Although you can create a file plan without a naming policy, naming policies enforce creation and labeling of a uniform file plan. There are two rules in a naming policy:

- Mask rule

Used for validation of an attribute against a defined pattern.

- Construct rule

Used to set an attribute based on an attribute from its parent and (optionally) an attribute defined on the object.

Construct rule applies for the object if parent and target attributes are of string type. Construct rule is violated if target attribute is given as non string type or the attribute does not exist. If the construct rule is created by specifying the parent attribute as Date type and not a string type, the object cannot be created for document or object.



Note: The construct rule should not be confused with the dmc_rm_attribute_copy_rule. The dmc_rm_attribute_copy_rule affects inheritance and is further discussed in “[Declaring electronic or physical documents as formal records](#)” on page 340.

You can specify one or the other or both.

About mask rules

The documents or objects put into those folders must match the naming pattern determined by the mask rule.

The mask rule uses two attributes:

- **Attribute Name**

Indicates which object attribute is to be validated.

- **Mask Pattern**

Indicates the naming pattern that must be matched.

[“Valid mask patterns” on page 369](#) lists all the valid patterns.

Table 5-16: Valid mask patterns

Mask	Description
%YYYY	Represents a 4-digit year. For example, 2010.
%YY	Represents a 2-digit year. For example, 10.
%MM	Represents a 2-digit month, values between 01-12. For example, 03 represents March, whereas 3 is not valid.
%DD	Represents a 2-digit day, values between 01-31. Must be 2 digits with a leading 0 for days 1-9.
%N	Represents one digit. Valid values are between 0-9. For example, 3 would match this mask.
#N	Represents any number. For example both 3 and 33 would match this example.
%X	Represents one character that is not numeric. For example, a-z, A-Z. Dashes and special characters are not valid.
#X	Represents any string. This pattern matches until a non-alphabetic character is encountered.

These mask patterns can be combined to create complex masks. Mask patterns can be 1-32 characters including the percentage symbol.

[“Mask pattern examples” on page 369](#) lists some examples.

Table 5-17: Mask pattern examples

Mask	Valid values	Invalid values	Notes
%YYYY-%MM-%DD	2010-03-15 1990-01-01	2010-15-03 2010 03 15 2010/03/15	Characters in between mask patterns must also be matched.
%N%N%N	123 012 999	1 12 a1 9999	This mask represents a 3-digit number.

Mask	Valid values	Invalid values	Notes
%N%N%N%N %N%N%N%N %N %N%N%N	1111 2222 3333 4444	x, 112, 111122223333444	This mask could represent a credit card number (4 sets of 4-digit numbers separated by spaces).
#X #X	John Doe	Steve 1X SteveS 1Steve John L Doe	This mask represents a non-numeric string followed by another non-numeric string.
%N%X%N #N #X	5c3 123 Hi 0A2 3 See	c14 123 XYZ 4T1 667 5c3 ABC	This pattern is looking for a number followed by a non-numeric character followed by a number, then a space, and then a number and then a string.

The mask rule, for example, could say you must specify a name that is a 4-digit year so that the folder is labeled with a 4-digit number. An attempt to enter anything other than a 4-digit number generates an error message. It could ask that you specify a name, say Fiscal, followed by a 2-digit year, in which case Fiscal plus a 2-digit number must be entered; anything else generates an error.

About construction rules

Construction rules allow an attribute to be calculated based on an attribute on its parent folder and another attribute on the object. This mechanism allows the ability to have a hierarchy structure to be stored in a string attribute.

The construct rule has 6 different values that can be set:

- Rule Object Type

If the object's type matches this rule then it will be acted on.

- Enable

If deselected, the rule is ignored (useful for testing your rules). Enabled by default.

- Parent Source Attribute

Indicates which attribute is used for parent source. If the parent folder does not have this attribute, it will not be copied (nor will the separator).

- Self Source Attribute

Indicates which attribute is used for self source. This attribute must be defined on the object type selected and must be a string. This attribute can be blank in

which case the value from the parent will be copied into the attribute that is being calculated.

- Separator

Indicates what kind of separator will be used. This can be blank.

- Target Attribute

Indicates which attribute will store the value. This is expected to be a repeating string and should be big enough to store the calculated value.

[“Example set of construction rules” on page 371](#) gives an example of how to create a set of construction rules.

Table 5-18: Example set of construction rules

Object type	Parent source attribute	Self source attribute	Separator	Target attribute	Notes
dmc_rm_dod 5015v3_cabinet	category_identifier	object_name	-	category_identifier	On a cabinet, effectively this rule copies the object_name to the category identifier any time the object name of the cabinet is changed.
dmc_rm_dod 5015v3_folder	category_identifier	object_name	-	category_identifier	If the folder is nested, take the parent's attribute and the object name to fill in the category identifier.
dmc_rm_dod 5015v3_std_rec	category_identifier			category_identifier	For the record, just make the category identifier the same as the parent folder's value.

The construct rule, for example, constructs a breadcrumb (file plan) so that the location of each folder in the file plan is known in relation to the root folder of the file plan. The parent_source_attrib could be any one of a number of attributes

associated with the parent, such as the title attribute or subject attribute to name a few. A delimiter is added based on the value that is specified for the separator. You can use any value for the separator, preferably a dash or, forward slash common to most breadcrumbs. The self_source_attrib looks for the value specified in the immediate folder below the parent and stores the value as the target_attrib. It is best to specify the same value for both the parent_source_attrib and the self_source_attrib to be consistent. For example, specify the title attribute for both so that the breadcrumb consistently specifies a title and not a title and a subject.

The rule type indicates order/priority of rule application. The mask rule is executed first followed by the Construct rule. You can specify as many rules as needed, only the rule that provides the closest match is executed. If the closest match to the mask rule cannot be found, no execution is performed and the construct rules are ignored.



Note: Due to the effects of cascading, you need to be concerned with which folder in the hierarchy you apply a naming policy to. For example, a policy is inherited by all folders in all branches of the hierarchy if you apply the policy to the root folder. If you apply it to the base folder of a branch, all the folders in the branch inherit the naming policy. If you apply it to the middle folder of a branch, only the folders in the branch under the middle folder inherit the naming policy. There are no other folders to inherit if you apply it to the last folder of a branch. Avoid applying multiple naming policies that affect the same type of objects.

Applying a naming policy to existing objects does not execute the Mask rule. The folder is grandfathered and only the next folder created is affected. For example, a mask rule that states YYYY that is applied to a cabinet that does not have YYYY in the name, would only apply going forward, in which case the next folder that is created under the cabinet would need YYYY.

Currently, you can:

- Apply a naming policy to a target object.
- Remove a naming policy from a target object.

Naming policies can be removed from managed objects. If a construction rule changed a value for an attribute, the attribute will not be reset to the value it was before the naming policy changed the value.

5.2.2.14 Records Manager system configuration options settings

There is a system configuration switch to turn mandatory retention on managed folders on or off. Selecting the checkbox for this option turns mandatory folder retention *on* so no one can declare formal records to any managed folder in a file plan unless each managed folder has a retention policy applied. All file plans in the repository require retention if you turn the configuration switch on! Deselecting the checkbox turns mandatory retention *off* to allow declaring formal records to managed folders with or without retention.



Note: Managed folders are invalid locations for formal records with this configuration switch turned on, only until a retention policy is applied or the configuration switch is turned off.

To set any of the Records Manager system configuration options:

1. Navigate to **Cabinets > System > Applications > RmConfig > RM DocbaseConfig**.
Set the filter in the upper right corner to **Show All Objects and Versions** if you see **No items found**.
rm_docbase_config is displayed.
2. Select *rm_docbase_config* in the content pane and click **View > Properties > Info** or right-click to select **Properties**.
The **Properties** screen appears displaying the **Info** tab.
3. Change the value for the attribute you want to affect. Each attribute is described in "[Records Manager System Configuration Options](#)" on page 374.

Table 5-19: Records Manager System Configuration Options

Options	Description
Declassification Threshold	<p>Only applicable if the Department of Defense classified dar file is installed. For a classified record it is possible to set the Declassify On field to Auto Calculated Date. The declassification date for classified records that have this setting will be the date the record was declared plus the declassification threshold which is in years. If this value is changed, the new value will be used when declaring new classified records. If you want this change to affect existing classified records, as a security officer (dmc_rm_security_officer) choose Records > Recalculate Auto Declassify On Date.</p> <p>A message at the bottom of the content pane will be displayed indicating the number of classified records that were updated, for example: Updated Auto Declassify On Date for 0 classified records.</p> <p>Only classified records that the security officer has permission to see (however they do not need write permission on the classified records).</p>
Retention mandatory on folder to declare Formal Record	<p>If the checkbox is selected when declaring a formal record the file plan location must have a retention policy applied. If not selected at least one policy must be applied to the folder.</p>
Working Paper Aging Period	<p>The destroy working paper job will wait this number of days before the job destroys the document. The starting point is the date the document was designated as working paper. If the working paper is put under retention or hold/permanent, the job will not delete the working paper until all retention is removed (including holds and retention policies).</p>

Options	Description
Source Email Type For Filing Email Records	The value set for this attribute decides the object type of the source email message that is imported into the repository either while declaring a Department of Defense Email Record using Records Activator for Microsoft Outlook client or while recreating Department of Defense Email records by importing XMLs in Department of Defense schema. The set of valid values for this attribute include dm_email_message and its subtypes. The default value for this attribute is dm_email_message.

4. Click **OK** to accept changes and close the **Properties** screen.

5.2.2.15 Containment policies

5.2.2.15.1 Creating a containment policy

For an overview of containment policies, rules, inheritance, and the file plan, refer to “[About containment policies](#)” on page 363.

New containment policies and the rules specified for a containment policy are all enabled by default, unless you explicitly disable them upon creation or at a later time from the Properties of the containment policy (or any policy for that matter). You can pick and choose which rules you want to have enabled or disabled. Policies however cannot be applied once it is disabled. Although a policy can no longer be applied once it is disabled, enforcement of the policy continues against those objects to which it has already been applied.

Containment is determined based on the sum of the policies if more than one containment policy is applied.



Note: In case of email message with attachments, some additional rules are required to allow the attachments folder and its contents (that is, email attachments) to get linked/moved/copied into container on which containment policy is applied. For more details, see “[Creating containment policy rules for emails with attachments](#)” on page 378.

To create a containment policy:

1. Navigate to **Records Manager > Containment Policies**.
2. Click **File > New > Containment Policy**. Make sure no containment policies are selected in the content pane.
The **New Containment Policy** screen is displayed and enabled by default.
3. Type a name in the **Name** field, for example: Formal Folders Only.

4. Optionally, type a description in the **Description** field to give it some significant meaning.
5. The checkbox next to **Enabled** is selected by default. Although the policy can no longer be applied once it is disabled, enforcement of the policy continues against those objects to which it has already been applied.
6. Click **Add** to create a containment rule. One or more rules can be created as necessary.

If you click **Finish** now, the New Containment Policy screen closes and the new containment policy, although empty, is displayed without any rules in the content pane. You can specify rules later in the Properties of the containment policy. The operation is aborted if you click **Cancel**.

The **New Containment Rule** screen is displayed and the rule is enabled by default.



Note: If the **Parent Object Type** and the **Child Object Type** selected are the *same*, the screen is updated to include two fields, one for the **Number of Links** and one for the **Number of Levels**.

7. Select the **Parent Object Type** from the list box.
For every parent container type selected, you are specifying by selecting a particular child type what is allowed to be included in the parent. In the example above, this means that a dm_folder can contain another dm_folder.
8. Select the **Child Object Type** from the list box.
It is specific to the type added and subtypes are not included.
9. Type a value to indicate the **Number of Links** allowed to other containers in the file plan; 0 implies an unlimited number of links.
Number of links means the number of times the child object can be linked into a container.
10. Type a value to indicate the **Number of Levels** if this field is available; 0 implies an unlimited number of levels.
Levels determine the number of consecutive containers that a hierarchy can contain of the same container type (for example, dm_folder). The option to set the number of levels is only available if the parent and child object types are the same. For example, assume a simple containment policy that has two rules as defined in “Containment policy example rules” on page 376.

Table 5-20: Containment policy example rules

Parent object type	Child object type	Number of links	Number of levels
dm_folder	dm_folder		3
dm_folder	dm_document	1	

The folder to which the containment policy is applied counts as a level, level 1. Adding a sub folder (dm_folder) to level 1 counts as level 2. Adding another

sub folder (dm_folder) to level 2 counts as level 3. An attempt to add a fourth sub folder is prevented.

```
Folder (level 1)
    Folder (level 2)
        Folder (level 3)
```

Containment policies grandfather existing objects, meaning that if existing objects do not match the containment policy that is being applied, the policy comes into effect for future objects placed into the container.

11. Optionally, although it is enabled by default, you can disable the rule if necessary, now or at a later time from its Properties, by deselecting the checkbox next to **Enable**.

You have now completed the fields for the attributes that define the first rule of this policy.

12. Click **OK** to accept and create the new rule.

If you click **Cancel**, entries are ignored and you are returned to the **New Containment Policy** screen to try again by clicking **Add**. You can also choose **Cancel** to abort.

The new rule is now displayed in the **New Containment Policy** screen.

This containment policy in the following example allows dm_folders to contain dm_folders only. If you tried for instance to place a dm_document into a folder with this containment policy applied you would not be able to do so as there is no rule that allows this.

13. Click **Add** to add another rule below the one already listed or, click **Finish** if you do not need to add any more rules. You can repeat adding rules as many times as needed before you click **Finish**. You can also select the checkbox next to a particular rule in the listing and click **Remove** if it is not needed.

The containment policy defined is displayed in the content pane of the Records Client user interface.



Note: The new containment policy may or may not be displayed if the two filters in the upper right-hand corner do not have the correct options selected. The two options for filtering are **Enabled Containment Policies** and **All Containment Policies**. You can choose to display only containment policies that are enabled **True** or both enabled and disabled by selecting the **All Containment Policies** filter. **Show Items, 10, 50, or 100** indicates how many items will be shown at a time in the list.

5.2.2.15.2 Creating containment policy rules for emails with attachments

The message archive emails with attachments have a hidden attachments folder associated with them. If the containment policy applied on the container into which the email message is being linked or moved or copied, contains rules only for dm_message_archive type or its subtypes, but not for the hidden attachments folder and/or its contents, then the containment policy does not allow the message archive emails with attachments to be linked into the container to which it is applied. Thus additional containment rules are necessary to allow the hidden attachments folder and its contents to also get linked or copied or moved into the container following the message archive email. These rules prevent blocking of the hidden attachments folder and/or its contents, and an error from occurring when a message archive email with an attachment is moved or linked or copied into the container with a containment policy applied on it. These additional rules are also applicable for the new emails with attachments during the following operations:

- While they are being imported into a container for which containment policy is applied with attachment extraction being enabled in mailapp.properties.
- While they are being moved or copied or linked into a container on which containment policy is applied.
- While declaring a Department of Defense email record through Records Activator for Microsoft Outlook client with the container, wherein the source email messages are added, having a containment policy applied on it.



Note: The new email messages are imported into the repository as objects of dm_document type or its subtypes, and not as dm_message_archive type (or any of its subtypes). Thus, the old containment rules (if any) defined for dm_message_archive type or its subtypes will not be applicable for these new email messages imported in .msg format. They are applicable for existing email messages of dm_message_archive type or its subtypes.

The new email messages imported into the repository in .msg format will either require a separate rule with child type as dm_document type (if not already defined) in the containment policy or these messages will have to be imported into repository as an object of a specific subtype/customtype of dm_document, and then a containment rule can be defined specifically for that subtype of dm_document. While declaring Department of Defense email records using Records Activator for Microsoft Outlook Client, the source email messages are imported into the destination directory as objects of dm_email_message or its subtypes. Therefore, in such cases, if a containment policy is applied on the destination directory where the source email message is going to be imported while declaring of email record, the containment policy will require an additional rule with child type as dm_email_message or its subtype selected for 'Source Email Type for Filing Email Record' attribute in Records Manager Docbase Configuration.

For moving/linking/copying an email message with attachments into a container (such as cabinet or folder) with a containment policy applied on it, requires the following rules:

- To allow the email message to get linked into the container, it requires a containment rule with parent type as container's object type and the child type as the object type of the email message
- To allow the attachment folder to get linked into the container, it requires a containment rule with parent type as the container's object type and the child type as the object type of the attachments folder.
- For the non-email type of attachments, it requires a containment rule with parent type as the object type of the attachments folder and the child type as the object type of the non-email attachments.
- For the nested/embedded email attachments present inside the attachments folder, it requires a containment rule with parent type as the object type of the attachments folder and the child type as the object type of the email message being linked into the container.

Emails with attachments that are moved into a container object such as a cabinet or a folder, require 2 rules to be defined (added) for successful containment. One rule for the email message itself and one rule for the attachment.

Follow the instructions in [“Creating a containment policy” on page 375](#). An example for creating the additional rule with `dm_attachments_folder` specified as the Child Type. If emails with attachments are moved to cabinets, select *Cabinet (dm_cabinet)* for the Parent Object Type from the list box on the **New Containment Rule** dialog.

5.2.2.15.3 Applying a containment policy

More than one containment policy can be applied to an object. The same containment policy however, cannot be applied to the same object more than once. The containment policy that was already selected and applied to an object will not be listed again for the same object if another containment policy is applied to it. The locator will not display the policy again for the same object. Only those policies that are not applied to the selected object will appear. Also note that only enabled policies will be available in the list. You can apply containment policies to container objects only, not to documents for example.

To apply a containment policy:

1. Navigate to a cabinet or folder, or formal cabinet or formal folder, so that it is displayed in the content pane where it can be selected.
You can apply a policy to an object that is not a managed object or one that is already managed. A managed object has at least one policy applied.
2. Select the desired object in the content pane and click **Records > Apply Record Policies** to apply a containment policy from the menu options or, right-click to select the same option.
The **Choose Record Policies** screen is displayed.
3. Select one or more policies you want to apply and click the **Add** button to add your selection to the content pane. Shift adds all of them between the first one

selected and the last one. The control key allows you to select non-contiguous items from the list.

4. Click **OK** to apply the selected policies.

5.2.2.15.4 Viewing applied policies

The procedure in this section demonstrates how to view policies on an object. You can see the different policies and how many of each are applied to the object selected for viewing.

The procedure used to view any applied policy or any applied extended security is essentially the same, with the exception of retention policies covered under Retention Policy Services. This includes:

- Containment policies
- Naming policies
- Retention policies
- Security policies
- Restrictive markings
- Shared markings
- Security levels

A separate procedure follows for viewing attribute markings applied to formal records.

To view applied policies:

1. Navigate to the managed object, parent or child object, typically a cabinet, folder, or content of a container object, so that it is displayed in the content pane. Managed objects can include physical objects as well.
2. Select the managed object in the content pane and click **View > Applied Record Policies** from the menu options or, right-click to select the same option. Otherwise, click **View > Applied Retention** to view retention policies.
All policies applied to the selected object, if there are any, are listed in the content pane.

To view the attribute markings for a particular record:

This procedure is restricted to records managers and Records Manager privileged users.

You can view an attribute marking applied to a formal record by selecting it and choosing the Attribute Markings tab from the Manage Record Security option under the Records menu. Alternatively, you may view the Properties of a formal record to see which markings have been applied:

1. Navigate to a formal record.
 2. Select the formal record listed in the content pane and click **Records > Manage Record Security** or right-click the formal record to select the same option.
- The **Manage Record Security** screen is displayed consisting of five tabs.
3. Select the **Attribute Markings** tab. Attribute markings listed, whether inherited or applied directly, are read-only. You can click the Name at the top of either list to present the list in either ascending or descending order.
 4. Click **Cancel**.



Note: Restrictive markings can only be viewed from this menu. To remove them go to the Properties of the formal record.

5.2.2.15.5 Removing applied policies

Four procedures are provided for removing policies:

- The procedure used to remove either a containment policy or a naming policy is the same and belongs to Records Manager functionality.
- The procedure used to remove security policies, restrictive markings, shared markings, and security levels is the same and belongs to Records Manager functionality.



Note: Removing a security policy is not done from the **Applied Record Policies** menu, it is instead done only from the **Manage Record Security** menu.

- The procedure used to remove attribute markings belongs to Records Manager functionality.
- The procedure used to remove a retention policy is unique and belongs to Retention Policy Services. For more information on this topic, refer to Removing an applied retention policy in the part of this document (or, in online help) that covers Retention Policy Services.

To remove a containment policy or a naming policy:

Use **View > Applied Record Policies** to remove containment policies or naming policies.

1. Navigate to the managed object, parent or child object that has the policy applied directly to it, typically a cabinet or folder, so that it is displayed in the content pane. Managed objects could include physical objects as well.
2. Select the managed object in the content pane and click **View > Applied Record Policies** from the menu options or, right-click to select the same option.

All containment policies and/or naming policies applied to the selected object are displayed in the content pane.

3. Select the containment policy or the naming policy to be removed and click **Records > Remove Applied Policies** from the menu options or, right-click to select the same option.

A confirmation screen is displayed asking you to confirm removing the selected containment policy or naming policy.

4. Click **OK** to confirm.

The selected containment policy or naming policy is no longer displayed in the content pane for the selected object.

The following procedure is restricted to records managers and Records Manager privileged users.

Use Records > Manage Record Security to remove security policies, security levels, restrictive markings, and shared markings. Only directly applied policies can be removed. Anything inherited cannot be removed as the menu shows Inherited (View Only). Attribute markings however, cannot be removed according to this procedure using the Manage Record Security screen.



Note: Although security levels can be applied directly to the object or applied using the metadata, only security levels that are applied directly (outside of the metadata) can be removed from this menu. To change a security level on a classified record for example, select its Properties page and change it there.

To remove a security policy or any extended security marking including security levels:

1. Navigate to the managed object, parent or child object, typically a cabinet, folder, or content of a container object, so that it is displayed in the content pane; managed objects could include physical objects as well.
2. Select the managed object in the content pane and click **Records > Manage Record Security** from the menu options or, right-click to select the same option.

The **Manage Record Security** screen is displayed with the following tabs:

- Security Policies
- Security Levels
- Restrictive Markings
- Shared Markings
- Attribute Markings

Each tab reveals two possible lists of what is applied by inheritance and what is applied directly to the selected object. Objects listed in the field labeled **Inherited** are for **View Only**. Objects listed under the field labeled **Direct** are eligible for removal. Use the **Direct** field to **Remove** an object from the list of directly applied objects.

Direct (View only) occurs when you are looking at a security level that was applied using the metadata, instead of applied directly. In such cases navigate

to the Properties of the object (such as a classified record) and change it from there.



Note: The option to **Remove** is not displayed unless at least one item is listed and selected.

3. Select the tab associated with the security type to be removed.
4. Select the security items in the list that were applied directly, listed under the **Direct** field.

The option to **Remove** is revealed when one or more security items are selected.

5. Click **Remove**.

A confirmation screen is displayed asking you to confirm removing the selected security item.

6. Click **OK** to confirm removing the selected security item.
7. Click **Finish** to complete the action.

Unlike other security options which use the Manage Record Security screen, attribute markings are removed on the same form used to add the attribute markings when the formal record was declared. Attribute markings can be removed at any time, during creation or afterwards.

To remove an attribute marking:

1. Navigate to the formal record, a standard or classified record for example, so that it is displayed in the content pane.
2. Select the formal record listed in the content pane and click **View > Properties** from the menu options or, right-click to select the same option.
3. Scroll down the form to the **Project Name** (or **Supplemental Marking**) multiple selection list box.
4. Select the item in the applicable **Selected** list box and move it back to the **Available** list box to remove it.
5. Click **OK** to complete the action.

5.2.2.15.6 Deleting policies and attribute markings

The procedure used to delete a policy or any extended security is essentially the same, with the exception of attribute markings. This includes:

- Containment policies
- Naming policies
- Retention policies
- Security policies
- Restrictive markings
- Shared markings
- Security levels
- Attribute marking sets

The procedure used to delete attribute markings is provided separately at the end of this section.

You cannot delete a policy that is currently applied to an object. The policy must not be in use to be deleted. If a policy is applied to many objects, you must remove it from all objects before deleting it. Security policies applied to various objects for example, must be removed all those objects first, before the security policy can be deleted.

To delete any policy (except attribute markings):

1. Navigate to **Records Manager** to delete a containment policy, security policy, naming policy, or attribute marking set. Or, navigate to **Retention Policy Services** to delete a retention policy.
 2. Select the node, in the navigation pane, consistent with the policy to be deleted.
- There are 2 filters, as shown [Figure 5-2](#), Enabled and All which includes disabled polices as well.

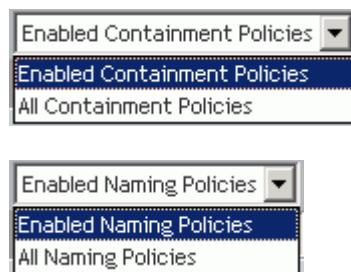


Figure 5-2: Filter options indicate the name of the selected policy

3. Select one or more of the policies listed in the content pane and click **File > Delete** from the menu options or, right-click to select the same option.

A confirmation message is displayed if the selected policies are not in use. The policy in this instance is deleted when you click **Yes** or, the operation is aborted when you click **No** to this message. The list in the content pane is refreshed to no longer display the selected policies when you click **Yes**.

A warning message however, is displayed if the selected policy is applied and still in use. The operation in this instance is aborted when you click **Close**.

To delete an attribute marking:

An attribute marking is deleted when it is removed from the attribute marking set it belongs to.

1. Navigate to **Records Manager > Attribute Marking Sets**.
2. Select the attribute marking set in the content pane and click **View > Properties > Info** from the menu options or, right-click to select **Properties**.
3. Select the attribute marking from the list and click **Remove**.
4. Click **OK** to complete the action.

5.2.2.16 Naming policies

5.2.2.16.1 Creating a naming policy

A naming policy controls the naming of a file plan according to a predefined pattern to create a uniform structure.

For an overview of naming policies and rules, refer to “[About naming policies](#)” on page 368. Naming policies, like all other policies, applied to a file plan, cascade down the file plan structure from the point of application to be inherited by all the objects below the point of application.

New naming policies and the rules specified for a naming policy are all enabled by default, unless you explicitly disable them upon creation or at a later time from the Properties of the naming policy (or any policy for that matter). You can also pick and choose which rules you want to have enabled or disabled. Policies cannot be applied once it is disabled. Although a policy can no longer be applied once it is disabled, enforcement of the policy continues against those objects to which it has already been applied.

To create a naming policy:

1. Navigate to **Records Manager > Naming Policies**.
2. Click **File > New > Naming Policy**. Make sure no naming policies are selected in the content pane.
The **New Naming Policy** screen is displayed and enabled by default.
3. Type a unique name for the mandatory **Name** to distinguish it from other naming policies.

Entries for all remaining fields can be completed at a later time using **Properties** for the naming policy in question.

4. Follow the remaining steps to provide entries for the rules now or at a later time from its Properties or, click **Finish** to create the naming policy.

You can create any policy without rules and disable the policy, deselect the checkbox for **Enabled**, until rules are specified. The **Description** could be used to explain what the naming policy is intended for or why it is needed.

5. Click **Add** to create a mask rule. You can create one or more **Mask Rules** as needed. The values you provide to create each mask rule are used to ensure the object type specified is the only object type that can be created and named according to the pattern specified. The mask pattern specified as a string, is used as a template to ensure naming of objects, as they are created while growing the file plan, are named to match the pattern. Follow the substeps to complete the entries for the **New Mask Rule**. Creating a folder in a file plan for example, where the mask rule is enforced, and naming it differently from the expected mask pattern will not be permitted. An error message will guide you for the expected entry.



Note: You cannot add two mask rules that specify the same object type. Each mask rule added must have a unique object type. Although you can add more than one mask rule, adding a second mask rule that uses the *same* object type will overwrite the initial entry of the same object type.

- a. Select an object type from the list box for the **Rule Object Type**.

The object type selected could be a supertype, meaning all objects or subtypes belonging to the supertype are also selected. Only those object types specified, once the rule is enforced, are accepted as valid choices for creation and rejected if not named according to the mask pattern defined. Two subtypes of Sysobject (dm_sysobject) include dm_cabinet and dm_folder for example. You can narrow the rule to a subtype or broaden it to many subtypes by selecting a supertype.

- b. Deselect the checkbox for **Enabled** only if or when you want to disable the rule.

Once the mask rule is disabled, any object can be created and named without further validation.

- c. Type the raw form of the desired attribute for the **Attribute Name** to indicate which object type attribute is to be validated.

The attribute value provided for the **Attribute Name** is valid only if it belongs to the object type selected, represents a string value, and is not repeating. Use the following guidelines:

- Only the raw form, not the localized form, of the attribute provided for the value is acceptable, and it must be accurately spelled.

For example, Subject is the localized form whereas subject is its raw form. Include the under scores if any and do not change from lower case to upper case.

- Make sure to use an attribute associated with a string, CHAR<xx> for example, where: xx represents the string length.

Do not use any repeating attributes. Some character strings are repeating while others are not (single).

Attribute values, other than string based, such as Boolean, Time, Integer, and ID are not acceptable.

- Attribute values that begin with r_, i_, and a_ must not be used.
- Use attribute values that make sense, title and subject for example are good choices for dm_document selected as the **Rule Object Type**.

The recommended choices for the **Attribute Name** if you have Sysobject (dm_sysobject) selected for the **Rule Object Type** are *title*, *subject*, or *object_name*.

- d. Type a value for the **Mask Pattern** consistent with the following valid formats currently supported. Refer to “[About naming policies](#)” on page 368 for mask pattern examples:

- %YYYY means a 4-digit year
- %YY means a 2-digit year
- %MM means a 2-digit month
- %DD means a 2-digit day
- %N means any single digit number
- %X means any single alpha character, must be a non-numeric character
- #X means any variable string of alpha characters (string must be separated by a non-alpha character)
- #N means any variable string of numeric characters

These formats can be used individually or combined to create the desired string pattern for the value. Attempting to create a container object named according to a different pattern other than the pattern specified for the value will be rejected and similarly attempting to contain an object named otherwise would also be rejected.

- e. Click **OK** to complete the rule.

You can repeat these substeps to create additional mask rules if needed or you can add more at later time from the Properties of the naming policy.

6. Click **Add** to create a construct rule if so desired. You can create one or more **Construct Rules** as needed. The values you provide to create each construct rule are used to identify the location of objects relative to each other within a file plan. It makes it easier for example, to know where objects are relative to one another within a file plan as you navigate the structure or where they are relative to one another in search results. Follow the substeps to complete the entries for the **New Construct Rule**:

- a. Select an object type from the list box for the **Rule Object Type**.

The object type selected could be a supertype, meaning all objects or subtypes belonging to the supertype are also selected. Only those object types specified, once the rule is enforced, are accepted as valid choices for constructing a breadcrumb according to a common attribute of the parent and child which is defined as the source attribute typically the title or subject attribute. Two subtypes of Sysobject (dm_sysobject) include dm_cabinet and dm_folder for example. You can narrow the rule to a subtype or broaden it to many subtypes by using a supertype.

- b. Deselect the checkbox for **Enabled** only if or when you want to disable further applications of the rule.
- c. Type the name of an attribute, in its raw form, for the **Parent Source Attribute** which is used to identify the parent object relative to the child. The raw name is the system name, typically includes underscores and is all lowercase, used to identify an attribute not the actual name used to label it on a form, object_name for example is the raw form of the Name attribute wherever it is used.

Each folder in a file plan can be a parent or a child depending on which folder you are in or looking up the file plan from (except the last folder which can only be a child, until a folder is added to it). The value specified for this attribute is used to pick up the value specified for the parent and display it. Based on the current location in a file plan, the **Parent Source Attribute** is picked up from the folder above the current folder which is used to obtain the value displayed for the **Self Source Attribute**.
- d. Type the same value for the **Self Source Attribute** that was provided for the **Parent Source Attribute**. The value gathered for the attribute specified in this field is used to populate the attribute specified for the **Target Attribute**.

Although you can specify an attribute that is not the same, it is preferable to see consistency in the naming so that a folder named according to the value picked up for its Name attribute is displayed with the Name attribute of the parent or child folder as well. It is preferable for example, to have results displayed such as Folder A/Folder B using the title attribute for the parent and self instead of mixing them using a title and date attribute. You would want to use a common attribute, something displayed in the navigation pane for example, that identifies the objects displayed in a file plan hierarchy such as the title or subject attributes used to label the folder. It gives you a better idea of where Folder A and Folder B are in relation to one another within the file plan. Folder A/2007 could be the results displayed if you mix the entries, using a title and a date attribute for instance. You cannot know that Folder B, according to its date attribute, is the child to Folder A.

- e. Type any value for the **Separator**. Although any value is valid, the dash or forward slash is recommended and is most commonly used.
- f. Type the name of an attribute, one that is a repeating string, in the **Target Attribute** field. The rule will be ignored if the attribute specified is not one

that specifies a repeating string. Acceptable repeating attributes are keywords and authors of dm_sysobjects. Any repeating strings created for your own custom sub-type of a dm_sysobject is also acceptable. The attribute entered will be used to store the value of the **Self Source Attribute** found in the immediate folder below the parent folder.

- g. Click **OK** to complete the rule. The rules are displayed.

You can repeat these substeps to create additional construct rules if needed or you can add more at later time from the Properties of the naming policy.

7. Click **Finish** on the **New Naming Policy** screen to accept all entries, or click **Cancel** to abort and ignore all entries.

5.2.2.16.2 Applying a naming policy

To view a list of naming policies, click **Naming Policies** in the navigation pane under the **Records Manager** node.

To apply a naming policy:

1. Navigate to a cabinet or folder, or formal cabinet or formal folder, so that it is displayed in the content pane where it can be selected.
You can apply a policy to an object that is not a managed object or one that is already a managed object. A managed object has at least one policy applied.
2. Select the desired object in the content pane and click **Records > Apply Record Policies** to apply a naming policy from the menu options or, right-click to select the same option.

The **Choose Record Policies** screen is displayed.



Note: You cannot apply the same policy to an object more than once. The locator does not display the policy again for the same object. Only those policies that are not applied to the selected object appear. Also note, only enabled policies are available in the list.

3. Click the **Naming Policies** icon to list naming policies.
4. Select one or more policies you want to apply and click the **Add** button to add your selection to the content pane. Shift adds all of them between the first one selected and the last one. The control key allows you to select non-contiguous items from the list.
5. Click **OK** to apply the selected policies.

5.2.2.16.3 Viewing an applied naming policy

The procedure used to view any applied policy or any applied security markings is the same. “[Viewing applied policies](#)” on page 380 provides the procedure for this topic.

5.2.2.16.4 Removing an applied naming policy

The procedure used to remove a naming policy or containment policy is the same. “[Removing applied policies](#)” on page 381 provides the procedure for this topic.

5.2.2.16.5 Deleting a naming policy

The procedure used to delete a policy or any extended security is the same. “[Deleting policies and attribute markings](#)” on page 384 provides the procedure for this topic.

5.2.2.17 Security policies

5.2.2.17.1 Overview of security

Records Manager provides five options for security, referred to as record security:

- Security Policies
- Restrictive Markings
- Shared Markings
- Security Levels
- Attribute Markings

They can be viewed or added, from the respective tab using the Manage Record Security interface when you select an object and click Records > Manage Record Security. The page layout for each allows you to determine whether security, depending on which tab you select, was applied to an object directly or through inheritance. Although the page displayed against the first 4 tabs allows you to add additional security, Attribute Markings do not.



Note: Application of any record security will change the ACL on an object and change the owner of the object and possibly prevent further access or reduce their access level. For example, a Records Manager might apply a security level to a folder which cascades to a checked out object and consequently the lock owner cannot check in the file anymore. The person who had checked-out the object may no longer be able to see or access the object and will therefore have to contact the administrator to resolve the situation. A resolution could be that the administrator removes the security level and temporarily manually update the ACL to grant the user access, allow the checkin, and then re-apply the security level. Note that when all record security is removed from an object, the original ACL on the object is not restored and a default ACL is applied.

To retrieve the file and to have your file checked in:

1. Locate your checked out file on the machine where the user checked out the file. Typically, it will be in your home directory under the folder Documentum\Checkout\. For example, on Windows the directory is C:\Documents and Settings\<username>\Documentum\Checkout\.
2. If no one has permission to check in the file, either remove all record security including attribute markings and then manually change the ACL on the document or modify the security policy (if none, add one) and give the administrator at least Version permission. The administrator can then cancel checkout and checkin the file sent by the original lock owner.

Derived Security, further described in “[Derived security and attribute marking sets](#)” on page 356, is only available to the install owner. Derived security is view only. It is a calculated value and not something that you can add or remove.

You can apply a Security Policy to an object and apply additional layers of security if needed. The additional layers, below Security Policies, provide extended security.

You can apply, at will, one or more of these four items to an object as needed.

Of greatest importance is the procedure used to create a security policy.



Note: When you create a security policy you must create at least one mandatory Target Object Type: dm_sysobject, any other Target Object Type is optional. Note that dm_sysobject is required as it is the catch all for objects that are not specified!

Target object types other than dm_sysobject are optional. What you decide to specify depends on what types of objects you wish to control with the security policy! If you are not interested in formal folders then you do not need to specify it. You could simply specify dm_sysobject but this would mean that everything has the same security. You can be as granular as necessary by adding whatever object types are required. The following is an example of three target object types:

- The target object being declared as formal record, for example: dm_sysobject
- The target object container, for example: dmc_rm_formal_rec_folder
- The target object formal record, for example: dmc_rm_dod5015v3_std_rec

The security policy, once applied to an object, is enforced based on the *best match* against the types specified. The dm_sysobject must be specified as it sits at the top of the hierarchy. It is last to be compared, if nothing else below dm_sysobject (in the hierarchy tree, not the listing) matches.

The object types added must be defined as a basic permission in the security policy. Container type objects added must also have **Link** permissions selected from their Properties for each User/Group that is added. For example, right-click dmc_rm_formal_rec_folder and select **Properties**. On its Properties select the **Permissions** tab and click **Add**, under **Grant access to**, to choose a user/group. The **Set Access Permissions** screen for the selected user/group is displayed, once you click **OK** to accept the selected user/group. Scroll down to **Records Manager**

Permissions on the **Set Access Permissions** screen and select the checkbox for **Link** and then click **OK**. The rules that you are listing are for the creation of formal records. This is not mandatory for the security policy as they could be employing one for use with typical records. As well, the object type of the subtype must be defined as a basic permission (in the security policy) and the records manager permission, *create*, must be enabled for that user.



Note: If you have applied a restrictive marking, shared marking, or security level, follow procedures to Add Members before you apply a security policy. Otherwise, only retention managers will be able to see the items that have the security marking applied.

To link objects or unlink objects from a records managed folder, the following rules of basic OpenText Documentum CM security must be followed:

- If folder security is ON (which is the default), you must either have write permission on the folder or have the **CHANGE_FOLDER_LINKS** permission (**IDfACL.CHANGE_FOLDER_LINKS**).
 - In the case of a link, these permissions are required on the target folder
 - In the case of an unlink, these permissions are required on the source folder (the folder the object is leaving)
 - In the case of a move, these permissions are required on both the source and target folders
- If folder security is OFF, you need to only browse on the object
- If retention is applied to the folder, these additional constraints are added:
 - Linking into a retained folder requires you to be in the **dmc_rps_contributor** role (both docs and folder)
 - Unlinking or moving a folder from a retained folder requires you to be in the **dmc_rps_retentionmanager** role
 - Moving a document from a retained folder can be done by the following four different roles:
 - **dmc_rps_retentionmanager** (with no restrictions)
 - **dmc_rps_move_unretained_folder** (with no restrictions)
 - **dmc_rps_move_any_retain_folder** (with the restriction that the destination folder must have at least one retention policy applied)
 - **dmc_rps_move_same_retain_folder** (with the restriction that the destination folder must have all of the same retention policies applied (if the retention policy is applied more than once on the source folder, it only needs to be applied once on the destination folder))
- If records security (security policy) applied is applied to the folder, these additional constraints are added:

- If entering a folder with records security, the folder needs to have the Records Manager security application permit LINK
- If leaving a folder with records security, the folder needs to have the Records Manager security application permit UNLINK
- If entering a folder with record security, the security policy must define the Records Manager security application permit CREATE for the type of object. If there is no explicit rule for that type of object, the system will find a default rule (dm_sysobject must be defined as a rule for any security policy that is the default)

5.2.2.17.2 Creating security policy

For an overview of security policy rules, refer to “[About security policies](#)” on page 364.



Note: A group or user added to a security policy also needs to be added to the Security User role if their permission is set to WRITE, DELETE, create, link, or unlink. A user for example, in the role also needs to be added to the Security User role to perform actions according to these permissions. Refer to “[Records Manager roles and functional access](#)” on page 316 to see the list of other roles that are automatically included in the Security User role.

A security policy will change the ACL of any sysobject to which it is applied. Each security policy created must have at least *dm_sysobject* added as a basic permission in the list of object types. It will be used as the matching rule if no other rules are added and is therefore mandatory.

To create a security policy:

1. Navigate to **Records Manager > Security Policies** and select **File > New > Security Policy**.
The **Security Policy** screen is displayed and enabled by default.
2. Enter a unique value for the mandatory **Name**. All **Description** fields are optional, on the **Security Policy** page as well as on the **New Permission Set** page. Although the policy is enabled by default you can always disable it anytime.
3. Click **Add**. The **New Permission Set** page is displayed showing the **Info** tab.
4. Click **Next** against the default value displayed for the **Target Object Type**. All security policies must include *dm_sysobject* as one of the target object types. The **Permissions** tab is now displayed.



Note: Although you can select an alternate object type, you will not be able to finish creating the security policy without it. It is mandatory and cannot be removed after it has been added. Follow the rest of the procedure to define its permissions and then return to this step to select another object type and define permissions for it. You can repeat this process to add as many target object types as necessary.

There are no **Accessors**, users or groups, other than *dm_world* listed, based on the default settings, that can access the object with this security policy applied. Although only *dm_world* is listed by default, its permissions is set to *None*. Any **Target Object Type** selected will have *dm_world* by default, which can be edited to change its permissions if necessary. All object types must have dm_world defined. *Dm_world* cannot be removed. Any other **Accessors** added however, can be removed, edited, or added to another group. The applicable actions, **Add**, **Edit**, **Remove**, and **Add to Group** are made available when any of the accessors listed is selected.



Note: Although you can set or edit the **Basic Permissions** and the **Extended Permissions** for *dm_world*, the **Records Manager Permissions** cannot be set. The checkboxes for **Link**, **Unlink**, and **Create** are not available for *dm_world*.

5. Click the respective **Add** button to add the desired accessors, whether it is to grant access or to deny access. When necessary, any user in a group granted access can be selectively excluded by being denied access.

The **Choose a user/group** locator is displayed. Follow these sub-steps to choose:

- a. Select all the users and groups desired and then click **OK** on the locator to finish adding. The **Set Access Permissions** page is displayed.
- b. On the **Set Access Permissions** page, click **OK** if you want to apply the default settings for the **Basic Permissions**, **Extended Permissions**, and the **Records Manager Permissions**. Or, change their default settings an then click **OK**.

Only the **OK** and **Cancel** buttons are displayed at the bottom of the page if only one entity, user or group, was selected. **Previous**, **Next**, **Finish**, and **Cancel** buttons are otherwise displayed if more than one entity was selected. This makes it possible to specify the same permissions for all of the entities selected or to selectively change the permissions. The settings for the entity that is currently displayed is applied to all of the remaining entities when you click **Finish**.

You are returned to the **Security Policy** page, whether you click **OK** or **Finish**.

6. On the **Security Policy** page, click **OK** to finish creating the security policy or proceed to **Add** another object type with permissions defined for it. That is, repeat steps 3, 4, and 5 to add all of the desired object types, before you click **OK**. The **Security Policies** page is displayed when you click **OK**. Objects types that have already been selected for this security policy are no longer displayed in the list box for the **Target Object Type**.

5.2.2.17.3 Creating restrictive markings

For an overview of restrictive markings, refer to “[About security policies](#)” on page 364.

To create a restrictive marking:

1. Navigate to **Records Manager > Restrictive Markings** and select **File > New > Restrictive Marking**. The New Restrictive Marking screen is displayed.
2. Type a unique value for the mandatory **Name**, deselect **Is Enabled** to disable it if necessary, leave it world selectable or limit its availability by deselecting the checkbox, and then click **Finish**.
Only members of the restrictive marking see it displayed in the locator screen if **World Selectable** is deselected. Members of the Records Manager role can see it regardless of the setting.
3. To add members, proceed to “[Adding members to restrictive markings](#)” on page 398.

5.2.2.17.4 Creating shared markings

For an overview of shared markings, refer to “[About security policies](#)” on page 364.

To create a shared marking:

1. Navigate to **Records Manager > Shared Markings**.
2. Click **File > New > Shared Marking**. Make sure no shared markings are selected in the content pane.
The **New Shared Marking** screen is displayed and enabled by default.
3. Type a unique value for the **Name**.
4. Optionally, you can deselect the checkbox next to **Is Enabled** to disable the shared marking. This option is selected by default.
5. Optionally, you can deselect the checkbox, selected by default, next to **World Selectable** so that the shared marking is not available for selection when someone tries to apply it from the locator screen, unless they are a member of the shared marking or in the role of Records Manager.



Note: Anyone in the role of *Records Manager* sees all shared markings.

6. Click **Finish**.
The new shared marking is displayed in the presentation pane.
7. To add members, proceed to “[Adding members to shared markings](#)” on page 398.

5.2.2.17.5 Creating security levels



Note: Although you can create a security level with a ranking of your choice for unclassified records, it is recommended to assign 0 to prevent possible declassification problems. Assigning a higher ranking leaves room for someone to inadvertently create a security level with a ranking lower than that already specified for unclassified records.

For an overview of security levels, refer to “[About security policies](#)” on page 364.

To create a security level:

1. Navigate to **Records Manager > Security Levels**.
2. Click **File > New > Security Level**. Make sure no security levels are selected in the content pane.
The **New Security Level** screen is displayed and enabled by default.
3. Type a name in the **Name** field, for example: Secret.
4. Type a unique number from 0-99999 for the **Ranking**.
Users that are part of a security level with a specific ranking value have access to that ranking level and any levels below it if available.
5. Optionally, you can deselect **Is Enabled** to disable the security level as it is selected by default.
6. Optionally, you can deselect **World Selectable** so that only users in this specific security level, and those with a higher ranking, will see this security level in the locator screen.
7. Click **Finish**.
An Error message is displayed if the number entered is not unique.
The new security level is displayed in the presentation pane.
8. To add members, proceed to “[Adding members to security levels](#)” on page 400.

5.2.2.17.6 Creating attribute marking sets

For an overview of attribute marking sets, refer to “[Derived security and attribute marking sets](#)” on page 356. Each existing attribute marking set out-of-the-box can represent a particular combination of unique attribute markings used in conjunction with Department of Defense formal records. Users can also create their own custom attribute marking sets on any form according to instructions To customize a record attribute so that a client of Records Manager can have its own attributes for marking in “[Attribute marking sets](#)” on page 358.

You can **Add** and **Remove** attribute markings from the existing sets named **Supplemental Marking** and **Project Name** when you select their **Properties**.

To create an attribute marking set:

When you follow this procedure you are creating a new custom attribute marking set. Once you complete this procedure, the new set will appear in the content pane. Although you can create an attribute marking set according to these instructions and see them displayed in the content pane under Attribute Marking Sets, they will not appear on the form until they are added to a form according to the instructions in “[Attribute marking sets](#)” on page 358. Steps are included in these instructions to also add the various attribute markings when you create a new set.

1. Navigate to **Attribute Marking Sets** and select **File > New > Attribute Marking Set**. The New Attribute Marking Set screen is displayed.
2. Type a unique value for the **Name**. Two attribute marking sets called Supplemental Marking or Project Name can be created as these are automatically supported on the Department of Defense Standard, Email and Classified forms.
3. Click **Add** to create an attribute marking for the set now or, click **Finish** if you want to add the markings at a later time from its **Properties**. Otherwise, follow the remaining steps to finish adding one or more attribute markings.
The **New Attribute Marking** screen is displayed.
4. Type a unique value for the mandatory **Name** to differentiate attribute markings. The name is what will appear on the form as the value that you can select.
5. Change the default settings for **Is Enabled** and **World Selectable** as needed according to the following description and then click **Finish** to add the attribute marking.

Each attribute marking added **Is enabled** by default, when the checkbox is selected, so that this marking can be displayed and selected on the form when a Department of Defense formal record is declared.

The attribute marking is displayed to all OpenText Documentum CM users, not just for members of the attribute marking group, if the checkbox for **World Selectable** is selected. It is otherwise displayed only to members in the attribute marking group only if the default setting is changed from selected to deselected.

Users in the Records Manager role are always able to view all markings even if the **World Selectable** option is unchecked and they are not a member of any of the attribute marking groups.

6. Repeat steps 3 - 5 if you want to add more than one attribute marking to the set being defined.
7. Click **Finish** on the **New Attribute Marking Set** screen when you are done adding all the attribute markings for the set specified.

You can see which attribute markings belong to their respective sets by navigating to **Attribute Markings**.

Each attribute marking added is tied to a group where access to the formal record is determined by group membership for the selected markings.

Members for any marking are defined or added according to a separate set of procedures.

Any attribute marking that is disabled will not be listed on the form, that is for the set that it belongs to.

To add members, proceed to “[Adding members to attribute markings](#)” on page 399.

5.2.2.17.7 Adding members to restrictive markings

A member of a restrictive marking must be in all restrictive markings applied to the object. For any object that has multiple restrictive markings placed on it, the user must be a member of all of the restrictive markings in order to access the item. For an overview of restrictive markings, refer to “[About security policies](#)” on page 364. The restrictive marking must be created first, before you can add members to it. To create a restrictive marking, refer to “[Creating restrictive markings](#)” on page 395.

To add members to a restrictive marking:

1. Navigate to **Records Manager > Restrictive Markings**.
2. Click the hyperlink of the restrictive marking listed in the content pane.
The **Members** view is displayed in the content pane. Add and remove members as necessary but do not remove the Internal Security Operations Role.
3. Click **File > Add Member(s)**.
4. The **Choose a user/group** locator screen is displayed.
5. Select the members in the navigation pane and add them to the content pane then click **OK**.
The **Members** view is updated displaying existing members and those currently added.
6. To apply a restrictive marking, proceed to “[Managing record security using restrictive markings](#)” on page 402.

5.2.2.17.8 Adding members to shared markings

A member of a shared marking must be in at least one of the user/groups specified. For any object that has multiple shared markings placed on it, the user must be a member of only one of the shared markings in order to access the item. For an overview of shared markings, refer to “[About security policies](#)” on page 364. The shared marking must be created first, before you can add members to it. To create a shared marking, refer to “[Creating shared markings](#)” on page 395.

To add members to a shared marking:

1. Navigate to **Records Manager > Shared Markings**.
2. Click the hyperlink of the shared markings listed in the content pane.

The **Members** view is displayed in the content pane. Add and remove members as necessary but do not remove the Internal Security Operations Role.

3. Click **File > Add Member(s)**.
4. The **Choose a user/group** locator screen is displayed.
5. Select the members in the navigation pane and add them to the content pane then click **OK**.

The **Members** view is updated displaying existing members and those currently added.

6. To apply a shared marking, proceed to “[Managing record security using shared markings](#)” on page 403.

5.2.2.17.9 Adding members to attribute markings

A member of an attribute marking must be in at least one of the user/groups specified. For any object that has multiple attribute markings placed on it, the user must be a member of all of the attribute markings in order to access the item. For an overview of attribute marking sets, refer to “[Derived security and attribute marking sets](#)” on page 356.



Note: You need to navigate to **Attribute Markings** to add members to each attribute marking specified in each attribute marking set.

Adding an attribute marking to a formal record allows access only to those individual users who are members of the attribute marking. A user must be a member of all attribute markings if more than one attribute marking is applied when a formal record is declared. The formal record cannot be accessed by anyone other than the Records Manager if its attribute marking applied has no members added. The formal record could inadvertently get blocked if it is declared with an attribute marking that has no members added. A Records Manager however would have access regardless, whether the formal record was declared with or without members added to the selected attribute marking.

To add members to an attribute marking:

1. Navigate to **Attribute Markings**.

Attribute markings are identified with their respective attribute marking sets.

2. Click the attribute marking hyperlink listed in the content pane. For an example of attribute markings listed in the content pane, refer to “[Creating attribute marking sets](#)” on page 396.

Members for the selected attribute marking are displayed only if one or more were already added. Add and remove members as necessary but do not remove the Internal Security Operations Role.

3. Click **File > Add Member(s)**. Make sure nothing is selected in the content pane otherwise the menu option gives you **Remove Member(s)**.

The **Choose a user/group** locator is displayed.

4. Select the groups and/or users on the locator and click **OK** to complete the process.

The selected groups and/or users are displayed in the content pane under **Members** for the selected attribute marking.

You can view an attribute marking applied to a formal record by selecting it and choosing the **Attribute Markings** tab from the **Manage Record Security** option under the **Records** menu. Alternatively, you may click the Property icon of a formal record and view the form to see which markings have been applied.

To apply an attribute marking, proceed to “[Managing record security using shared markings](#)” on page 403.

To view an attribute marking applied to a formal record, refer to “[Viewing applied policies](#)” on page 380.

5.2.2.17.10 Adding members to security levels

A user must have a security ranking value *equal to or greater than* the value specified to access the object. Security levels that have a higher ranking are considered members of security levels with lower rankings. For further details, refer to “[About security policies](#)” on page 364.

To add members to a security level:

1. Navigate to **Records Manager > Security Levels**.
2. Click the hyperlink of a security level listed in the content pane.
The **Members** for the security level of Top Secret for example, are displayed in the content pane. Add and remove members as necessary but do not remove the Internal Security Operations Role.
3. Click **File > Add Member(s)**.
4. The **Choose a user/group** locator screen is displayed.
5. Select the members in the navigation pane and add them to the content pane then click **OK**.
The **Members** view is updated displaying the members for the selected security level.
6. To apply a security level, proceed to “[Managing record security using security levels](#)” on page 401.

5.2.2.17.11 Managing record security using security policies

To apply a security policy:

1. Navigate to a cabinet or folder or individual object.

You can apply a security policy directly to a document for example. It does not have to be a folder or cabinet. although security policies are normally applied to container type objects.

2. Select the object in the content pane and click **Records > Manage Record Security**.

The **Manage Record Security** screen is displayed displaying the **Security Policies** tab.

3. Click **Add** to select a security policy and apply it directly to the object.

The **Choose a security policy** screen is displayed.

4. Select a security policy from the navigation pane and add it to the content pane of the locator.

5. Click **OK** to accept.

The **Manage Record Security** screen is updated listing the selected security policy and also adds an option to **Remove**. If the security policy listed is not the one you intended to select, select the checkbox next to it and click **Remove**.

6. Click **Finish** to apply the security policy listed.

5.2.2.17.12 Managing record security using security levels

You can apply a security level independently of a security policy. Make sure the security level being applied has members added to it. To add members, refer to “[Adding members to security levels](#)” on page 400.



Note: Applying a security level to a classified record is done on the form. You cannot apply a security level to a classified record according to this procedure as you can for other formal records including email records.

To apply a security level:

1. Navigate to a cabinet or folder or individual object.

You can apply a security level to any object with or without a security policy.

Objects belonging to a cabinet or folder or individual object are displayed in the content pane.

2. Select an object in the content pane that belongs to a cabinet or node.

3. Click **Records > Manage Record Security**.

The **Manage Record Security** screen is displayed displaying the **Security Policies** tab.

4. Click the **Security Levels** tab.
5. Click **Add** to add a security level.

The **Choose a security level** locator screen is displayed displaying a list of security levels.

6. Select a security level and click **OK** to accept.

The **Security Levels** tab is updated listing the selected security level and also adds an option to **Remove**. If the security level listed is not the one you intended to select, select the checkbox next to it and click **Remove**.

7. Click **Finish** to accept and apply the selected security level.

5.2.2.17.13 Managing record security using restrictive markings

You can apply a restrictive marking independently of a security policy. Although restrictive marking should have members, you can add them later. To add members, refer to “[Adding members to restrictive markings](#)” on page 398.

To apply a restrictive marking:

1. Navigate to a cabinet or folder or individual object.

You can apply a restrictive marking regardless of whether there is a security policy applied or not.

Objects belonging to a cabinet or node are displayed in the content pane.

2. Select an object in the content pane that belongs to a cabinet or folder or individual object.

3. Click **Records > Manage Record Security**.

The **Manage Record Security** screen is displayed displaying the **Security Policies** tab.

4. Click the **Restrictive Markings** tab.

5. Click **Add** to add a restrictive marking.

The **Choose a restrictive marking** screen is displayed displaying a list of restrictive markings.

6. Select a restrictive marking and click **OK** to accept.

The **Restrictive Markings** tab is updated listing the selected restrictive marking and also adds an option to **Remove**. If the restrictive marking listed is not the one you intended to select, select the checkbox next to it and click **Remove**.

7. Click **Finish** to apply the restrictive marking listed.

5.2.2.17.14 Managing record security using shared markings

You can apply a shared marking independently of a security policy. Although restrictive marking should have members, you can add them later. To add members, refer to “[Adding members to shared markings](#)” on page 398.

To apply a shared marking:

1. Navigate to a cabinet or folder or individual object.

You can apply a shared marking regardless of whether there is a security policy applied or not.

Objects belonging to a cabinet or node are displayed in the content pane.

2. Select an object in the content pane that belongs to a cabinet or node.

3. Click **Records > Manage Record Security**.

The **Manage Record Security** screen is displayed displaying the **Security Policies** tab.

4. Click the **Shared Markings** tab.

5. Click **Add** to add a shared marking.

The **Choose a shared marking** screen is displayed displaying a list of shared markings.

6. Select a shared marking and click **OK** to accept.

The **Shared Markings** tab is updated listing the selected shared marking and also adds an option to **Remove**. If the shared marking listed is not the one you intended to select, select the checkbox next to it and click **Remove**.

Click **Finish** to apply the shared marking listed.

5.2.2.17.15 Managing record security using attribute markings

The Manage Record Security interface allows you to view any applied attribute markings. Attribute markings are used with Department of Defense formal records and are added on the standard record, email record, and classified record forms.

Although attribute markings can be created without members, you can add them later. To add members, refer to “[Adding members to attribute markings](#)” on page 399.



Note: You cannot apply an attribute marking from the Manage Record Security menu. You have to open a standard record, email record, or classified record form to apply attribute markings.

The attribute sets must be named Project Name and Supplemental Marking for the out-of-the-box implementation of Department of Defense. Values for the Project Name will not appear in the multiple selection list box unless the Attribute Markings are in an attribute marking set named Project Name. Similarly, values for the Supplemental Marking will not appear in the multiple

selection list box unless the Attribute Markings are in an attribute marking set named Supplemental Marking.

To apply an attribute marking:

1. Navigate to the **Info** tab of either a Department of Defense document, Department of Defense standard or classified record, Department of Defense formal folder or Department of Defense formal cabinet, whether you are:

- Creating a new formal folder or cabinet or a Department of Defense Document.
- Declaring a formal record.
- Declaring a new version of a formal record.
- Viewing Properties.

2. Scroll to **Project Name** or to **Supplemental Marking**.

 **Note:** For Department of Defense documents, click the **Edit** link next to the **Project Name** or the **Supplemental Marking** to select attribute markings. For the other Department of Defense objects, attribute markings can be selected directly on the **Info** tab.

3. Select the desired attribute markings.
4. Click **OK** to accept the values.

 **Note:** The security as specified by the marking, which has been applied to a Department of Defense document or Department of Defense classified record, will be in effect once it has been applied and saved. An additional records policy does not have to be applied to the object for the marking to take effect.

5.2.2.17.16 Viewing applied security policies

The procedure used to view any applied policy or any applied security markings is the same. “[Viewing applied policies](#)” on page 380 provides the procedure for this topic.

5.2.2.17.17 Removing applied security policies

Four separate remove procedures are provided. “[Removing applied policies](#)” on page 381 provides the procedure for this topic.

5.2.2.17.18 Deleting a security policy

The procedure used to delete a policy or any extended security is the same. “[Deleting policies and attribute markings](#)” on page 384 provides the procedure for this topic.

5.2.2.18 Record relations

5.2.2.18.1 Overview

Record relation definitions are used to define the behavior of a template that can be used to create the relationship in a OpenText Documentum CM repository. The definition set defines the template for how relationships are formed between two items in the system. Only members of the Record Relation Administrator role (dmc_rm_record_rel_admin) can administer record relation definitions, define, update, delete, and view. The Record Relation Administrator when they create a record relation definition also adds members that can create, declare, remove, and view record relationships. The parent and child objects selected for the relationship must match the rules specified for the Relation Name. In other words, the rule or option selected in the list box for the Relation Name determines what object types can participate in the relationship. Regardless of the relationship selected for the Relation Object Type, participants must match the rule selected for the Relation Name. For example, if the parent and the child according to the rule must be a dm_document, then the objects that are going to be related must be dm_documents instead of being any dm_sysobject. Options in the list box for the Relation Name are dm_relation_type. For more information on dm_relation_type, refer to Documentum CM Server documentation.

The record relationships that are shipped out-of-the-box include the following:

- Suspend
- *Supporting
- Supersede
- *Email Attachment Record Relation Definition
- *Cross-reference

Records Manager restricts which users can create these record relationships.



Note: 1) *Supporting, Email Attachment Record Relation Definition, and Cross-reference all have the same business logic. Relationships made with these create a pointer between the child and parent.

2) Objects, typically documents or records, you want to include in a suspend or a supersede record relationship must be under individual retention. This means that objects on both ends of the relationship must have their own individual retainers instead of one that is shared. Objects in a folder for example that age together with the retainer on the folder are not eligible. Suspend and supersede can be created only if the Retention Strategy on the

retention policy applied to the file plan, is set to *Individual* instead of *Linked*. It does not matter however what the Retention Strategy setting is when the retention policy is applied directly to the objects involved. An object will get its own direct retainer when a retention policy is applied directly, regardless of the Retention Strategy setting. Suspend and supersede are not available choices when you try to create a record relationship against objects that are not tied to their own retainers. They are for example filtered from the list of relation definitions if you click Create Record Relationship while declaring a formal record against an object that does not have its own retainer.

About Suspend Record Relation (dmc_rm_suspend_rel)

The parent object in a suspend record relationship suspends aging on the child object and in effect clears its qualification date. The child object as a result cannot be promoted or disposed. The qualification date is restored as follows:

- The OLD qualification date on the child object is restored (to the value before it was suspended) if the relationship is severed, for example, the relationship is removed (remove record relationship) or if the parent is destroyed.
- The OLD qualification date is restored if the child has a conditional retention.
- A NEW qualification date is calculated, based on a new start date (which is the resumption date), only if the child has a chronological retention and it was resumed through a trigger on a phase exit or phase entry action specified in the retention policy of the parent.

The screen is displayed from a retention policy, when the Add button on the Phases tab for Action Name is selected.

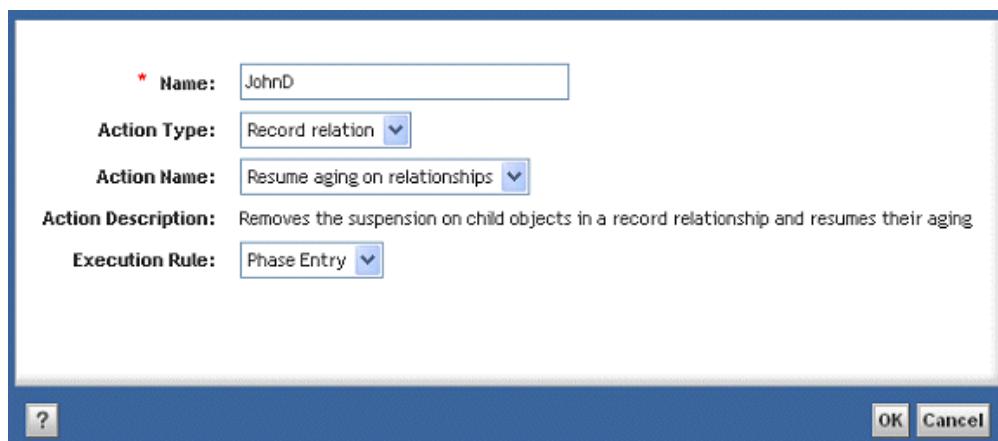


Figure 5-3: Action type for a record relation

You can verify, as shown in [Figure 5-4](#) from the Properties of the retention policy applied to the parent, if *Record relation* was added for the Type under the Action Name on the Phases tab.

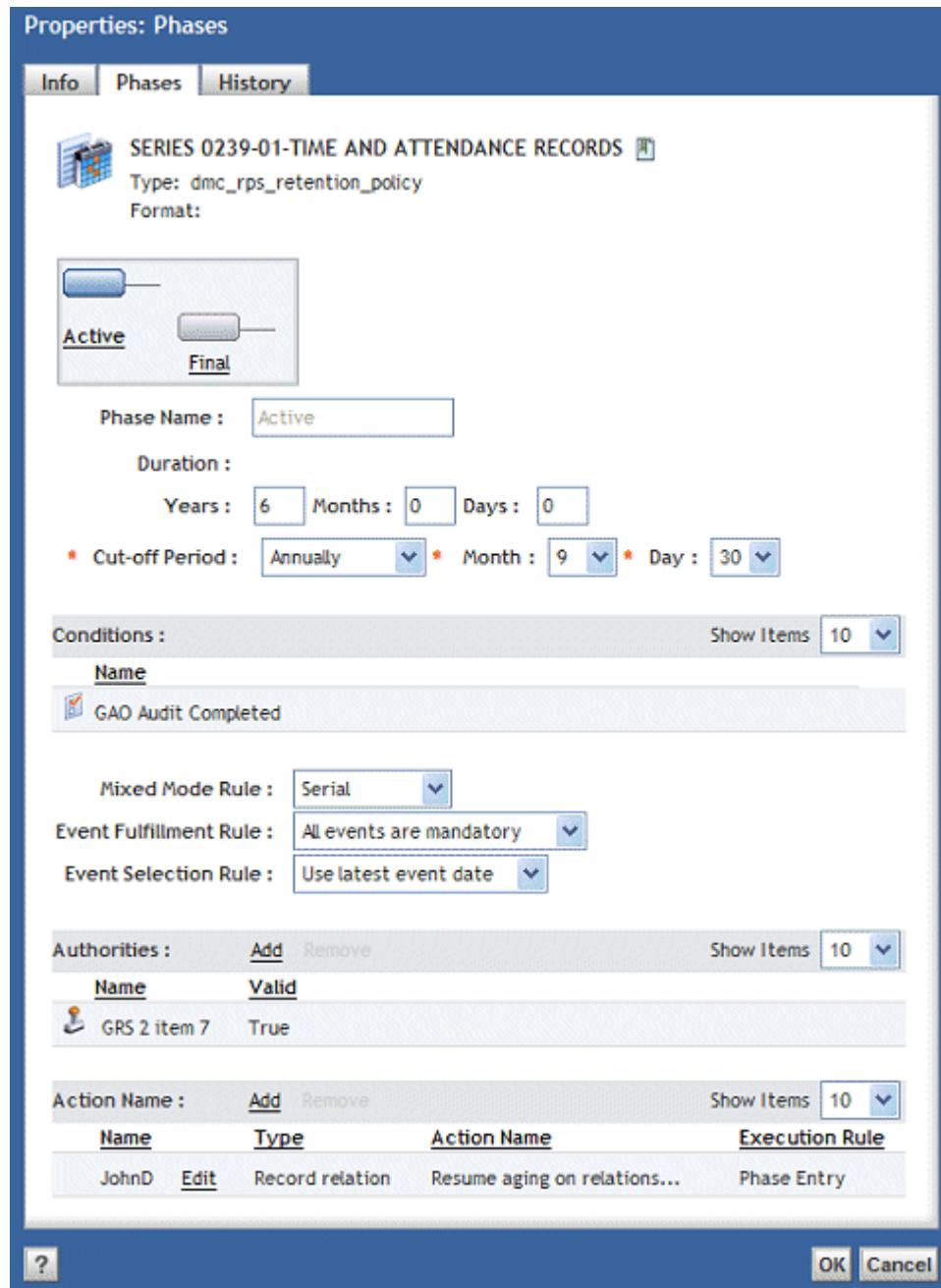


Figure 5-4: Properties for parent retention policy

Validation Rules for Applying a Suspend Record Relation

The following is a list of the validation rules for applying the Suspend Relationship to any of the objects selected for a record relation:

1. Parent must be under retention.

2. Child must be under retention.
3. The parent object must be under retention against a policy that has the trigger defined to release the suspension on a current or forthcoming phase, including rollover retention. At least one of the parent's retainers' or rollovers has a remaining phases (phases that have not expired) with the suspension release control option set (that is, that the Action Name is set to Resume aging on relationships).
4. The record relation must not result in a cyclical relationship among the related objects, or in its relationship chain, that will result in a suspension deadlock. Must make sure that the child is not the parent of any suspend relationship that might result in this parent being its either direct or indirect child.

To further clarify, regarding items 1 and 2, only those objects that are under retention are eligible for a relationship, regardless of which object is designated the parent. Regarding item 3, although any object selected for a relation must be under retention, the retention on the object that will be designated as the parent must have Resume aging on relationships selected. If retention on the parent specifies a rollover policy, the roll over to policy must also have Resume aging on relationships selected. Regarding item 4, to prevent suspension deadlock, you would be prevented from making cyclical relations that would result in suspending the child object indefinitely. For example, although a relation where parent object A suspends object B is acceptable, you would be prevented from creating another relationship, using the same objects, where you designate object B as the parent. If it were allowed, both objects would end up in a loop suspending one another. If you consider more than two objects, for example, objects A, B, and C where A relates to B and B relates to C. Although the 2 relations are acceptable, you would be prevented from closing the loop with a relation from C to A. You can still create alternate relations from already related objects so long as they do not result in a loop that causes a suspension deadlock.

Ending suspension

The following table describes different methods for removing suspension.

Table 5-21: Removing suspension

Method	Reset chronological start date	Notes
Manually remove record suspend relation	No	

Method	Reset chronological start date	Notes
Promote the parent into or out of a phase that has the action to Resume aging on relationships configured (upon Phase Entry or Phase Exit)	Yes	For chronological date calculations, the starting date becomes the date the suspension is lifted (cutoff is applied (if configured) and then duration). This means that suspending an object can push out the qualification date.
Privileged delete on the parent	No	
Disposition (destroy all) of a parent that is missing the action to resume	No	It is recommended if the date should be reset to apply the action to the retention policy on the final phase when leaving.
Remove last retention policy that is directly applied to the parent (or last individual retention policy inherited)	No	

About Supersede Record Relation (`dmc_rm_supersede_rel`)

A supersede record relationship can be used to replace one document with another document.

In a supersede record relation, all retainers on the child are moved to the Final phase for disposition processing the moment the relationship is created. New retainers are also moved to the Final phase if another retention policy is applied to the child after the relationship has been established.



Note: The supersede functionality in the Supersede relationship is independent of the Supersede setting on a retention policy. Supersede, in other words, occurs regardless of whether the retention policy applied to the child has Supersede set or not.

In this record relation type the child can never be returned to the phase it was moved from.

5.2.2.18.2 Create record relation definition

Record relation definitions are used to create record relationships. Record relation definitions define rules for custom record relationships. You can create your own custom record relation definitions and include them among those already available out-of-the-box. Each record relation definition created is associated to one Relation Object Type.

Users, when they create a record relationship, can select from a list of custom record relation definitions. The Records Manager system creates the record relationship with the user specified information. To create a record relationship, refer to “[Create record relationship](#)” on page 414.

Record relation definitions when created with one of the Relation Object Types, supported out-of-the-box, are each represented with an icon of their own.

Record relation definitions specify an instance of dm_relation_type, a dm_relation subtype, and additional user configurable permissions to control who can apply and remove the relationships. Users can create their own record relations, according to a specific dm_relation subtype, and modify who can create record relationships and who can delete record relationships, given a specific record relation definition.

To create a record relation definition:

1. Navigate to Records Manager > Record Relation Definitions and select File > New > Record Relation Definition.
2. Enter values for the attributes described in “[New record relation definition attributes](#)” on page 410 and then click **Finish**. “[Default setup for record relations](#)” on page 412 shows the default setup for record relations that are available out-of-the-box.

Table 5-22: New record relation definition attributes

Attribute (*) indicates mandatory attributes	Description
*Name	Used to identify the object. The value entered is the name displayed in the list box for the Record relation definition attribute on the Create a Record Relationship screen.

Attribute (*) indicates mandatory attributes	Description
<p>*Relation Object Type</p>	<p>The value assigned determines the object type for the intended relation.</p> <p>Options in the list box for this attribute include:</p> <ul style="list-style-type: none"> • Email Attachment Record Relation (dmc_rm_email_attachment_rel) • Record Relation (dmc_rm_record_rel) • Supersede Record Relation (dmc_rm_supersede_rel) • Support Record Relation (dmc_rm_support_rel) • Suspend Record Relation (dmc_rm_suspend_rel) <p> Note: Business logic behind supersede and suspend are described in the Overview.</p> <p>The relation object type dictates the business behavior so do not mix different relation object types with relation names because users will get confused if the relation name indicates supersede but the relation object type does not match.</p>

Attribute (*) indicates mandatory attributes	Description
<p>*Relation Name</p>	<p>These are the relation types. Each contains rules about the objects that can be selected to participate in record relations.</p> <p>Relationship types define the following:</p> <ul style="list-style-type: none"> • Permitted object type of the parent (often set to dm_sysobject), subtypes are allowed • Permitted object type of the child (often set to dm_sysobject), subtypes are allowed • Label for the parent when viewing the relation • Label for the child • Security for the relationship for deletion (please refer to the relation type section) <p>Options in the list box for this attribute include:</p> <ul style="list-style-type: none"> • dmc_rm_rec_crossref_rel_type • dmc_rm_rec_emailattach_rel_type • dmc_rm_rec_rendition_rel_type • dmc_rm_rec_supersede_rel_type • dmc_rm_rec_support_rel_type • dmc_rm_rec_suspend_rel_type
<p>*Creation Group Name</p>	<p>Members of the group name selected can apply relationships using this record relation definition object.</p>
<p>*Removal Group Name</p>	<p>Members in the role selected for this attribute can remove or undo the record relationship that uses this definition.</p>

Table 5-23: Default setup for record relations

Name	Relation object type	Relation name	Parent label	Child label	Parent object type	Child object type
Supersede	Supersede Record Relation (dmc_rm_supersede_rel)	dmc_rm_rec_supersede_rel_type	Supersedes	Superseded By	dm_document	dm_document

Name	Relation object type	Relation name	Parent label	Child label	Parent object type	Child object type
Suspend	(dmc_rm_suspend_rel)	dmc_rm_recsuspend_rel_type	Is Suspending	Is Suspended By	dm_document	dm_document
Supporting	(dmc_rm_support_rel)	dmc_rm_rec_suppor_t_rel_type	Supported By	Supports	dm_sysobject	dm_sysobject
Email Attachmen	(dmc_rm_email_attachmant_rel)	dmc_rm_rec_emailattach_rel_type	has an Email Attachmen	is an Email Attachmen	dmc_rm_formal_record	dmc_rm_formal_record
Cross-reference	(dmc_rm_record_rel)	dmc_rm_rec_crossref_rel_type	Cross Reference	Cross Reference	dm_sysobject	dm_sysobject

The suspend and supersedes relations require retention on both the parent and child.

5.2.2.18.3 Creating your own relation types

When creating record relation definitions it is expected that customers may wish to specify a specific label when viewing the relationship from the parent and a label when viewing the relationship from the child.

In order to do this, the administrator must first create a new relation type. To do this, refer to *OpenText Documentum Content Management - Composer User Guide (EDCPC-UGD)*. The instructions for *Creating a relation type* can be found in the chapter *Managing Relation Types*.

It is recommended that for relationship types that are going to be used for record relation definitions that the security type is set to the default None and the referential integrity is set to the default Allow delete. The relation direction should also be set to the default From parent to child.

5.2.2.18.4 Update record relation definition

1. Navigate to **Records Manager > Record Relation Definitions**.
2. Right-click a record relation definition and select **Properties**.
3. Change entries for the attributes as necessary and then click **OK**.

5.2.2.18.5 Delete record relation definition

A record relation definition cannot be deleted if there are any record relationships created that use the definition. To find out, right-click the definition and select **View > Record Relationship Definition Usages**. You can delete the relationships from the **Record Relationship Definition Usages** page if desired, or directly as follows if it is not in use:

1. Navigate to **Records Manager > Record Relation Definitions**.
2. Right-click a record relation definition and select **Delete**.

5.2.2.18.6 View record relation definitions

To view record relation definitions, navigate to **Records Manager > Record Relation Definitions**.

5.2.2.18.7 Create record relationship

Refer to “[Creating and viewing record relationships](#)” on page 345.

5.2.2.18.8 Remove record relationship

Refer to “[Removing a record relationship](#)” on page 348.

5.2.2.18.9 View record relationships

Refer to “[Creating and viewing record relationships](#)” on page 345

5.2.2.19 Classification subscription lists

5.2.2.19.1 Overview

A classification subscription list (CSL) provides shortcuts to common locations of the file plan that users may file formal records to. Each item added to a CSL is a shortcut to the appropriate file plan location. Users declaring formal records can choose the CSL icon on the Choose a folder locator component displayed when they select the file plan on the Create tab. Users will need to contact their administrator if nothing is listed when they click the CSL icon.

Each item on a classification subscription list represents a logical association between a repository location and a list of users, roles, or groups. The object type for a CSL is called `dmc_rm_class_subscrip_list`. This object type has a repeating attribute `subscription_items` that has the IDs of `dmc_alias_set` objects containing classification location information. Each entry of a CSL is a repository location that is a subtype of `dm_folder`. Only Records Manager privileged users have access to a listing of classification subscription lists.

A user in the `dmc_rm_csl_admin` role can:

- Create and delete a CSL.
- Modify a CSL.

- Add an item to a CSL.
- Remove an item from a CSL.

A user with relate permissions to a CSL can:

- Select a classification item from a CSL for filing a record (declaring a record) from the Records menu.



Note: This allows them to select a shortcut for filing. It does not mean or give the user the ability to file, as this is determined by other policies.

To follow instructions for this operation, refer to “[Declaring electronic or physical documents as formal records](#)” on page 340.

When a user declares a formal record, the user is prompted for the file plan location from the creation page. The locator component brings up a screen that lists the CSL as an option for selecting the location in the file plan to file the formal record. Each CSL has an associated ACL which only Records Manager privileged users can modify and can grant or revoke access to or from any user, role, or group. Creators and administrators of a CSL are included in the atomic role dmc_rm_csl_admin. Records Manager (dmc_rm_recordsmanager) are automatically nested in the dmc_rm_csl_admin atomic role. All ancillary objects related to a CSL reside in the Records Manager dar file.

5.2.2.19.2 Creating a CSL

To create a CSL:

1. Navigate to **Records Manager > Classification Subscription Lists** and select **File > New > Classification Subscription List**.

Each new CSL is active by default. You can disable a CSL by deselecting the checkbox, when creating it or from its Properties when necessary.

2. Type a unique value for the mandatory CSL **Name**.

This is the name that appears to users when filing a record and selecting the CSL option.

3. Click **Add** to add a location. The **Add Classification Location** screen is displayed.

This is the shortcut to a specific location in the file plan.

4. Type a unique value for the mandatory location **Name**.

This name appears when a user selects an entry from the CSL list and double-clicks it to reveal its entries. You can use a friendly name to abstract the location from end users or the full path if desired.

5. Click **Edit** on the **Add Classification Location** screen . Click **OK** on the resulting **Choose a folder** locator screen once you select a location.

The value selected for the location is displayed next to the mandatory **Selected Location**.

6. Click **OK** on the **Add Classification Location** screen to accept.
 **Note:** The **Status** value for the selected location is *Valid*, to indicate that the folder exists.
7. Optionally, repeat steps 3 - 6 if you want to add more than one location to a CSL.
You can click the attribute name in the header at the top of a column to reverse the order of the subscriptions listed. The arrow next to the attribute name selected will point up or down.
8. Click **Next** to set the permissions for all users/groups and roles added to the CSL. Users need *Relate* permissions in order to see the CSL when filing a record.
The `dmc_rm_csl_admin` role with *Delete* permissions is automatically added to the **Permissions** tab.
9. Click **Finish**. All classification subscription lists, both active and inactive, are displayed in the content pane by default. Make sure that you change the filter setting for the preferred view.

5.2.2.19.3 Deleting a CSL

Using these instructions you can delete either an active or an inactive CSL. The filter setting on the content pane is set to *Classification Subscription Lists* by default, to display all classification subscription lists whether they are active or inactive.

To delete a CSL:

1. Navigate to **Records Manager > Classification Subscription Lists**.
2. Right-click the CSL and click **Delete**.
3. Click **OK** to confirm.

5.2.2.19.4 Adding a location to a CSL

Instructions to add a location are also included in the instructions used to create a CSL. These instructions are intended to add locations to existing classification subscription lists on their Properties screen. The Properties screen can also be used to change the permissions set against any of the users/groups and roles if necessary. The same permissions are shared against all locations listed for a particular CSL.

To add a location to an existing CSL:

1. Navigate to **Records Manager > Classification Subscription Lists**.
2. Right-click a CSL in the content pane and select **Properties**.
3. Click **Add** on the **Properties** screen.
4. Type a unique value for the mandatory location **Name**

5. Click **Select a Location** on the **Add Classification Location** screen. Click **OK** on the resulting **Choose a folder** locator screen once you select a location.

The value selected for the location is displayed next to the mandatory **Selected Location**.

6. Click **OK** on the **Add Classification Location** screen to accept.



Note: The **Status** value for the selected location is *Valid* unless the folder does not exist in the repository or the current user does not have permissions to see the folder.. The **Status** changes automatically to *Invalid* when the folder for the selected location is removed from the repository. Even if the status is valid the classification location may not be usable for declaring formal records. At least one policy must be applied and if the configuration setting for requiring retention is set, a retention policy needs to be applied to the folder.

Each item added to the subscription list can be removed when necessary if you select an item and then click **Remove**. The option to remove is revealed when you select at least one item.

7. Optionally, repeat steps 3 - 6 if you want to add more than one location to a CSL.

You can click the attribute name in the header at the top of a column to reverse the order of the subscriptions listed. The arrow next to the attribute name selected will point up or down.

8. Click **Next** to set the permissions for all users/groups and roles added to the CSL.
9. Click **Finish**. All classification subscription lists, both active and inactive, are displayed in the content pane by default. Make sure you change the filter setting for the preferred view.

5.2.2.19.5 Removing an item from a CSL

Instructions to remove a location are also included in the instructions used to create a CSL. These instructions are intended to remove locations from existing classification subscription lists on their Properties screen.

To remove an item from an existing CSL:

1. Navigate to **Records Manager > Classification Subscription Lists**.
2. Right-click a CSL in the content pane and select **Properties**.
3. Select a CSL listed on the **Info** tab and click **Remove**.
4. Click **OK** to close the Properties screen.

5.2.2.19.6 Selecting a classification item from a CSL when declaring a record

To select an item from a CSL when declaring a record, refer to the instructions for declaring formal records, “[Declaring electronic or physical documents as formal records](#)” on page 340.

5.2.2.20 About default forms and customized forms

Forms are tied to object types. Declaring a formal record, for example, is based on the object-type chosen. A variety of attributes are associated with each form template whereby some are mandatory, optional, read-only, repeating (multiple values), and possibly pre-populated. To create, open, enter data, or to format the content in regular OpenText Documentum CM forms, refer to “[Forms](#)” on page 668. To enter data in a form for formal records, refer to “[Declaring electronic or physical documents as formal records](#)” on page 340.

You are not required to have Documentum Forms Builder installed unless you plan to customize any of the existing forms shipped or plan to create new forms. The RM-Forms-Adaptor.dar must be installed wherever forms are being used. You are not able to fill out a formal record form, for example, if the Forms.dar is not installed on the applicable repository.

A new form must be created and installed for each new subtype of formal records (dmc_rm_formal_record).



Notes

- To declare formal records only, only the Default dar (RM-Default.dar) has to be installed.
- To declare Department of Defense standard records only, only the Department of Defense Standard dar (RM-DoD5015v3-Standard-Record.dar) has to be installed.
- To declare both formal records and Department of Defense standard records, the Department of Defense Standard dar must be installed on top of the Default dar.

To declare Department of Defense email records, the Department of Defense Standard dar must be installed.

- To declare Department of Defense classified records, the Department of Defense Classified dar ((RM-DoD5015v3-Classified-Record.dar) must be installed on top of the Department of Defense Standard dar.
- To declare any record, formal, Department of Defense standard, and Department of Defense classified, all three dars must be installed, that is Standard on top of Default and Classified on top of Standard.

This is further summarized in the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*.

You must use Documentum Forms Builder to customize a form template and you must refer to the Documentum Forms Builder documentation for instructions on

how to use it. Information here describes what forms are available and what the settings should be.

There are three categories of form templates, used to support the various object-types, to choose from whereby each category is associated with a set of forms:

- Forms for *formal records*:
 - Formal Record (dmc_rm_formal_record)
Default form for declaring formal records that do not have to be Department of Defense compliant.
 - Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec)
Department of Defense Standard form for declaring DoD compliant non-classified formal records.
 - Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec)
Department of Defense Classified form for declaring Department of Defense compliant formal records that are classified.
 - Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)
Department of Defense Email form for declaring email formal records that are Department of Defense compliant.
- Forms for *formal cabinets*:
 - Formal Cabinet (dmc_rm_formal_rec_cabinet)
 - Cabinet DoD 5015 V3 (dmc_rm_dod5015v3_cabinet)
- Forms for *formal folders*:
 - Formal Record Folder (dmc_rm_formal_rec_folder)
 - Folder DoD 5015 V3 (dmc_rm_dod5015v3_folder)

You can see in the following tables what attributes are mandatory, read-only, repeating, and pre-populated on the existing forms shipped.

Table 5-24: Formal Record Cabinet (dmc_rm_formal_rec_cabinet)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Name	x				
Subject					
Unique Cabinet Identifier	x	x		x	
Authors			x		
Keywords			x		

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship.

Table 5-25: Cabinet DoD 5015 V3 (dmc_rm_dod5015v3_cabinet)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Name	x				
Subject					
Unique Cabinet Identifier	x	x		x	
Record Category Identifier					
Authors			x		
Title					
Keywords			x		
Location					
Vital Record Indicator					If a retention markup with a designation of vital is applied the box becomes checked.
Project Name					Attribute markings need to be created for the values to appear.

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Supplemental Marking					Attribute markings need to be created for the values to appear.
Record Category Description	x				
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship .

Table 5-26: Formal Record Folder (dmc_rm_formal_rec_folder)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Name	x				
Subject					
Unique Cabinet Identifier	x	x		x	
Authors			x		
Keywords			x		
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship .

Table 5-27: Folder DoD5015 V3 (dmc_rm_dod5015v3_folder)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Name	x				
Subject					
Record Category Identifier	x	x		x	
Unique Folder Identifier	x	x		x	
Authors			x		
Keywords			x		
Attribute Marking Sets	x				
Record Category Description	x				
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship.

Table 5-28: Formal Record (dmc_rm_formal_record)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Name	x				
Subject					
Authors			x		
Keywords			x		

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship .

Table 5-29: Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Record Name	x				
Record Category Identifier	x	x		x	
Unique Record Identifier	x	x		x	
Subject	x				
Media Type	x				
Application Format	x				
Originating Organization	x				
Date Filed		x		x	
Received Date					
Publication Date	x				
Authors	x		x		
Keywords					
Primary Addressees			x		
Other Addressees			x		
Locations			x		
Attribute Marking Sets					

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Vital Record Indicator					If a retention markup with a designation of vital is applied the box becomes checked.
Record Category Description	x				
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship .

Table 5-30: Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Record Name	x				
Record Category Identifier			x		
Unique Record Identifier	x	x		x	
Subject	x	x		x	
Media Type	x				
Application Format	x				
Originating Organization	x				
Date Filed		x		x	
Received Date		x		x	
Publication Date	x	x		x	

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Email Priority		x		x	
Authors	x	x	x	x	
Keywords			x		
Addressees		x	x	x	
Other Addressees			x		
Hidden Addressees		x		x	
Locations			x		
Project Name					
Supplemental Marking					
Attribute Marking Sets			x		
Vital Record Indicator		x			If a retention markup with a designation of vital is applied the box becomes checked.
Record Category Identifier		x		x	
Attachment Reference		x		x	The checkbox is checked if there are attachments.
Record Category Description					
Create Record Relationship					This button is used optionally and opens the process or screen used to Create a Record Relationship.

Table 5-31: Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec), includes all Record DoD 5015 V3 Standard attributes in the table above plus these

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Derived From	x				Mandatory only when either of the first two of the four radio buttons is selected.
Multiple Sources			x		
Downgrade on Schedule					More options are displayed at the bottom of the form when this option is selected.
Upgrade					More options are displayed at the bottom of the form when this option is selected.
Review					More options are displayed at the bottom of the form when this option is selected.
Initial Classification	x				
Current Classification	x			x	
Classifying Agency					
Classified By	x				
Reasons for Classification					Becomes mandatory if Classified By has a value.

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Auto Declassify On		x		x	It is pre-populated if Declassify On is set to Auto Calculated Date.
Declassify On Event					
Exemption Category					Becomes mandatory when Declassified On has Exemption Category selected.
Declassified On				x	
Declassify on Date	x				Only shown (mandatory) if Declassified On has either Date or Date and Event selected.
Declassify on Event	x				Only shown (mandatory) if Declassified On has either Event or Date and Event selected.
Declassified By				x	
Hidden attributes displayed when <i>Downgrade on Schedule</i> is selected					
Downgrade On					

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Downgrade On Date					Becomes mandatory if Declassified On has either <i>Date</i> or <i>Date and Event</i> selected.
Downgrade On Event					Becomes mandatory if Declassified On has either <i>Event</i> or <i>Date and Event</i> selected.
Target Downgrade Level					Becomes mandatory if Downgrade On has a value (not blank).
Downgrade Instructions					Becomes mandatory if Downgrade On has a value (not blank).
Downgraded On		x		x	Only populated if the Security Level is downgraded (decreased).
Downgraded By		x		x	Only populated if the Security Level is downgraded (decreased).
Hidden attributes displayed when <i>Upgrade</i> is selected					

Attribute	Mandatory	Read-Only	Repeating	Pre-Populated	Notes
Upgraded On		x		x	Only populated if the Security Level is upgraded (increased).
Upgraded By		x		x	Only populated if the Security Level is upgraded (increased).
Reasons for Upgrade					Becomes mandatory if the Security Level is upgraded (increased).
Hidden attributes displayed when <i>Review</i> is selected					
Reviewed On					
Reviewed By					

5.2.2.21 Creating a formal cabinet

A formal cabinet is akin to a normal OpenText Documentum CM cabinet with the exception that form data is associated to it and carries a different icon to distinguish it from its normal counterpart.

A formal cabinet is associated with a form so that you can customize the attributes, and their behavior, displayed on the form used to create the formal cabinet.

There are two formal cabinet types. One for general use named *Formal Record Cabinet* that can be used to contain formal records, and the other named *Cabinet DoD 5015 V3* used to contain Department of Defense formal records.

Regardless of the role a user is in or the client the user uses, the user also has to be in the *form_user* role to create formal records, formal cabinets, and formal folders. The menu option File > New > Formal Cabinet will not be enabled for the user if the user is not in the *form_user* group.

To create a formal cabinet (Formal Record Cabinet or Cabinet DoD5015 V3):

1. Navigate to **Cabinets**.

2. Click **File > New > Formal Cabinet**. The New Formal Cabinet screen is displayed.
3. On the **Create** tab, enter the name and, if necessary, change the default setting for the **Type**. The form templates associated with the type will be displayed.
You can also make it possible for members to subscribe to the cabinet, to facilitate access from a shortcut added to the Subscriptions node, or you can make it private for your personal use.
4. Click **Next**.
5. On the **Info** tab, enter values as necessary according to the attributes described in “**Formal cabinet attributes**” on page 430 and then click **Next**. If you are working with Department of Defense records, refer to “**Formal cabinet attributes for Department of Defense records**” on page 431. Although only the mandatory attributes are necessary to create the object, you can always revisit it from its Properties to add to the optional attributes and if necessary modify existing entries.

Table 5-32: Formal cabinet attributes

Attribute (*) indicates mandatory attributes	Description
*Name	Identifies the formal cabinet. The value typed on the Create tab is displayed.
Type	The object type.
*Form Template	Is automatically populated according to the object Type selected.
Subject	Categorizes content by topic or department for example.
*Unique Cabinet Identifier	Read-only field, pre-populated (system generated) to identify and differentiate formal cabinet objects.
Authors	A contact responsible for the formal cabinet. You can Insert additional fields to identify more than one contact if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete .  Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.

Attribute (*) indicates mandatory attributes	Description
Keywords	<p>An attribute of this cabinet for example that can be used to facilitate searching. You can Insert additional fields to provide more than one keyword if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Create Record Relationship	<p>Lets you create a record relationship. For further details about record relationships, refer to "Record relations" on page 405.</p>

Table 5-33: Formal cabinet attributes for Department of Defense records

Attribute (*) indicates mandatory attributes	Description
*Name	Identifies the formal cabinet. The value typed on the Create tab is displayed.
Type	The object type.
*Form Template	Is automatically populated according to the object Type selected.
Subject	Categorizes content by topic or department for example.
*Unique Cabinet Identifier	Read-only field, pre-populated (system generated) to identify and differentiate formal cabinet objects.

Attribute (*) indicates mandatory attributes	Description
Record Category Identifier <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>	 Note: You need Department of Defense naming policy with a specific mask rule applied in order for this to work. This field is automatically populated according to the naming policy applied when one is applied to a Department of Defense formal cabinet. This field shows the actual file plan naming convention based on the value specified for the Attribute Name in the Mask Rule of the applied naming policy. This attribute is defined on the following object types: <ul style="list-style-type: none"> • Cabinet DoD 5015 V3 (dmc_rm_dod5015v3_cabinet) • Folder DoD 5015 V3 (dmc_rm_dod5015v3_folder) • Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec) • Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec) • Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)
Location <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>	This text box is used to specify the path to the formal cabinet
Vital Record <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>	The checkbox is selected only if a markup with the vital designation has been placed on the cabinet itself. If you are creating the cabinet for the first time, it will be blank. However, if someone were to add a retention markup with a vital designation to it, then the checkbox would be on when you select the properties of the cabinet.

Attribute (*) indicates mandatory attributes	Description
Authors	<p>A contact responsible for the formal cabinet.</p> <p>You can Insert additional fields to identify more than one contact if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Keywords	<p>An attribute of this cabinet for example that can be used to facilitate searching.</p> <p>You can Insert additional fields to provide more than one keyword if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Project name	<p>Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.</p> <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>
Supplemental Marking	<p>Add supplemental markings to add additional security to the object.</p> <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>
Record Category Description	<p>Use this for example, to describe and differentiate cabinets within a file plan.</p> <p> Note: This attribute is not displayed for Formal Record Cabinets.</p>
Create Record Relationship	<p>Lets you create a record relationship. For further details about record relationships, refer to "Record relations" on page 405.</p>

- On the **Permissions** tab, click **Next** to accept the default settings or change the default settings as needed to provide the desired level of basic and/or extended permissions needed for each user or group specified. You can ignore making

any entries or changes in the **Permissions** tab if you plan to apply any record security to the formal cabinet.



Note: Do NOT change the permissions if you plan to apply any record security, such as a security policy or shared marking, to the formal cabinet. The record security will override permissions on the formal cabinet and dictate the appropriate permissions.

You can add all the users and/or groups needed for the membership and assign the required level of permissions for each of their permissions. A **Search** button is available so you can see and examine what permissions are associated with a particular user or group before deciding to add it. A **Select** button is also available to change the permission set in instances where you would want to change the current membership so that the formal cabinet is associated with the permissions of a different set of members.

You can also single out one or more members under **Restrictions** if you have to reduce their level of permissions.

Advanced Permissions also makes it possible to specify one or more groups in which case a user must be a member of each to access the cabinet or to specify a set of groups in which case the user must be a member of at least one of the groups to access the cabinet.

7. Click **Finish**.

5.2.2.22 Creating a formal folder

A formal folder is associated with an icon easily differentiated from folders which are not associated with any form metadata as are formal folders. Formal folders are intended for storing formal records which are also associated to form metadata.

A formal folder is associated with a form so that you can customize the attributes, and their behavior, displayed on the form used to create the formal folder.

There are two formal folder types. One for general use named *Formal Record Folder* that can be used to contain formal records, and the other named *Folder DoD 5015 V3* used to contain Department of Defense formal records.

Regardless of the role a user is in or the client the user uses, the user also has to be in the *form_user* role to create formal records, formal cabinets, and formal folders. The menu option *File > New > Formal Folder* will not be enabled for the user if the user is not in the *form_user* group.

To create a formal folder (*Formal Record Folder* or *Folder DoD5015 V3*):

1. Navigate to the file plan or formal cabinet where you want to create a formal folder.
2. Click **File > New > Formal Folder**.

3. On the **Create** tab, enter the name and, if necessary, change the default setting for the **Type**. The form templates associated with the type will be displayed. You can also make it possible for members to subscribe to the folder, to facilitate access from a shortcut added to the Subscriptions node, or you can make it private for your personal use.
4. Click **Next**.
5. On the **Info** tab, enter values as necessary according to the attributes described in “Formal folder attributes” on page 435 and then click **Next**. If you are working with Department of Defense records, refer to “Formal folder attributes for Department of Defense records” on page 436. Although only the mandatory attributes are necessary to create the object, you can always revisit it from its Properties to add to the optional attributes and if necessary modify existing entries.

Table 5-34: Formal folder attributes

Attribute (*) indicates mandatory attributes	Description
*Name	Identifies the formal cabinet. The value typed on the Create tab is displayed.
Type	The object type.
*Form Template	Is automatically populated according to the object Type selected.
Subject	Categorizes content by topic or department for example.
*Unique Folder Identifier	Read-only field, pre-populated (system generated) to identify and differentiate formal cabinet objects.
Authors	A contact responsible for the formal cabinet. You can Insert additional fields to identify more than one contact if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete .  Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.

Attribute (*) indicates mandatory attributes	Description
Keywords	<p>An attribute of this cabinet for example that can be used to facilitate searching. You can Insert additional fields to provide more than one keyword if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Create Record Relationship	<p>Lets you create a record relationship. For further details about record relationships, refer to "Record relations" on page 405.</p>

Table 5-35: Formal folder attributes for Department of Defense records

Attribute (*) indicates mandatory attributes	Description
*Name	Identifies the formal cabinet. The value typed on the Create tab is displayed.
Subject	Categorizes content by topic or department for example.
Type	The object type.
*Form Template	Is automatically populated according to the object Type selected.
Unique Folder Identifier	Read-only field, pre-populated (system generated) to identify and differentiate formal cabinet objects.

Attribute (*) indicates mandatory attributes	Description
Record Category Identifier  Note: This attribute is not displayed for Formal Record Cabinets.	 Note: You need a Department of Defense naming policy with a specific mask rule applied in order for this to work. This field is automatically populated according to the naming policy applied when one is applied to a Department of Defense formal cabinet. This field shows the actual file plan naming convention based on the value specified for the Attribute Name in the Mask Rule of the applied naming policy. This attribute is defined on the following object types: <ul style="list-style-type: none"> • Cabinet DoD 5015 V3 (dmc_rm_dod5015v3_cabinet) • Folder DoD 5015 V3 (dmc_rm_dod5015v3_folder) • Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec) • Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec) • Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)
Location  Note: This attribute is not displayed for Formal Record Cabinets.	This text box is used to specify the path to the formal cabinet.
Vital Record  Note: This attribute is not displayed for Formal Record Cabinets.	The checkbox is selected only if a markup with the vital designation has been placed on the cabinet itself. If you are creating the cabinet for the first time, it will be blank. However, if someone were to add a retention markup with a vital designation to it, then the checkbox would be on when you select the properties of the cabinet.

Attribute (*) indicates mandatory attributes	Description
Authors	<p>A contact responsible for the formal cabinet.</p> <p>You can Insert additional fields to identify more than one contact if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Keywords	<p>An attribute of this cabinet for example that can be used to facilitate searching.</p> <p>You can Insert additional fields to provide more than one keyword if necessary, though you are able to select only one using the radio button. You can also delete additional fields inserted by selecting the radio button and clicking Delete.</p> <p> Note: Multiple fields are reorganized if there is more than one author so that the author selected appears on top.</p>
Project name  Note: This attribute is not displayed for Formal Record Cabinets.	Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.
Supplemental Marking  Note: This attribute is not displayed for Formal Record Cabinets.	Add supplemental markings to add additional security to the object.
Record Category Description  Note: This attribute is not displayed for Formal Record Cabinets.	Use this for example, to describe and differentiate cabinets within a file plan.
Create Record Relationship	Lets you create a record relationship. For further details about record relationships, refer to " Record relations " on page 405.

- On the **Permissions** tab, click **Next** to accept the default settings or change the default settings as necessary to provide the desired level of basic and/or extended permissions needed for each user or group specified. You can ignore

making any entries or changes in the **Permissions** tab if you plan to apply any record security to the formal folder.



Note: Do NOT change the permissions if you plan to apply any record security, such as a security policy or shared marking, to the formal folder. The record security will override permissions on the formal folder and dictate the appropriate permissions.

You can add all the users and/or groups needed for the membership and assign the required level of permissions for each of their permissions. A **Search** button is available so you can see and examine what permissions are associated with a particular user or group before deciding to add it. A **Select** button is also available to change the permission set in instances where you would want to change the current membership so that the formal folder is associated with the permissions of a different set of members.

You can also single out one or more members under **Restrictions** if you have to reduce their level of permissions.

Advanced Permissions also makes it possible to specify one or more groups in which case a user must be a member of each to access the folder or to specify a set of groups in which case the user must be a member of at least one of the groups to access the folder.

7. Click **Finish**.

5.2.2.23 Searching records

Using the Formal Records tab on the Advanced Search screen you can search formal records. Formal records can be searched by object type in the current repository location or in other locations. An advanced search for formal records using the General tab does not filter subtypes. Results returned for the object you are searching will include all of its subtypes. A simple search or an advanced search can be performed according to the procedures provided in ["Search" on page 578](#). For additional details regarding advanced searches, using the General tab, against objects other than formal records, refer to ["Run an advanced search" on page 582](#).

Options in the list box for the Object Type include:

- Formal Record (dmc_rm_formal_record)
- Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec)
- Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)
- Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec)

Options in each list box for the Date include:

- Accessed
- Checkout Date
- Created

- Date Filed
- Effective Date
- Expiration Date
- Last Review Date
- Modified
- Retain Content Until

Records returned can be limited to a particular size. Only those records according to one or more properties can also be returned or according to text contained in filenames or content.

You can search for records directly whether they are formal records or typical records according to the record filename, or you can search the different container types used to store records. Container types include formal cabinets, cabinets, formal folders, and folders, including physical containers such as a warehouse, bay, shelf, physical folder, bin, or box.



Note: Clear the Search cache or turn Search caching *off* to avoid unintended search results.

Also, records under retention that have been transferred might have its metadata or its content destroyed. Search results that include a record with its content destroyed does not mean that the user has a permissions or browser problem. The user should not think they have such a problem.

5.2.2.24 Records Manager Reports

Only the working paper report is available with Records Manager, unless Department of Defense classified records functionality is installed to include the declassification report.

Follow this link to run the working paper report [“Running a working paper report” on page 354](#).

Follow this link, to the appendix, to run the declassification report [Appendix C, Records Manager and Department of Defense functionality on page 723](#).

For a reports overview, refer to [“Records reporting” on page 86](#).

5.2.2.25 Records Manager audit events

“Audited events in Records Manager” on page 441 describes the information, in the audit trail object, that is stored in string_1 to string_5 of the audit trails for Records Manager events. Only the strings that are populated are listed. Objects are also described for audit trails that pass one or more object IDs.

For an overview of auditing and the procedures to enable auditing, to activate the audit policy schema, to verify an auditing of an event, and to view and remove an audit refer to, **“Records auditing” on page 78**.



Note: Although up to five strings can be utilized by an event, only strings 1 and 2 are displayed in the results of an Audit Trail Report. Also, the content of one string may spill into the next string if it needs extra space.

Table 5-36: Audited events in Records Manager

Records Manager audit events (Application Code = dmc_rm)		
<i>Target Object Type: dm_sysobject</i>		
Check the Include all subtypes on the Register Audit screen when adding/selecting the various events for only this object type.		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_apply_attribute_marking	string_1: name of attribute marking	n/a
dmc_rm_apply_containment_policy	string_1: name of containment policy	n/a
dmc_rm_apply_naming_policy	string_1: name of naming policy	n/a
dmc_rm_apply_restrictive_marking	string_1: name of restrictive marking	n/a
dmc_rm_apply_security_level	string_1: name of security level.	n/a
dmc_rm_apply_security_policy	string_1: name of security policy	n/a
dmc_rm_apply_shared_marking	string_1: name of shared marking	n/a
dmc_rm_remove_attribute_marking	string_1: name of attribute marking	n/a
dmc_rm_remove_containment_policy	string_1: name of containment policy	n/a
dmc_rm_remove_naming_policy	string_1: name of naming policy	n/a
dmc_rm_remove_restrictive_marking	string_1: name of restrictive marking	n/a

Records Manager audit events (Application Code = dmc_rm)		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_remove_security_level	string_1: name of security level	n/a
dmc_rm_remove_security_policy	string_1: name of security policy	n/a
dmc_rm_remove_shared_marking	string_1: name of shared marking	n/a
<i>Target Object Type: dm_document</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_added_to_formal_record The object was declared as a formal record.	string_1: name of formal record. Examples: genius.htm, john.doc string_2: type of formal record. Examples: dmc_rm_formal_record, dmc_rm_dod5015v3_std_rec	ID1: formal object id
dmc_rm_removed_from_formal_record The formal record was undeclared. Each child object will generate this event.	string_1: name of formal record string_2: type of formal record	ID1: formal object id
<i>Target Object Type: dmc_rm_security_policy</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_add_sp_perm This event is generated when a new rule is added to a security policy. The rule specifies permission that are applied based on object type.	string_1: target object type. Examples: dmc_rm_formal_record, dm_folder, dm_cabinet, dm_document, dm_sysobject string_2: ACL name. Examples: dmc_rm_450011b780001128, dmc_rm_450011b780001126	n/a
dmc_rm_remove_sp_perm	string_1: target object type string_2: ACL name	n/a
<i>Target Object Type: dmc_rmContainment_policy</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_add_cp_rule This event is generated when a new rule is added to a containment policy. The rule specifies a pair of object types that indicates what type of object can be contained in another object type.	string_1: parent object type. Example: dm_folder string_2: child object type. Example: rm_dod5015ch4record	ID1: object id

Records Manager audit events (Application Code = dmc_rm)		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
<i>Target Object Type: dmc_rm_naming_policy</i>		
dmc_rm_remove_cp_rule	string_1: parent object type string_2: child object type	ID1: object id
<i>Target Object Type: dmc_rm_class_subscript_list</i>		
dmc_rm_add_np_rule This event is generated when a new rule is added to a naming policy. The rule is either a mask rule or a construct rule that acts based on an object type.	string_1: object type. string_2: rule type, 0=mask rule, 1=construct rule	ID1: object id
dmc_rm_remove_np_rule	string_1: object type string_2: rule type, 0=mask rule, 1=construct rule	ID1: object id
<i>Target Object Type: dmc_rm_dod5015v3_class_rec</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_new_class_subscript_list	string_1: object name of the subscription list string_2: description	ID1: object id of subscription list
dmc_rm_delete_class_subscription	string_1: object name of the subscription list string_2: description	ID1: object id of subscription list
dmc_rm_add_class_subscription_item	string_1: object name of the item string_2: description	ID1: object id of the subscription list item
dmc_rm_remove_class_subscription_item	string_1: object name of the item string_2: description	ID1: object id of the subscription list item
<i>Target Object Type: dmc_rm_dod5015v3_class_rec</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rm_record_declass_purge_in_progress This audit indicates that the system is about to purge the classified record. The result of the purge will be tracked in a later audit based on dmc_rps_dispose.	n/a	ID1: object id of declassified record

Records Manager audit events (Application Code = dmc_rm)		
dmc_rm_record_declass_purge_ready This audit indicates that the administrator has confirmed that the purge can take place and that the object can be disposed (e.g. it does not have a hold/permanent). This is usually followed by the dmc_rm_record_declass_purge_in_progress. That audit will not happen if one of the children of the classified record can't be destroyed.	string_1: justification	ID1: object id of declassified record
dmc_rm_record_declassify This audit indicates that the classified record's classification was lowered to the lowest classification	string_1: from previous classification string_2: to the lowest classification	ID1: formal object id
dmc_rm_record_downgrade This audit indicates that the classified record's classification was lowered (but not to the lowest classification)	string_1: from previous classification string_2: to the new classification	ID1: formal object id
dmc_rm_record_upgrade This audit indicates that the classified record's classification was raised.	string_1: from previous classification string_2: to the new classification	ID1: formal object id
<i>Target Object Type: dm_user</i>		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_records_performed_search	If the query length is less than 200 characters, string 1 will contain the query. Among all 5 strings, the query will be broken up so that a maximum of 1000 characters of the query can be stored. If the query length is greater than 1000, the query will be truncated. Example: SELECT object_name,a_content_type,r_modify_date,r_object_id,r_object_type, ...and so forth.	ID1: object id

5.2.2.26 Records Manager jobs

Jobs can automate certain processes and can be scheduled to work continuously. Job objects are available and executable on a user-defined schedule.

Actions performed by Records Manager jobs are described in “[Records Manager jobs and method arguments descriptions](#)” on page 445. You can find further details about a job, Last Run and Job Status for example, under Job Management (Administration > Job Management > Jobs) if you log in to Documentum Administrator.

Administrators can disable a job from its Properties to prevent it from running automatically. To enable or disable a job, right-click the job and select Properties. On the Properties screen for the State attribute select *Inactive* to disable or *Active* to enable.

Although a job may be disabled from running automatically, it can at any time be run manually. To run a job manually, if you cannot wait until it is run automatically, right-click the job and select Run.

Table 5-37: Records Manager jobs and method arguments descriptions

Job name	Description	Method arguments	Description
dmc_rm_DeclassificationJob	Declassifies classified records when the value specified for the Declassify On Event or Declassify On Date is reached. It is based on either attribute depending on the one selected when the classified record was declared. For further details about these attributes, refer to Entering values for Department of Defense classified records form, page 80. (Declassify and Downgrade Job)	No arguments.	
dmc_rm_Destroy_WorkingPaperJob	Deletes working papers from the repository after a configurable number of days. (Destroy Working Paper Job)	No arguments.	

5.3 Commonwealth administration



Note: Each records product is role based and therefore all users and administrators must be in the correct role for the expected functionality to work properly. It is equally important that each instance of the Records Client, which hosts each of the records products, is registered for Privileged DFC.

5.3.1 Overview

Records Manager Commonwealth Edition is available with the purchase of Records Manager.



Note: To avoid potential problems and unnecessary troubleshooting, make sure 1) that you are in the correct Records Manager Commonwealth Edition role for the operation you are attempting and 2) that the instance of the Records Client you are working on, is approved for Privileged DFC. Each instance of the Records Client must be Privileged DFC approved for any of the records products, Retention Policy Services, Records Manager, and Records Manager Commonwealth Edition, to work properly. To determine which Records Manager Commonwealth Edition role an administrator or end user has to be a member of for specific operations, refer to [“Commonwealth roles and functional access” on page 448](#).

Records Manager Commonwealth Edition provides the ability to manage content records in a manner that is compliant with Commonwealth Records standards. Records Manager Commonwealth Edition deploys on top of Records Manager. Features include:

- Classification schemes
- Files and file parts (volumes)
- Series numbering and titles
- Records containers (electronic, physical, hybrid)
- Sentence on creation
- Basic bulk load capability
 - Business Classification Scheme (BCS)
 - Retention Disposal Authority (RDA) (Retention Policies)
- For column preferences, refer to [“Setting column preferences” on page 77](#)

The Commonwealth Administration node is available when Records Manager is installed. Although it is available when Records Manager is activated, its dar files have to be installed along with the Records Manager dar files for its activation to be successful. The Commonwealth Administration node provides additional records management functionality to meet records management requirements of the Australian State and Federal Governments and other organizations. Commonwealth

administration is based on policies of National Archives of Australia (NAA) and is closely related to ISO 15489, VERS, and MoReq.

Commonwealth files or simply files and commonwealth file parts or simply file folders, are unique containment objects meant to handle records as files and file parts. You can think of a file as a drawer that can contain one or more documents. If necessary, you can further organize and divide the drawer into sections called file parts. For example, GM can represent the file. Pontiac, Buick, and so on, can be used to divide the file into file parts. Files must be associated to a thesaurus term in the Functional Thesaurus. All file parts added to a file, retain their content by inheritance, according to the retention policy associated to the thesaurus term selected/applied against the parent file. Files and file parts containment is administered using thesaurus terms and if desired, series control to provide additional classification metadata for numbering and titling based on a mask pattern defined/entered for the Series when you create a commonwealth file.

Thesaurus terms can be imported from an xml file referred to as the Business Classification Scheme (BCS), or they can be created directly in the Functional Thesaurus. The BCS is a collection or hierarchy of thesaurus terms (also known simply as classification terms) used to create files. When a file is created, its Function is selected from a controlled vocabulary (a thesaurus term) that dictates the retention policy for that file, its parts, and all content. Thesaurus terms must also be associated to a retention policy before using them to classify a file. Retention policies have *linked* retention as the default setting for the Retention Strategy, so that all content added ages as a single unit. The entire file or file part and all of its contents and metadata are disposed of in a single action according to the Disposition Strategy.

Series Control, which is optional, provides additional classification metadata to further organize files, when they are created, by a file part number and period, one or more years for example, according to the mask pattern defined on the Series tab for the series control file selected from the Series Control node. Patterns on the series control file, selected for a commonwealth file, can be modified to the desired pattern from the Series tab on its Properties screen. Refer to additional details within the instructions for creating a file.

You must be in one of the following four roles to access commonwealth functionality.

- Records Manager Commonwealth Edition Administrator (rmce_administrator):
 - Administers the records implementation including bulk operation functionality.
 - This role is also a member of the Records Manager role.
- Records Manager Commonwealth Edition Records Manager (rmce_record_manager):
 - Manages records structures and supporting objects such as retention policies, BCS terms, Locations, and so on.
 - This role is also a member of the Records Manager role.

- Records Manager Commonwealth Edition Creator (rmce_creator):
 - Creates and updates files and file parts.
 - This role is also a member of the Privileged User role.
- Records Manager Commonwealth Edition Contributor (rmce_contributor):
 - Can add documents/objects to a file making them a record.
 - This role is also a member of the Records Contributor role.

“Commonwealth roles and functional access” on page 448 identifies each role and the functions a user can access if the user is a member of that role. Procedures following the table, contain the instructions for each of the functions listed in the table.

Table 5-38: Commonwealth roles and functional access

Function	Administrator	Manager	Creator	Contributor
Create Files	x	x	x	
Close Files	x	x		
Reopen Files	x	x		
Update Files	x	x		
Create File Parts	x	x	x	
Close File Parts	x	x		
Reopen File Parts	x	x		
Update File Parts	x			
Import BCS	x			
Import Retention Policy	x			
Classify a File	x	x	x	
Add to a File	x	x	x	x
Remove from a File	x	x		
Add to a File Part	x	x	x	x
Remove from a File Part	x	x		
Create Thesaurus Term	x	x		

Function	Administrator	Manager	Creator	Contributor
Update Thesaurus Term	x	x		

The following physical marking attributes included on the Physical Info tab of a physical object are also included on the General tab of a Commonwealth file or file part:

- Barcode
- Lost
- Mark for Export
- Mark for Shipped
- Mark for Destruction
- Physical Object Destroyed
- Mark for Contained Objects Destruction
- Contained Objects Physically Destroyed
- Home Location
- Current Location
- Next Location

5.3.2 Create a file

Although you can create/define a thesaurus term without associating it to a retention policy, you cannot create a commonwealth file unless the thesaurus term selected is associated to a retention policy. You can associate a retention policy to a thesaurus term upon defining the thesaurus term or from its properties at a later time. And, Business logic built into files is intended to prevent you from creating a file within another file and from creating folders, formal folders, and physical containers in files. Although you can create files outside of these containers, you can also create them within these containers, cabinets, folders, or physical containers.



Note: All files consequently behave differently depending on the thesaurus term selected and its associated retention policy. Documents in a file or file part cannot be promoted if the associated retention policy does not have a valid authority specified.

To create a file:

1. Navigate to a cabinet, folder, or physical container where you want to create a file and select **File > New > Commonwealth File**.
2. Click **Next** on the **Create** tab after you are done entering a unique value for the mandatory **Name**.
3. On the **General** tab, click **Browse** to select a **Classification Term**.

If no terms are listed in the **Term Selector** screen under **Functional Thesaurus** for **Terms**, follow instructions to either create or import one or more thesaurus terms from the **Functional Thesaurus** node under **Commonwealth Administration**.

 **Note:** The mandatory **Date Opened** attribute can be edited so that the file can be back dated. Changes to this date will change the qualification date used to control aging of the retainer and the promotion of its contents from one phase to the next. Although the qualification date is used to determine whether or not an object can be promoted, a valid authority must also be specified on the retention policy for that phase.

Values for the optional attributes can be changed now or at a later time if necessary. If a classification term you want to specify has not already been created, create one and then return to this procedure to Browse to it. You may need to contact someone who is in the appropriate role, if you are not already in a role that gives you the permissions to create a thesaurus term.

 **Note:** If used, the **Series Name** and the **Series Period** attributes rely on the files listed in the **Series Control** node. The list box for the **Series Name** for example, is populated against all series control files listed in the **Series Control** node. The list box for the **Series Period** however is populated against the series control file selected for the **Series Name**. The **Properties: Info** screen is an example of a series control file listed on the **Series Control** node.

Values entered for the **File No** determines the entry for NNNNNNNN. Values entered for the **Period** determines the entry for PPPP. Valid masks are:

- PPPP
The period shown as four numerals.
- NNNNN
The file or part number shown as five numerals.
- {}
Value of the attribute entered between {}.
- THESAURUS_FULL
The full path of the BCS term.
- THESAURUS_NAME
The assigned BCS term name.
- /~
Separator.

The result of adding series control, populates the **Title** and the **File Number** attributes as can be seen if you compare the **Properties** of two files after they are

created. One created with series control and the other created without series control.

4. Click **Finish** if you want to accept default settings on the **General** tab, or enter values for the attributes as necessary and then click **Finish**, or click **Next** to change default settings on the **Permissions** tab if necessary, and then click **Finish** to complete the operation.

5.3.3 Close a file

You can close a file to prevent documents from being added to it. Business logic built into files is intended to prevent you from closing them unless all of the file parts contained are closed first. A file can be closed only if it is empty or if all file parts contained are closed. The option displayed in the list box to close a file part is not available (grayed) if it is already closed.



Note: The Retention Policy Services Close/Reopen menus, if you are working with the Records Manager Commonwealth Edition, are not available for Commonwealth files and file parts.

To close a file:

1. Right-click a file displayed in the content pane and from the list box displayed, select **Close Commonwealth File**.
2. Click **OK** on the confirmation screen to continue and finish the operation.
The Format displayed in the content pane, after the screen refreshes, indicates that the file is closed.

5.3.4 Reopen a file



Note: The Retention Policy Services Close/Reopen menus, if you are working with the Records Manager Commonwealth Edition, are not available for Commonwealth files and file parts.

To reopen a file:

1. Right-click a closed file displayed in the content pane and from the list box displayed, select **Reopen Commonwealth File**.
2. Click **OK** on the confirmation screen to continue and finish the operation.
The Format displayed in the content pane, after the screen refreshes, indicates that the file is reopened.

5.3.5 Update a file

Attribute settings defined for a file after it has been created can be updated at any time when necessary from its properties. You may want to update for example, if you have to change the current thesaurus term.

To update a file:

1. Right-click a file displayed in the content pane and from the list box displayed, select **Properties**.
2. Pick and choose the attributes you want to change settings for and then click **OK** to finish the operation.

The Properties screen, unlike the Create screen, includes a fourth tab for the History.

5.3.6 Create a file part

File parts are created within files. Only one file part may be open at a time however, multiple file parts can be reopened.

To create a file part:

1. Navigate to a file and select **File > New > Commonwealth File Part**.
2. Click **Next** on the **Create** tab after you are done entering a unique value for the mandatory **Name**.
3. Click **Finish** if you want to accept default settings on the **General** tab, or enter values for the attributes as necessary and then click **Finish**, or click **Next** to change default settings on the **Permissions** tab if necessary, and then click **Finish** to complete the operation.

A value must be specified on the **General** tab for the **Date Opened** and for the **Storage Type** to finish the operation.

5.3.7 Close a file part



Note: The Retention Policy Services Close/Reopen menus, if you are working with the Records Manager Commonwealth Edition, are not available for Commonwealth files and file parts.

To close a file part:

1. Right-click a file part displayed in the content pane and from the list box displayed, select **Close Commonwealth File Part**.
2. Click **OK** on the confirmation screen to continue and finish the operation.

The Format displayed in the content pane, after the screen refreshes, indicates that the file part is closed.

5.3.8 Reopen a file part



Note: The Retention Policy Services Close/Reopen menus, if you are working with the Records Manager Commonwealth Edition, are not available for Commonwealth files and file parts.

To reopen a file part:

1. Right-click a closed file part displayed in the content pane and from the list box displayed, select **Reopen Commonwealth File Part**.
2. Click **OK** on the confirmation screen to continue and finish the operation.
The Format displayed in the content pane, after the screen refreshes, indicates that the file part is reopened.

5.3.9 Update a file part

To update a file part:

1. Right-click a file part displayed in the content pane and from the list box displayed, select **Properties**.
2. Pick and choose the attributes you want to change settings for and then click **OK** to finish the operation.

The **Properties** screen, unlike the Create screen, includes a fourth tab for the History.

5.3.10 Import the business classification scheme (BCS)

The BCS is essentially a collection of terms that are imported and made available in the Thesaurus Terms node on the client application for creating commonwealth files and commonwealth file parts. To import a BCS, you must first prepare an XML schema file with the thesaurus term definitions and then import it from the Tools menu. Terms are created when the XML schema file is imported. Terms can be associated with a retention policy and include additional data such as scope notes and links to related terms. Although it is optional to specify a retention policy for a term, terms that do not specify a retention policy cannot be used for filing or classification. Classification Terms used to create commonwealth files and commonwealth file parts must be associated to retention policy. Terms once the BCS is imported are created and then matched to retention policies (RDAs).

Terms are created successfully if the XML schema file is constructed correctly according to the following example.

The attribute tags for each term in the example are defined in the following list.

- <term>
 - <name> identifies the name of the term

- <rda> identifies the name of the retention policy the term applies to. Some terms in the example omit this entry as it is optional. The system will create the retention policy if it does not already exist. The system ignores those terms that do not have a rda entry. Only terms with a retention policy specified can be used for classification.
- <source> identifies the entity that mandated the term for example, and populates the Thesaurus Source on the Properties: General tab for a thesaurus term
- <termlevel> populates the Full Qualification attribute. Community Relations for example is displayed first if it has a term level of 1 whereas Acquisition (1001) is displayed next, as the second term, if it has a term level of 2. Terms with term level 2 are nested one after the other below terms with term level 1. Compare the sample BCS XML schema file to the terms listed in the term selector illustrated below.
- <scopenotes> populates the Scope Notes attribute
- <preferredterm> populates the Preferred Term attribute
- <obsoleteterm> populates the Related Terms attribute

Sample BCS XML schema file

Make sure to configure the BCS XML schema file as follows to successfully import retention policies:

```
<bcs>
  <term>
    <name>COMMUNITY RELATIONS</name>
    <rda>repol_1</rda>
    <source>AFDA</source>
    <termlevel>1</termlevel>
    <scopenotes></scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
  </term>
  <term>
    <name>Acquisition (1001)</name>
    <source>AFDA</source>
    <termlevel>2</termlevel>
    <scopenotes>Records documenting the acquisition of goods and services (eg catering services) required to support the community relations function where there is no tender or contracting-out process (ie where the cost of the acquisition is below the threshold for tendering or where a purchase is made against a period contract).</scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
  </term>
  <term>
    <name>Addresses (presentations) (1002)</name>
    <source>AFDA</source>
    <termlevel>2</termlevel>
    <scopenotes>Final version of addresses made by the portfolio Minister or senior agency officers at major public occasions.</scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
  </term>
  <term>
    <name>Customer Service (1021)</name>
    <source>AFDA</source>
```

```

        <termlevel>2</termlevel>
        <scopenotes>Records documenting the planning, monitoring and
            evaluation of customer services provided to the agency's
            public clients.</scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>Functions (social) (1031)</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>2</termlevel>
        <scopenotes>Records documenting the organisation and management of
            an official or formal social occasion. Includes venue bookings,
            guest lists, invitations and catering.</scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>Reporting (1060)</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>2</termlevel>
        <scopenotes>Final version of internal formal reports and reports made
            to external agencies relating to the community relations
            function.</scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>FLEET MANAGEMENT</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>1</termlevel>
        <scopenotes></scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>Accidents (1292)</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>2</termlevel>
        <scopenotes>Records detailing accidents/incidents involving Commonwealth
            vehicles. Includes:/n/n vehicle accident reports/n investigation
            reports/n documents authorising the use of the vehicle/n records of
            driver/operator/pilot licences and certificates of competencies/n logs
            of vehicle operations /n booking schedules and other evidence supporting
            the use of the vehicle.</scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>Disposal (1311)</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>2</termlevel>
        <scopenotes>Records documenting the return of leased vehicles.
            Includes:/n/n written notices and correspondence with leasing
            companies/n handover reports /n notification that the agency or
            its nominee wishes to purchase a vehicle/n arrangements for the
            restoration of the vehicle to the original condition.</scopenotes>
        <preferredterm></preferredterm>
        <obsoleteterm></obsoleteterm>
    </term>
    <term>
        <name>Infringements (1312)</name>
    <rda>repo1_1</rda>
        <source>AFDA</source>
        <termlevel>2</termlevel>
        <scopenotes>Records documenting breaches of the agency's rules and/or
            regulations.</scopenotes>
    </term>

```

```
    driving, traffic, aeronautical or marine laws. Includes copy of
    infringement notice, correspondence with relevant authority and other
    supporting documentation.</scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
</term>
<term>
    <name>LEGAL SERVICES</name>
<rda>repo1_1</rda>
    <source>AFDA</source>
    <termlevel>1</termlevel>
    <scopenotes></scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
</term>
<term>
    <name>Advice (1567)</name>
<rda>retpol_1_dec_1</rda>
    <source>AFDA</source>
    <termlevel>2</termlevel>
    <scopenotes>Records documenting advice received from an internal or
    external legal service provider relating to:/n/n Cabinet matters/n
    international law/n national security/n agency-wide industrial
    issues/n interpretation of an agency's own legislation/n proposal
    for new or amended agency legislation./n/nIncludes instructions to
    the provider, records of ongoing discussions, revisions of
    instructions and drafts.</scopenotes>
    <preferredterm></preferredterm>
    <obsoleteterm></obsoleteterm>
</term>
</bcs>
```

After the BCS XML schema file is imported, you can then navigate to Commonwealth Administration > Thesaurus Terms to see the results in the content pane and view the Properties.

Clicking the Browse button on the Properties screen for a thesaurus term displays the Term Selector. Add or remove the desired values for the Preferred Term and the Related Terms.

Commonwealth files and commonwealth file parts rely on the terms in the Functional Thesaurus for classification. Terms in the Functional Thesaurus can be nested in other existing term folders depending on how you specify the value in this procedure for the Starting Branch. You can follow these instructions to import thesaurus terms or create them directly in the repository. The BCS is used to populate the Functional Thesaurus with the thesaurus terms used to create commonwealth containers. Administrators can share copies of the same BCS for their repositories and modify terms if necessary to suit their needs.

If you are importing a BCS, you are in effect importing an xml schema file that has to be stored somewhere in the repository. The Import: Folder Selection screen is used to locate a preferred storage location for the xml file. Terms are read into the Functional Thesaurus during the import process, regardless of where it is stored in the repository. The path you select for the Starting Branch on the subsequent BCS Import screen determines where in the Functional Thesaurus the terms will appear, in the root or within one of the folders in the root. The root path to the Functional Thesaurus is /System/Applications/RmceConfig/Functional Thesaurus. You can select the root or drill deeper if necessary. Though the xml file is no longer used after

it is imported, it is always available in the storage location specified for anyone who might later need a copy they can modify for another repository.

To import the BCS:

1. Navigate to **Commonwealth Administration** and select **Tools > RMCE > Thesaurus > Import**.
2. On the **Folder Selection** screen, navigate to the preferred cabinet or folder to store the xml file, select it and then click **Next**.
Log in to the selected repository if the **Authentication** screen is displayed, select the cabinet or folder and then click **Next**.
3. On the **BCS Import** screen, enter values for the **File** location and for the **Starting Branch** and then click **Finish**. The **Description** is optional.
Click **Browse** to locate the xml file.
Click **Select** for the **Starting Branch**, to add all thesaurus terms on the xml file to the Functional Thesaurus folder in the System cabinet under the Cabinets node, its root or any of the existing terms in the root. The root path to the Functional Thesaurus is /System/Applications/RmceConfig/Functional Thesaurus. You can select the root or drill deeper if necessary. If you make the **Starting Branch** the root, it means users do not have to navigate to another existing term folder under the **Functional Thesaurus** node to view the terms.
4. Click **Finish** to complete the import.
All thesaurus terms on the xml file are displayed in the content pane under **Functional Thesaurus** or within one of the term folders listed in the content pane.

5.3.11 Import a retention policy

To import retention policies, you first need to prepare an XML schema file with the retention policy definitions and then import the XML schema file from the Tools menu. Retention policies are created when the XML schema file is imported.

Retention policies are created successfully if the XML schema file is constructed correctly according to the example below. The attributes in the example are defined in the following list. The attributes listed are currently supported. Currently, the schema creates linked 1 phase plus Final phase retention policies:

- The <rda> block (between beginning and end tags) associates the values of the following attributes, at the top of the schema, to all retention policies:
 - The value for the <source> though it is not involved in any processing can be used to identify the entity that mandated the policy for example
 - The value for the <authorityname> is assigned to all retention policies added to the schema



Note: The authority is created for you by the system if the authority with the value entered does not exist.

- The value for the <authoritydescription> is an attribute of the authority object
- The <rdaentry> contains one or more retention policy definitions
- Each <activity> represents the first phase of a retention policy, the system creates the final phase. This tag is used to specify a value for the name of the retention policy:

- <entryno>

This tag is used to specify a number for the retention policy in addition to the name specified for the <activity>. You can see this value, once the retention policy is created after the schema is imported, appended to the beginning of the retention policy name, that is to the beginning of the value specified for the <activity>. You can see this value appended to the beginning of the retention policy name, after the schema is imported and the retention policy created.

- <description>

This and the remaining tags are attributes of the retention policy.

- <action>

This tag is used to specify a Disposition Strategy. The value should match an existing strategy.

- <durationyears>

This and the remaining tags are the attributes of the first phase of the retention policy created.

- <durationmonths>

- <durationdays>

- <condition>

Upon import, linked 1 phase plus Final phase retention policies are created.

Sample RP XML schema file

Make sure to configure the retention policy XML schema file as follows to successfully import retention policies:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rda>
    <source>BP</source>
    <authorityname>BPRA</authorityname>
    <authoritydescription>BP Records Authority</authoritydescription>
    <rdaentry>
        <activity>EQUIPMENT & STORES-Disposal</activity>
        <entryno>1142</entryno>
        <description>Records documenting the disposal of leased equipment and stores. Includes written notices and correspondence to and from leasing companies in relation to return of equipment and stores, handover reports and notifications that an agency or their nominee wish to purchase equipment and stores.</description>
```

```

<action>Destroy all</action>
<durationyears>3</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after disposal</condition>
<activity>FINANCIAL MANAGEMENT-Budgeting</activity>
<entryno>1242</entryno>
<description>Records documenting spending progress or revenue collection against allocations within the budget estimates.</description>
<action>Destroy all</action>
<durationyears>3</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after action completed</condition>
<activity>INFORMATION MANAGEMENT-Risk Management</activity>
<entryno>1550</entryno>
<description>Risk register relating to the information management function.</description>
<action>Destroy all</action>
<durationyears>7</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after next risk assessment </condition>
<activity>LEGAL SERVICES-Claims</activity>
<entryno>1576</entryno>
<description>Records documenting the provision of legal representation relating to claims that do not proceed to litigation or settlement by an agreement. Includes withdrawn claims.</description>
<action>Destroy all</action>
<durationyears>7</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after settlement or withdrawal of claim</condition>
<activity>TECHNOLOGY & TELECOMMUNICATIONS-Security</activity>
<entryno>2167</entryno>
<description>Requests for approval to connect equipment to agency networks, either on agency premises or via dial-up communications links.</description>
<action>Destroy all</action>
<durationyears>3</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after action completed</condition>
<activity>TECHNOLOGY & TELECOMMUNICATIONS-Security</activity>
<entryno>2168</entryno>
<description>Records documenting the control of removable media in secure systems. Includes inventory of removable items, media musters and register of media import and export (eg floppy disks and the removal of hard disks).</description>
<action>Destroy all</action>
<durationyears>7</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after action completed</condition>
<activity>TECHNOLOGY & TELECOMMUNICATIONS-Standards</activity>
<entryno>2170</entryno>
<description>Records documenting the implementation of industry and agency standards to support the technology and telecommunications function.</description>
<action>Destroy all</action>
<durationyears>7</durationyears>
<durationmonths>0</durationmonths>
<durationdays>0</durationdays>
<condition>after action completed</condition>
</rdaentry>
</rda>
```

Retention policies created based on the example XML schema file imported are listed under Retention Policies. Notice how the <entryno> is appended to the name

of the retention policies listed. The descriptions too should match the definitions on the XML schema file.

Select the Properties of a retention policy created from the XML schema file, to see how the attribute values match up with the definitions.

Select the Info tab, to see how the attribute values match up with the definitions on the XML schema file.

Select the Phases tab, to see how the attribute values match up with the definitions on the XML schema file. Click the Active phase to see its attribute values.

Click the Final phase, to see its attribute values.

Make sure the XML schema file is available for import.

You can import retention policies into the repository and use them as necessary if the retention policy associated to a thesaurus term has to be updated/replaced.

To import a retention policy:

1. Navigate to **Commonwealth Administration** and select **Tools > RMCE > Retention Policies > Import**.
2. On the **Folder Selection** screen, select a storage location for the XML schema file, and then click **Next**.
Log in to the selected repository if the **Authentication** screen is displayed, select the cabinet or folder and then click **Next**.
3. On the **Retention Policy Import** screen, click **Browse** to enter a value for the **File** location and then click **Finish**. Entering a value for the **Description**, though optional, will help you differentiate XML schema files stored in the same location.
4. Navigate to **Retention Policy Services > Retention Policies** to see the list in the content pane.

5.3.12 Classify a file

Commonwealth files are classified upon creation.

To classify a file:

1. Select **File > New > Commonwealth File**
2. Type a unique name on the **New File: Create** tab and click **Next** to continue.
3. Enter values for the mandatory attributes, **Classification Term**, **Date Opened**, and the **Storage Type**, on the **General** tab and then click **Finish**. Values for the optional attributes can be changed now or at a later time if necessary. Or, click **Next** to change default settings on the **Permissions** tab if necessary, and then click **Finish** to complete the operation.

5.3.13 Add to a file

Documents and file parts can be added to files. Documents can be created directly in the file or existing documents can be imported. A document or file part added to a file is under retention according to its functional term and the retention policy it is associated to.

To add to a file:

1. Navigate to a file and select **File > New > Document** or, select **File > Import**.
In either case, the document is locked with a key appearing next to the document icon in the content pane.
2. Right-click the new document and select **Check In**.
3. Click **OK** on the **Check In** screen to accept the default settings or, update entries for the various attributes as necessary and then click **OK**.

5.3.14 Remove from a file

To remove from a file:

1. Navigate to a file, select a document in the content pane and select **Edit > Add to Clipboard**.
2. Navigate to the new container location and select **Edit > Move Here**.

5.3.15 Add to a file part

Adding to a file part is the same as adding to a file or folder, either by creating a new document or by importing an existing document. A document added to a file part inherits retention from the parent file.

To add to a file part:

1. Navigate to a file and select **File > New > Document** or, select **File > Import**.
In either case, the document is locked with a key appearing next to the document icon in the content pane.
2. Right-click the new document and select **Check In**.
3. Click **OK** on the **Check In** screen to accept the default settings or, update entries for the various attributes as necessary and then click **OK**.

5.3.16 Remove from a file part

To remove from a file part:

1. Navigate to a file part, select a document in the content pane and select **Edit > Add to Clipboard**.
2. Navigate to the new container location and select **Edit > Move Here**.

5.3.17 Create a thesaurus term

Thesaurus terms (also called classification terms) in the Functional Thesaurus are used to classify files and file parts and, can be either imported from a Business Classification Scheme according to instructions above, or they can be created according to the instructions in this procedure.

To create a thesaurus term:

1. Navigate to the **Functional Thesaurus** node and select **File > New > Thesaurus Term**.
2. On the **New Folder: Create** tab, type a unique value for the mandatory **Name** and click **Next**.
The value entered for the name is used to populate the value for the **Full Qualification** attribute on the **General** tab.
3. On the **New Folder: General** tab, type a value for the mandatory **Thesaurus Source**. All attributes are described in “[Attribute descriptions for creating a thesaurus term](#)” on page 462. Optional entries can be addressed during creation or at a later time from the **Properties** of the thesaurus term. Preferred and related terms are based on other thesaurus terms and therefore must be created ahead of time before they can be selected when you browse.

Table 5-39: Attribute descriptions for creating a thesaurus term

Attribute	Description
Name	The value typed for the Name on the Create tab.
Preferred Term	Enter a preferred term if you would like to recommend an alternate from existing terms in the Functional Thesaurus. The current term for example, if it becomes obsolete for any reason, would use the preferred term.  Note: A term that is preferred cannot be deleted unless all references to the term are removed.

Attribute	Description
Related Terms	<p>Enter one or more related terms if you would like to recommend related terms from existing terms in the Functional Thesaurus. Filing documents according to this term you are creating might be meant for another term. For example, documents that were filed against this term should now be filed against the related term going forward.</p> <p> Note: A term that is related cannot be deleted unless all references to the term are removed.</p>
Citation	<p>Authorized personnel, the thesaurus administrator for example, can enter text for this from the properties.</p>
Full Qualification	<p>Read-only calculated field that indicates the relative location of the term. This is the full qualified thesaurus entry. For example: PERSONNEL/Accidents.</p>
Mandate	<p>Authorized personnel can enter text for this from the properties.</p>
Retention Policy	<p>This is the entry ID of the retention policy ID to be applied to this thesaurus category entry. The retention policy you select for this attribute will be used to retain documents added to files or file parts that use this term. Although optional, if a retention policy is not specified, the term cannot be used to create a commonwealth file. If the term is meant to organize terms only, then you may not want to specify a retention policy.</p>
Scope Notes	<p>Text is automatically extracted from the imported XML or can be entered manually by authorized personnel.</p>
Thesaurus Source	<p>The value typed here could be used to represent an authority (person or entity), the name of your organization, department, or other entity.</p> <p>This indicates the source of the thesaurus category. The entry is either generated from the core Keyword AAA ce thesaurus or a government department developed one.</p> <p>This is captured when the thesaurus is first imported into Records Manager Commonwealth Edition.</p>

4. Click **Finish** to complete the operation, or click **Next** if you want to set/change the default permissions settings on the **Permissions** tab and then click **Finish**.
5. Optionally, you can select a thesaurus term and create another term under it, similar to a subfolder.

To do this, double-click a thesaurus term, *PERSONNEL* to continue with our example, and select **File > New > Thesaurus Term** to repeat steps 2-4. The name entered for this new term, *Injuries* for example, is now appended to the value displayed for the **Full Qualification** attribute. For example, */PERSONNEL/Injuries*. You can repeat this to nest additional terms as necessary.

To see the results, navigate to **Functional Thesaurus**. Double-click the thesaurus term that is in question, *PERSONNEL*. Right-click the term displayed, *Injuries*, and select **Properties**. **Properties** is displayed. You can see the hierarchy of the thesaurus terms in the **Term Selector**, when you click **Browse**. For example, when creating a thesaurus term, viewing its **Properties**, or when creating a commonwealth file.

5.3.18 Update a thesaurus term

Thesaurus terms can be updated from their properties, whether they are imported or created.

To update a thesaurus term:

1. Navigate to the **Functional Thesaurus** node or to one of the term folders.
2. Right-click a thesaurus term displayed in the content pane and select **Properties**.
3. Click **OK** when you are done making the desired changes.

5.3.19 RM Commonwealth audit events

“Audited events in RM Commonwealth Edition (RMCE)” on page 465 describes the information, in the audit trail object, that is stored in string_1 to string_5 of the audit trails for Records Manager Commonwealth Edition events. Only the strings that are populated are listed. Objects are also described for audit trails that pass one or more object IDs.

For an overview of auditing and the procedures to enable auditing, to activate the audit policy schema, to verify an auditing of an event, and to view and remove an audit refer to, *“Records auditing” on page 78*.



Note: Although up to 5 strings can be utilized by an event, only strings 1 and 2 are displayed in the results of an Audit Trail Report. Also, the content of one string may spill into the next string if it needs extra space.

Table 5-40: Audited events in RM Commonwealth Edition (RMCE)

Records Manager for Commonwealth Administration (RMC) audit events (Application Code = dmc_rmc)		
<i>Target Object Type: dm_sysobject</i> Check the Include all subtypes on the Register Audit screen when adding/selecting the various events for only this object type.		
<i>Event name</i>	<i>Strings usage</i>	<i>Object ID</i>
dmc_rmc_add_to_file	string_1: object name of the object added	ID1: of the object added
dmc_rmc_remove_from_file	string_1: object name of the object removed	ID1: of the object removed
<i>Target Object Typedmc_rmc_file</i>		
dmc_rmc_classify_file	string_1: name of the thesaurus category string_2: name of the retention policy associated with the thesaurus category	ID1: of the thesaurus category ID2: of the retention policy
dmc_rmc_file_close	n/a	n/a
dmc_rmc_file_reopen	n/a	n/a
<i>Target Object Typedmc_rmc_file_part</i>		
dmc_rmc_file_part_close	n/a	n/a
dmc_rmc_file_part_reopen	n/a	n/a

Chapter 6

Physical Records Manager

Physical Records Manager provides capability to manage paper assets, that is functionality to represent and administer all real-world objects as physical objects.

6.1 Introduction



Note: To avoid potential problems and unnecessary troubleshooting, make sure 1) that you are in the correct Physical Records Manager role for the operation you are attempting and 2) that the instance of the Records Client you are working on, is approved for Privileged DFC. Each instance of the Records Client must be Privileged DFC approved for any of the records products, Retention Policy Services, Records Manager, Records Manager Commonwealth Edition, and Physical Records Manager, to work properly. To determine which Retention Policy Services role an administrator or end user has to be a member of for specific operations, refer to “[Physical Records Manager roles and functional access](#)” on page 474.

6.1.1 Administration components

Physical Records Manager consists of the following components. Components preceded by an asterisk are the administration components that appear under the Physical Records Manager administration node in the navigation pane.

Functionality associated with all other components is available to both end users and administrators:

- *Library requests
- *Charge-outs
- *Barcode generation rules
- *Label printing rules
- *Pass-along requests
- Physical objects
- Barcodes
- Barcode manager
- Physical record report
- Library request report

6.1.2 About privileged clients and accessing repositories



Caution

The Records menu options associated to a particular product Retention Policy Services or Records Manager is disabled if they are not registered for Privileged DFC. Do not approve the Privileged Clients setting for those client instances that do not require Privileged DFC. Users who are not expected to create administrative components do not require their clients to be approved for Privileged DFC. Administrators can use Documentum Administrator to make sure the Approved setting of the clients for those users not expected to create administrative components is set to *No*. Administrators can change this setting from the Properties of privileged clients listed in the content pane. The session listener also checks for Privileged DFC and provides a dialog to administrators immediately after they log in to Retention Policy Services or Records Manager on the Records Client.

The use of Privileged DFC is pervasive throughout the general Records application stack for all categories of operations. As such, it is a mandatory requirement that the Foundation Java API instance that is being used to carry out the business functions, has been approved for privilege.

Operations that require Privileged DFC are listed by category in Appendix B.

Why privileged clients are necessary

Privileged clients are necessary for use cases where business logic needs to temporarily grant additional powers that are only needed for a brief period of time during certain operations. A classic example is when a user creates an object in a retained folder. The new object requires a retainer to be applied but a normal user is not expected to require the ability to apply retention directly to objects. An administrator has decreed that objects put into a folder (going into the future) must adhere to policies that they have decided. The end user's documents merely inherit this intent.

What determines the need for a privileged client

The Records Client for example, must be privileged if it is used to create or import objects into policy managed folders. Administrative components cannot be created unless the client is approved for privilege. You will need to use Documentum Administrator to list and approve the Foundation Java API instance for the desired client. You will also notice in the list that the Foundation Java API instance for the Documentum CM Server may already be approved, as its Foundation Java API instance is pre-approved. Make sure to approve it however if it is not already approved. Administrators need to think long and hard about potentially giving a client extra capabilities that they normally do not have.

The Foundation Java API instance on the Documentum CM Server and the Application server, for Records Client must be approved.

Clients that have their Foundation Java API instance approved for privilege can be verified from the Documentum Administrator user interface. The privileged clients listed are marked Yes under the Approved column if they have been approved. The Documentum CM Server and Application servers listed in this example are all approved. If you do not see the Documentum CM Server or Application server listed in the Privileged Clients content pane for which you want to approve their Foundation Java API instances, click the Manage Clients button and add the desired clients to the Privileged Clients list from resulting locator screen. Their Approved status remains No until you right-click the client listed in the content pane and select Approve. For complete details, refer to Documentum Administrator documentation.

6.1.3 Setting up Physical Records Manager

6.1.3.1 Configuration options

The application configuration options for Physical Records Manager are described in [“Physical Records Manager system configuration options settings” on page 473](#).

6.1.3.2 User preferences and column preferences

Use Preferences to make the Records Client user interface appear according to your personal needs.

To personalize your column preferences for certain features, refer to [“Setting column preferences” on page 77](#).

Preferences provides tabs you can select from to customize your view of Physical Records Manager in the Records Client user interface.

To change your Preferences:

1. Click Tools > Preferences.

The Preferences screen appears exposing the following tabs:

- General
- Columns
- Virtual Documents
- Repositories
- Search
- Formats

2. Click the applicable tab for which you want to change the preferences.

Radio buttons, checkboxes, drop-down lists, as well as links such as edit links and locator boxes are provided as needed to facilitate your changes.

3. Apply your changes as needed in the applicable tab(s).

4. Click **OK** to accept (save) the changes, or click **Cancel** to exit Preferences and ignore your changes.

6.2 Physical Records Manager Administration

6.2.1 About Physical Records Manager functionality

6.2.1.1 Physical Records Manager functionality

Physical Records Manager is intended primarily to manage physical objects within a OpenText Documentum CM repository.

Physical Records Manager features include:

- Library services
- Barcoding capabilities
- Representation of real-world objects such as:
 - Warehouses
 - Bays
 - Bins
 - Shelves
 - boxes
 - folders
- Reports

For more information about Physical Records Manager features, refer to “[Overview of Physical Records Manager](#)” on page 471

6.2.2 Physical Records Manager



Note: Each records product is role based and therefore all users and administrators must be in the correct role for the expected functionality to work properly. It is equally important that each instance of the Records Client, which hosts each of the records products, is registered for Privileged DFC.

6.2.2.1 Overview of Physical Records Manager

Physical Records Manager is intended for the management of paper assets providing library services to reserve, borrow, and return physical objects. Barcode management capability is also included to track physical objects if needed.

Physical Records Manager, when integrated with Retention Policy Services, Records Manager, and Documentum Webtop, provides additional paper functionality to enforce Records Manager and Retention Policy Services policies on real-world objects. Real-world objects are called physical objects in Physical Records Manager. It is the physical object that represents the real-world object in Physical Records Manager that can be managed according to Records Manager and Retention Policy Services policies. A barcode can also be generated, if needed, along with the physical object when it is being created. The barcode generated, though logically associated with the physical object, also needs to be printed so it can be attached to the associated real-world object for tracking purposes.

Two handy utilities for searching and reporting include Barcode Manager and Physical Record Report.

Barcode Manager can be used to search and list physical objects by barcode.

Physical Record Report can be used to generate customized report results against physical objects.

Functionality built into Physical Records Manager covers the following areas:

- Library services, which is used to:
 - Create library requests to reserve a box or folder
 - Charge out a physical box or folder that someone needs to borrow for a period of time
 - Charge in a physical box or folder that someone needs to return after a period of time
- Barcoding capabilities of real-world objects
The ability to barcode and create an inventory for tracking physical records in a variety of real-world objects.
- Representation of real-world objects such as:
 - Warehouses
 - Bays
 - Bins
 - Shelves
 - Boxes
 - Folders

- Documents
- Locations
- Addresses

The administration node is displayed in the navigation pane as shown in [Figure 6-1](#).



Figure 6-1: Physical Records Manager administration node

Conceptually, there are two parts to paper functionality:

1. Creating content, as shown in [Figure 6-2](#); when someone creates content and wants to register it with the system.

In this case someone creates content which a Records Manager takes, labels, and decides:

- Where the content should be put within a file plan (logical location).
- Where the physical content should be stored (physical location or also known as home location).

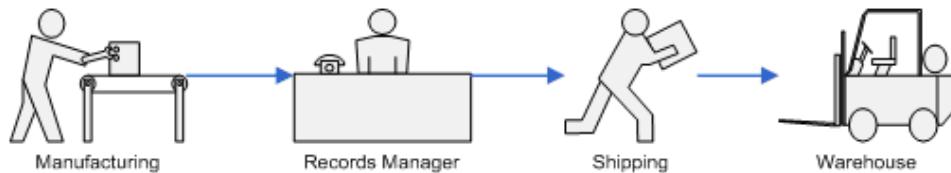
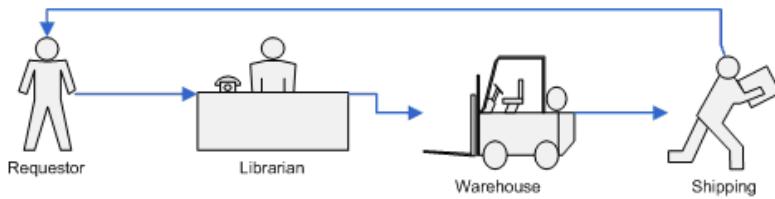


Figure 6-2: Content creation

2. Retrieving and borrowing content from long-term storage, as shown in [Figure 6-3](#); supported by library services. Temporary storage locations for physical content in transition may include:

- In transit to the warehouse
- In transit to the librarian (records administrator)
- Charged-out to a particular individual (which could be free-format text)

**Figure 6-3: Physical content management**

6.2.2.2 Physical Records Manager system configuration options settings

To set any of the Physical Records Manager system configuration options:

1. Navigate to Cabinets > System > Applications > PrmConfig > PRM DocbaseConfig.
Set the filter in the upper right corner to **Show All Objects and Versions**.
PRM DocbaseConfig is displayed.
2. Select *prm_docbase_config* in the content pane and click **View > Properties > Info** or right-click to select **Properties**.
The **Properties** screen appears displaying the **Info** tab.
3. Change the value for the attribute setting as applicable. Attributes for the Physical Records Manager system configuration options are described in [“Physical Records Manager System Configuration Options” on page 473](#).

Table 6-1: Physical Records Manager System Configuration Options

Options	Description
*Name	Mandatory field representing the default name of the file.
Charge-out Lifecycle	Name of the lifecycle for charge-outs.
*Default Due Date Offset	Mandatory due date to return a charged out physical object is set to 30 days by default.
*Default Request Date Offset	The value entered is used to set the date for the Date Requested on the Make Library Request form. 0 represents the current day. Any other integer value represents the number of days. For example, when a library request is created, the Date Requested date is set to the current date if 0 is entered, or to the date 30 days from the current date if the default 30 is entered.
Held Back Lifecycle	Name of the lifecycle for held backs. Do not edit (not-used).

Options	Description
Batching Synchronous	Allows batch operations to be done synchronous. Default is set to false which means Physical Records Manager must be installed. Rerunning of batch operations does not use this setting and requires Physical Records Manager to be installed.
Library Request Job Last Ran Date	Do not modify. Used by a job to record the last time the job to notify administrators ran.
Passalong Workflow	ID of the workflow that is used for ordinary pass-along workflow.
Privileged Passalong Workflow	ID of the workflow that is used for privileged pass-alongs which do not require a library administrator.
Request Lifecycle	Name of the lifecycle used for library requests. Default value is set to a lifecycle that uses 4 states. This lifecycle is used for new library requests. The default value is EnhancedLibraryRequest.
Temporary Target Object Folder for Last Printing	A repository path that is used to store PDF images when making library requests. The file is deleted during a label print operation. Default value is: /Temp (which means they will be stored in the Temp cabinet). Users that print labels must have WRITE permission on this folder.

- Click **OK** to accept changes and close the **Properties** screen.

6.2.2.3 Physical Records Manager roles and functional access

“Physical Records Manager roles and functional access” on page 474 describes the roles associated with Physical Records Manager and the functional access associated with each role. Each role grants a specific set of rights within Physical Records Manager for its members.

Table 6-2: Physical Records Manager roles and functional access

Role	Description
Physical Records Manager (dmc_prm_physical_records_manager)	Able to create administrative components.
Inventory Manager (dmc_prm_inventory_manager)	Able to create physical objects. Inventory Managers should have Browse access on all physical objects.

Role	Description
Library Administrator (dmc_prm_library_administrator)	Able to perform administrative tasks specific to library services.
Library User (dmc_prm_library_user)	Able to make library requests for objects.
Label Template Administrator (dmc_prm_label_template_administrator)	Able to perform administrative tasks specific to label templates.
Privileged Pass-along (dmc_prm_privileged_pass_along)	Able to pass-along charged out objects. The workflow for users in this role does not require a library administrator to approve the pass-along.
Label Print Request (dmc_prm_label_print_request)	Able to perform print label requests.
Pass-along Requestor (dmc_prm_pass_along_requestor)	Able to make a pass-along request for charged out objects. The workflow for users in this role require a library administrator to approve the pass-along.
Pass-along Recipient (dmc_prm_pass_along_recipient)	Users that can be the recipient of items that are passed along.
Batch Uploader (dmc_prm_batch_uploader)	Able to upload batch operations xml files.
All Physical Records Manager roles require that the user has at least Contributor client capability.	

Table 6-3: Physical Records Manager roles and functional access

Action	Physical Records Manager	Inventory Manager	Library Administrator	Library User	Notes
<i>Library Services</i>					
Make library request	Yes	No	Yes	Yes	Need READ permission on requested objects. Records administrators can create new contacts.
Cancel library request	Yes	No	Yes	Yes	Affects only those requests that have not been processed. Need WRITE permission on the library request.

Action	Physical Records Manager	Inventory Manager	Library Administrator	Library User	Notes
Edit/View library request	Yes	Yes	Yes	Yes	Library user can only change requested date. Must have WRITE permission on request.
Edit/View Charge-out	Yes	Yes	Yes	Yes	Library user has only BROWSE. Other roles can see associated held-backs.
List own library requests	Yes	No	Yes	Yes	This is a special menu item not a search item.
List library requests	Yes	No	Yes	No	All library requests that an Administrator would see.
List charge-outs	Yes	No	Yes	No	Library user could view charge-out associated to a library request (from the Properties screen).
Convert to charge-out (library request)	Yes	No	Yes	No	Must have at least browse on all objects (including contents) to process.
Charge-in (charge-out)	Yes	No	Yes	No	Currently, must charge in all contents of charge-out.

Action	Physical Records Manager	Inventory Manager	Library Administrator	Library User	Notes
Send recall notice	Yes	No	Yes	No	Send a recall notice against any physical object that has been charged out but needs to be returned before the return date (Date Due) specified on the library request.
Send overdue notice (charge-out)	Yes	No	Yes	No	Overdue notices are sent automatically if the object has not been returned to the system by the Date Due specified for a library request.
<i>Physical Objects</i>					
Create physical object (doc/container)	Yes	Yes	No	No	Note that others could create but those objects will not be treated as true physical objects (missing aspect).
View/Edit physical object	Yes	Yes	Yes	Yes	Access controlled by ACL. Administrators can see fields on aspect (availability, barcode for example)

Action	Physical Records Manager	Inventory Manager	Library Administrator	Library User	Notes
Delete physical object (doc/container)	Yes	Yes	No	No	Must have been already marked that the physical representation has already been destroyed.
Mark for destruction	Yes	Yes	No	No	Must have BROWSE permission. Contents of folder must be separately marked. (escalated writes make)
Mark physical object destroyed	Yes	Yes	No	No	Physical object must be available.
Mark physical object shipped for charge-out	Yes	Yes	Yes	No	Apply this marking to the physical object when its real-world counterpart is actually shipped. Though an object may have been charged out it does not mean it was shipped to an address or sent for pickup.

Action	Physical Records Manager	Inventory Manager	Library Administrator	Library User	Notes
Mark physical object picked up for charge-out	Yes	Yes	Yes	No	Apply this marking to the physical object when its real-world counterpart is actually sent for pickup. Though an object may have been charged out it does not mean it was shipped to an address or sent for pickup.
Privileged delete	No	No	No	No	An error message is displayed if attempted.
<i>Barcodes</i>					
Design barcode	Yes	Yes	No	No	
Print barcode label	Yes	Yes	No	No	There is a dedicated role for this capability: Label Print Request (dmc_prm_label_print_request)
Change barcode	Yes	Yes	No	No	
Barcode Manager	Yes	Yes	Yes	Yes	
<i>Reports</i>					
Physical Record Report	Yes	Yes	Yes	No	

6.2.2.4 Library requests

6.2.2.4.1 Overview of library requests

Use the Library Request feature to borrow one or more physical objects. Physical objects such as container objects and the contents within, boxes and folders for example and the documents inside. You can make library requests for yourself if you are a member of one of the applicable Physical Records Manager roles or for someone else if you are in an administrator role such as Physical Manager, Library Administrator, Retention Manager, or Records Manager.

Email notifications from record centers are sent to the OpenText Documentum CM Inbox of the user or group when their library request is submitted. The notification is a standard OpenText Documentum CM Inbox notification informing the recipients that a library request has been submitted. The email notification also indicates the number of library requests submitted since receiving the last notification.

Library Requests are displayed in the content pane according to the following attributes:

- Name
- Requestor
- Request Date
- Current State

Library Request right-click options:

- Cancel Request
- Convert to Charge-out
- Properties

The above options are displayed when you select a library request, from the list in the content pane, and click the right mouse button. Only Properties of the three options listed displays a dialog box. The other two options are either acknowledged or ignored when selected, as described below, displaying results in the column under Current State.

The column for the Current State is represented by one of four state values:

- *Submitted*, a user has made a request.

This state is the initial state for a library request (all objects in the request are pending). The library request remains in this state until at least one object in the request, if more than one physical object is requested, is processed.

- *Pending*, at least one item has been charged out to the user.
- *Processed*, all items requested have either been charged-out or held back. The library administrator no longer needs to take any action on the library request.

After the library request is processed, the library request cannot be changed or updated.

This state is indicated when a physical object in a library request is converted to charge-out (one or more objects are borrowed), even if it is only one physical object that is converted though there may be more than one physical object. Objects requested cannot be processed until they are available for processing, returned to the system.

- *Completed*, all items have been returned.

This state is indicated when the objects charged out is/are charged in (all objects in the request are returned) or when the library request (reservation) is canceled.

After the library request is completed, the library request cannot be changed or updated.

The Current State for a library request, changes from *Submitted* to *Completed* when the library request is canceled using Cancel Request.

Cancelling a library request is ignored when the Current State displays *Processed*. You cannot cancel a request that has been processed. The object(s) must be either charged in or notification sent to the borrower to have it charged in.

Convert to Charge-out is also ignored if the Current State displays *Completed*. You cannot convert a request to a charge-out after all the requested objects have been returned to the system.

Convert to Charge-out is applicable only if the Current State for any library request displays *Submitted* or *Pending*. *Submitted* changes to the *Processed* state when the selected library request is converted to a charge-out.

The Properties for a library request, can be used to find out the details about a library request, what physical objects were requested, which of the physical objects requested are not available, what was borrowed, and the history. The value for some of the attributes can also be changed if necessary.

6.2.2.4.2 Library request email notifications

Email notifications from record centers are sent to the OpenText Documentum CM Inbox of the user or group when their library request is submitted. Use this procedure if you want to change the recipients, or add to the list of recipients specified for a library request. The notification is a standard OpenText Documentum CM Inbox notification informing the recipients that a library request has been submitted. The email notification also indicates the number of library requests submitted since receiving the last notification. The Notification List is a new property/attribute added to the Properties of an address object.

To configure who receives an Inbox notification:

1. Log in to the Records Client and navigate to the address object that specifies the shipping address for the target library request.

2. Right-click the address object and select **Properties**. The Properties screen is displayed.
3. Click **Add** next to **Notification List** and choose the user(s) and/or group(s) you want to make recipients.
The option to **Remove** is displayed next to **Add** when at least one user or group is selected.
4. Click **OK** on the locator when you are done adding users and groups and then click **OK** on the Properties if you are satisfied with the users and groups added to the Notification List.

6.2.2.4.3 Making a library request

Make Library Request is the right-click option, or menu option, used to reserve one or more physical objects for yourself or on behalf of someone else.

Members of the following roles can make library requests:

- Physical Records Manager
- Library Administrator
- Library User

All physical objects selected for a library request must have at least READ permissions.

The value for the Name must be unique and is used to identify the library request.

The mandatory Contact information, is used to track who is requesting the item.

The value for the Date Requested is automatically set by default to 30 days from the day the library request is made. The default setting for the Date Requested can be changed as needed.

The Notification Preference you select indicates the means by which to communicate with the Physical Records Manager who can honor your request.

The shipping option can be selected so that the physical objects are shipped to the contact directly. Ship to Contact directly however, is disabled if the contact specified is not associated to an address.

The Shipping Address is mandatory. The value for the Shipping Address is automatically populated if the shipping option is set to Ship to Contact directly and an address is associated with the contact specified. Though the Shipping Address is automatically populated, if the contact specified is associated to an address, it can be edited to specify a new or different address by selecting Ship to address instead of Ship to Contact directly.

Regardless of the radio button selected for the shipping option, the checkbox for Send all at once can also be selected if all items requested need to be sent together.

The Shipping Address is displayed only if you change the default setting for the Shipping Options to either Ship to Contact directly or Ship to address. The Shipping Address is automatically populated if Ship to Contact directly is selected. The Shipping Address must otherwise be specified manually if Ship to address is selected.

The request, is being made for someone else when the For me checkbox is deselected and leaves it up to you to specify a contact, from an existing list or by adding a new contact. The New contact button is only displayed if the user is a Retention Manager. Only retention managers can create new contacts on the fly. If you click the button, a new contact can be created.



Note: The contact is not removed if the library request is canceled.

If you choose Edit, a locator lets you select the contact for whom you are making the request for.

The interface assumes the reservation is being made for yourself when only one contact is associated to you. You can tell that the reservation is for you when you see the For me checkbox displayed. The value for the Contact is automatically populated and displayed along with a For me checkbox, selected by default, for the logged in user only if the logged in user is already associated to exactly one contact. The name or value for the Contact and the For me checkbox are otherwise not displayed, as the system will not know which contact to display if you are associated to none or more than one contact.

Deselect the For me checkbox if you are making the library request for someone else. Then, click Edit to specify the contact from an existing list of contacts or add the new contact name using the New contact button (which is made available only if you are in the Retention Policy Services Retention Manager role). The New contact button, when displayed, facilitates specifying a new contact saving you the extra steps of leaving this procedure to create a new contact. As well, the contact information will automatically be filled in when you return from making the contact.



Note: The phone number provided for the Contact, if the Via Phone option is selected for the Notification Preferences, is by default taken from the top of the list if the contact specified has more than one number listed. The string of five numerals would be the phone number used.

The phone numbers listed for the Contact can be rearranged as necessary when you select Edit. Email listings are edited similarly.



Note: Each new number added however gets added to the bottom of the list, so if you want the new number to be used by default, make sure to move it to the top of the list before you click OK. For example, if you want 777.777.7777 to be the default number for the contact, move it to the top of the list and then click OK.

If you are making a request on behalf of another user, you need to select the contact from a list. The requestor is defined to be the person who will be getting the item

and is associated to an Retention Policy Services contact. As well, the contact must have an email address or be associated with a OpenText Documentum CM user.

The same physical object(s) can be requested by multiple library requests; the physical object(s) you have requested can also be requested by others. Library requests are fulfilled at the discretion of the administrator, not necessarily on a first come first served basis.

To make a library request (reservation):

1. Navigate to a physical object that you would like to reserve: typically a box, physical folder, or physical document.

Contents in a container such as a box or physical folder are identified on the manifest for a library request once the library request is created. Creating a library request for a box, for example, will include any physical folder(s) and/or physical document(s) on the manifest if those physical objects are in the selected box. The manifest only identifies the container if no other physical objects are included in it.

2. Right-click the physical object, and select **Make Library Request**.

You can select multiple physical objects, two boxes for example could be included in a single library request, by selecting the two boxes and then right-clicking one of them to select **Make Library Request**.

The **Make Library Request** screen is displayed.

3. Enter values on the **Make Library Request** screen for the three mandatory attributes, and if needed for the optional attributes, according to “[Attributes on the Make Library Request screen](#)” on page 484.

Table 6-4: Attributes on the Make Library Request screen

Attribute	Description
*Name	Type a unique name so it can be identified when listed with other library requests.
*Contact	Use this attribute to make a library request for yourself or to make it for someone else. Deselect the For me option when making the request for someone else. Click Edit if you need to add or change a contact. Click the New contact button, revealed to Retention Managers only, if you cannot find the needed contact from the existing list using Edit .

Attribute	Description
*Date Requested	The default value for this mandatory attribute is set to 30 days from the current date. Pickup or shipment of requested items is expected 30 days from the day the request was made. You can change the default setting as needed. You can change the default setting from dmc_prm_docbase_config as needed. To change the default setting refer to instructions in “Setting up Physical Records Manager” on page 469 .
Notification Preference	Select the preferred means of communicating. Make sure that if you use the OpenText Documentum CM Inbox option that the contact is associated with a OpenText Documentum CM user.
Shipping Options	Regardless of the radio button selected for the shipping option, you can also select the checkbox to send all requested items at the same time, limiting the request to only one charge-out. The default option is set to Pickup . The Shipping Address is automatically populated if the shipping option selected is Ship to Contact directly . You need to specify the Shipping Address if the shipping option is Ship to address .
*Shipping Address	The address locator or chooser is displayed when you click Edit . To create an address, or home location, navigate to your home cabinet or other folder location and click File > New > Address . For further details, refer to “Create physical object (document/container/address)” on page 497 .
Note	Any additional instructions needed can be expressed.

The **Choose an item** screen is displayed, when you click **Edit** for the **Shipping Address**. Only address objects, if other objects are listed as well, are valid choices.

- Click **Finish** on the **Make Library Request** screen to accept the values entered.

The new library request is now displayed in the content pane under *Library Requests*. The value for the **Current State** is *Submitted* and remains so until the library request is converted to a charge-out.

6.2.2.4.4 Cancel a library request

You must be in one of the following roles to cancel a library request:

- Physical Manager
- Library Administrator
- Library User

Members in any of the roles listed above have access to the following right-click options for this action:

- Cancel Request
- Convert to Charge-out
- Properties

Anyone else outside of the specified roles can access only Properties.

You can cancel a library request only if the value for its Current State displays *Submitted*. You can not cancel a library request if its Current State displays *Processed* or *Completed*.

To cancel a library request:

1. Navigate to **Physical Records Manager > Library Requests**.
2. Right-click the library request listed in the content pane and select **Cancel Request**.

The value of the **Current State** for the selected request changes from *Submitted* to *Completed*.

6.2.2.4.5 View/edit a library request

You must be in one of the following roles to view or edit a library request:

- Physical Manager
- Inventory Manager
- Library Administrator
- Library User

You can view and edit values associated with a library request from its Properties.

To view or edit a library request:

1. Navigate to **Physical Records Manager > Library Requests**.
2. Right-click the library request listed in the content pane and select **Properties**.
The **Properties** screen is displayed displaying the **Info** tab by default.
The **Properties** screen for library requests includes tabs for:

- **Info**
 - **Requested Items**
 - **Pending Items**
 - **Associated Charge-outs**
 - **History**
3. Click the tab you want to view or edit.
 4. Click **OK** to accept all changes if any. Click **Cancel**, when necessary, to ignore any unintended changes.
Click **OK** or **Cancel** if no changes were made.

6.2.2.4.6 View/edit charge-outs

View or edit a charged out (borrowed) physical object according to instructions in this section. All charge-outs are listed according to these instructions. You can also view/edit the list of charge-outs that belong to you only, refer to “[View/edit my charged out items](#)” on page 488 for instructions.

You must be in one of the following roles to view or edit a charge-out:

- Physical Manager
- Inventory Manager
- Library Administrator
- Library User

To view or edit a charged out physical object:

1. Navigate to **Physical Records Manager > Charge-outs**. Library requests that have been charged out are listed.

Attributes displayed in column headers left to right include:

- Name
- Charge-out
- Due Date
- Current State
- All Items Returned Date
- Library Request
- Note

Right-clicking an item lets you select its properties or lets you charge it in.

2. Right-click the charged out physical object listed in the content pane and select **Properties**. The **Info** tab is displayed.

The **Properties** screen is displayed with the following tabs:

- **Info**
 - **Manifest**
 - **Returned Items**
 - **Heldback**
3. Click the tab you want to view or edit.
 4. Click **OK** to accept all changes if any. Click **Cancel**, when necessary, to ignore any unintended changes.
Click **OK** or **Cancel** if no changes were made.

6.2.2.4.7 View/edit my charged out items

Use this procedure to view/edit a list of physical objects that are charged out to you only.

To view/edit my charged out items:

1. Select **View > My Charged Out Items**. **My Charged Out Items** is displayed.
2. Optionally, you can right-click one of your charge-outs listed in the content pane and select Properties if you want to edit.

6.2.2.4.8 View/edit my library requests

View or edit your library requests according to instructions in this section if you do not need to view all library requests. To view all library requests, refer to “[List library requests](#)” on page 489.

Anyone who wants to view or edit their own library requests, must be in one of the following roles:

- Physical Manager
- Inventory Manager
- Library Administrator
- Library User

To view or edit my library requests:

1. Navigate to one of the following nodes:
 - **Physical Records Manager**
 - **Library Requests**
 - **Charge-outs**
 - **Barcode Generation Rules**

2. Click **View > My Library Requests**.
3. Optionally, if you want to modify one of your library requests, you can right-click it and select **Properties**.

6.2.2.4.9 List library requests

List all library requests according to instructions in this section. To list only your library requests, refer to “[View/edit my library requests](#)” on page 488.

You must be in one of the following roles to list all library requests:

- Physical Manager
- Inventory Manager
- Library Administrator

Members in any of the roles listed above can perform actions according to the following right-click options:

- Cancel Request
- Convert to Charge-out
- Properties

To list all library requests:

- Navigate to **Physical Records Manager > Library Requests**.

Library requests are listed according to:

- Name
- Requestor
- Request Date
- Current State

6.2.2.4.10 List charge-outs

You must be in one of the following roles to list charge-outs:

- Physical Manager
- Inventory Manager
- Library Administrator

Members in any of the roles listed above can perform actions according to the following right-click options:

- Charge-in
- Properties

- Delete

To list all charge-outs (physical objects that are borrowed and removed from the system):

- Navigate to **Physical Records Manager > Charge-outs**.

Library requests are listed according to:

- Name
- Due-date
- Charge-out Date
- Current State
- Library Request
- Note

6.2.2.4.11 Convert library request to charge-out

Convert a library request to charge-out using the option Convert to Charge-out when one or more of the physical objects requested are available in the system for borrowing. Requested objects listed on the manifest for a particular charge-out can also be held back when necessary. Reasons for objects which are held back can also be mentioned along with the name or address of the temporary location to which requested objects, as well as any that are held back, are exported to; for shipping or pickup. Users are presented with a series of screens which allow a user to specify exactly which charged out object(s) are being picked up or shipped. A manifest contains the initial selection from which they can exclude items. For containers, it means that all of the charged out contents within it can be marked along with the container in one operation.

Mark physical objects as shipped or picked up after they have been converted to charge-out only when you have been advised that their real-world counterpart was actually shipped to an address or was actually sent for pickup. The two markers for this are:

- Mark physical object shipped for charge-out
- Mark physical object pickedup for charge-out

These two options are available when you right-click the physical object. For more information on these two markers, refer to “[Mark physical object shipped \(or picked up\) for charge-out](#)” on page 508.

You must be in one of the following roles to process a library request (Convert to Charge-out):

- Physical Manager
- Library Administrator

Both roles must have at least BROWSE access on all of the items requested (including sub-contents or folder contents).

The requestor is given objects that have at least READ permissions. If the contact is not associated with a OpenText Documentum CM user, then the Physical Manager or typically the Library Administrator is responsible to determine what requested items should be given to the requestor (since there is no way to know what the user should have access to).

Members in any of the roles listed above have access to the following right-click options on the selected library request:

- Cancel Request
- Convert to Charge-out
- Properties

Anyone else outside of the specified roles can access only Properties. Library users can also Cancel Request (only if the user has WRITE permissions on the library request).

An administrator converts physical objects within a library request to charge-out to indicate that they will be borrowed. Depending on the library request, the requestor may need to pick up the items or the items may need to be shipped to an address.

By default, the manifest is the list of items that the requestor has permissions to see from the Records Client, but not from Documentum Webtop. The administrator however, can override and decide what a person gets. As well, the library administrator can choose which requestors get the requested object(s) when there are multiple library requests for the same physical object(s). Not all the requested physical object(s) within a library request might be available for charge-out if the requested physical objects are already charged out. Physical objects that are not available in the system are *Pending* until they are physically returned to the system.

When viewing a library request, when initially created, the pending list is the list of objects that may be sent to the user. Partial processing of a library request can be done and depending on the number of physical objects requested, you may have to Convert to Charge-out several times to complete or fulfill a library request.

Though there could be more than one physical object requested, converting any one physical object in a library request to charge-out, automatically changes the Current State displayed under Library Requests from *Submitted* to *Pending*.

This procedure is applicable to only those library requests that display *Submitted* or *Pending* for the Current State. A library request that displays *Completed* for its Current State implies that all physical objects requested have been returned to the system.



Note: A convert to charge-out operation will fail if none of the items in the library request are available for charge-out. A particular physical item in the pending list may not be available for any one of the following reasons:

- Item has been charged-out to someone else and has not been returned yet
- The intended recipient does not have Read permission .
- The item is marked:
 - As lost
 - For destruction
 - For export

To convert a library request to charge-out and hold back any items if necessary:

1. Navigate to **Physical Records Manager > Library Requests** and right-click the library request that needs to be processed.
2. Select **Convert to Charge-out**. The **Convert to Charge-out** screen is displayed. Attributes on each of the tabs are described in “[Attributes described for converting a library request to charge-out](#)” on page 493.
3. Type a unique name for the mandatory **Charge-out Name** and enter a return date for the mandatory **Date Due** on the **Info** tab. All other attributes are optional. You can provide entries for optional attributes if needed according to the table that follows this procedure.
4. Click **Next** to display the **Manifest** tab.
5. Follow these substeps if there are items listed in the **Manifest** that need to be held back. Otherwise, click **Next** again, if there is nothing listed on the **Manifest** tab that needs to be held back, and then click **Finish**:



Note: Objects listed in the manifest cannot be held back after the library request has been converted to a charge-out. If there is anything to hold back, it must be done during this step while the library request is being converted, before you click **Finish**.

- a. Click an item in the **Manifest** list that needs to be held back.
The screen refreshes adding another field that identifies the **Selected Object**. The **Hold Back** button is also added next to the **Selected Object**.
- b. Click the **Hold Back** button to acknowledge the selected object.
The selected object is now removed from the **Manifest** list.
- c. Repeat these substeps for the other objects in the manifest, which for one reason or another need to be held back. Reasons for objects being held back can optionally be mentioned for the **Note**. The **Temporary Location** can also be identified if the object(s) have been or are being exported for pickup or to an address if shipped.



Note: You can add information to the fields for the **Temporary Location** and for the **Note**, only if there are items held back.

- d. Click **Finish**.

The **Current State** for the selected library request changes from *Submitted* to *Pending* when any one item is converted, even though there may be more than one item requested.

Table 6-5: Attributes described for converting a library request to charge-out

Attribute	Description
<i>Convert to Charge-out tab</i>	
Charge-out Name (mandatory)	Type a unique name so it can be identified under Charge-outs.
Library Request Name	The value for this field is automatically populated for you and can not be edited.
Due Date (mandatory)	Click the Calendar button and scroll as needed to provide the expected return date.
Contact: Name and Email	Values for this field, against Name and Email, are automatically populated for you and can not be edited.
Shipping Address	The value for this field is automatically populated for you and can not be edited.
Note	Type any instructions or details as needed regarding borrowed items.
<i>Manifest tab</i>	
Library Request Name	The value for this field is automatically populated for you and can not be edited.
Manifest	Items in the library request are identified under this attribute.
<i>Heldback tab</i>	
Library Request Name	The value for this field is automatically populated for you and can not be edited.
Temporary Location	Identify a temporary location, if necessary, according to the following criteria: <ul style="list-style-type: none"> • If the borrowed item is in transit to warehouse • If the borrowed item is in transit to librarian (records administrator) • If the borrowed item is charged-out to a particular individual (which could be free-format text)

Attribute	Description
Note	Type any instructions or details as needed regarding any items that are held back.
Heldback	The value for this field is automatically populated for you and can not be edited. Any items that are held back are listed under this attribute.

6.2.2.4.12 Charging in a charge-out

Physical objects requested in a library request are charged out when they are borrowed and removed from the system. The physical objects borrowed must be charged in when they are returned so that they are once again available in the system for processing against other library requests. Physical objects that were held back also need to be put back into their original physical container(s) before they are returned to the system.

The Current State for a charge-out displays *Charge-out* until the charged out object is returned or charged-in to the system. The Current State for a charge-out displays *Completed* once the object(s) are charged-in. Though the Current State for a charge-out might indicate *Completed*, the Current State for a library request will not indicate *Completed* until all charge-outs are charged-in.

You must be in one of the following roles to charge-in objects being returned to the system:

- Physical Manager
- Inventory Manager
- Library Administrator

Members in any of the roles listed above can perform actions according to the following right-click options for this action:

- Charge-in
- Properties
- Delete

Anyone else outside of the specified roles can access only Properties.

To charge in a charged out physical object:

1. Navigate to **Physical Records Manager > Charge-outs**.
2. Right-click the charge-out listed in the content pane, that is associated with the library request being processed, and select **Convert to Charge-in** from the list box.

The **Current State** for the selected charge-out changes from *Charge-out* to *Completed*.

6.2.2.4.12.1 Held-back

Physical objects requested according to a library request can be held back if the administrator finds it necessary to do so.

 **Note:** Physical objects can be held back only when a library request is being converted to a charge-out, not after it has been converted. The Properties page of a library request or of a charge-out cannot be used to hold back an object. It can only be done at the time that the library request is being converted.

Physical objects that are held back can be found on the Heldback tab of a charge-out for any library request. Though there could be more than one charge-out processed to fulfill a library request, each charge-out identifies its own set of held backs against its manifest. You can identify what the available objects are in a charge-out on the Manifest tab and which of the available objects will be held back on the Heldback tab.

You can hold back objects in a library request *when it is* converted to charge-out or *after it has* been converted, from the Properties of the individual charge-outs. For more information about physical objects that are held back, refer to “[Convert library request to charge-out](#)” on page 490. Follow that procedure as it can be used to view requested items on the Manifest list, convert to charge-out, and hold back requested objects.

6.2.2.4.12.2 Manifest

The manifest identifies what physical objects are charged out according to a library request.

The manifest identifies the physical objects that are charged out according to a library request. Physical objects requested according to a library request are accounted for on the Manifest tab of a charge-out for any library request. The physical objects requested may be spread across more than one charge-out if more than one charge-out is needed to fulfill a library request.

Items listed in the manifest for each charge-out can also be held back, selected for hold back. For more information about physical objects that are listed on the Manifest, refer to “[Convert library request to charge-out](#)” on page 490. Follow that procedure as it can be used to view requested items on the Manifest list, convert to charge-out, and hold back requested objects.

6.2.2.4.13 Send recall notice

Send a recall notice for any physical object that needs to be returned before the return date or more specifically before the Date Due selected according to the library request. Recall notices must be sent individually against the physical object borrowed, not the library request or associated charge-outs. **Send recall notification** functionality is not available if you have more than one physical object selected.

To send a recall notice:

1. Navigate to the physical object that needs to be recalled.
2. Right-click the physical object listed in the content pane and select **Send recall notification**.

If the person for a library request is a OpenText Documentum CM user, a standard recall notification is sent to the Inbox and to the email address of that person. Recall notification is sent only to the email address if the library requestor is not a OpenText Documentum CM user.

6.2.2.4.14 Send overdue notice

Overdue notices are sent automatically when the return date (Date Due) that was specified for the library request is reached. An overdue notice is sent automatically against the charge-outs associated with a library request, not the individual physical objects as is done manually for recall notices. Overdue notices can also be sent manually if overdue notification needs to be sent more than once.

6.2.2.5 Physical objects

The “Disposition of physical objects” on page 509 is exposed at higher level for ease of reference in the table of contents.

6.2.2.5.1 Overview of physical objects

Physical objects or real-life objects that need to be represented in the system (Physical Records Services) include:

- Warehouses
- Bays
- Bins
- Shelves
- Boxes
- Folders
- Non-electronic documents
- Locations
- Addresses

Not all of these physical objects can be charged out (borrowed). Obviously, warehouses cannot be charged out though there is functionality that permits it. Similarly, bays, bins, and shelves are physical objects that also cannot be charged out. Physical objects in a library request cannot be charged-out if they are checked out. Physical objects that are checked out, for modifications for example, means that the following actions will not be available until it is checked in:

- Charge-in
- Make library request
- Mark for destruction
- Mark for export
- Mark physical object destroyed
- Mark physical object exported
- Mark physical object picked up for charge-out
- Mark physical object shipped for export
- Mark physical object shipped for charge-out
- Pass along
- Send recall notification



Note: The default setting for physical objects being created that should not be available for charge-out should be deselected. Make sure to deselect the option Library requests can be made for this object if the physical object being created is one that should not be available for library requests and possible charge-out.

6.2.2.5.2 Create physical object (document/container/address)

Real-world objects are represented in Physical Records Manager by physical objects. A physical object must be created in Physical Records Manager for each real-world object. Warehouses, locations, and addresses for example are represented as physical objects along with the other various container type objects. Not all physical object types can be charged-out. The optional setting for those that should not be charged out should be set so that they cannot be charged out.

All physical objects entered into the Physical Records Manager system are represented using various icons. Each physical object type created is associated to a particular icon. All warehouses created for example, display the same type icon. The Type on the Create tab for New Physical Document is not displayed/required though it is on the Create tab for New Physical Container, as there are various container types you need to be able to select from.

Physical objects can be created within a file plan and structured to suit your organizational needs, as shown in [Figure 6-4](#). Location objects and address objects can also be created according to this procedure so that each physical object created can be, if necessary, associated to an address using the Home Location option.



Figure 6-4: Physical objects added to a cabinet

You can select a Home Location for a physical object when it is being created. Though optional the Home Location will be required to export the physical object if ever it needs to be transferred according to export procedures. The value or address specified for the Home Location will be the same value used to populate the Current Location on the form used to Mark for export.

Automatic barcode generation is an optional setting which can be selected or deselected as needed for each new physical object created. The Auto Generate Barcode option however is disabled unless a barcode generation rule has been created (already exists) for the selected Type. Create the appropriate barcode generation rule first before following this procedure. Though the setting for automatic barcode generation is covered in this procedure, creating the barcode generation rule is not; follow procedures according to ["Barcode generation rules" on page 513](#) whether you need to generate barcodes automatically or manually.

The system will look for the best matching rule based on object type, if the Auto Generate Barcode option is selected. If an exact match is not found, the system will look for a rule that matches the supertype and will continue to look until it reaches dm_sysobject. An error message will be displayed if there is no rule for dm_sysobject.

To create a physical object:



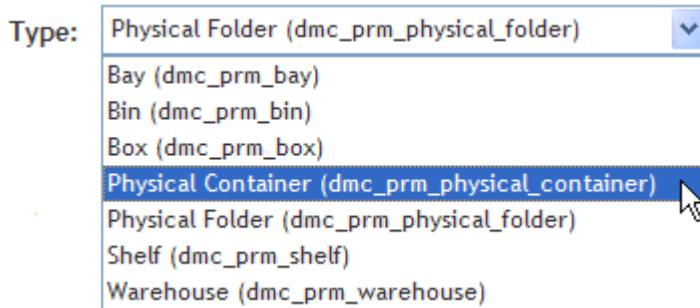
Note: Though the **Name** is the only mandatory value needed to create a physical object, make sure the optional **Type** selected is set appropriately. When creating and naming a warehouse for example, make sure the default setting is changed from *Physical Folder (dmc_prm_physical_folder)* to *Warehouse (dmc_prm_warehouse)*.

Also note that a tab for **Transfer Info** is displayed only when you view the Properties of a physical object:

1. Navigate to a cabinet, your Home Cabinet, or other file plan location where you want to create one or more physical objects. The option to create a new physical object is not available if you navigate to an unacceptable location.
2. Click **File > New** and select the desired option, **Physical Container** or **Physical Document**.

The **New Physical Container** screen or **New Physical Document** screen is displayed, depending on the option selected. The **Create** tab in either case is displayed by default.

The **Permissions** tab is not displayed on the resulting screen for *Physical Document*.



A Physical Container is included among the standard physical container object types listed. It can be used if no other physical object type suits the need. The following icon represents the Physical Container type:



3. Type a unique value for the mandatory **Name** against the desired **Type** and then click **Next** or **Finish**. All other attributes are optional and therefore only the name is required to create a physical object.
Use **Next** to review default entries and if necessary to provide entries on each of the remaining tabs.
Use **Finish** if you are satisfied with the default entries and have nothing else to enter.

You can select a **Home Location** now while creating the object or later from its properties. You will however have to create the home location object if it is not already available. The home location indicates the address at which the physical object is located. The value entered for the **Home Location** is used to populate the **Current Location** whenever the physical object is exported, transferred to a new address.

You can also deselect **Allow library requests to be made for this object** to prevent library requests.

Auto Generate Barcode is not available if a **Barcode Generation Rule** has not been created. For further details and instructions to create rules, refer to “Barcode generation rules” on page 513.



Note: You can specify any value for the home location, a street address, the name of a warehouse, or the name of a shelf or any other container within a warehouse. You can combine them as well and include as much detail as necessary. For example, you can create a home location object named Shelf_A in Warehouse-A at 3 Forest Gate. To create a Home Location object click **File > New > Address**. Make sure to take note of the

cabinet name under which you create the Home Location object. It is displayed in the upper left-hand corner of the Create tab, rmadmin for example in the screenshot provided. This will help you to know which cabinet to navigate, on the locator, when you click **Select** for the Home Location.

dmc_prm_location is of subtype of dm_folder and it is used to organize addresses into geographic regions.

Optionally, you can expand **Show options** and select **Subscribe to this physical container** or **Subscribe to this file**, depending on the object type you are creating. Typical object details available on the **Info** tab can also be viewed or edited if necessary, **Title**, **Subject**, **Keywords**, and so forth for example.

Attributes on the **Physical Info** tab are described within the instructions for viewing or editing a physical object.

The default settings for the Permissions is set to:*Read* for dm_world
Version for docu
Delete for dm_owner

6.2.2.5.3 View/edit physical object

View or edit the details (properties) of a physical object from its Properties.

To view or edit a physical object:

1. Navigate to the physical object you need to view or edit.
2. Right-click the physical object displayed in the content pane and select **Properties**.
3. Select the **Physical Info** tab to view or edit a physical object. Tabs you can select from include:
 - **Info**
 - **Physical Info**
 - **Close Folder Info**

This tab is displayed on the properties of physical container objects only. It is not displayed against physical documents. The 2 attributes **Marked Contained Objects for Destruction** and **Contained Objects Physically Destroyed** are also displayed on the properties of only physical container objects.

 - **Permissions**
 - **History**
 - **Transfer Info**

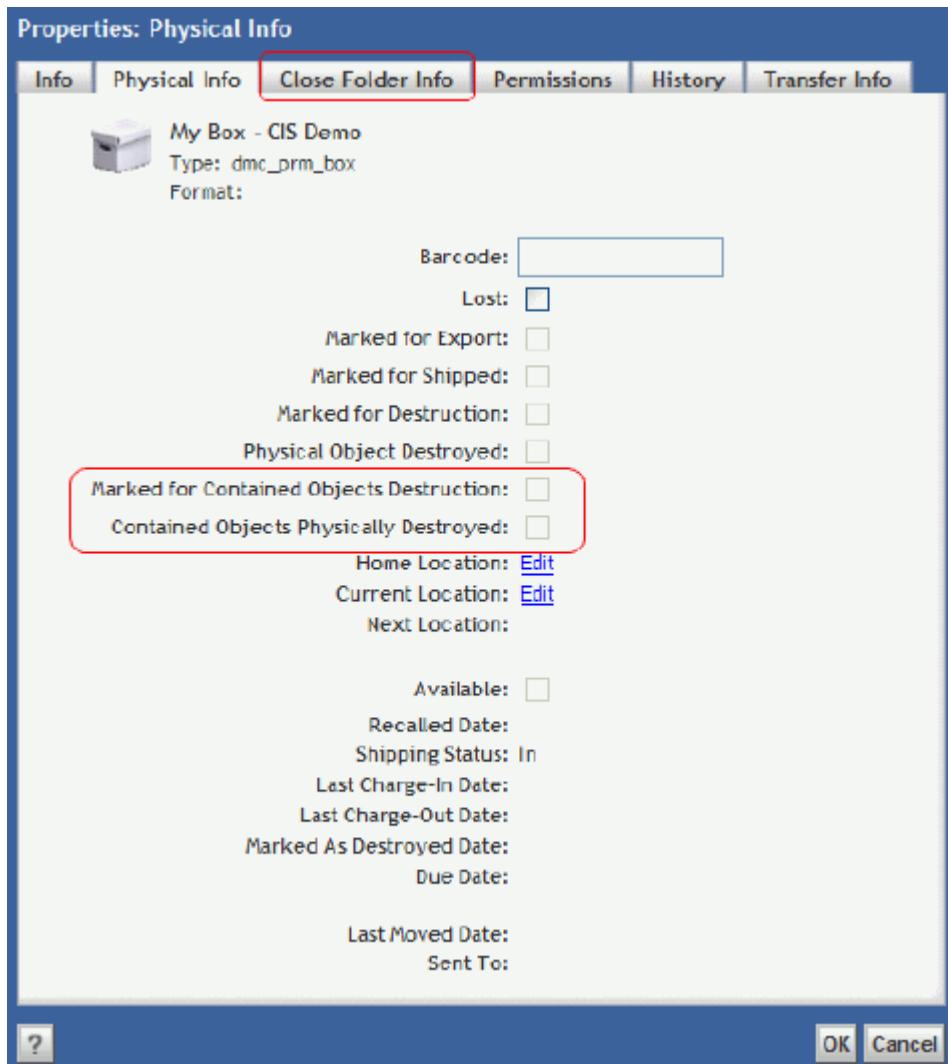


Figure 6-5: Physical Info tab



Note: Although it is possible to right-click a physical container object that is under retention and mark it for destruction, any container object that is under structural retention cannot be marked for destruction. Only the contained objects of a structurally retained container can be marked for destruction. Container objects that are structurally retained are meant to be permanent fixtures. For further details about structural retention, refer to About the Content Intelligent Services (CIS) integration with Retention Policy Services in “Retention policy overview” on page 146. The **Structural Retention Type** attribute setting is further described in “Creating a retention policy” on page 156.

4. Click **OK** to accept changes or **Cancel** to ignore changes.

Attributes on the Physical Info tab are described in “Physical Info attribute descriptions” on page 502.

Table 6-6: Physical Info attribute descriptions

Physical Object Attribute	Description
Barcode	This field is populated when the checkbox for Auto Generate Barcode is selected on the Create tab.
Lost	This checkbox can be selected at any time when the physical object cannot be found.
Marked for Export	<p>The checkbox is automatically selected after a user manually selects the physical object and marks it for export. That is, when the user right-clicks the physical object and selects the menu option Mark for Export. A physical object that is moved from one inventory managed location to a new inventory managed location must first be exported before it can be shipped. Mark for Export is no longer displayed on the right-click menu list after the physical object is successfully exported. Mark Shipped for Export is instead displayed. The user can then select Mark Shipped for Export to indicate that it was shipped.</p> <p>This option is also automatically set when disposition is run and the retention strategy is set to any of the export strategies.</p> <p>Regardless of how the checkbox is selected, it can be deselected if it is decided not to continue the action.</p> <p> Note: Both of the right-click menu options Mark for Export and Mark Shipped for Export are available depending on the desired action.</p>
Marked for Shipped	The checkbox is automatically selected after a user manually selects the physical object, after it has been exported, and marks it as shipped. That is, when they right-click the physical object and select the menu option Mark Shipped for Export .

Physical Object Attribute	Description
Marked for Destruction	<p>The checkbox is automatically selected after a user manually selects the physical object and marks it for destruction. That is, when the user right-clicks the physical object and selects the menu option Mark for Destruction. A physical object that has to be destroyed must first be marked for destruction before it can be destroyed. Mark for Destruction is no longer displayed on the right-click menu list after the user confirms to destroy it. Mark Physical Object Destroyed is instead displayed. The user can then select Mark Physical Object Destroyed to indicate that it was destroyed.</p> <p>This option is also automatically set when disposition is run and the retention strategy is set to any of the destroy strategies.</p> <p>Regardless of how the checkbox is selected, it can be deselected if it is decided not to continue the action.</p>
Physical Object Destroyed	<p>The checkbox is automatically selected after a user manually selects the physical object, after it has been destroyed, and marks it as destroyed. That is, when they right-click the physical object and select the menu option Mark Physical Object Destroyed.</p>
Marked Contained Objects for Destruction	<p>The checkbox is automatically selected after a disposition run if the applied retention policy has the Structural Retention Type selected. The checkbox can be deselected if it is decided not to continue the action. For further details about the Structural Retention Type, refer to “Creating a retention policy” on page 156</p> <p> Note: This option and the Contained Objects Physically Destroyed option are not displayed for physical documents, only for physical container object types such as a bay, bin, box, shelf, or even a warehouse.</p>

Physical Object Attribute	Description
Contained Objects Physically Destroyed	<p>This option must be set manually, after the disposition run, to indicate that the objects were indeed destroyed.</p> <p> Note: This option and the Marked Contained Objects for Destruction option are not displayed for physical documents, only for physical container object types such as a bay, bin, box, shelf, or even a warehouse.</p> <p>If a physical container object is a structural container, all markings should no longer be displayed after it has been reset. A physical container becomes a structural container when a retention policy applied to it has the Structural Retention Type option selected. A structural container is one that cannot be destroyed when disposition is run, only the contained items. Once the contents are destroyed, the structural container is reset and therefore any markings that were displayed should no longer be displayed.</p>
Home Location	The value you enter for this is the physical location for storing a physical object. You can edit the value as necessary to change the home location.
Current Location	The value entered for the Home Location is used to populate the Current Location when a physical object is created. You can edit the current location without affecting the home location if the physical object is being moved around, for pickup for example.
Next Location	Read-only field, populated when a physical object is marked for export, meaning that it will be transferred to a new address whereby logical ownership is changed. If you right-click a physical object and select Mark for Export you can specify the new location for Export to Location. The value entered for Export to Location is displayed for this attribute.
Available	Read-only checkbox, displayed as selected when the physical object is created. The checkbox is automatically deselected when the physical object is charged out or is lost.

Physical Object Attribute	Description
Recalled Date	Read-only field, populated with a date value when a recall notice is sent for a physical object that was charged out. A recall notice can be sent when you right-click a physical object and select the menu option Send Recall Notification.
Shipping Status	Read-only field, populated, set to In by default, when the physical object is created. In is displayed even if it is lost. Possible values include: In, Waiting to Ship for Charge-out, Waiting for Pickup, and Out.
Last Charge-In Date	Read-only field, populated with the date the physical object was last returned on.
Last Charge-Out Date	Read-only field, populated with the date the physical object was last charged out (borrowed) on.
Marked As Destroyed Date	Read-only field, populated with the date the physical object was marked for destruction on.
Due Date	Read-only field, populated according to the value selected for the Due Date on the Info tab of the Convert to Charge-out page.
Last Moved Date	Read-only field, populated with the date when a physical object is moved by the Move or the Reconciliation batch operations.
Sent To	Read-only field, populated with the address to which the physical object was sent, based on the Charge-out or the Mark shipped for charge-out/export batch operations.

6.2.2.5.4 Delete physical object

No physical object can be deleted directly. A physical object must be marked two times before it can be deleted. Any physical object that is retained however cannot be deleted according to this procedure. To delete a physical object that is under retention, refer to “Disposition of physical objects” on page 509.

To delete a physical object:

1. Navigate to the physical object that needs to be deleted.
2. Right-click the physical object displayed in the content pane and select **Mark for destruction**.
3. Wait for the screen to refresh.
4. Right-click the physical object again after the real-world object has been destroyed and select **Mark physical object destroyed**.

5. Wait for the screen to refresh.
6. Right-click the physical object for a third time and select **Delete**.
The screen refreshes no longer displaying the selected physical object.

6.2.2.5.4.1 Mark for destruction

Mark for Destruction is a right-click menu option that can be selected against a physical object to indicate that the real-world object it represents *can be* destroyed. Mark the physical object for destruction when its real-world counterpart is ready to be destroyed. A physical object once marked for destruction will no longer be available for charge-out.

6.2.2.5.4.2 Mark physical object destroyed

Mark Physical Object Destroyed is a right-click menu option that can be selected against a physical object to indicate that the real-world object it represents *has been* destroyed. Mark the physical object destroyed after its real-world counterpart has been destroyed. A physical object must be marked destroyed before it can be deleted.

6.2.2.5.4.3 Mark physical contents have been destroyed

Mark Physical Contents have been Destroyed is a right-click menu option for physical objects that are under structural retention. A retention policy that specifies structural retention prevents the container object it is applied to from being destroyed upon disposition, but not any of its contents. Only the contents of a structural container, physical or electronic container (box or folder for example), can be destroyed. Once the contents of a structural container are destroyed, aging on the container is reset. A container that is under structural retention can never be destroyed, only its contents. For further details about structural retention, refer to About the Content Intelligent Services (CIS) integration with Retention Policy Services under [“Retention policy overview” on page 146](#). Physical objects can include Records Manager Commonwealth Edition files and file parts.

6.2.2.5.5 Export physical object

A physical object needs to be exported when the logical ownership of its real-world object is transferred to another address. Export a physical object when its real-world counterpart needs to be transferred from one home location address to another home location address. A real-world object for example, that needs to be moved is transferred from its current address in one warehouse to a different warehouse at another address requires its physical object to be exported.

The physical object(s) to be exported need to be marked three times to complete the entire process. Markings involved are:

- Mark for export to initiate the export process and identify the new transfer destination or new home location address. This might already be done automatically for you if the physical object has a retainer applied to it as described by the note below

- Mark shipped for export to indicate that someone has shipped the real-world object
- Mark physical object exported when the real-world object did reach its destination



Note: You do not need to explicitly Mark for export a physical object that is retained according to a retention policy for which the Disposition Strategy is set to *Export All* or *Export Content*. The retention policy will do it for you.

To export a physical object:

1. Navigate to the physical object that needs to be exported.
2. Skip this step if the physical object is retained according to a retention policy that specifies *Export All* or *Export Content* for the **Disposition Strategy**. Otherwise, right-click the physical object displayed in the content pane and select **Mark for export**.

The **Select Export Location** screen is displayed. A value for the **Current Location** is displayed only if a **Home Location** was specified for the physical object when it was created.

3. Click **Edit** to find and select the new address from the locator. The address object is needed to complete this step.

The **Choose an item** locator is displayed.

The new address object needs to be created ahead of time, if it is to be picked up by the locator. Follow procedures to create physical objects if not.

The new address acknowledged, when you click **OK** on the locator is, for now, displayed next to **Edit** on the **Select Export Location** screen. It will later appear next to the **Current Location** when the export process is completed, that is after the last or third marking is processed.

4. Click **Finish** to acknowledge the new address selected for this marking.
5. Right-click the physical object again only when you know that the real-world object was shipped and select **Mark shipped for export**.
6. Right-click the physical object for a third time only when you know that the real-world object did indeed reach its destination and select **Mark physical object exported**.

6.2.2.5.5.1 Mark for export

Mark for export is a menu or right-click option, the first of three export markings, needed to complete the transfer of a physical object whose real-world counterpart needs to move to a new address or home location. This marking is used to identify the new home location, the new address in particular, for the physical object being transferred.

Although the home location for a physical object could change it will still be available for library requests accept that it will be charged out from the new location and similarly charged in to the new location.

6.2.2.5.5.2 Mark shipped for export

Mark shipped for export is a menu or right-click option, the second export marking needed to complete the transfer of a physical object whose real-world counterpart needs to move to a new address or home location. This marking is used to indicate that the real-world object was shipped and is in transit to its new address or home location.

6.2.2.5.5.3 Mark physical object exported

Mark physical object exported is a menu or right-click option, the third export marking needed to complete the transfer of a physical object whose real-world counterpart needs to move to a new address or home location. This marking is used to indicate that the real-world object made it to its new address or home location.

6.2.2.5.6 Mark physical object shipped (or picked up) for charge-out

Mark physical object shipped for charge-out and Mark physical object picked up for charge-out are menu or right-click options you would apply to a physical object only when its real-world counterpart was actually shipped to an address or picked up. Though a charged out physical object is available for shipping or pickup, it does not mean its real-world counterpart was actually shipped or picked up. These markers can be used anytime after the physical object(s) within a library request have been converted to a charge-out.

Users can specify exactly which charged out object(s) are being picked up or shipped. Users are presented with a manifest that lists the initial selection from which they can exclude items. For containers, this means that all of the charged out contents within it can be marked along with the container in one operation. For example, consider a charge-out with items in the Manifest. The manifest list for a library request is the same on the form used to Convert to Charge-out and on the forms used to Mark physical object picked up for charge-out or to Mark physical object shipped for charge-out. Although the manifest list is the same, their usage is different. The manifest list on Convert to Charge-out allows library administrators to hold back items requested at their discretion, that is to deny or not approve lending one or more of the items requested. The manifest list on Mark physical object picked up for charge-out or Mark physical object shipped for charge-out is used to mark items that are shipped or picked up, or to exclude them if not shipped or picked up.

Selecting an item from the Manifest when you convert a library request to a charge-out refreshes the screen with the option to Hold Back the selected item(s).

Selecting an item from the Manifest when you mark items in a charge-out refreshes the screen with the option to Exclude the selected item(s). Item(s) held back on the Heldback tab can be moved back to the manifest list when you select an item.

To exclude an item if it was not already held back when the library request was converted to a charge-out, navigate to the item, right-click it in the content pane.

Then select Mark physical object picked up for charge-out or Mark physical object shipped for charge-out depending on which of these two options is selected on the library request. The default screen is displayed showing the Manifest. Expanding the Manifest and selecting an item from its list reveals the Exclude button to pick and choose which items to exclude. Items excluded on the Excluded tab can be moved back to the manifest when you select an item.

This marker is also discussed in “[Convert library request to charge-out](#)” on page 490.

6.2.2.6 Disposition of physical objects

6.2.2.6.1 Overview

Physical objects that are retained cannot be deleted directly. When running disposition on physical objects, additional steps need to be taken as the items represent real-world objects. For example, if a box is being destroyed through disposition, the real-world box needs to be destroyed before we remove the representation from the repository. Disposition Manager will mark a physical object for destruction and will stop disposition processing until someone goes and destroys the real-world object and advises the administrator that it has been destroyed. The administrator marks the physical object destroyed and then re-starts disposition to delete the physical object. To run Disposition Manager, refer to “[Running Disposition Manager](#)” on page 230. The following disposition strategies will cause the initial disposition to go incomplete because the real world objects need to be acted on:

- Destroy all
- Destroy content
- Export all
- Export all, Destroy all
- Export all, Destroy content
- NARA Transfer, Destroy all
- NARA Transfer, Destroy content

6.2.2.6.2 Completing disposition for a paper object with a Destroy all strategy



Note: Ensure the physical object is in the final state, and is eligible for disposition (qualification date in the past).

1. From Disposition Manager (or by the Disposition job), dispose the items. The items will remain in Disposition manager, but the physical status of the item will change to either Marked for destruction or Contents marked for destruction. The object will only have its contents marked for destruction if it is a physical container and the retention policy is linked structural.
2. From the Physical Record report, do a search for items that have been marked for destruction or contents marked for destruction.
3. If the status is Marked for Destruction, then select the right-click menu option, Mark Physical Content Destroyed. If the status is Marked for Content Destruction, then select the right-click menu option, Mark Contents Physically Destroyed.



Note: If marking the status of a physical container, all of the contained items need to be in the correct state, otherwise the operation will fail but any of the items that can be marked, will be marked. For example, if someone after running disposition created a new physical document inside the folder, it won't be marked for destruction and this will cause the marking on the folder to fail. To fix, just run disposition again which will cause the physical document to be marked for destruction.

4. Run disposition again and now the object is removed from the repository unless the retention was structural and the item was a container, in which case only the contents are destroyed (physical containers inside will also have their contents marked as destroyed).

6.2.2.6.3 Completing disposition for a paper object with Destroy content strategy

The steps are the same as the Destroy all strategy except at step 4, the physical object will rollover to a new retention policy instead of being removed from the repository.

6.2.2.6.4 Completing disposition for a paper object with a Export all, Destroy all strategy

This disposition strategy is for scenarios where the physical items are sent to perhaps a different company and we no longer want to manage the physical item. The physical item in the real world is not destroyed but the representation in the repository is removed.



Note: Ensure the physical object is in the final state, and is eligible for disposition (qualification date is in the past).

1. From Disposition Manager (or via the Disposition job), dispose the items. The items will remain in Disposition manager, but the physical status of the item will change to Marked for Export.

2. From the Physical Record report, do a search for items that have been marked for export. The location that item is supposed to be sent to can be seen in the Export Address column.
3. Select the right-click menu option, Mark Shipped for Export for the physical object. Note that the item is a physical container, this step must be repeated for each item in the container.
4. Once confirmation that the physical item has reached its destination, select the right-click option, Marked Exported. Note that the item is a physical container, this step must be repeated for each item in the container.
5. Run disposition again and now the physical item is removed from the repository unless the retention was structural and the item was a container, in which case only the contents are destroyed (physical containers inside will also have their contents marked as destroyed).

6.2.2.6.5 Completing disposition for a paper object with Export all, Destroy content strategy

The steps are the same as the Export all, Destroy all strategy except at step 5, the physical object will rollover to a new retention policy instead of being removed from the repository.

 **Note:** At the end of disposition, the physical object will be marked that it is destroyed but it has not been destroyed in the real world. The system will not ask for the item to be marked for destruction.

6.2.2.6.6 Completing disposition for a paper object with Export all strategy

The steps are the same as the Export all, Destroy all strategy except at step 5, the physical object will rollover to a new retention policy instead of being removed from the repository.

 **Note:** At the end of disposition, the physical object will not be marked that it is destroyed.

6.2.2.6.7 Completing disposition for a paper object with a NARA Transfer, Destroy all strategy

This disposition strategy involves an additional confirmation that both the electronic and physical objects have been transferred.

 **Note:** Ensure the physical object is in the final state, and is eligible for disposition (qualification date in the past).

1. From Disposition Manager, dispose the items. The items may also be disposed through the Disposition Job if it is running. The status of the retainer will change to Waiting (note that it may take some time as the disposition may be running asynchronously) and the physical status of the item will change to Marked for Export.



Note: By default, retainers in the Waiting state are not shown. Choose the Waiting checkbox and then do a Search (you may see the retainer status go to the Pending state, but just wait a few minutes for the operation to complete).

2. From the Physical Record report, do a search for items that have been Marked for Export. The location that item is supposed to be sent to can be seen in the Export Address column.
3. Select the right-click menu option, Mark Shipped for Export for the physical object. Note that the item is a physical container, this step must be repeated for each item in the container (this is not required for mark for destruction or Mark Contents Destroyed).
4. Once confirmation that the physical item has reached its destination, select the right-click option, Marked Physical Object Exported. Note that the item is a physical container, this step must be repeated for each item in the container.
5. From the disposition run bundle node, find your run bundle, and open the run bundle.
6. Choose the NARA Transfer and Destroy all, right-click on it and choose confirm transfer.



Note: If all of the physical items have not been marked as exported, you will not be able to confirm the transfer. Use the Open manifest from the NARA Transfer and Destroy all to determine the full list of items that need to be marked.

The confirm action will cause disposition to be continued and the work order can be viewed to see what happened. If the disposition was successful, the physical items will be removed from the repository unless the retention was structural and the item was a container, in which case only the contents are destroyed (physical containers inside will also have their contents marked as destroyed).

6.2.2.6.8 Completing disposition for a paper object with NARA Transfer, Destroy content strategy

The steps are the same as the NARA Transfer, Destroy all strategy except at step 6, choose the NARA Transfer, Destroy content object. At step 6, the physical object will rollover to a new retention policy instead of being removed from the repository. Structural retention is not allowed for this type of retention strategy.



Note: At the end of disposition, the physical object will be marked that it is destroyed but it has not been destroyed in the real world. The system will not ask for the item to be marked for destruction.

6.2.2.7 Barcodes

This feature provides the ability to specify per physical object type, information that can be used to create unique identifiers for scanning and tracking. You can for example, scan the warehouse, its address, all of its contents, as well as its shipping, pickup and return locations or other locations. Each unique identifier is associated with a physical object and its real-world object counterpart.

6.2.2.7.1 Copying a record

When an existing record or its metadata is copied/used to create a new record, the barcode ID along with other attributes are blanked out in the existing record.

6.2.2.7.2 Barcode generation rules

Barcode generation rules are used to create unique identifiers within a specified range that can be prefixed and/or suffixed according to your organizational requirements. A barcode generation rule is needed, must be created first, if you want to be able to select or deselect the option to automatically generate a barcode when you go to create a physical object. The Rule Object Type you select according to this procedure will determine whether or not you can auto generate a barcode when you go to create certain physical objects. The Auto Generate Barcode option on the Create tab, in the procedure for creating a physical object, is otherwise disabled when a barcode generation rule is not specified or when the barcode generation rule is explicitly disabled (when the Enabled option is *deselected*).

To create a barcode generation rule:

1. Navigate to **Barcode Generation Rules**.
2. Click **File > New > Barcode Generation Rule**.

The screen for the **New Barcode Generation Rule** is displayed.

Three mandatory values are needed for the:

- **Rule Object Type**
- **Barcode Lower Range**
- **Barcode Upper Range**



Note: The value for the **Rule Object Type** you select according to this procedure should match (or be a supertype of) the value selected for the **Type** in the procedure used to create physical objects. The option to automatically generate a barcode (**Auto Generate Barcode**) when you follow procedures to create certain physical objects will be disabled if a matching barcode generation rule (or match to a supertype object rule) has not already been created to support the value selected for the **Rule Object Type**. Similarly, the option to automatically generate a barcode (**Auto Generate Barcode**) when you follow procedures to create certain physical objects will be disabled if the rule is disabled. You will not be able to automatically generate a barcode for any containers, for example, if the

only barcode generation rule created is for Physical Documents. Conversely, you will not be able to automatically generate a barcode for a document if the only barcode generation rule created is for Physical Containers. The following object types are subtypes of the supertype for Physical Container (`dmc_prm_physical_container`):

- *Warehouse* (`dmc_prm_warehouse`)
- *Bay* (`dmc_prm_bay`)
- *Bin* (`dmc_prm_bin`)
- *Shelf* (`dmc_prm_shelf`)
- *Box* (`dmc_prm_box`)
- *Folder* (`dmc_prm_folder`)

The numbers you provide for the **Barcode Lower Range** and the **Barcode Upper Range** represent the start and end values of the range. You could specify ranges, for example, from 1 to 1000, 1001 to 2001, and so on. An exception or error message will be displayed when the number of physical objects created reaches the end bound value specified for the **Barcode Upper Range**. No such message will be displayed if the barcode generation rule specifies an **Unlimited Upper Range**.

3. Optionally, you can *select Unlimited Upper Range*, which is deselected by default, and avoid specifying a value for the **Barcode Upper Range**.
4. Optionally, you can *deselect Enabled*, which is selected by default, to disable the barcode generation rule. Disabled rules are labeled *False*.
5. Click **Finish**.

The new barcode generation rule is displayed in the content pane under **Barcode Generation Rules**.

Barcode Generation Rules are displayed or listed as *True* or *False*, *True* when **Enabled** is selected or *False* when deselected.



Note: Change the default filter setting in the upper right-hand corner from *Enabled Barcode Generation Rules* to *All Barcode Generation Rules* to see both enabled and disabled rules.

6.2.2.7.3 Generating and regenerating barcodes

Generating barcodes is optional. It is available for enhanced management of physical objects. A barcode can be printed anytime after it has been generated.

Barcodes can be generated either manually or automatically. There are two procedures you need to follow to generate barcodes automatically; one procedure to create a barcode generation rule and the other procedure that uses the rule to automatically generate a barcode when the physical object is being created.

To automatically generate barcodes, refer to “[Barcode generation rules](#)” on page 513 to create a rule and then refer to “[Create physical object \(document/container/address\)](#)” on page 497 to create the physical object and generate the barcode for it.

Follow this procedure to manually generate a barcode. The ability to manually enter a barcode value makes it possible to change the original value that was automatically generated when the physical object was created. Regenerating a barcode however assigns the next barcode value based on the original value that was automatically generated according to the applicable barcode generation rule. Assume for example, the original barcode value generated for a physical object is HR1001 then later changed manually, for temporary reasons, to some random value say TEMP80567. You could regenerate the barcode in which case the barcode generation rule is referenced for the next available barcode, in this example HR1002 is generated while the manual entry is ignored.

To manually generate a barcode:

1. Navigate to the physical object.
2. Right-click the physical object displayed in the content pane.
3. Select **Properties** and click the **Physical Info** tab.
4. Type the characters and numbers you want for the **Barcode**.

You can overwrite an existing string, the original string that was auto generated, for temporary reasons if necessary and then later follow the procedure to regenerate a new barcode that will replace the original with the next available barcode string.

5. Click **OK**.

To regenerate a barcode:

1. Navigate to the physical object.
2. Right-click the physical object displayed in the content pane.
3. Select **Regenerate barcode**. The next available barcode value is assigned to the selected physical object.

The screen refreshes and a new barcode string replaces the original barcode value with the next available value according to the applicable barcode generation rule if one exists for the physical object selected. If the original value,

for example, specified 100 the new regenerated value would be 101, though it could be higher if someone else used 101 for their physical object before you. Regenerating again would assign a value of 102.

Any physical object selected that is not associated to a barcode generation rule is assigned the value of 1. Regenerating again against the same physical object assigns the next available value of 2.

4. Optionally, you can right-click the same physical object, select **Properties** and then select the **Physical Info** tab to see the new regenerated value for **Barcode**.

6.2.2.7.4 Scanning and transferring scanned barcodes into the system (barcode manager)

Barcodes generated for the various physical objects can be scanned in or out of the system. Movable or portable objects can be scanned in or out of the system against any fixed objects.

Barcode Manager helps you search and list physical objects which have barcodes and those which do not have barcodes. Any barcodes searched that are missing also get listed.

To run Barcode Manager:

1. Click **Records > Barcode Manager**. Barcode Manager is displayed.
2. You can either click **Search** directly or use the filters to narrow the search.
Clicking **Search** directly, with no barcodes (nothing) typed or added to the filters, returns a list of physical objects that have *any* barcodes.

Search results are returned exclusively for only those barcodes added to the **Barcode List**. The results list will include physical objects that have *no* barcodes if no value is typed and inadvertently added as an empty field along with the rest of the list; the results listed would no longer be exclusive. Avoid clicking **Add** with nothing typed for a barcode value unless you want to use it to your advantage to see what physical objects have *no* barcodes.

Any barcode added to the **Barcode List** that cannot be found will get pushed to the **Missing List**.

6.2.2.7.5 Change barcode

The barcode value assigned to a physical object can be changed from its Properties screen on the Physical Info tab or using the option to Regenerate barcode. To change a barcode for a physical object, refer to “[Generating and regenerating barcodes](#)” on page 515 for the preferred procedure.

6.2.2.8 Label printing rules

6.2.2.8.1 Overview

Label templates are used to define label printing rules for physical objects and are used to control what metadata is printed on the label for certain physical object types. One or more rules to select from can be created for a particular physical object type, for boxes or for shelves for example, depending on the attribute values entered/selected on the label template. The label template namely Sample NiceLabel <version> Template, available by default, can be used to create label printing rules.

Make sure NiceLabel Pro software is installed according to *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*.

Members in the Label Template Administrator role can create and modify label templates.

Label templates stored in the repository can be imported to any folder the user decides on, assuming it is allowed through the folder's ACL.

When a user wants to print a label for a physical object:

- The system will throw an error if there is no rule supplied for the physical object type.



Note: Label printing rules may or may not apply to subtypes. So, for a particular physical object type, the system will also look for rules under its super type.

- If there is at least one rule, a GUI will display a screen allowing the user to choose one of the label templates associated with object type.
- If the OK button is clicked, the code will create an XML file with the attributes that are required. At minimum, this would include:
 - The name of the label template
 - The value of the barcode
- The request is submitted to the NiceLabel integration for rendering and displayed to the user in a popup window for printing.

6.2.2.8.2 View/edit a list of label printing rules

Label printing rules displayed in the content pane can also be deleted when necessary if you right-click a label printing rule.

To view/edit a list of label printing rules:

1. Navigate to **Physical Records Manager > Label Printing Rules**.

Only enabled Label Printing Rules are displayed in the content pane unless you change the filter option in the upper right-hand corner from the default setting for **Enabled Label Printing Rules** to **All Label Printing Rules**.

Also, make sure the setting for **Show Items** is set accordingly as the list of items could be spread across more than one page. The item you want to see could be displayed on a page other than the first page depending on the length of the list and the number of items displayed per page. **Show Items** allows you display up to a maximum of 100 items per page.

You can also narrow the list to display only those rules whose Rule Name **Starts with** the characters you enter in the text field.

2. Optionally, if you need to modify an existing label printing rule, in particular if you want to disable or enable a rule, right-click the rule displayed in the content pane and select **Properties**.

6.2.2.8.3 Create a label printing rule

To Create a label printing rule:

1. Navigate to **Cabinets > Templates**.
2. Right-click **Sample NiceLabel <version> Template** and select **Create Label Rule**. **Create Label Printing Rule** is displayed.
3. Enter values for the attributes, described below, on the **Create Label Printing Rule** dialog box displayed and click **Finish** when you are ready to accept the entries.

The mandatory **Name** for each Label Printing Rule must be unique. You can create a rule with only the name and provide values for the rest of the entries at a later time from its Properties though you might want to consider disabling it until you provide values for the remaining entries.

Select the appropriate label template name for **Label Template** field while creating label printing rule. For example, for creating a label printing rule for **Sample NiceLabel <version> Template**, ensure that the **Label Template** field is set as **Sample NiceLabel <version> Template**.

The value you select for **Applies to Object Type** should match the actual physical object type. If for example, you are creating a rule for boxes, select **Box (dmc_prm_box)** or for shelves, select **Shelf (dmc_prm_shelf)**. **Physical Document (dmc_prm_document)** is the selected item displayed by default. The association could also be made to **Physical Container (dmc_prm_physical_container)**.

Applies to Subtypes if selected/checked, means the rule applies to all physical objects that are subtypes of the item selected for **Applies to Object Type**.

The rule is enforced immediately as **Is Enabled** is selected by default though you can deselect it to disable the rule.

Any information to describe the rule can be added to the **Description**.

Click **Select**, to display the attribute locator, if you want to configure more than just the Barcode Value for the rule. The value(s) for the **Attribute Name** selected will also be printed, as additional metadata, to the label, in addition to the Barcode Value.

4. Navigate to **Physical Records Manager>Label Printing Rules** to verify that the Label Printing Rule got created as expected, and if necessary to modify or edit the rule from its **Properties**, in which case you would right-click the rule and select **Properties**.

The steps listed above are applicable while creating other label templates as well (including **Sample NiceLabel <version> Template** or other custom label templates, if any).

6.2.2.8.4 Print a label

To print a label:

1. Navigate to the physical object for which you want to print a label, a physical object displayed in the Home Cabinet for example.
2. Right-click the physical object displayed in the content pane and select **Print Label**.

The label will not be printed and a message is displayed if a label printing rule has not been created for the selected object. You will need to click **OK** or **Cancel** to close the message.

The **Label Print Request** dialog is displayed if a rule has been created for the selected physical object.

6.2.2.9 Batch processing using a portable scanner

6.2.2.9.1 Overview

Batch processing or bulk operations relies on scanning barcodes for one or more operations and uploading scanned results in XML files, also called a Batch File or XML schema, to maintain accurate inventory records such that the actual physical objects in the warehouse match what is in the repository. The family of batch/scanning operations include:

- Mark shipped for charge-out/export

This operation involves scanning a physical container and only its physical content that will be shipped for a library request.

- Mark as destroyed

This operation involves scanning physical objects that will be destroyed.

- Charge-in

This operation involves scanning physical objects that are returned.

- Move

This operation involves scanning physical objects that will be moved from one location to another. The requirement is to only scan the destination box. The software will automatically unlink the object from any other folders that have been marked as physical.

- Reconciliation

This operation involves scanning a physical container object and its contents.

Each operation is associated to an XML file geared to process the scanned information accordingly. The XML file for a particular operation specifies the action type consistent with the desired operation. The XML file selected for a particular operation can be renamed as necessary to help you identify it more easily once it has been uploaded.

The means by which you select a scanning operation is dependent on your organization's preference, scan a barcode that represents an operation or select an operation that is configured on the scanner application. Regardless of the method implemented for selecting an operation, you will first need to select the desired operation, whether it is done by selecting the desired operation on the scanner or scanning the appropriate barcode operation, before scanning the barcodes of the physical objects.

The application on the scanner, once it is docked, automatically exports an XML file for each operation that is uploaded (imported) and processed by Records Manager. The XML file itself must be formed correctly to begin with for the upload to complete successfully. **Figure 6-6** shows an example of an upload failure due to incorrect form whereby the code itself has a problem, in this case a typo. Contact your administrator if you encounter such problems.

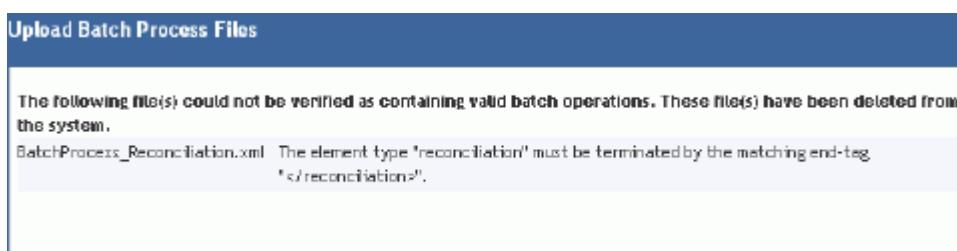


Figure 6-6: Upload error

There are two ways to import/upload the resulting XML file:

- Using the Records menu import option called Upload Batch Processing File

- Using hot-folder functionality that monitors files placed into a folder in the native file system from which they are automatically imported for processing
Hot-folders are based on BPM workflow functionality.

Instructions for the manual method described in the first bullet item using the Records menu option is documented below. Notifications, regardless of the method, are sent to the Records Client Inbox.

Batch Operations are performed asynchronously, therefore any interaction with the user is made through the Records Client Inbox. The Batch File will indicate whether the user wishes to be notified of the successful completion of each operation (to the Inbox) individually, or as a consolidated report on completion of the entire batch. Where errors occur during processing, the system will report the error to the user (via the inbox), and will in addition create an XML file to allow the failed operation to be replayed. Each operation error within a batch is treated individually, although multiple errors within the same operation will result in a single notification and replay file. Replay files are related to their original Batch Files by name - suffix '.issue #n' may be appended to the original Batch File name (where 'n' is the number of the issue in the particular batch). Although supported by OpenText Documentum CM, the name of each Batch File should be unique within the folder into which it is uploaded. This will resolve any ambiguity when errors are reported.

6.2.2.9.2 To manually upload a batch processing file for bulk operations

Follow these instructions when you are done scanning and the scanner has been docked in its cradle:

1. Log in to the Records Client.
2. Select **Records>Upload Batch Processing File**.
The **Upload Batch Process Files** screen is displayed.
3. Click **Add Files** and browse to the XML file(s) you want to upload and then click **Finish**.
Click **Finish** again when the confirmation message is displayed on the same screen.

The XML file, once it is uploaded successfully, will be locked, while Records Manager processes the scanned information in the upload location, the Home Cabinet.

6.2.2.9.3 To view the operation status and/or to view the report for an operation

Follow these instructions when you are done uploading the XML file.

1. Navigate to the upload location, the Home Cabinet for example, where the XML file is being processed or has been processed.

A key is displayed next to the XML file to lock it until it has been processed. An example of the key displayed can be seen in the procedure above.

2. Right-click the XML file and select **Properties** after it has been processed. You can click **OK** or **Cancel** if you do not want to view the report or, you can continue to the next step.

The **Operation Status** screen is displayed listing all the operations executed under the **Operation List**. The same operation can be repeated for one or more containers or the same container if necessary, whether the containers are of the same type or different types. Each operation is sequentially indexed beginning with 0 for the first operation. **All Operations** are displayed by default though you can change the filter setting as needed to display Operations without errors, Operations with errors, Unexpected Operations, or Incomplete Operations. It should be noted that the operations listed are of the same **Type** based on the XML file selected for the desired operation as described in the [“Overview” on page 519](#). Two container objects and their contents were scanned.

The following message is displayed, in the Properties of the XML file if it is locked when you select its Properties: **The selected batch object is marked as being in use by another process. No additional operations may be performed on the object at this time.**

3. Optionally, click **View Report** to see further details regarding the scanned objects.

Although **All Reports** are displayed by default, you can change the filter setting to display only **Error Reports**, **Warning Reports**, **Ok Reports**, or **Fixable Reports**.

4. Click **OK** or **Cancel** to close the report screen then click **OK** or **Cancel** again to exit the Operation Status.

6.2.2.9.4 Batch processing notifications

A notification is sent to the Records Client Inbox of the user specified on the XML file when the XML file is uploaded for processing, whether the upload is successful or not.

To view a batch processing notification:

1. Log in to the Records Client and navigate to the **Inbox**.
2. Double-click the batch notification you want to view.

Batch notifications contain the filename of the XML file uploaded in the following format, making it easier for you to find the notification you want to open: Batch '<uploaded XML filename>' Notification. For example, **Batch**

'BatchProcess_Reconciliation.xml' Notification. The notification illustrated below is an example of a charge-in operation.

You can see that the operation was performed only once and that it had executed successfully.

You can also double-click the XML file listed under **Attachments** to open it.

3. Click **Close** to exit the notification or **Delete** to delete the notification.

6.2.2.10 Pass-along requests

A pass-along request makes it possible for a requestor to give their charged out items to another person using the same library request. Items in a pass-along as a result do not have to be charged-in. A new library request is not necessary and the same items do not have to be charged-out again. A pass-along request can be created even if the objects requested were never shipped or picked up. The Library Administrator however can prevent a pass-along at his or her discretion in favor of redirecting the pass-along to someone else when necessary.



Note: Users requesting pass-along must be part of the dmc_prm_library_user role.

The requestor is asked to choose another addressee/contact if the one selected for a pass-along does not have READ access. A workflow is started and an internal pass-along object, passalong_request, is created when the requestor commits (presses OK) to the pass-along. The passalong_request sets a default due date based on a configurable offset on the Physical Records Manager system configuration object. A task, as a result of the workflow, shows up in the Inbox of the requestor to confirm that the original contact wants to pass-along the set of items. The passalong_request object shows up in the attached lists on the workflow along with the items being passed along. If the requestor agrees/confirms, the system then sends a task to the Library Administrator who then decides whether to accept or reject the pass-along request for the new contact/requestor selected. The Library Administrator will have to provide a due date if accepted. An Inbox task is sent to the original requestor advising that they can pass-along the items and can then finish the task once they hand the items to the recipient. The current location of the items is sent to In Transit. The recipient finishes his or her task once he or she receives the items. The system then automatically sets the current location of the items to their location (or sets it to Unknown if the contact has no known address).

There are two different roles for pass-along requests to satisfy the workflow that does not require an administrator and one for the workflow that does require an administrator:

- dmc_prm_passalong_requestor
- dmc_prm_privileged_passalong_requestor

The requestor would not have to depend on the Library Administrator to accept or reject the pass-along if he or she is in the privileged role.

To create a pass-along request:

1. Log in to the Records Client.
2. Navigate to the physical object that is requested for pass-along.
3. Right-click the physical object displayed in the content pane and select **Pass-along**.
You can select one or more physical objects for a Pass-along.
4. Click **Select Addressee for Pass-along** and select the user who is now going to obtain the physical objects listed.
You can also include **Notes** if necessary.
5. Click **OK** to complete the process.

6.2.2.11 Physical Records Manager reports

There are two reports available with Physical Records Manager. Select from the following links to run the desired report:

- “Running a physical record report” on page 524
- “Running a library request report” on page 530

For a reports overview, refer to “Records reporting” on page 86.

6.2.2.11.1 Running a physical record report

A physical record report is used to list physical objects whether they are under retention or not, based on the combination of filter options selected. Use this reporting feature to determine primarily, among other things, address, status, and availability details for each of the physical objects reported. Right-click actions can also be performed on any one or more of the physical objects reported. You could for example, right-click a reported physical object and select Make Library Request or select any other preferred action.

To run a physical record report:

1. Select **Records > Reports > Physical Record Report**. The **Physical Record Report** is displayed.
Column Preferences, if you click the icon to the right of the columns displayed, can be used to customize the columns displayed. For further details regarding column preferences, refer to “Setting column preferences” on page 77.
2. Click **Report** to obtain results according to the default settings or change the default settings to create your own custom report.
Queries can be set to target any status displayed. You can narrow the reported results to a particular type, a specific folder, and also report from their subtypes and subfolders. Objects associated to a particular address can also be reported. You can also report current versions or all versions of the physical objects reported.

The search feature, that is based on standard Documentum Webtop functionality **Starts With**, is available to search the results returned.

Table 6-7: Physical record report filter descriptions

Filter Name	Description
Type	Filters physical records against one or more of the desired object types selected. All physical records against the object type selected are reported. All physical records are reported if nothing is selected. Click Select Type to specify the desired object type. Subtypes of the selected object types can also be reported if you select Include Sub-types .
In Folder	Allows targeting one or more specific folder locations within the repository, / Temp for example and all of its sub-folders if desired. All folders are searched if nothing is selected.
Home Address	Filters against one or more of the addresses selected. The Home Address specified for a physical object type can be the value selected on its Physical Info tab for the Home Location , Current Location , or Next Location .
Record Version	Only the current record version or all record versions can be filtered. The Current version is selected by default.
Show Physical Record Status	A physical object can be filtered based on one or more records statuses: Marked for Export Shipped for Export Marked for Destruction Marked for Content Destruction Destroyed Contents Destroyed Unmarked Lost
Show All Physical Objects	When selected, reports all objects that are physical objects. Not all of the objects for a selected Type are necessarily physical objects. You can find out using this option if a particular object type, within any targeted folders or the repository, has any physical objects.

Filter Name	Description
Show Physical Objects that cannot be Charged Out	When selected, reports only physical objects that cannot be charged out. Though you can choose to Show All Physical Objects against a particular object type, you might want to determine, using this filter, which ones cannot be charged out before trying to convert a library request that has such an object in its manifest, or before adding it to another library request.
Show Physical Objects that can be Charged Out	When selected, reports only physical objects that can be charged out. A library request can be converted to a charge-out if the objects listed in its manifest can be charged out. Physical objects can be reported regardless of their charge-out status or based on any combination selected for Show Charge-out Status: <input checked="" type="checkbox"/> In <input type="checkbox"/> Waiting to Ship for Charge-out <input type="checkbox"/> Waiting for Pickup <input type="checkbox"/> Out These checkbox options are displayed only when the radio button for this filter is selected.

Table 6-8: Physical record report column descriptions

Column	Description
Name	The value assigned for the Name of the physical object.
Barcode	The barcode value assigned to the physical object.
Home Address	The home location of the physical object reported. The value is blank if the Physical Info tab on the Properties of a physical object does not include a value for the Home Location . The value for the Home Address and Current Address could be the same.
Current Address	The current location of the physical object reported. The value is blank if the Physical Info tab on the Properties of a physical object does not include a value for the Current Location . The value for the Home Address and Current Address could be the same.

Column	Description
Export Address	<p>The next address location, as opposed to the current address location, to where the item will be exported. The value may be set as a result of either:</p> <ul style="list-style-type: none"> • Disposition processing using any export disposition strategy or NARA transfer strategy • Charging out an item • Passing along an item • Manually exporting <p>The value could be reported from one of two sources, from the physical object or from the RPS Application Configuration object.</p> <p>The value specified on the RPS Application Configuration object. The value is blank if there is no value specified for the Export Address on the RPS Application Configuration object or for the Home Location on the physical object. All physical objects that undergo disposition against a disposition strategy that requires the object to be exported, are exported to this location. Export processing upon disposition is prevented for any physical object if the RPS Application Configuration object does not have a value specified for this field.</p>
Status	<p>The record status of the physical object reported: Marked for Export Shipped for Export Marked for Destruction Marked for Content Destruction Destroyed Contents Destroyed Unmarked Lost</p> <p>The physical objects reported can be narrowed based on the checkboxes selected for the Show Physical Record Status filter.</p>

Column	Description
Charge-out Status	<p>The charge-out status of the physical object reported could be in one of the following states:</p> <p>In, the physical object is charged in and is therefore available for charge-out</p> <p>Waiting to Ship for Charge-out, the physical object in a library request has been converted to charge-out and is now waiting to be shipped to the pickup location</p> <p>Waiting for Pickup, the charged out item has been shipped to the pickup location but has not yet been picked up</p> <p>Out,</p> <p>The physical objects reported can be narrowed based on the checkboxes selected for the Show Charge-out Status filter.</p>
Availability	<p>The value is either <i>Yes</i> or <i>No</i>. <i>Yes</i> to indicate that it can be added to a library request or <i>No</i> if not. The value is always <i>Yes</i> if the Charge-out Status displays <i>In</i>.</p>
Assembled From Id	<p>Set only if the physical item is a snapshot of a VDM. For physical items, the value will always be <i>0000000000000000</i>, as a snapshot cannot be considered a physical object.</p> <p>This field is used to set the icon and it is recommended to avoid showing this field.</p>
Current Address Id	<p>The object Id of the address selected for the Current Address.</p>
Export Address Id	<p>The object Id of the address selected for the Export Address.</p>
Format	<p>This field is normally blank. However, if content was associated programmatically with the physical object, this would show the format of the content. Physical objects do not usually have content. This field is used to set the icon and it is recommended to avoid showing this field.</p>
Has Frozen Assembly	<p>The value is <i>Yes</i> or <i>No</i> against virtual documents or is left blank if the physical object is not a virtual document. A frozen assembly is created when the snapshot of a virtual document has the Freeze Snapshot attribute selected.</p> <p>This field is used to set the icon and it is recommended to avoid showing this field.</p>

Column	Description
Home Address Id	The id of the home address. Normally the current address is sufficient to show.
Is Replica	Set if the physical item was replicated from another repository. This field is used to set the icon and it is recommended to avoid showing this field.
Is Virtual Document	Normally this field is set to FALSE. However, if the physical object was converted to a VDM. this field is set to TRUE. This field is used to set the icon and it is recommended to avoid showing this field.
Link Count	The link count is a default field defined for all dm_sysobjects. Please refer to the Documentum CM Server documentation for more information. This field is used to set the icon and it is recommended to avoid showing this field.
Reference	The reference is a default field defined for all dm_sysobjects. Please refer to the Documentum CM Server documentation for more information. This field is used to set the icon and it is recommended to avoid showing this field.
Type	Indicates the object type (r_object_type), Normally this type inherits from physical document or a physical container. Known types that ship with the product include: Physical Document (dmc_prm_physical_document) Bay (dmc_prm_bay) Bin (dmc_prm_bin) Box (dmc_prm_box)Physical Container (dmc_prm_physical_container) Physical Folder (dmc_prm_physical_folder) Shelf (dmc_prm_shelf) Warehouse (dmc_prm_warehouse)
Version	Indicates the current version of the physical object, CURRENT, 1.0 or CURRENT, 2.0 and so on for example.

3. Optionally, if you want to capture all of the results in comma-separated values, click **Export All to CSV**. Or, to capture the results of one or more rows, select the desired rows and then click **Export Selections to CSV**. You can also right-click a reported item and perform the desired menu action. You can for

example, select **Make Library Request** for the selected object if its **Charge-out Status** is *In* and its **Availability** is *Yes*.

6.2.2.11.2 Running a library request report

A library request report is used to list library requests made for physical objects. Library requests are made to borrow one or more physical objects which can only get processed when the requested physical objects do become available. A library request may not get processed for some time if all the objects requested are asked to be sent or picked up at the same time. A library request is completed when all the physical objects requested are charged out and taken possession of. A request report can be used to query library requests by Request Date, Requestor, Shipping Address, Home Address, and its Current State. You can also perform right-click actions on a reported item to Convert to Charge-out, Cancel Request, or edit its Properties.

The library Request Report makes it possible for you to save and reload whatever settings you configure using the new Load and Save buttons. Criteria, as well as column sort preferences can be saved. Each save performed overwrites the previously saved information.

A new filter option is also added to report library requests for which the current state is Pending.

To run a library request report:

1. Select **Records > Reports > Library Request Report**. The **Library Request Report** is displayed.
Column Preferences, if you click the icon to the right of the columns displayed, can be used to customize the columns displayed. For further details regarding column preferences, refer to "[Setting column preferences](#)" on page 77.
2. Click **Report** to obtain results according to the default settings or change the default settings to create your own custom report.
The **Creation Date** is used to identify library requests according to the entry for the **Date Requested** attribute on the form used to make a library request. You can query against a single date or range of dates. You can further narrow the query according to Requestor, Shipping Address, Home Address, and state. Requests for physical objects to be sent or picked up all at once can also be included in the report or excluded from the report.
3. Optionally, you can right-click a reported item and perform the action needed. You can for example, right-click a reported item and select Convert to Charge-out.

6.2.2.12 Physical Records Manager jobs

Jobs can automate certain processes and can be scheduled to work continuously. Job objects are available and executable on a user-defined schedule.

Actions performed by Physical Records Manager jobs are described in “[Physical Records Manager jobs and method arguments descriptions](#)” on page 531. You can find further details about a job, Last Run and Job Status for example, under Job Management (**Administration > Job Management > Jobs**) if you log in to Documentum Administrator.

Administrators can disable a job from its Properties to prevent it from running automatically. To enable or disable a job, right-click the job and select **Properties**. On the **Properties** screen for the **State** attribute select *Inactive* to disable or *Active* to enable.

Although a job may be disabled from running automatically, it can at any time be run manually. To run a job manually, if you cannot wait until it is run automatically, right-click the job and select **Run**.

Table 6-9: Physical Records Manager jobs and method arguments descriptions

Job Name	Description	Method Arguments	Description
dmc_prm_CareTaker Job	Deletes the library requests after they have been in the final state for a set duration. (Requests in a final state for a set duration)	durationInDays	<p>The value you enter determines the number of days a library request can stay in the final state before the job can delete it. The default value is set to 5 days.</p> <p> Note: The countdown starts over whenever there is a modification to a library request. Changing an entry, the Shipping Address for example, resets the clock for that particular library request.</p>

Job Name	Description	Method Arguments	Description
dmc_prm_LibRecAFTERDateJob	Sends a notification to a library administrator for any new incoming library requests since the job last ran. The date the job last ran is stored in the PRM Configuration object. Library administrators can register for notifications based on the home address for physical objects. (Sends Notifications On Library Requests After A Date)	durationInDays The default is 1 day.	The value you enter determines the number of days before notification is sent to a library administrator.
dmc_prm_NotificationJob	Sends notifications for overdue charge-outs. When this job runs, it will send a notification to any library user who has the items and to return the items which are now overdue. This notification is sent only once per charge-out, for example if a person is sent a group of items, one notification is sent against all of the items that were charged-out. The library administrator could later manually send a recall notice if the user still does not return the items. Contacts specified for the charged-out items receive the notifications. (Notification for overdue charge-outs)	No arguments.	

6.2.2.13 Physical Records Manager audit events

[“Audited events in Physical Records Manager” on page 533](#) describes the information, in the audit trail object, that is stored in string_1 to string_5 of the audit trails for Physical Records Manager events. Only the strings that are populated are listed. Objects are also described for audit trails that pass one or more object IDs.

For an overview of auditing and the procedures to enable auditing, to activate the audit policy schema, to verify an auditing of an event, and to view and remove an audit refer to, [“Records auditing” on page 78](#).



Note: Although up to 5 strings can be utilized by an event, only strings 1 and 2 are displayed in the results of an Audit Trail Report. Also, the content of one string may spill into the next string if it needs extra space.

Table 6-10: Audited events in Physical Records Manager

Physical Records Manager audit events (Application Code = dmc_rps)		
Application events appended to target object type: <i>dm_sysobject</i> Check the Include all subtypes on the Register Audit screen when adding/selecting the various events for only this object type.		
<i>Event Name</i>	<i>Strings Usage</i>	<i>Object ID</i>
dmc_prm_generated_barcode	string_1: the barcode that was generated	ID1: rule used to generate the barcode
dmc_prm_marked_for_destruction	string_1: consists of 1 of 2 values: 1) value based on initiated_via_disposition, when Disposition Manager is run, or 2) value based on initiated_manually, when the disposition job is run	n/a
dmc_prm_marked_for_export	string_1: consists of 1 of 2 values: 1) value based on initiated_via_disposition, when Disposition Manager is run, or 2) value based on initiated_manually, when the disposition job is run	ID1: home address ID2: current addressID3: export location
dmc_prm_marked_lost	n/a	n/a
dmc_prm_marked_physically_destroyed	n/a	n/a

Physical Records Manager audit events (Application Code = dmc_rps)		
dmc_prm_marked_shipped_for_export	n/a	ID1: home address ID2: current addressID3: export location
dmc_prm_physiclaly_exported	n/a	ID1: home address ID2: current addressID3: export location
dmc_prm_picked_up	n/a	ID1: library request ID2: charge-outID3: pickup address
dmc_prm_sent_pickup_notice	string_1: contact name string_2: library request name string_3: charge-out name	n/a
dmc_prm_sent_recall_notice	string_1: contact name string_2: library request name string_3: name of object being recalled	n/a
dmc_prm_shipped_to_address	n/a	ID1: charge-out ID2: library requestID3: contact sent to ID4: address sent to
dmc_prm_chargeout	string_1: contact name string_2: library request name string_3: charge-out name string_4: due date in time format, DF_TIME_PATTERN4 dd-mon-yyyystring_5: shipping address	ID1: contact ID2: library requestID1: charge-out
dmc_prm_chargein	n/a	ID1: library request ID2: contactID3: charge-out ID4: current address of object
dmc_prm_umarked_for_destruction	n/a	n/a
dmc_prm_umarked_for_export	n/a	ID1: home address ID2: current addressID3: export location
dmc_prm_umarked_lost	n/a	n/a
dmc_prm_umarked_physically_destroyed	n/a	n/a
dmc_prm_umarked_shipped_for_export	n/a	ID1: home address ID2: current addressID3: export location

Physical Records Manager audit events (Application Code = dmc_rps)		
dmc_prm_request_item	string_1: library request name string_2: contact name string_3: requested date in time format, DF_TIME_PATTERN4 dd-mon-yyyy	n/a
dmc_prm_found_on_chargein	n/a	ID1: library request ID2: contactID3: charge-out ID4: current address
Application events appended to the target object type: <i>dmc prm batch</i>		
dmc_prm_batch_initialized	string_1: batch processing initiated string_2: processed by: consists of the user specified in the XML file. If no user in the XML is specified then the install owner is used when run asynchronously. Otherwise, the user who uploaded the XML file is used when it is run synchronously.	n/a
dmc_prm_batch_operation_executed	string_1: operation shown is a number that represents the operation that was executed string_2: operation name string_3: status shown as 0 if it failed or 1 if it completed	n/a
dmc_prm_batch_processing_complete	string_1: batch processing completed string_2: status shown as 0 if it failed or 1 if it completed	n/a
Application events appended to the target object type: <i>dmc prm library request</i>		
dmc_prm_converted_to_chargeout	string_1: due date in time format, DF_TIME_PATTERN4 dd-mon-yyyy string_2: contact name string_3: shipping option string_4: next address items are shipped to string_5: displays the pick up address only if string_3 is set to pick up at address	ID1: charge-out ID2: contact ID3: next address ID4: pickup address
dmc_prm_canceled_request	n/a	n/a

Physical Records Manager audit events (Application Code = dmc_rps)		
dmc_prm_passalong_CONVERTED_TO_chargeout	string_1: due date in time format, DF_TIME_PATTERN4 dd-mon-yyyy string_2: contact name string_3: shipping option string_4: next address items are shipped to string_5: name of user originating the passalong	ID1: charge-out ID2: contact ID3: next address ID4: pass-along request
Application events appended to the target object type: <i>dmc_prm_chargeout</i>		
dmc_prm_sent_overdue_notice	string_1: user name receiving the notice string_2: charge-out name	n/a
Application events appended to the target object type: <i>dmc_prm_passalong_request</i>		
dmc_prm_passalong_request_ed	string_1: user name of the recipient	n/a
dmc_prm_passalong_approved	n/a	n/a
dmc_prm_passalong_rejected	n/a	n/a
dmc_prm_passalong_completed	n/a	n/a
dmc_prm_passalong_initiated	n/a	n/a
dmc_prm_passalong_handover_started	n/a	n/a
dmc_prm_passalong_handover_completed	n/a	n/a
dmc_prm_passalong_failed	n/a	n/a
dmc_prm_passalong_cancelled	n/a	n/a

Chapter 7

Core OpenText Documentum CM functionality

Although the Documentum Webtop Client provides limited records functionality, all Documentum Webtop functionality is always available whether you purchase one or more of the records products, Retention Policy Services or Records Manager. The **Records** menu on the Records Client provides total records functionality. This means that the **Records** menu on the Records Client provides many more options than only the three possible options on the **Webtop** client.

The **Records** menu on the *Documentum Webtop Client* provides limited records functionality specific to Records Manager. The three options available are:

- declare formal records
- create record relationships
- make library requests



Note: The client, whether it is the Records Client or the Documentum Webtop client, must be registered (approved) for Privileged DFC. All records functionality, regardless of the records products it supports, is dependant on Privileged DFC. If you encounter any problems with records functionality, make sure you are in the correct records role and that the client you are working from is Privileged DFC approved.

7.1 Repositories

7.1.1 Log in to a repository

To log in to a repository, you need:

- Records Client URL
- Repository name
- Your user name, and password for the repository
- Records Client Network location (if applicable)
- Microsoft Windows NT domain name (if applicable)
- Language (if applicable)

To log in to a repository:

1. In your web browser, type the Records Client URL.

If you use either saved credentials or an SSO-based authentication, Documentum Webtop prompts you to select a repository in the **Repository list** of the Login screen, if you log in the first time or if the repository information is

not available in the cache. Select a repository and click **OK** to log in to Documentum Webtop. Alternatively, the SSO-based authentication logs you in to Documentum Webtop automatically when you access the Documentum Webtop URL. Skip the rest of this procedure.

2. If the **Login** page appears, type your login name, and password for the repository. Login names, and passwords are case sensitive.
3. In the **Repository** list, select the repository.
4. In the **Location** list (if available), select the location on your organization network from which you are accessing Records Client.
This allows you to access content from the nearest storage area in the network. Depending on your organization's setup, this location might be a fixed value.
5. To save credentials so that you log in automatically the next time you run Records Client from this computer, select **Remember my credentials for next time**. Once you are logged in, you can view or delete your saved credentials through your preferences.
6. To enter a Microsoft Windows NT domain name, click **More Options**, and enter the domain.
7. To select language, click **More Options**, and select the language.
8. To use accessibility features, click **More Options**, and select **Additional Accessibility Options**.
The accessibility mode provides linear navigation; tab navigation; lists instead of menus; and additional descriptive text.
9. To change your password, complete these steps:
 - a. Click **More Options**.
 - b. Click **Change Password**.
 - c. Type your current password, and new password.
 - d. Click **Apply**.



Note: If your organization uses Lightweight Directory Access Protocol (LDAP), you cannot change your password from the login page. Ask your system administrator how you can change your password.

10. Click **Login**.

7.1.1.1 Log in as an express user

If your application includes the **express user** role, and if you have been assigned that role, then when you log in you are given limited access to repository functionality.

If you have been assigned the express user role, you log in with the usual procedure for logging in, as described in “[Log in to a repository](#)” on page 537

7.1.1.2 Log into another repository

To log into another repository:

1. If the repository is listed in the navigation pane, select the repository, and skip to [step 3](#).
2. If the repository is not listed in the navigation pane, do these:
 - a. Select **Add Repository**.
 - b. If the repository is listed on the **Add a Repository** page, select the repository, and click **OK**. Skip to [step 3](#).
 - c. If the repository is not listed on the **Add a Repository** page, click **more repositories**.
 - d. On the **Connection Brokers** page, enter the name of a connection broker, and click **Add**. A connection broker determines the repositories available to log into. Ask your administrator for the names of connection brokers your organization uses.
 - e. Click **OK**.
 - f. On the **Add a Repository** page, select the repository, and click **OK**.
3. Type your user name, and password for the repository.
4. Click **Login**.

7.1.1.3 Log out of all repositories

To log out, select **File > Logout**.

7.1.1.4 Set your favorite repositories

To set your favorite repositories:

1. Select **Tools > Preferences**.
2. Select the **Repositories** tab.
3. In the **Select a Repository** list, select the repository to add, and click the add arrow.
4. To remove a repository from your **Favorite Repositories** list, select the repository, and click the remove arrow.

5. To change the order in which repositories appear, select a repository in the **Favorite Repositories** list, and click the up or down arrow.
6. Click **OK**.

7.1.2 Navigate a repository

A repository is a virtual storehouse for your organization's content. Your organization might use multiple repositories. Each repository is comprised of nodes that give access to the repository's content, and functions. For example, the My Home Cabinet node contains your personal files, and folders. Records Client displays the repository's nodes in the navigation pane.

To navigate the repository, do any of these. Try each to see how the actions differ:

- Click a node in the navigation pane.
- Double-click a node in the navigation pane.
- Click the plus sign adjacent to the node in the navigation pane.
- Click a location in the content pane.
- Click a location in the navigation path at the top of the content pane.

To select an item in the content pane, click the item.

To select multiple items that are adjacent to each other in the content pane, click the first item, and then hold down *Shift*, and click the last item.

To select multiple items in the content pane that are not adjacent to each other, click each item while hold down *Ctrl*.

To select all items in the content pane, select an item in the content pane and press *Ctrl+A*.

To deselect a single selected item, click the item.

To deselect an item in a group of selected items, hold down **Ctrl**, and click the item.

To change how items are displayed in the content pane, do any of these:

- To display only those items that begin with a certain character string, type the character string in the text field at the top of the content pane, and click .
- To return to the original list, click .
- To filter the list to display only certain types of items, select the appropriate filter in the drop-down menu above the list.
- To display or hide thumbnails, click .
- To sort a column, click the column heading. To reverse the sort order, click the heading a second time.

To sort by lock owner, click . To change the columns that appear, see “Select the columns that appear in lists” on page 541.

See also:

“Navigate categories” on page 542

7.1.2.1 Select the columns that appear in lists

This topic includes several different procedures for selecting the columns that appear in a list.

To select the columns that appear in the current list:

1. Navigate to the list.
2. In the column header select .
3. To add a column, do these:
 - a. In the **Select object type** list, select the type of item that contains the property to display.
 - b. In the **Select attributes to display** list, select the property to be displayed in a column.
 - c. Click the add arrow.
 - d. Repeat a on page 541 through c on page 541 for as many properties as you want to add.
4. To change the order in which columns appear, select a property in the **Selected attributes to display as column**, and click the up or down arrow.
5. To remove a property that is displayed as a column, select the property in the **Selected attributes to display as column**, and click the remove arrow.
6. When you are done adding, and removing properties, click **OK**.

To select the columns that appear in a particular location:

1. Select **Tools > Preferences**.
2. Select the **Columns** tab.
3. Scroll to the appropriate view, and click **Edit**.
4. To add a column, do these:
 - a. In the **Select object type** list, select the type of item that contains the property to display.
 - b. In the **Select attributes to display** list, select the property.
 - c. Click the add arrow.
 - d. Repeat a on page 541 through c on page 541 for each property to add.

5. To change the order in which columns appear, select a property in the **Selected attributes to display as column** list, and click the up or down arrow.
6. To remove a property from display, select the property in the **Selected attributes to display as column** list, and click the remove arrow.
7. Click **OK** twice.

To remove a column from a list:

1. Navigate to the list from which to remove a column.
2. Right-click the column header, and select **Remove Column**.

7.1.2.2 Navigate categories

Categories provide alternate ways to organize files from the way they are organized in cabinets. Categories are available if Records Client is integrated with Documentum Content Intelligence Services Server, and if the repository has been enabled for category navigation. Ask your administrator if, and how your organization uses categories.

To navigate categories, click **Categories**, and use the standard procedures for navigating through the hierarchy structure.

If your organization uses categories, then:

- You might be able to submit files for categorization.
- When you create a new document from a template, the template might specify that the new document is linked to one or more categories.

To submit a file for categorization:

1. Navigate to, and select the file to be submitted.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Submit for Categorization**.
3. At the confirmation prompt, do one of these:
 - If submitting one file, click **OK**.
 - If submitting multiple files, confirm submission for each file separately by clicking **Next**. For the last file, click **Finish**.

To confirm submission for all remaining files at once, click **Finish**.

7.1.3 Locate an item in a selection dialog box

To locate an item in a selection dialog box, use any of these actions:

- To open a directory location, click the location.
- To return to a previous location, click the location in the navigation path above the list.
- To look in a different repository, select the repository in the **Repository** drop-down list, if available.
- To display only those items that begin with a certain character string, type the character string in the text box above the list, and press Enter.
- To narrow the types of items displayed, select a different filter in the drop-down menu above the list.

To select an item, click it. If the selection dialog box includes two list boxes, then you must also click the arrow to move your choice to the second list box. You can move multiple items to the second list box.

7.1.4 Set your preferences

Preferences determine your choices for how Records Client displays repositories, and performs certain actions.

Most preference settings are stored in the repository so that if you log in from a different machine, those settings still apply.

Some preference settings, such as login settings, are stored in a cookie on your local machine. Those settings are used only on that machine.

This topic describes general preferences. To set preferences for a specific functionality within Records Client, see the topic that covers that functionality.

To set your general preferences:

1. Select **Tools > Preferences**.
2. Select the **General** tab, and complete the fields in “[General preferences on page 543](#)”.

Table 7-1: General preferences

Field	Description
Section to Start In	The page that opens when you log in.
Checkout Location	The location of your checkout directory. Your checkout directory is the location on your computer where Records Client copies files when you check them out from the repository.

Field	Description
Saved Credentials	Your user names, and passwords for logging in automatically to certain repositories.
Theme	The set of colors, patterns, and fonts used in your display.
Drag and Drop	This enables you to drag-and-drop items with your mouse. This option requires that you restart your browser for the change to take affect.
Autocomplete	If the autocomplete option is enabled, then when you begin typing text in a field, autocomplete displays suggestions for completing the field. To accept a suggestion, click it. Autocomplete displays suggestions from a record of your previously entered words, and phrases, and in some case from your organization's list of common text that all users might enter. To clear the cache of your previously entered words, and phrases, click Reset .
Hidden Objects	In file lists, this displays items marked as hidden.
Document Links	If available, select this option to let Records Client scan each imported or checked-in document for any linked documents. If linked documents are found, they are imported or checked in, and the original document becomes a virtual document. The linked documents become descendants.
Accessibility Options	The accessibility mode provides linear navigation, tab navigation, lists instead of menus, and additional descriptive text.

3. To save your changes, click **OK**.

To set your formats preferences:

This topic describes formats preferences.

1. Select **Tools > Preferences**.
2. Select the **Formats** tab, and complete the fields in “[Formats preferences](#)” on page 545.
3. Click **Add**.

You can add custom viewing, and editing applications, and set your formats preferences for viewing, and editing.

Table 7-2: Formats preferences

Field	Description
Choose object type	Select the object type from the dropdown list.
Primary format	Select the primary format of the object you have selected.
Format for viewing	Select the format for viewing. By default, it may appear based on your primary format
Would you like this content to appear in the web browser	Select the option.
Application for viewing	Select the application for viewing the object from the dropdown list or use the Select Application link to browse, and select the application for viewing.
Application for editing	Select the application for editing the object from the dropdown list or use the Select Application link to browse, and select the application for editing.

4. To save your changes, click **OK**.

7.1.5 Open an additional repository window

To open an additional window that displays the repository, select **Tools > New Window**.

7.1.6 Drag-and-drop

Users can select multiple files and perform a drag and drop. The multi-select drag and drop functionality is available for all areas where single file drag and drop was previously available. For example, users can multi-select files and drag and drop them to another folder in the repository or to the desktop. Multi-select drag and drop also works when exporting and importing multiple files to and from the local file system.

To use drag-and-drop, you must first enable the drag-and-drop option in your general preferences, as described in “[Set your preferences](#)” on page 543.

To perform an action with drag-and-drop:

1. Navigate to, and select the items to drag-and-drop.
2. Click the items to drag, and continue to hold down the mouse button. While continuing to hold down the mouse button, drag the items to the drop target, and then release the mouse button.

If you are dragging the items to a target that is not currently displayed, you must first navigate to the target by doing one of these:

- Navigate to the target using the other Records Client pane.
- Navigate to the target by opening a new window. You can open a new window by selecting **Tools > New Window**.

7.1.7 Right-click

To perform an action on an item you can right-click the item, and select the action from the shortcut menu.

7.1.8 View messages

Success, and error messages are displayed in the status bar at the bottom of the page. If a message is longer than the status bar's display area, you can view the full message by selecting **Tools > View Messages**.

7.1.9 View the status of background operations

To display the status of background operations, select **Tools > Job Status**.

A background operation is an operation that can perform while allowing you to do other work. For example, if you check in a file, and are given the option to first store the content on your local network before storing it globally, then the global operation will occur in the background.

7.1.10 Refresh page

Documentum Webtop improves performance by reducing the amount of refreshes and by making better utilization of the AJAX framework. The following are a few examples:

- User chooses a folder in the browser tree to view a list of content contained in the folder. Before Documentum ECM 6.5, there was first a refresh of the browser tree applet and then there was a refresh of the content list. In Documentum ECM 6.5, there is no refresh of the browser tree.
- In the content list pane, the user double-clicks on a subfolder to see contained content. Before Documentum ECM 6.5, the browser tree applet refreshed and then the content pane refreshed to show the content. The browser tree refreshes in order to show a selection of the folder in the browser tree and to expand that folder if needed. In Documentum ECM 6.5 the selection and expansion is accomplished without a refresh.
- User has a checked out document. The user decides no changes are needed and wants to cancel the checkout. The user selects the content and chooses the menu option to cancel checkout. Before Documentum ECM 6.5, the screen went blank before bringing up a dialog to choose OK on the cancel. After choosing OK, the user saw another blank screen and a progress bar to show the user progress of

the action. The application then returned to the content pane. While returning to the content pane, the browser tree applet and content pane refreshed. The removal of refreshes, the enhanced transfer progress bar, the use of modal dialogs, as well as the improved performance, significantly enhances the user experience in this case.

The reduction of screen refreshes are found throughout the product. These are just a few examples.

7.1.11 Select HTTP or UCF content transfer

Documentum Webtop 6.5x enables administrators to specify HTTP or UCF content transfer for different users within the same Documentum Webtop installation. Before Documentum ECM 6.5, all users within the same Documentum Webtop installation had to use either HTTP or UCF content transfer.

UCF content transfer is more usable and performs better. The following lists the UCF enhancements for Documentum ECM 6.5x:

- Reduction in the number of round trips between the UCF client and server. This feature is especially effective for improving transfer performance for smaller files over a high latency WAN.
- The following UCF client initialization/startup improvements:
 - Sharing a JVM instance across multiple web sessions
 - Starting JVM upon login
- Support for PDF byte streaming through a native viewer.
- Use of parallel streams to increase content transfer rate. This feature is especially effective for improving content transfer performance of large files over a high latency WAN (outbound and inbound).
- Freeing up stuck threads to optimize resources and increase concurrency.
- Reduction in unnecessary WDK UCF client calls.

An improved content transfer dialog shows the action that is running (in the header of the dialog), the file which is transferring at the time, and progress of that transfer. The new dialog is easier to understand and is similar to other applications with which a user may be familiar.

7.1.12 Use modal dialogs

This feature provides modal popup dialogs for action screens involving dialogs. A modal dialog is a child window which requires the user to interact with it before they can return to the parent application. This feature enhances performance and allows the user to see the context from where the action was launched. Previously, the user choose an action, the screen refreshed and took the user to a new screen. With modal dialogs, a new window pops up on top of the previous screen. The previous screen is viewable, but no actions may be taken on that screen while the modal dialog is active.

7.1.13 Work with repository documents offline through My Documentum

My Documentum for the Desktop is a client application that lets you work on your documents in the offline mode when you are not logged into Records Client. My Documentum for the Desktop must be installed on your local machine in order to be used. If you are not certain whether it is installed, ask your system administrator.

My Documentum for the Desktop keeps selected repository files available on your machine so that you can still work with the files even if you are disconnected from Records Client. When you again log in, My Documentum for the Desktop synchronizes the documents on your machine with those in the repository. You can perform synchronization manually or can set synchronization to occur automatically at a prescribed time or event.

If installed on your machine, you access My Documentum through Windows Explorer or through Microsoft Office applications. The folder hierarchy within the My Documentum folder matches the folder hierarchy used in the repository.

You can search, edit, save, and create documents in the My Documentum folder. When you next log in, and synchronize, your changes are uploaded to the repository. For more information on My Documentum, see the *My Documentum help system* or the *OpenText My Documentum for the Desktop (File Share Services) - User Guide (EDCDC-UGD)*.

7.1.14 View product information

To view the version number, and other product information, select **File > About Records Client**.

The product information includes version of Web Development Kit (WDK), upon which Records Client is built. WDK is the OpenText Documentum CM framework used to build applications that access repositories by using web browsers.

7.2 Files and folders

7.2.1 Create a file

To create a new file:

1. Navigate to the folder in which to create the new file.
2. Select **File > New > Document**.
3. If a selection dialog box appears, select a template for the new file, and click **OK**. For detailed steps see ["Locate an item in a selection dialog box" on page 543](#).
If the repository's Templates cabinet does not contain a template for a custom type, then you cannot create a file of that type now. Instead, you can create a file on your local computer, import it into the repository, and then assign it the custom type.
4. In the **Create** tab, do these:
 - a. Type the name of the new file.
 - b. To apply a lifecycle to the file, click **Apply Lifecycle**, then select the lifecycle. Then, if the option is available, select the lifecycle state.
 - c. Enter additional information in the **Create** tab as needed.
5. In the **Info** tab, set properties as described in ["Common tabs in the Properties dialog box" on page 551](#) in the topic ["Set properties" on page 550](#).
6. If other tabs appear, enter information in those tabs as appropriate. For information on the functionality affected by those tabs, see the topic that covers that functionality.
7. Click **Finish**.

7.2.2 Create a folder

To create a new folder:

1. Navigate to the location in which to create the new folder.
2. Select **File > New > Folder**.
3. In the **Create** tab, enter the name, and the type of the new folder. Enter additional information as needed.
4. In the **Info** tab, set properties as described in ["Common tabs in the Properties dialog box" on page 551](#) in the topic ["Set properties" on page 550](#).
5. In the **Permissions** tab, specify the access that specific users, and groups have to the folder. For instructions, see ["Edit permissions" on page 696](#).

6. If other tabs appear, set information in those tabs as appropriate. For information on the functionality affected by those tabs, see the topic that covers that functionality.
7. Click **Finish**.

7.2.3 Create a cabinet

Cabinets display the highest level of organization in a repository. Cabinets contain folders, and files.

To create a new cabinet:

1. Navigate to the repository in which to create the new cabinet.
2. Select the **Cabinets** node.
3. Select **File > New > Cabinet**.
4. In the **Create** tab, type the name of the new cabinet, and type of cabinet. Enter additional information as needed.
5. In the **Info** tab, set properties as described in “[Common tabs in the Properties dialog box](#)” on page 551 in the topic “[Set properties](#)” on page 550.
6. In the **Permissions** tab, specify the access that users, and groups have to the cabinet. For instructions, see “[Edit permissions](#)” on page 696.
7. If other tabs appear, set information as appropriate. For information on the functionality affected by those tabs, see the topic that covers that functionality.
8. Click **Finish**.

7.2.4 Set properties

To set properties for an item:

1. Navigate to, and select an item.
To select multiple items at once, click each item while holding down *Ctrl*.
2. Select **View > Properties > Info**.
If the  icon appears next to an item, you can click the icon to display the item's properties.
3. In each tab, set properties as described in “[Common tabs in the Properties dialog box](#)” on page 551. If your product includes tabs not covered in this table, search this documentation for the topics that describe the functions governed by those tabs.
If you are setting properties for multiple items at once, then the properties dialog box displays only those properties that are common to all the items you selected.

4. To save changes, click **OK**.

Table 7-3: Common tabs in the Properties dialog box

Tab	Description
Info tab	To edit a property, do any of these that apply: <ul style="list-style-type: none"> • Type a new value. • Click Edit or Select, and select the value. • Select the property's checkbox. • Click the property's icon, and select the value. • If available, click See CIS Values to view suggested property values. To display additional properties, select Show More . To display all the properties, select Show All Properties .
Permissions tab	Displays the access that different users have to the item. To change permissions, see “ Edit permissions ” on page 696.
History tab	Displays a list of events that have occurred to the item, such as checkout, checkin, and promote.

7.2.5 Check out and edit files

7.2.5.1 Overview of check out and edit

To edit files, you check them out to your local computer. When you check out a file, Records Client locks the file in the repository so that no one else can edit it except you. Other users can view the file, but they cannot make changes to it. If you check out a file that is linked to multiple locations in the repository, the file is locked in all those locations.

When you check out a file, Records Client either copies or streams the file to your computer, depending on the file's editing application.

If the file uses an external editing application, Records Client downloads the file to your checkout directory. You can open, and close the file directly from your checkout directory. Your modifications are not saved into the repository until you check in the file.

By default, the checkout directory is these, depending on the operating system:

- Windows
//Documentum/Checkout

- Macintosh

Root:Users:<user_name>:Documentum:Checkout

If the file uses an internal editing application, then when you check out the file, Records Client streams the file directly to the appropriate editing application. The file is not copied to your computer. When you save the file in the editing application, the file is saved directly to the repository. However, the file remains checked out. To unlock the file, you must check the file back in.

To check out a file, use either the Edit command or the Check Out command. The Edit command immediately opens the file upon checkout.

Records Client displays a key icon next to the files that you currently have checked out. Records Client displays a lock icon next to the files that other users currently have checked out.

To view a list of the files that you currently have checked out, click **My Files**, and then click the key icon in the column headings.

You can open, edit, and close the file directly from your checkout directory, whether or not you are connected to the repository.

When a file is downloaded to your checkout directory, the file has the same name as it has in the repository, unless a naming conflict arises. A conflict arises if another file with that name already exists in checkout directory. In that case, Records Client appends a number to the name of the newly downloaded file. When the file is checked back in, it keeps its original filename, and the appended number is dropped.

7.2.5.2 Check out a file

To check out a file:

1. Navigate to the file in the repository, and select it.

You can perform this procedure on multiple files by selecting multiple files.

2. Do one of these:

- To check out a file without opening it, select **File > Check Out**.
- To check out a file, and automatically open it, select **File > Edit**.

You can also check out, and open the file by double-clicking it.

3. If prompted to enter additional information, enter the information, and then do one of these:

- If checking out one file, click **OK**.
- If checking out multiple files, enter information for each file separately by clicking **Next**. For the last file, click **Finish**.

To apply entries for all remaining files at once, click **Finish**.

When checkout completes, the file is locked in the repository, and copied to your local checkout directory. You can open the file directly from your checkout directory.

7.2.5.3 Check in a file

When a file is versioned upon checkin, its renditions, including any thumbnail renditions, are not maintained with the new version of the file. The renditions remain with the previous version. However, depending on your setup, a PDF rendition request is automatically submitted if you check in your file as the same version, and a PDF rendition already exists.

When a file is versioned upon checkin, its relationship to any parent document is not maintained, unless the parent document is checked in as a new version as well.

To check in a file:

1. Navigate to the file in the repository, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **File > Check In**.
3. If Records Client cannot locate the file on your computer, and prompts you for the location, browse to locate the file on your computer.
4. If prompted for checkin information, enter the appropriate information. Checkin information varies depending on your organization's setup. For an explanation of common checkin fields, see "[Checkin information](#)" [on page 553](#).
5. Do one of these:
 - If checking in one file, click **OK**.
 - If checking in multiple files, enter information for each file separately by clicking **Next**. After the last file, click **Finish**.

To apply information to all remaining files at once, click **Finish**.

7.2.5.3.1 Checkin information

See "[Checkin information](#)" [on page 553](#) for an explanation of common checkin fields. Some of the fields may not appear.

Table 7-4: Checkin information

Field	Description
Save as	Sets the version number. Selecting the same version number overwrites the original file with the updated one. For more information, see " Versions " on page 553 .

Field	Description
Version label	Lets you label the updated version.
Description	Lets you write an optional description of the file.
Format	Defines the type of file.
Lifecycle ID	Assigns a lifecycle to the file.
Check for links to other Microsoft documents, and check in linked documents	If available, select this option to have Records Client scan the document for linked documents. If linked documents are found, they are checked in as descendants of the original document.
Upload options	<p>Determines how quickly the new content is available to other users, and whether you can use Records Client while the checkin occurs.</p> <p>If you used drag-and-drop you are not given this option.</p> <p>Select one of these:</p> <ul style="list-style-type: none"> • Send for immediate global access: Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Records Client. • Send first for local access: Updates the repository immediately for the users in your geographic area, but Records Client takes more time to update the repository for all users. This allows you to continue using Records Client while the update occurs. <p>If checking in multiple files using the Next button, this option appears only for the first file. The choice you make automatically applies to all remaining files.</p>
Show Options	Retain Lock
Make this the current version	Makes the updated file the current version. For more information, see "Versions" on page 555 .
Keep a local copy after checkin	Retains a copy of the file on your local computer. But you no longer have the file checked out, and any changes you make to the local copy have no effect on the file in the repository.
Subscribe to this file	The file is linked to your Subscriptions.

Field	Description
Check in from file	Replaces the repository file with a file you choose.

7.2.5.3.2 Versions

A version is a copy of a file at a particular time the file was checked into the repository. A new version can be created each time the file is checked in. Versions lets you keep track of changes to a file.

When you create or import a new file into the repository, it receives a version number of 1.0.

When you check in a file, you can decide whether to create a new version of the file or overwrite the existing version (You must have adequate permissions on the file to be given these choices).

- Creating a new version gives the file a higher version number than it had when you checked it out, and also leaves a copy of the previous version in the repository.
- Overwriting the existing version keeps the same version number on the file as the previous version, and does not save a copy of the previous version.

Depending on your configuration, you might be able to select whether to increase the version number by a whole number or by just a decimal point (that is, by a tenth). Increasing the version number by a whole number is considered a *major revision*; increasing by a decimal point is a *minor revision*. For example, if you check out version 1.0 of a file, and check it in as a minor revision, the file is stored as version 1.1. If you repeat this process, the file is next stored as version 1.2. If you then decide to check out the file, and then check it in as a major revision, the file's version number jumps from 1.2 to 2.0.

The most recently checked-in file is marked CURRENT. File lists always display the current versions of files, unless you select to display all versions.

To display all the versions of a file:

1. Navigate to the file, and select it.
2. Select **View > Versions**.

To display all the versions of all the files in a list, select **Show All Objects and Versions** in the drop-down filter above the list.

You can work with an older version of a file using the same procedures you would use for working with any file in the repository.

If you edit an earlier version of the file, then when you check in the edited file, you are given these options:

- You can check in the older version of the file as the *new, current* version. If you select this option, Records Client assigns the file a version number higher than the file's previous current version.
- You can check in the older version of the file as a *branched* version. This increments the older file by a new decimal-appended number. The incremented version becomes the current version in a new branch of version numbers. For example, if a user checks out version 5.0 of a document, edits it, and then checks it back in as a major version, the version number becomes 6.0. Version 6.0 is now the current version of the document. If another user then checks out, and edits version 5.0, which is no longer the current version, then when the user checks it back in, Records Client creates a new branch of the document, which starts with version 5.0.1.

7.2.5.3.3 Replace a repository file with a different file

To replace a repository file with a different file:

1. Check out the repository file. For instructions, see “[Check out a file](#)” on page 552.
2. Select the checked-out file in the repository, and select **File > Check In**. Instead of using the File menu, you can drag-and-drop the replacement file from your local computer to the checked-out file in the repository. If you use drag-and-drop, you are not given the option to update content locally prior to updating globally. The update immediately occurs globally.
3. If prompted for checkin information, make sure the **Check in from file** option is selected. Enter other information as appropriate. Checkin information varies depending on your organization's setup. For an explanation of common checkin fields, see “[Checkin information](#)” on page 553.
4. Click **OK**.

7.2.5.4 Cancel checkout of a file

Canceling checkout unlocks the file, and discards the changes you made to the copy of the file on your computer. The repository retains the last version of the file as the current version.

To cancel checkout of a file:

1. Navigate to the file in the repository, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **File > Cancel Checkout**.
3. If prompted to confirm cancellation, do one of these:
 - If canceling checkout on one file, click **OK**.
 - If canceling checkout on multiple files, confirm cancellation for each file separately by clicking **Next**. After the last file, click **Finish**.

To confirm cancellation for all remaining files at once, click **Finish**.

7.2.5.5 View currently and recently checked-out files

To view your list of recently used files, click **My Files**.

My Files displays both the files that you currently have checked out as well as files that you have checked back in. The files that you currently have checked out are designated by the key icon.

To view the files you currently have checked out, sort the My Files list according to lock owner by clicking the key icon in the column headings row.

You can perform all the standard file operations from My Files. Use the same procedures as you would for any location in the repository.

If your organization's setup includes multiple-repository functionality, then My Files also displays the files you have recently accessed from other repositories, as well as the repository you are currently viewing. You can perform all the standard operations on files from other repositories, so long as you have user names, and passwords for those repositories.

7.2.6 View a file in read-only mode

When you view a file, Records Client either streams the file to your computer or downloads a copy of the file to your view directory. The file is not checked out from the repository. You can make changes to the file locally, but you cannot save your changes to the repository.

For Windows users, the default view directory is this:

C:\Documentum\Viewed

If another file with the same name already exists in the view directory, Records Client appends the name with a number.

You can view a file even if it is checked out by another user.

To view a file without check out:

1. Navigate to, and select the file.
2. Select **File > Open (Read Only)**.

To view links inside an HTML file, you must have virtual link installed.

7.2.7 Change the format associated with a type of file

Every item in the repository has an associated object type. The object type defines what kind of item an item is, and determines properties, and actions available for the item. By default, an object type is associated with a file format for editing, and a file format for viewing.

To change the format associated with a type of file:

1. Select **Tools > Preferences**.

2. Select the **Formats** tab.

The **Formats** tab lists types for which the associated applications have been changed from the default associations.

3. Do one of these:

- To associate an application for a type that is not listed, click **Add**.
- To associate an application for a type that *is* listed, select the type, and click **Edit**.

4. Complete the fields in “Formats tab” on page 558:

Table 7-5: Formats tab

Field	Description
Choose object type	Select the type for which to set the format.
Primary format	Select the file format to associate with the type.
Format for viewing	Select the file format to associate with a read-only viewing of a file of this type.
Would you like this content to appear in the web browser?	If the application can be opened by using a web browser, you can make that the default viewing application. To do so, select Yes .
Application for viewing	Click Select Application , and select the application used when viewing items of this type.
Application for editing	Click Select Application , and select the application used when editing items of this type.

5. To save your changes, click **OK**.

7.2.7.1 Restore associated file formats to the defaults

To restore the associated file formats to the defaults:

1. Select **Tools > Preferences**.
2. Select the **Formats** tab.
3. Select the object type.
4. Click **Restore Default**.

7.2.8 Import files to the repository

If you import a folder, the folder's contents are also imported.

Depending on your organization's setup, there might be a limit on the number of items you can import at one time.

If your setup allows the creation of renditions upon import, there is a delay between the time of import, and the creation of the renditions.

When you import a document containing linked descendant documents, you can not specify values for properties of the linked documents while importing the parent document.

To import into the repository:

1. Navigate to the repository location to import.
2. Select **File > Import**. Then click either **Add Files** or **Add Folders**. Select the file or folder, and click **OK**. To add multiple files or folders, repeat the sequence. When you have finished, click **Next**.

Instead of using the File menu, you can drag-and-drop the file or folder from your local computer to the location in Records Client. If you use drag-and-drop, you are not given the option to import locally prior to importing globally. The import immediately occurs globally.

3. If prompted to set properties for imported files, set properties as described in ["Properties for imported files" on page 559](#). The table describes common properties. Your installation of Records Client might include different properties.

Table 7-6: Properties for imported files

Field	Description
Type	<i>Do not change this property</i>
Format	<i>Do not change this property</i>
Lifecycle ID	Assigns a lifecycle to each imported item.

Field	Description
Check for links to other Microsoft documents, and import linked documents	If this field appears, check this to have Records Client scan each imported document for linked documents. If linked documents are found, they are also imported. The original document becomes a virtual document, and the linked documents become descendants.
Upload options	If this field appears, you can determine how quickly the imported content is available to other users, and whether you can use Records Client while the import occurs. Select one of these: <ul style="list-style-type: none"> • Send for immediate global access Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Records Client. • Send first for local access Updates the repository immediately for the users in your geographic area, but Records Client takes more time to update the repository for all users. This allows you to continue using Records Client while the update occurs.

4. Do one of these:
 - If importing one file, click **OK**.
 - If importing multiple files, set properties for each file separately by clicking **Next**. After the last file, click **Finish**.
- To apply the selected properties to all remaining files at once, click **Finish**.

7.2.9 Import OLE linked objects

You can import OLE linked objects in Documentum Webtop only after enabling the OLE linked objects for import.

To enable the import of OLE linked objects:

1. Open the *app.xml* file in the WDK/custom folder of the Documentum Webtop application.
2. Enable the <embedded-links-scan> in <WebApp Root>/wdk/app.xml
3. Save and close the *app.xml* file.

To import OLE linked objects into the repository:

1. Log in to Documentum Webtop and navigate to the repository location to import.
2. Select **File > Import**.
The File selection dialog box is displayed.
3. Select the **Check for links to other Microsoft documents and import linked documents** option.
4. Click **Add Files or Add Folders**.
The Select Files or Select Folders dialog box is displayed.
5. Select an OLE linked object file, or a folder that contains OLE linked objects, and click **OK**.
6. Click **Next**.
7. Set the attributes of the selected OLE linked object files or the attributes of the folder from which OLE linked object files are imported.
8. Click **Finish**.
9. If prompted, set properties for imported files.



Tip: You can drag-and-drop OLE linked object file or folder from your computer to the relevant location in Documentum Webtop instead of using the **File** menu.

7.2.10 Export files from the repository

You can export a file or all the contents of a folder from the repository. For information about deep exporting a folder, see [Deep export](#).

When you export a file or folder, you create a copy of the file or folder in a location outside of the repository. When you export a folder, the folder's files, and subfolders also are exported.

While exporting a file or folder from the repository, if Documentum Webtop finds the selected file or folder on the local machine, Documentum Webtop displays a message prompting you to confirm whether you want the export operation to overwrite existing files and folders, or not overwrite existing files and folders on the local machine.

To export from the repository:

1. Navigate to one or more files or folders, and select them.
2. Select **File > Export**.

If you are using Internet Explorer (IE), you can drag-and-drop the items from the repository to the appropriate location on your local computer.

3. Specify the location to which to export, select the location, and click **OK**.
4. If you are prompted to set export options, perform one of the following steps:
 - If you are exporting one file, set options, and click **OK**.
 - If you are exporting multiple files or folders, set options for each file or folder separately by clicking **Next**. After the last file or folder, click **Finish**.
To select options for all remaining files or folders once, click **Finish**.
5. If the file or folder already exists on the local machine, a message is displayed.
Do the following:
 - a. Click **Yes** to overwrite or replace a specific file or folder on the local machine. Click **Yes to all** to overwrite or replace all existing files or folders.
 - b. Click **No** to cancel overwriting a specific file or folder on the local machine. Click **No to all** to cancel overwriting all existing files or folders.

7.2.10.1 Deep export

Documentum Webtop provides the ability to export one or many folders and allow the structure of those folders to remain intact depending on the permission set of the files and folders.

By default, Deep export is disabled, and you have to enable Deep export in app.xml file to make it work.

When you export files containing special characters (for example, ;, ?, <, " , |, *) in their names, Documentum Webtop exports the files after removing the special characters from the file name.

Deep export of a hidden folder is allowed when you export a parent folder. If a folder is not visible in Documentum Webtop, then all the sub-folders including hidden folders get exported during Deep export.

Some rules apply when using Deep export:

- Deep export is supported for UCF content transfer, not HTTP content transfer.
- Only the primary content is exported, no renditions are exported.
- Only the current versions of documents are exported.
- Deep export is trimmed down *not to support VDM*
- Deep export is automatic when a folder is selected for export.

7.2.11 Delete an item from the repository

To delete an item from the repository:

1. Navigate to the item, and select it.

You can perform this procedure on multiple items by selecting multiple items.

2. Select **File > Delete**.

3. If prompted to select whether to delete related items, make the appropriate selections, and then do one of these:

- If deleting one item, click **OK**.
- If deleting multiple items, make selections for each item individually by clicking **Next**. After the last item, click **Finish**.

To apply selections to all remaining files at once, click **Finish**.

7.2.12 Move an item to a new location in the repository

You can move an item to another location within the same repository. By default, Records Client moves only the selected version of the item. Your administrator might have instead configured Records Client to move all versions. Ask your administrator which behavior applies.

You cannot move an item that is locked. If an item is locked, the lock owner must first unlock it.

You can also move items by drag-and-drop.

To move an item to a new location:

1. Navigate to the item, and select it.

You can select multiple items.

2. Select **Edit > Add To Clipboard**.

You can repeat the previous steps to add items from multiple locations to your clipboard. When you complete this procedure, all the items on your clipboard will be moved to the same location.

3. Navigate to the location to which to move, and open the location so that the location's files, and folders are displayed in the content pane. Select **Edit > Move Here**.

Instead of using the Edit menu, you can right-click on the location, and select **Move Here**.

The items are moved to the new location. The items remain on your clipboard until the next time you add items to the clipboard. To view your clipboard, select **Edit > View Clipboard**.

7.2.13 Copy an item to a new location in the repository

You can copy an item from one repository to another, as well as within a repository. When you copy an item, only the selected version is copied.

To copy an item to a new location:

1. Navigate to the item, and select it.

You can select multiple items.

2. Select **Edit > Add To Clipboard**.

You can repeat the previous steps to add items from multiple locations to your clipboard. When you complete this procedure, all the items on your clipboard will be copied to the same location.

3. If copying to another repository, open that repository in the navigation pane. For more information, see “[Log into another repository](#)” on page 539.
4. Navigate to the location to which to copy, and open the location so that the location's files, and folders are displayed in the content pane. Select **Edit > Copy Here**.

Instead of using the Edit menu, you can right-click the location, and select **Copy Here**.

5. If the clipboard appears, select the items to copy, and click **Copy**.

The items are copied to the new location. The items remain on your clipboard until the next time you add items to the clipboard.

If you copied an item to a location that already includes that type of item with the same name, Records Client adds **Copy** to the name of the copied item.

7.2.14 View your clipboard

Your clipboard holds the files, and other items you are moving, copying, or linking to another location in the repository. Your clipboard can hold multiple files at once.

To view your clipboard, select **Edit > View Clipboard**. If an expected item does not appear, make sure you have set your view filters to display the item.

To remove an item from your clipboard, select the item, and click **Remove**.

7.2.15 Links

7.2.15.1 Link an item to another location in the repository

When you link an item to another location in the repository, the item can be accessed from the new location in the same way it is accessed from its original location.

You cannot link an item that is locked. If the item is locked, the lock owner must first unlock it.

To link an item to another location in the repository:

1. Navigate to the item, and select it.

You can select multiple items.

2. Select **Edit > Add To Clipboard**.

You can repeat the previous steps to add items from multiple locations to your clipboard. When you complete this procedure, all the items on your clipboard will be linked to the same location.

3. Navigate to the location to which to link, and open the location so that the location's files, and folders are displayed in the content pane. Select **Edit > Link Here**.

Instead of using the Edit menu, you can right-click the location, and select **Link Here**.

The items are linked to the new location. The items remain on your clipboard until the next time you add items to the clipboard. To view your clipboard, select **Edit > View Clipboard**.

7.2.15.2 Link an item to another repository

You can link an item from one repository to another. This creates a shortcut to the selected item.

You can perform most of the standard file, and folder operations on shortcuts. For example, you can export, copy, and check out shortcuts. You use the standard procedures to perform such operations. When you perform an operation, Records Client performs the operation on original item in the original repository. For example, when you check out the shortcut, Records Client also checks out the original in the source repository.

Shortcuts are designated by a small, duplicate-icon overlay on the file icon. The overlay looks like a little copy of either the folder or file icon.

Shortcuts allows users of different repositories to share files over great distances, while making the shared files local to each office. A shortcut can have both global, and local properties. When you change a global property value, the value is changed in the source item, and in any other shortcuts. When you change a local property value, the value is changed only in the current shortcut.

To navigate from the shortcut to the original item, select the shortcut, and then select **File > Go to Target**.

To link an item to another repository:

1. Navigate to the item, and select it.
2. Select **Edit > Add To Clipboard**.
3. In the same Records Client window, open the repository to which to link.
4. Navigate to the location in the new repository.
5. Select **Edit > Link Here**.

The Documentum CM Server uses automated jobs to synchronize shortcuts, and originals.

- Replication jobs automatically synchronize the shortcut with the original file. You can manually synchronize the shortcut without waiting for the automated synchronization to occur by refreshing.
- Any operations that modify an item are implicitly performed on the source item, and the shortcut item is updated to reflect the change.
- If your configuration supports translations, then when you create a translation of a shortcut, you create a new file in the repository. You do not create a shortcut.
- You can perform lifecycle operations on shortcuts that already have lifecycles applied to them.

7.2.15.3 View all locations to which an item is linked

To view all locations to which an item is linked:

1. Navigate to the item, and select it.
2. Do one of these:
 - Select **View > Locations**.
 - Select **View > Memberships**.

7.2.15.4 Link a repository item to your computer

To link a repository item to your computer:

1. Navigate to, and select the item.
2. Select **View > Properties > Info**.
A shortcut icon appears next to the items name.
3. Drag-and-drop the shortcut icon to the appropriate location. For example, drag-and-drop the icon to a folder on your computer.

7.2.15.5 Add a document or folder to your browser's bookmarks or favorites

To add a document or folder to your browser's bookmarks or favorites:

1. Navigate to the document or folder in the repository, and select it.
2. Select **File > Add to Favorites**.
3. Click **OK**.

To open a document or folder from your browser's bookmarks or favorites:

1. In your browser, select the document or folder from the bookmark or favorite menu.
2. If prompted to log in, enter your login information, and click **Login**.

To bookmark a document or folder from the Properties dialog box:

1. Navigate to the document or folder in the repository, and select it.
2. Select **View > Properties > Info**.
The **Properties** dialog box is displayed with the Info tab selected.
3. Click <insert the attached icon> and select **Add to Favorites to bookmark the document or folder**.
The **Add Favorite** dialog box is displayed.
4. Click **OK**.

7.2.15.6 Use email to send a link to a repository item

To send a link in an email message:

1. Locate the repository item, and select it.
You can perform this procedure on multiple items by selecting multiple items.
2. Select **File > Email as Link**.
Your email application opens a new email message, and inserts the link to the repository item.
3. Type the email address, and any message as appropriate, and send the email.

7.2.15.7 Convert Desktop DRLs to Documentum Webtop URLs

Documentum Webtop provides existing Documentum Desktop client users with the DRLInvoker application (DRLInvoker.exe) that converts desktop DRLs to Documentum Webtop URLs and open linked documents in a browser window, seamlessly. After installing the DRLInvoker application, users must associate the Desktop DRL converter utility with the OS as a one time configuration.



Note: The .NET 3.5 or later platform is required to ensure that the conversion of Desktop URLs to Documentum Webtop URLs functions properly.

To download the DRLInvoker application:

1. Download the DTC-DRL-To-Webtop-URL.zip file from the FTP site.
2. Extract the contents of the zip file to a local folder.
3. Ensure that the config file DRLInvoker.exe.config is extracted successfully, and placed under the same folder where the application resides.
4. Edit the config file and make the following changes using a text editor:
 - a. Modify host entry to point the location where the Application server that hosts Documentum Webtop is installed.
 - b. Modify the port entry to point to the Application server listening port of Documentum Webtop.
 - c. Modify the contextURI entry to the appropriate context name with which Documentum Webtop is registered on the application server (For example, if the URL used to access Documentum Webtop is <http://mypictet.com:8080/webtopdev>, then the contextURI entry must be webtopdev.)
 - d. Save the config changes and close the text editor.

To associate the Desktop DRL converter utility with the OS (one time only):

1. Open the e-mail message containing the DRL.
2. Right-click the DRL and save the linked document on the local machine.

3. Locate the *.drl* file on your local machine.
4. On Windows, perform the following steps:
 - a. Select the file.
 - b. Hold down the Shift key and right-click the file.
 - c. Select the option **Open With**. The Open With dialog box is displayed.
 - d. Locate the *DRLInvoker.exe* as the program to open files of this type.
 - e. Select the checkbox **Always use this program to open files of this type**.
 - f. Click **OK**.

Subsequently, you can double-click *.drl* files to open linked documents.

7.2.15.8 Open a link sent by email

To open a link sent by email:

1. Click the link.
2. If prompted to log in, enter your login information, and click **Login**.
3. If prompted to select how to open the file, make selections as appropriate.

7.2.15.9 Access the DRL of a document version that is deleted from the repository

With Documentum Webtop 6.6, when you click a DRL to access a document version that is deleted from the repository, a warning message is displayed indicating that the version is no longer available. When you click **OK**, Documentum Webtop accesses the current version of the document and prompts you to choose to view or edit the document before opening the document. For example, if you click the DRL of version 1.2 of a document, and if that version has been deleted from the repository, a warning message is displayed indicating that version 1.2 is no longer available. When you click **OK**, Documentum Webtop prompts you to view or edit the Current Version of the document.

Configure Documentum Webtop to enable access to the current version of a document when you use the DRL of the deleted version of the document. For more information about configuring Documentum Webtop see the *OpenText Documentum Web Development Kit - Development Guide (EDCPKCLWT-PGD)*.

7.2.16 Subscriptions

The items you subscribe to appear in your Subscriptions node. When you access an item through this node, the item is retrieved from its original repository location.

When you subscribe to a repository item, you are subscribed only to the current version, which is the latest version of the item. For example, if you select a repository item that has multiple versions, and the latest version is 1.3, and you subscribe to version 1.2, you are subscribed to version 1.3 of the repository item, and not to version 1.2 of the same item.

To subscribe yourself to a repository item:

1. Navigate to the item, and select it.
2. Select **Tools > Subscribe**.

Instead of using the Tools menu, you can drag-and-drop the items to the **Subscriptions** node in the navigation pane.

To subscribe another user to a repository item:

1. Navigate to the item, and select it.
2. Select **Tools > Subscribe Others**.
3. In the selection dialog box, select one or more users, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.

To cancel your subscription to an item:

1. Navigate to the item, and select it.
2. Select **Tools > Unsubscribe**.

7.2.17 Receive notification when a file is read or changed

To have a notification sent to you when a file is read or changed:

1. Select the file.
You can perform this procedure on multiple files by selecting multiple files.
2. Do one of these:
 - To have notification sent any time a file's content is viewed, whether by opening, checking out, or exporting, select **Tools > Turn on read notification**.
 - To have notification sent any time a file is changed, select **Tools > Turn on change notification**.

Notifications are sent to both your Records Client inbox, and your email inbox.

You can later turn notification off by selecting the file, and selecting either **Tools > Turn off read notification** or **Tools > Turn off change notification**.

7.2.18 Export the information displayed in a list

When you export the property values of the items in a particular list, the information is saved as a .csv file, which opens in your default application for .csv files.

Before performing this procedure, make sure your browser's security settings allow file downloads.

To export information displayed in a list:

1. Navigate to list.
2. Select **Tools > Export to CSV**.
3. Select the columns to export as metadata.
4. Click **OK**.
5. Select whether to view or save the .csv file.
6. If you chose to save, select the location to which to save.
7. Do one of these:
 - If using a browser other than Internet Explorer (IE), click **OK**.
 - If using IE, press, and hold down **Ctrl**, and click **OK**.

If have exported columns that contain special characters, and if you open the .csv file in Microsoft Excel but Excel does not display them correctly, then save the file to your computer, and close it, and then use the **Data > Import External Data > Import Data** menu option to import the .csv file.

7.2.18.1 Export specific search results as a CSV file

You can export selected items in a list from the repository to a comma-separated values (.csv) file. When you choose specific items from a search result list and export the items, the data is exported to a .csv file.

To export selected rows:

1. Navigate to a list.
2. Select the items to export as comma separated values.
3. Right-click and select **Export To CSV** or select **Tools > Export to CSV**.
The Export Contents To CSV dialog box is displayed.
4. Move the columns you want to export from the **Select columns** list to the **Selected columns** list.

5. Click OK. You are prompted to open or save the .csv file.

7.3 Using the Brava! HTML Viewer

The OpenText Brava! HTML Client provides users the capability to load a wide variety of document types from the Brava! Server online using a web browser. Files are processed with the Brava! Enterprise Server as HTML output and are presented in the HTML Client which supports view, search, annotation, redaction, print, and publish. The Brava! HTML Client provides a wide range of tools for annotating and redacting files, including tools for group discussion and for signing documents, and can publish renditions of those files with the markup layers you create.

Markups allow you to annotate documents without altering the document itself. All markup entities are saved in a markup file, which is associated and overlaid on the image. There can be more than one author per markup file. A new layer is automatically created for each new markup file author (determined by the login user name), allowing them to see other authors' markups, but not edit them.

You can create new markups, open an existing markup for editing, overlay one or more markups on its source file for review, or permanently publish markups and redactions to PDF, or TIFF output files.

To access a file using Brava! Viewer:

1. Navigate to a list.
2. Select the document to which you want to add markups without altering the actual document itself.
3. Right-click and select **Brava! HTML Viewer** or select **File > Brava! HTML Viewer**.

The *OpenText Brava! HTML Viewer - Brava! Enterprise Classic View Client User Guide* (CLBRVW-UHD) available on Brava HTML Viewer page contains detailed information about the following features:

- Annotating Files
- Working with Stamp templates
- Working with Signatures
- Creating a Markup file
- Redacting files
- Publishing a file

7.4 Email messages

7.4.1 Changes in email processing

Email messages are now imported into repository in their native Microsoft Outlook (.msg) format as objects of dm_document type or its subtypes. To support the new email processing functionality in .msg format, installation of MailApp dar is mandatory. For more information about the import of new email messages, see “[Importing email messages to the repository](#)” on page 573.

For utilizing all the email processing functionality, the MailApp.dar file must be installed.

7.4.2 Operations supported on email messages

- *Import:* The new email messages are imported into repository in their native .msg format as objects of dm_document type or its subtypes. “[Importing email messages to the repository](#)” on page 573 contains detailed information.
- *Export:* Export of email messages is supported for new email messages stored in .msg format. “[Exporting email messages from the repository](#)” on page 576 contains detailed information.
- *View:* The view operation is supported on the new email messages imported in .msg format. “[Viewing email messages](#)” on page 577 contains detailed information.
- *Transform:* Email messages in the .msg format can be transformed to PDF and other formats. “[Transforming email messages](#)” on page 577 contains detailed information.
- *Search:* Advanced search is enhanced to allow searching of email messages in .msg format. “[Searching email messages](#)” on page 577 contains detailed information.

7.4.3 Importing email messages to the repository

Email messages are imported into repository in their native Microsoft Outlook (.msg) format as objects of dm_document type or its subtypes. The import of email messages in EMCMF format as objects of dm_message_archive type or its subtypes is no more supported from Records Client. The additional processing performed on the email messages during their import through Records Client is decided based on the values configured for different properties in mailapp.properties. The mailapp.properties file is present under /WEB-INF/classes directory of records war deployment.

The values set for different properties of MailApp.properties file define the additional processing performed on the email messages while being imported through Records Client. The properties of MailApp.properties file are described in “[Properties of MailApp.Properties file](#)” on page 574.

Table 7-7: Properties of MailApp.Properties file

Property	Default value	Description
shouldParseMsgFile	Property set to true	<p>When this property is set to true, the email message is imported into the repository in .msg format as an object of dm_document type or its subtypes and then email specific functionality is enabled.</p> <p>If this property is set to false, then the email messages will be imported as a normal document.</p>
shouldSeparateAttachments	Property set to false	<p>This property is applicable only when shouldParseMsgFile is true.</p> <p>When this property is set to false, then the attachments are not extracted from the email message and they are not stored as separate objects in the repository.</p> <p>If this property is set to true, then all the attachments stored inside the email message are extracted and stored in the repository as separate objects. The attachments are stored inside an attachments folder. This folder is hidden by default.</p>

Property	Default value	Description
objectTypeForAttachments	The value of this property is set to dm_document	<p>This property is applicable only when <code>shouldParseMsgFile</code> and <code>shouldSeparateAttachments</code> properties are set to true.</p> <p>Whenever extracting of attachment is enabled by setting <code>shouldSeparateAttachments</code> property to true, all the non-email type of attachments present inside the email message are extracted and stored in the repository as separate objects of this type.</p> <p>The object type of the nested email attachments is set to the same type that was selected by the user for the main email message during the import operation.</p>



Notes

- Regardless of whether extraction of attachment is enabled or not, the email messages imported in .msg format will always contain all its attachments inside it.
- Whenever attachment extraction is enabled in mailapp.properties, you can view the hidden attachments folder by selecting **Tools > Preferences > Show Hidden Files**.

To import email messages to the repository:

1. In Microsoft Outlook, do one of these:
 - Drag and drop one or more email messages to an appropriate repository location through Records Client. Skip to [step 4](#)
 - Save one or more email messages to a location on your computer. It can then later be imported using **File > Import**.
2. In Records Client, navigate to the repository location to which you must import the email messages.
3. Select **File > Import**, click **Add Files**, select an email message, and click **OK**. To add multiple email messages, repeat the sequence. Click **Next**.
4. Set properties as described in [“Properties for imported email messages” on page 576](#). If you are importing more than one email message, click **Next**, and set properties for each message individually.

Table 7-8: Properties for imported email messages

Field	Description
File	You cannot change this property.
Name	By default, the name of the email message is set to the subject of the email. By default, this property is not editable. To change the name of the email message, set the value of <override-object-name> element under <mailMessage-support> element of wdk / app .xml to true. By default, the value of <override-object-name> element is set to false.
Type	By default, the type for email messages is dm_document. You can also import the email message as one of the subtypes of dm_document type.
Format	You cannot change this property.
Lifecycle ID	To assign a lifecycle to the email message, click Select , and assign the lifecycle.

5. Click **Finish**.

7.4.4 Exporting email messages from the repository

When you export the email message stored in .msg format imported from Records, Records creates a copy of the email message in .msg format in the location you choose. The email message thus exported will contain all the attachments embedded within it.

To export email messages from the repository:

1. Navigate to one or more email messages, and select them.
2. Select **File > Export**.

 **Tip:** Instead of using the File menu, you can drag and drop the email messages from the repository to the appropriate location on your local computer.
3. If prompted to set export options, do one of these:
 - To export one message, set options, and click **OK**.
 - To export multiple messages, set options for each separately by clicking **Next**. After the last message, click **Finish**.

 **Tip:** To select options for all remaining messages at once, click **Finish**.

4. If prompted for the location to which you must export, select the location, and click **OK**.

7.4.5 Viewing email messages

To view the new email messages imported in .msg format:

1. Navigate to the email message, and select it.
2. Select **File > View**.

The email message opens in Microsoft Outlook.

7.4.6 Transforming email messages

To transform email messages:

1. Navigate to the email message, and select it.
2. Select **Tools > Transform > More Formats**.

You can transform to the available rendition options in **More Formats** depending on the deployment.

7.4.7 Searching email messages

In the enhanced advanced search screen, select **Switch to Search Emails**. It opens a form to search for email messages based on criteria. *To search for .msg only:* Select the object type as **dm_document** and click **Search**.

7.4.8 Locating and opening an email attachment

The attachments are embedded but can also be separately stored based on the configuration set for mailapp.properties.file. You can view the embedded attachments similar to viewing of the email message, as described in “[Viewing email messages](#)” on page 577. If the attachments are separately stored, it can be located in the location where the email is stored. By default, attachments are hidden. To view the attachments, select **Tools > Preferences > Show Hidden Objects**.

 **Tip:** You can also perform the search operation to locate an attachment. To do so, type all or part of the attachment's name into the search box. “[Search](#)” on page 578 contains detailed information.

 **Note:** All operations available on a document can also be performed on attachments.

7.4.9 Locating the email to which an attachment belongs

To locate the email to which an attachment belongs:

1. Type all or part of the attachment's name into the search box. “[Search](#)” on page 578 contains more information.
2. Right-click the attachment, and select **View > Location**.

7.5 Search

7.5.1 Run a simple search

When you enter a search term (a word or phrase) in the simple search box, the term is matched to documents or other objects that have the search term within the document itself or within the object's properties. This kind of search is called a “full-text” search.

It searches the files in your default search location. Your default search location is specified in your search preferences. “[Set search preferences](#)” on page 598, describes how to add a search location. You can search several repositories at the same time but you also have the possibility to search external sources such as external databases, web sources or your desktop.

If your repository has been indexed for parts of speech, Records Client displays files that include variations of the words you typed. For example, if you type *scanning* then Records Client also looks for files that contain the words *scan*, or *scanned*.



Note: If OpenText™ Documentum™ Content Management Search is enabled on Documentum CM Server, performing a search for an individual document in the Records Client may return multiple results. This is a known limitation.

To run a simple search:

1. In the box above the navigation pane, type the words for which to search.
To further define your search, see “[Further define search terms](#)” on page 579.
 2. Click .
- If your search includes several terms, and if the index server is Fast, the results displayed first will contain all search terms, then Records Client will display the results that contain only some of the search terms.
- If your search includes several terms, and if the index server is xPlore, all the results displayed will contain all search terms.
- To stop the search, click **Stop** .
3. See “[View search results](#)” on page 587.

7.5.1.1 Further define search terms

You can use the syntax in “[Further define search terms](#)” on page 579 to further define search terms within a simple search or within the **Contains** field in an advanced search.

Table 7-9: Further define search terms

Syntax	Description
Quotation marks around a word or phrase:	<p>To search for an exact word or phrase, type quotation marks around the word or phrase.</p> <p>For a simple search (including the Contains field in an advanced search), if you do not use quotation marks, Records Client displays files that contain both the exact words you typed as well as variations of the words, such as <i>scanning</i> for the word <i>scanner</i>.</p> <p>This option is disabled when searching for more than one word or if your repository has not been indexed for variations.</p> <p>Quotation marks cannot be used to match the exact case of a word.</p>
The AND and OR operators	<p>To get results that contain two search terms, type AND between the terms. A term can be a word or quoted phrase.</p> <p>To get results that contain at least one term, type OR between the words or the quoted phrases.</p> <p>You can string together multiple terms with the AND and OR operators. The AND operator has precedence over the OR operator. For example, if you type: <i>knowledge or management and discovery</i> then your results must contain either <i>knowledge</i> or they must contain <i>management, and discovery</i>.</p>

Syntax	Description
The NOT operator	<p>To get results that do not contain a term, type NOT before this term. The term can be a word or a quoted phrase. Only the term that follows the operator is taken into account.</p> <p>The NOT operator can be used after the AND or OR operator, separated by a space.</p> <p>Valid syntaxes would be: <i>Documentum NOT adapter</i> or <i>Documentum AND NOT adapter</i>, both queries will return results that contain Documentum but do not contain adapter.</p> <p>If you type <i>Documentum OR NOT adapter</i>, you get results that either contain Documentum (and possibly contain adapter) or that do not contain adapter. <i>Use this syntax cautiously</i>. It can generate a very large number of results.</p> <p>The NOT operator can be used alone at the beginning of the query. For example, if you type <i>NOT adapter</i>, you get results that do not contain adapter. <i>Use this syntax cautiously</i>. It can generate a very large number of results.</p> <p>The NOT operator is not supported for queries on external sources when it is alone at the beginning of the query or if used with the OR operator.</p> <p>The NOT operator cannot be used with parentheses. This is invalid: <i>A NOT (B OR C)</i>. However, the NOT operator can be used inside parentheses. This is valid: <i>(A NOT B) OR (A NOT C)</i>.</p> <p>ANDNOT (in one word) is not an operator, if you enter ANDNOT in a query, it will be considered as a search term.</p>

Syntax	Description
Parentheses around terms: ()	<p>To specify that certain terms must be processed together, use parentheses. When using parenthesis, you <i>must</i> type a space before, and after each parenthesis mark, as shown here: (<i>management or discovery</i>)</p> <p>As an example, if you type <i>knowledge and management or discovery</i>, then your results will contain both knowledge, and management or they will contain discovery. But if you type <i>knowledge and (management or discovery)</i>, then your results will contain knowledge, and <i>either</i> management or discovery.</p>
The multiple-character wildcard: *	<p>If the repository is indexed with Fast index server, you can use the multiple-character wildcard to indicate additional characters anywhere in a word. It matches zero or more characters.</p> <p>If the repository is indexed with xPlore index server, the multiple-character wildcard works only on whole words, not parts of words, but results can include variations of the words you typed. For example, a query for <i>computer*</i> matches <i>computer store</i> or <i>computer parts</i> but not <i>computerize</i>. By default, xPlore does not support search for word fragments because searching for whole words is much faster. To change this default behavior to work like the Fast index server, the xPlore administrator can turn on the option to search for word fragments.</p> <p>The multiple-character wildcard is only available for a simple search (including the Contains field in an advanced search).</p> <p>The multiple-character wildcard is not available for searches on non-indexed repositories, for searches of property values, or for searches on external sources. For those, you should use truncation operators, such the Begin with operator.</p> <p>If you use wildcards, then Records Client will not display results that include variations of the words you typed. For example, if you type <i>d*ment</i> then your results must contain: document, development, deployment, department, etc. but not documented or documentation.</p>

Syntax	Description
The single-character wildcard: ?	<p>If the repository is indexed with Fast index server, you can use the single-character wildcard to indicate a single, unknown character anywhere in a word.</p> <p>The single-character wildcard is only available for a simple search (including the Contains field in an advanced search).</p> <p>The single-character wildcard is not available for searches on non-indexed repositories, for searches of property values, or for searches of external sources. It is not available with xPlore index server.</p>



Notes

- The operators AND, OR, and NOT are reserved words. To search a term that includes an operator, use quotation marks. For example, if you search for hardware and software, Records Client returns documents with that string of three words. If you type hardware, and software without quotation marks, Records Client returns all of the documents that contain both words.
- The operators AND, OR, and NOT are not case-sensitive. For example, for your convenience, you can type: AND, and, And.

7.5.2 Run an advanced search

To search for a document by one of its properties, use advanced search. An advanced search enables you to define more precisely your query on the properties of the document. For example, you can search the current version of the documents whose author is John Smith, and modified between November 1, 2006 and December 31, 2006.

To run an advanced search:

1. On the Records Client main page, click the arrow next to the magnifying glass icon, and then click **Advanced**.
2. Enter values for the search. See “Enter values for an advanced search” on page 583.
3. Click **Search**.
To stop the search, in the result page, click **Stop**
4. See “View search results” on page 587.

7.5.2.1 Enter values for an advanced search

This procedure assumes you have already opened the Advanced Search page. If you have not, see “Run an advanced search” on page 582.

In the Advanced Search page, you can clear any existing values, and start with empty fields by clicking **Clear**.

To enter values for an advanced search:

1. In the **Contains** field, type the text for which to search.

This field is similar to the simple search. To further define your search, see “Further define search terms” on page 579.

2. In **Locations**, select the locations to search.

To add locations, do these:

- a. Make sure that **Current location only** is not selected, then click **Edit**.
- b. In **Available Repositories** or **Available Sources**, navigate to, and select the location. The location in **Available Repositories** can be a repository, a cabinet or a folder. **Available Sources** is displayed only if Records Client is configured to search external sources.
If you select repositories or sources for which your credentials are not saved, a login window may appear.
- c. Click the arrow to add it to the **Included in Search** list.
- d. Repeat b on page 583 and c on page 583 for as many locations as needed.
- e. To remove a location, select it, and click the remove arrow.
- f. To set the locations as your default locations for every new search, select **Set as default**.
- g. Click **OK**.

3. In the **Object Type** list, select the type of files to search for.

4. Enter remaining properties as appropriate. “Common properties in an advanced search” on page 584 describes common properties. The properties available depend on the type of file you search for, as selected in the **Object Type** list in step 3.

Table 7-10: Common properties in an advanced search

Field	Description
Properties list	<p>Enter one or more property values to search for by doing these:</p> <ol style="list-style-type: none"> 1. If no fields appear, click Select a property. 2. On a given line: In the first drop-down list, select a property. In the second drop-down list, select a property-to-value relationship. For a description of possible relationships, see "Select a property-to-value relationship" on page 585. In the remaining fields, select or type values. <p>If you type multiple words, they are searched for as a phrase. For example, if you type knowledge management then Records Client searches for values that contain the phrase knowledge management but not for values that contain knowledge and management separated from each other by other words such as "knowledge and process management". If you want your results to include both terms either as a phrase or separately, you must create two subqueries, and use the AND operator.</p> <ol style="list-style-type: none"> 3. To add additional properties, click Add another property, and then select one of these operators: <ul style="list-style-type: none"> • And: Selecting this means that the search results must match both the property value on this line, and the property value on the previous line. • Or: Selecting this means that the results can match either the property value on this line or the property value on the previous line. If you search external sources, do not use the OR operator between different types of properties. This query is valid: <i>Author contains Lewis OR Author contains Twain</i>, but this query is not valid: <i>Author contains Lewis OR Name contains Knowledge management</i>. <p>If you add three or more lines of properties, the order of operations follows the order of definition. Each time you add And or Or, the previous operators are grouped together. For example, if you define the query <i>Name contains Knowledge Management AND Author contains Lewis OR Author contains Twain</i>, then the results either must contain the documents whose name is Knowledge Management, and whose author is Lewis or they must contain all the documents whose author is Twain. To find all the documents whose name is Knowledge management, and whose author is either Lewis or Twain, you must define the following query: <i>Author contains Lewis OR Author contains Twain AND Name contains Knowledge management</i>.</p>

Field	Description	
	4. To remove a property from the search criteria, click Remove for that property.	
Date	Select the type of date to search for. Specify a date range, either a fixed date range using today's date or by typing the From and/or To dates. Months can be written in figures or in full. Years can be written with two or four figures. When specifying a date From, the date is not included in the date range. Conversely, when specifying a date To, the date is included in the date range.	
Size	Select a size range.	
<i>Properties when searching for email messages</i>	Subject	Type the words for which to search.
	To	
	From	
	Sent	Select the date the email message was sent.
	Received	Select the date the email message was received.
Find hidden objects	Choose to include hidden items in the search. The search displays only those hidden items that you have permission to view.	
Find all versions	Choose to search for past versions of the file, as well as the current version.	

The relationship between a property, and its corresponding value is defined by operators. “[Select a property-to-value relationship](#)” on page 585 describes the operators available in the Advanced Search page.

Table 7-11: Select a property-to-value relationship

Operator	Description
<i>Relational operators:</i>	
Less than <	You can use these operators with numerical values or strings.
Less than or equal to <=	
Greater than >	
Greater than or equal to >=	
Equal to =	Returns results in which the property value contains only the exact value you typed.
Not equal <>	Returns results in which the property value never matches the value you typed.

Operator	Description
<i>Truncation operators:</i>	The truncation operators can be used in place of the multiple-character wildcard.
Begins with	Returns results in which the property value begins with the value you typed. Same as using an ending wildcard.
Ends with	Returns results in which the property value ends with the value you typed. Same as using an starting wildcard.
Contains	Returns results in which the property value contains the value you typed anywhere within it. Same as using starting, and ending wildcards.
Does not contain	Returns results in which the property value does not contain the value you typed anywhere within it.
<i>Other operators:</i>	
In	Returns results in which the property value matches one of the values you typed. Potential values are typed as a comma-separated list.
Not in	Returns results in which the property value does not match any of the values you typed.
Is null	Returns results in which the property value is not defined. If you know that a property contains no value, you can use this operator to narrow a search.
Is not null	Returns results in which the property value is defined, but with no specific value. You can use this operator to find only documents whose properties are defined. For example, if you select keywords is not null then your results must contain only documents with keywords.

7.5.3 View search results

In search results, you can do these:

- Highlight the results.
Click  to turn highlighting on.
Click  to turn highlighting off.
- The results appear in the navigation pane as well as the content pane. The results in the navigation pane are arranged according to property.

To view results that include a certain property, click the property. For more information, see “Smart navigation” on page 587.

- To get additional information about the search, click **Status** . This displays search statistics according to search location. If your organization includes the search monitoring feature, this also displays the statistics in real time, as described in “Monitor search results in real time” on page 588.
- To revise the search, and run it again, click **Edit** , and set values as described in “Enter values for an advanced search” on page 583, and click **Search**.
- To run the search again without revising it, click **Restart** .
- To save the search so that it can be run again to receive updated results, see “Save a search to run again later” on page 593.
- To save the search as a search template so that it can be run again with different parameters, see “Create a search template” on page 596.
- To save results from an external source into a repository, see “Save search results from external sources” on page 589.

7.5.3.1 Smart navigation

When you run a search, your results are not only displayed in the content pane, but they are also grouped into clusters of related results in the navigation pane.

To collapse or expand the **Smart Navigation** list, click the minus/plus sign at the top of the list.

To expand a cluster or sub cluster, click the plus sign next to the cluster.

To display a sub cluster's results in the content pane, click the sub cluster.

To refresh the **Smart Navigation** list with new results, click . The icon appears only if new results are available.

Records Client computes sub clusters using the strategy defined in your user preferences. To set your preferences, click , and then follow the appropriate steps in “Set search preferences” on page 598.

7.5.3.2 Monitor search results in real time

Search monitoring displays the status of your search in real-time. The real-time status appears in both an animated display, and in a table, as shown in [Figure 7-1](#). Search monitoring allows you to see which search sources return results the fastest.

To display search monitoring, click **Status**  as soon as the search has started.

 the animation after the search has completed, click the Refresh icon, . When you replay the animation, you see a replay of how the search occurred. Replaying the animation does not rerun the query.

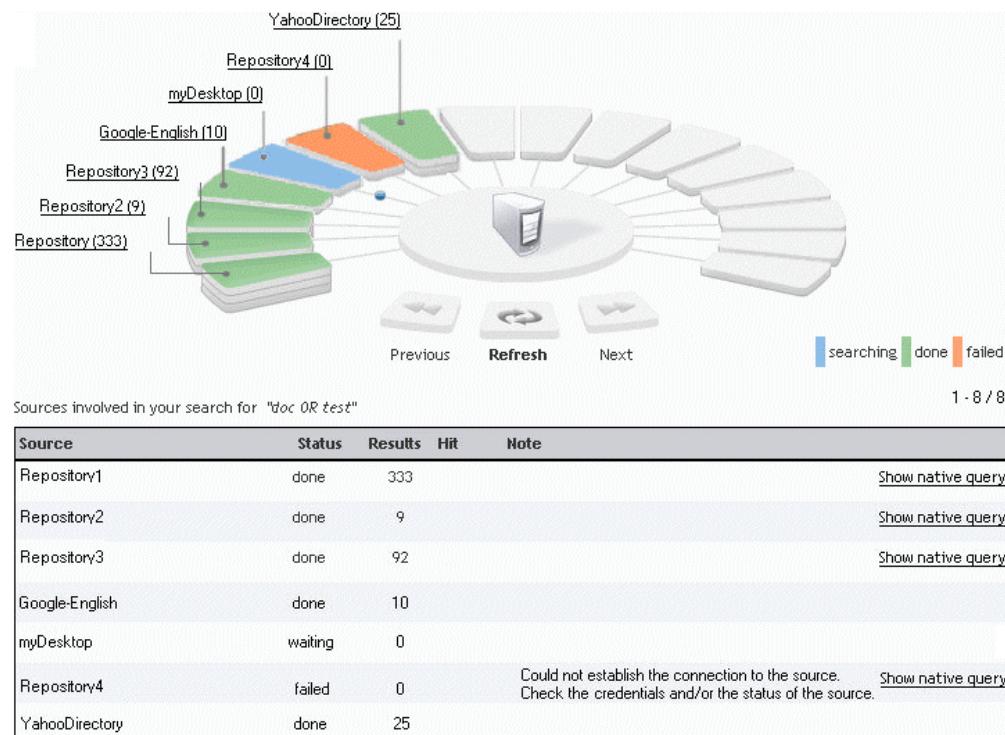


Figure 7-1: Real-time results in the search monitor screen

In the animation, each search source is represented by a pie slice. The number of layers in a slice corresponds to the number of results: one layer indicates no results; two layers indicate 1 to 50 results; and three layers indicate 51 or more results. Modified configurations might vary.

The color of a slice indicates the source status: blue when searching, green when the search is completed, and orange if the search has failed.

Click a source's slice to highlight its corresponding row in the table.

Click **Show native query** to view the native query that indicates how the query was translated for the source

The animation displays the sources sixteen by sixteen, so the first view of the animation only displays the first sixteen sources. If you are running the search against more than sixteen sources, you can see the next sixteen sources by clicking **Next** below the animation.

If a search fails for a given source, a detailed error message is displayed in the **Note** column of the table. To get additional information about the error, select **Tools > View messages**.



Note: If you launch the monitoring when viewing the results of saved searches or the last search results, the query is not rerun, and the animation does not replay entirely. The source status is first waiting with zero result then it is immediately updated to show the final status of the sources, and the number of valid results returned by each of them.

7.5.3.3 Save search results from external sources

This procedure enables to save results from an external source into a repository.

To save a search result of an external source into the repository:

1. Select the result(s).
2. Select **File > Save to repository**.
3. In the **Folder selection** window, select the target folder from the list of available repositories.
4. Click **Next** to check the object definition or **Finish** to complete the procedure.
5. In the **Object Definition** window, modify the object properties as needed.
6. Click **Next** to check the object definition for these result(s) or **Finish** to complete the procedure.
7. Repeat **step 5**, and **step 6** as many times as needed.

Saved results are available in the selected folder but they are also displayed in **My files**.

7.5.4 View your most recent results but do not relaunch the search

This procedure applies only to your current Records Client session.

To view your most recent search results:

1. At the top of the Records Client page, click the arrow next to the magnifying glass icon.
2. Click **Last Results**.

7.5.5 Improve your search experience

Your search experience can be restricted or improved by your understanding of the search syntax, and of the various parameters that define the search environment. The search syntax is the way you write the query, which implies the use of operators, and special characters such as parentheses, quotation marks or wildcards. The search syntax is documented at the beginning of this chapter in [“Run a simple search” on page 578](#), and [“Run an advanced search” on page 582](#). The search environment corresponds to the circumstances when the query is run; that is: the repository configuration, external sources configuration, the configuration of your WDK application. All these parameters are not visible nor accessible to users; however, they should be taken into consideration when running queries in order to get the most relevant results.

7.5.5.1 How configuration can impact your search experience

The search functionality description given in this manual refers to the default configuration. However, your system administrator can configure this functionality in many ways. This list details possible configurations that may affect your search experience:

- *Indexing*

Whether a repository is indexed is not of your interest, and usually, you don't need to know it. However, in some cases, indexing capabilities can be used to define more precise queries. For example, wildcards can only be used if the repository is indexed, if not, they are skipped. In OpenText Documentum CM, two index servers are supported: Fast and xPlore. The behavior of search operators may be slightly different between the two. For example, when searching for several terms separated with spaces, the spaces are interpreted as an OR operator with Fast index server, while they are interpreted as an AND operator with xPlore index server. If you want to run complex queries, consult the system administrator for details on the indexing configuration of the repository. The section [“Index a repository” on page 592](#), provides more information about indexing.

- *Relevancy ranking*

The system administrator can specify a bonus ranking for specific sources, add weight for a specific property value or improve the score for a specific format.

- *Presets*

The system administrator can define a preset to restrict the list of available types in the Advanced search page. Presets can be different from one repository to another. If you select only external sources, the preset of the current repository applies.

- *Customization of the Advanced search page*

The Advanced search page can be fully customized to guide you in running queries. For this reason, all the options described in this guide may not be available, and other may appear to narrow and/or condition your queries.

- *Maximum number of results*

The maximum number of results is defined at two levels. By default, the maximum number of results, taking all sources together, is 1000 and 350 results per source. However, your system administrator can modify these parameters. When querying an external source, the maximum number of results also depends on the configuration set for this source. Results are selected according to their ranking. This way, you always get results with the best ranking; other results are skipped.

- *Case-sensitivity*

If the repository is indexed, queries are case-insensitive by default, even using quotation marks. If the repository is not indexed, then queries are case-sensitive. However, for non-indexed repositories, case-sensitivity can be turned on, and off by the system administrator.

- *Grammatical normalization (lemmatization)*

When you do not use quotation marks, Records Client displays files that include variations of the words you typed in addition to the exact words. These variations are based on the word's root. This behavior depends on the configuration of the full-text engine, and is called grammatical normalization. The variations are based on the grammatical context of the word. For example, a search for the verb run also finds ran but does not find the noun running.

- *External sources*

When querying an external source, the results displayed in Records Client depend partly on the configuration of this source. For example, if the source does not return information on dates, then dates cannot be filtered.

- *Multiple repositories*

As for external sources, the results depend on the configuration of each repository. For example, the indexing may be set differently on various repositories.

7.5.5.2 Index a repository

Indexing a repository is the administrator's job, and you could think you don't need to know what is indexing, and whether the repository you are using is indexed or not. However, indexing can have an impact on the search experience. When a repository is indexed, a data structure, the index, is created to store information. The information can either be on the files' properties only or on the properties, and the content of the files. Searching an indexed repository facilitates a rapid retrieval of documents because it does not require scanning all files but only searching the index. In this guide, when referring to an indexed repository, we mean a repository for which both content, and properties are indexed, and not only properties. When the repository is indexed, you run full-text queries when using the simple search box or the Contains field of the advanced search window. When the repository is not indexed, the query is converted into a query on the most relevant properties: name, title, and subject. This mechanism is transparent, and enables you to retrieve the most relevant results.

7.5.5.3 Searchable items

Only the documents that are indexable can be searched. For example, pictures or binary content cannot be searched because they are not indexable.

Moreover, not all characters are searchable. Searchable characters are alphabetic, numeric, extender, and custom characters. Custom characters enclose Chinese, Japanese, Korean letters, and months.

Other characters, including punctuation, accent, and diacritical marks, and characters such as | and #, are not indexed or searched. Such nonsearchable characters are removed from the indexed text, and treated as if they are blank spaces. The index server treats these characters as white space: !@#\$%^_.&;()+=<

When these characters appear in indexable content, they are replaced by white space. For example, when the email address MyName@company.com is indexed, it appears as "MyName company com" in the index. The text is treated as three words. Documents returned by a search for MyName@company.com are treated as if they contain the words "MyName company com".

If a special character is included in a query, it is removed. For example, querying on Richard+Dodd would return a document containing the text Richard=Dodd because the + and = signs are both replaced by a blank space. If a search term includes an accent or diacritical mark, the search returns all matching words with or without the accent or diacritical mark.



Notes

- Unlike web browser search, you cannot use the plus, and minus signs as operators. You must use the AND operator, and the OR instead.
- The asterisk, and the question mark can be used as wildcards.

7.5.6 Saved searches

Searches can be saved so that you can launch them regularly without redefining them, share them between users, or to quickly retrieve the corresponding results. In the Saved Searches node, public, and private searches are distinguished by one of the following icons:

-  means this saved search is public, and accessible to any user.
-  means you are the only one that can access this saved search.

Saved searches are displayed outside of the Saved Searches node with a general icon: .

7.5.6.1 Save a search to run again later

You can save a search so that it can be run again later to retrieve updated results.

To save a search to run again later:

1. From the search results page, click **Save** .
2. Type a name for the saved search.
3. To display the results of this search in the **Saved Searches** node without having to run the search again, select **Include Results**.
4. To allow other users to access this search, select **Make Public**.
5. Click **OK**.

The saved search is stored in the repository's **Saved Searches** node.

Though the saved search is stored in one repository, you can use the saved search to search across multiple repositories.

7.5.6.2 Run a saved search

When you run a saved search, the search uses the same parameters but returns updated results.

To run a saved search:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Saved Searches** link in the content pane. Otherwise, skip this step.
3. Select the saved search, and select **File > View**.
Records Client runs the search.
To stop the search, in the result page, click **Stop** .
4. See “View search results” on page 587.

7.5.6.3 View the results of a saved search but do not relaunch the search

To view the results of a saved search:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Saved Searches** link in the content pane. Otherwise, skip this step.
3. Double-click any saved search for which the **Results** column indicates that the search turned up one or more items.



Note: If the results were not saved with the search then the search will be relaunched when you double-click it. If you don't want to possibly relaunch the search, use the context menu. To do so, right-click the saved search, and select **View saved results**. This command is only available when results were saved with the search.

7.5.6.4 Edit a saved search

To edit a saved search:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Saved Searches** link in the content pane. Otherwise, skip this step.
3. Select the search, and select **File > Edit**.
4. Set values as described in “Enter values for an advanced search” on page 583, and then click **Search**.
5. Click **Save Search** to apply the changes. You should also save your search if you modified the results display.
6. Click **OK**.
7. Click **Overwrite**.

7.5.6.5 Copy a saved search

To copy a saved search:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Saved Searches** link in the content pane. Otherwise, skip this step.
3. Select the search, and select **File > Edit**.
4. Set values as described in “Enter values for an advanced search” on page 583, and then click **Search**.
5. From the results page, click **Save Search**.

6. To save the search as a copy with a different name, type a new name for the search. Otherwise the search is saved as a copy with the same name.
7. Edit additional information as needed.
8. Click **OK**.
9. Click **Save as New**.

7.5.7 Search templates

Like saved searches, search templates are designed to be easily reused. A search template is a predefined search for which some search values are fixed, and other search value can be defined by the current user. Search templates can be private or public. In the Saved Searches node, public, and private search templates are distinguished by one of the following icons:

-  means this search template is public, and accessible to any user.
-  means you are the only one that can access this search template .

Search templates are displayed outside of the Saved Searches node with a general icon: .

7.5.7.1 Run a search from a search template

You can run a search from a search template created by you or by another user.

To run a search based on search template:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Search templates** link in the content pane. Otherwise, skip this step.
3. Select the search template, and select **File > View**.
4. If prompted for search values, enter values as appropriate.
5. Click **Search**.
To stop the search, in the result page, click **Stop** .
6. See “View search results” on page 587.

7.5.7.2 Create a search template

A search template is a predefined search in which you can change certain search values each time you run it. For example, a search template could search for invoices dated this month for the customer you choose. You could run the search template to retrieve invoices for numerous different customers.

A search template cannot include the OR operator.

To create a search template:

1. Run an advanced search (see “Run an advanced search” on page 582), and select the properties, and values to include in the search template. You must select at least one property, and value combination.
To include a property for which the user will set the search value, set a temporary value for that property. You can make that property editable later in this procedure.
2. From the search results page, click **Save template** 
3. Type a name for the search template.
4. To allow other users to access this search, select **Make this search available to others**.
5. To allow users to change values for a property, use the arrow to move that property to the **Input fields** box.
To keep a user from changing the value of a property, leave the property in the **Fixed values** box.
6. Click **Save**.

7.5.7.3 Edit a search template

To edit a search template:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Search templates** link in the content pane. Otherwise, skip this step.
3. Select the search template, and select **File > Edit**.
4. To allow other users to access this search, select **Make this search available to others**.
5. To allow users to change values for a property, use the arrow to move that property to the **Input fields** box.
To keep a user from changing the value of a property, leave the property in the **Fixed values** box.
6. Click **Save**.

7.5.7.4 Modify a search template definition

To modify the search template definition:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Search templates** link in the content pane. Otherwise, skip this step.
3. Right-click the search template, and select **Edit Definition**.
4. Modify the search values. See “Enter values for an advanced search” on page 583.
5. Click **Search**.
To stop the search, , in the result page, click **Stop** .
6. From the search results page, click **Save template** .
7. Type a name for the search template.
8. To allow other users to access this search, select **Make this search available to others**
9. To allow users to change values for a property, use the arrow to move that property to the **Input fields** box.
To keep a user from changing the value of a property, leave the property in the **Fixed values** box.
10. Click **Save**.
11. In the navigation pane, click **Saved Searches**.
12. Select the search template, and select **File > Edit**.
13. In the **Name** field, type a new name for the search template.
14. Edit the description of the template. By default, this field is updated with the search terms but you can modify it. The description is visible as a column in the **Saved Searches** node.
15. Click **Save**.



Note: Unlike saved searches, when you save a template after a modification, the old version is not overwritten: a new template is created.

7.5.7.5 Copy a search template

To copy a search template:

1. In the navigation pane, click **Saved Searches**.
2. If necessary, click the **Search templates** link in the content pane. Otherwise, skip this step.
3. Select the search template, and select **File > Edit**.
4. In the **Name** field, type a new name for the search template.
5. Edit the description of the template. By default, this field is updated with the search terms but you can modify it. The description is visible as a column in the **Saved Searches** node.
6. Click **Save**.

7.5.8 Set search preferences

To set your search preferences:

1. Select **Tools > Preferences**.
2. Select the **Search** tab.
3. In the **Default Search Locations** area, do one of these:
 - To set your default search locations to the repositories in your default repositories list, select **My Favorite Repositories**.
 - To set your default search location to the repository you are currently viewing, select **Current repository only**.
 - To set your default search locations to other locations, select **Others**, and then **Select**. In **Available Repositories** or **Available Sources**, navigate to, and select a specific location, and then click the appropriate arrow to add the location. Add as many locations as appropriate. The location can be a repository, a cabinet or a folder. **Available Sources** is displayed only if Records Client is configured to search external sources.
4. In the **Smart Navigation** area, select whether to enable the grouping of search results in clusters according to a specific properties.
If you select **Enabled**, select the properties used for smart navigation by clicking **Edit**, and then selecting properties in the drop-down lists. To add or remove properties, use the appropriate buttons.
5. To save your changes, click **OK**.

To select the columns displayed in the result pages, set your column preferences as described in “[Select the columns that appear in lists](#)” on page 541.

To retrieve the default configuration of the search locations, and of smart navigation, click **Restore defaults**.

7.6 Inbox

7.6.1 Inbox overview

Your Inbox contains tasks, and notifications. Tasks are electronic assignments. Notifications are messages that an event has occurred.

A task can be assigned to you manually by another user or automatically by a business process known as a workflow. A workflow is a series of tasks assigned sequentially from user to user. When you complete a workflow task, the workflow automatically sends a task to the next user in the workflow.

In some cases, a task that appears in your Inbox might be assigned not only to you but also to other users. In such a case, the first user to accept the task becomes the one who performs it. The task is automatically removed from the other users' inboxes.

If your organization uses work queues, you can request task assignments, as described in ["Work queue tasks" on page 604](#).

A task can include attached files that you are asked to edit or review. Attached files continue to the next user in the workflow.

7.6.2 Open a task or notification

To open a task or notification:

1. Click **Inbox**.
2. Click the name of the task or notification.
3. Do one of these:
 - To close the task or notification, click **Close**.

7.6.3 Perform a task

To perform a task:

1. In your Inbox, open the task by clicking its name.
2. On the **Info** tab, do these:
 - a. The **Info** tab might display a form customized to a particular task in your organization. If so, enter the appropriate information. Ask your administrator for details.
If the **Info** tab includes a link for creating a new form for the next user in the task, click the link, and follow the instructions on the screen.

- b. To perform operations on attached files, use the standard procedures for those operations.
 - c. To attach additional files, click **Add Attachments**, select the files, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
 - d. If the **Time**, and **Cost** fields appear, record your time, and cost to perform the task.
3. In the **Comments** tab, add comments as follows:
 - a. Click **Add or Edit**.
 - b. In the **Comment** field, type a comment.
 - c. If these options appear, select one:
 - **For subsequent recipients**
Sends the comment to all users performing *all* future tasks in the workflow.
 - **For next recipients only**
Sends the comment only to the users performing the next task in the workflow.
 - d. Click **OK**.
 - e. Repeat these steps for as many comments as needed. To remove a comment, click **Remove**.
 4. Select the **Progress** tab to view task's history.
 5. Do one of these:
 - To mark the task as finished, see “[Complete a task](#)” on page 600.
 - To close the task without marking it as finished, click **Close**.
The task closes. You can reopen it to mark it as finished at a later time. When you are ready to mark the task as finished, see “[Complete a task](#)” on page 600.

7.6.4 Complete a task

Completing a task sends it to the next user or activity in the workflow. Any changes you make to attached files travel with the task if the version of the attached files, and the checked in files are the same version.

To complete a task:

1. Open the task by selecting it in your Inbox.
2. Click **Finish**. The task is deleted from the Inbox and the Finish page is displayed.

3. Select the **Do not show this confirmation again** checkbox if you do not want to see the Finish page after completing a task, and click **OK**.



Note: You can also configure webcomponent/app.xml to disable the appearance of the Finish page for all users of the Documentum Webtop instance. Set the <suppress_task_confirmation> element to <true> in webcomponent/app.xml:

```
<suppress_task_confirmation>true</suppress_task_confirmation>
```

4. If prompted for a password, type your password.
5. Click **OK**.
6. If prompted to select the next performers, do these:
 - a. Click **Click To Assign** next to the task for which to select performers.
 - b. In the selection dialog box, select one or more performers, and click **OK**. For detailed steps see "[Locate an item in a selection dialog box](#)" on page 543.
 - c. Click **OK**.
7. If prompted, select the next task to forward from the **Select Next Forward Tasks** list.
8. Click **OK**.

7.6.5 Accept a task that has been assigned to multiple users

When a task has been sent to a group, the first user to accept the task is the one who performs it. If you accept such a task, it is automatically deleted from the other users' inboxes.

To accept a task that has been assigned to multiple users:

1. Click **Inbox**.
2. Select the task to accept.
3. Click **Accept**.
4. Do one of these:
 - To close the task, click **Close**.
 - To perform an action, see the appropriate procedure:
 - "[Perform a task](#)" on page 599
 - "[Complete a task](#)" on page 600
 - "[Reject a task](#)" on page 602
 - "[Delegate a task](#)" on page 602
 - "[Repeat a task](#)" on page 603

7.6.6 Reject a task

If the workflow allows, you can reject a task. When you do, the task goes to another step as defined in the template. If the task is directed to a group of users, it is deleted from your Inbox. Depending on the template definition, the task may or may not remain in the Inboxes of the other users in the group.

To reject a task:

1. In your Inbox, open the task by clicking its name.
2. Click **Reject**.
3. If required, type a message explaining the reason for the rejection.
4. Click **Next**.
5. To select other tasks to reject, do so from the **Select Next Reject Tasks** list.
6. If required, type your password in the **Sign Off Required** field to electronically sign off the task.
7. Click **OK**.

7.6.7 Delegate a task

If the workflow allows, you can give another user the responsibility of performing a task that originally had been assigned to you.

To delegate a task:

1. In your Inbox, open the task by clicking it.
2. Click **Delegate**.
3. If prompted to specify the user to whom to delegate the task, do these:
 - a. On the task's line item, click **click to assign**.
 - b. In the selection dialog box, select the user to whom to delegate, and click **OK**. For detailed steps see "[Locate an item in a selection dialog box](#)" [on page 543](#).
4. Click **OK**.

7.6.8 Repeat a task

If the workflow allows, you have the option of asking another user or group to repeat a task that you have just completed.

To repeat a task:

1. In your Inbox, open the task by clicking it.
2. Click **Repeat**.
3. On the task's line item, click **click to assign**.
4. In the selection dialog box, select the user to whom to delegate, and click **OK**.
For detailed steps see "[Locate an item in a selection dialog box](#)" on page 543.
5. Click **OK**.

7.6.9 Change your availability for tasks

The top of your Inbox displays your availability to receive tasks. You can either set the status as **I am available** or **I am currently set to unavailable**.

To delegate tasks to another person when your status is set to unavailable, see the *OpenText Documentum Content Management - Advanced Workflow User Guide (EDCPKLR-UGD)*.

To set your status to Unavailable:

1. Click **Inbox**.
2. Click **I am available**.
The Workflow Availability dialog box is displayed.
3. Select the **I am currently unavailable** option.
4. Click **edit**.
5. Select the user or a group to whom the tasks will be assigned.
6. Click **OK**.
7. Click **OK** to close the Workflow Availability dialog box.



Note: When you make yourself unavailable, this only affects future tasks that have been marked as delegable. This option does not affect tasks that are currently in your Inbox or any future tasks that do not allow delegation.

To set your status to Available:

1. Click **Inbox**.
2. Click **I am currently set to unavailable**.

- The Workflow Availability dialog box is displayed.
3. Clear the selection of the **I am currently unavailable** option.
 4. Click **OK**.

7.6.10 Work queue tasks

Work queues hold tasks that are to be performed by available processors who are assigned to the queue. When a task enters the system, the server assigns it to a work queue based upon the task, and the work queue properties. Processors assigned to work on that queue receive tasks in their Inboxes in priority order. Users with the advance queue processor role can selectively pull items from their queue regardless of their priority, and without waiting for the item to be assigned to the processor's Inbox.

7.6.10.1 Manage tasks in your queue Inbox

Work queue processors have different options available to help manage tasks, and the workload in their work queue Inbox.

To suspend a task in your queue:

If you are working on task, and need to wait for some other supporting document or task to take place, you can suspend the task. As a reminder, you assign a date for the task to be unsuspended, and active back in your queue. The system runs a job that unsuspends the task based on this date. You can also manually unsuspend a task.

1. Select the task to suspend
2. Select **Tools > Work Queue Management > Suspend**
3. Select the date, and time that the task will no longer be suspended.
4. Click **OK**.

The status of the task appears as paused.

To unsuspend a task in your queue:

1. Select the task to unsuspend
2. Select **Tools > Work Queue Management > Unsuspend**.

The status of the task appears as acquired.

To unassign and reassign a task in your queue:

1. Select the task to unassign.
2. Select **Tools > Work Queue Management > Unassign**.

The system returns the task to the work queue, and the status of the task appears as dormant until you reassign the task to another user.

3. Select **Tools > Work Queue Management > Reassign**.
4. Select a user to assign to the task.
5. Click **OK**.

7.6.10.2 Get the next available task in a work queue

If your organization has implemented work queues, you can acquire the next task in the queue without having to wait for a supervisor or the system to assign it to you. Your next task is the task of the highest priority from among your assigned work queues. You can select your next task manually from an option in the Inbox menu or you can choose to have your next task appear in your Inbox automatically when you reject or complete your current task.

Items that are automatically sent to your Inbox by the system appear as not assigned in the assigned column of the worklist. Items that have been manually assigned by the queue manager show yes in the assigned column. Use the label in this column to distinguish how the task has been sent to your Inbox.

To manually retrieve your next work queue task:

- In your **Inbox**, select **Tools > Work Queue Management > Get Next Task**.
The next task appears at the top of the task list in your **Inbox**.

To turn on automatic receipt of work queue tasks:

- In your **Inbox**, select **Get next task automatically**.

To turn off automatic receipt of work queue tasks:

1. Close any open work queue tasks.
2. In your **Inbox**, clear **Get next task automatically**.
3. Re-open your currently assigned task, and finish it, so that you do not have an unfinished task in your **Inbox**.

7.6.10.3 Select a task from the queue

Processors with the queue_advance_processor role have the ability to view the work queue tasks that they are eligible to work on, and acquire them regardless of their priority. They also have access to the Work Queue node in the main directory tree that shows all of their assigned work queues displayed as separate Inboxes. From these Work Queue Inboxes, they can select any unassigned tasks that they are eligible to work on based on their skill set or any unassigned tasks that do not require any skills.

Processors with the queue_advance_processor role have the option to filter the Work Queue Inbox view. Selecting **All Eligible Tasks** shows all unassigned tasks that the processor is qualified or eligible to work on. **All Tasks** shows the tasks that the

processor is eligible to work on, as well as any tasks that the processor has already acquired or that have been assigned by the queue supervisor.

Users with the queue_advance_processor role cannot assign tasks to other queue processors or pull a task that is already assigned to or has been pulled by another queue processor.

To acquire an unassigned task:

1. Navigate to the Work Queues node in the directory tree, and click the work queue to open.
2. Select the filter to show **All Eligible Tasks** or **All Tasks** in the Work Queue Inbox.
3. Select one or more tasks to acquire.
4. Select **Tools > Work Queue Management > Get Task**.

The system assigns the tasks to you, and sends them to your Inbox. If you select only one task, the system opens the task in Task Manager so that you can work on it immediately.

This action is also available through the **Task Manager** using the **Get Task** button that is available to advance queue processors. This option enables advance queue processors to examine the task before deciding to pull it. Using the **Get Task** button from within the task in Task Manager assigns the task to you, and refreshes the page, enabling you to work on the task immediately.

7.7 Workflows and quickflows

7.7.1 Start a workflow

A workflow is an automated process that passes files, and instructions between individuals in sequence, to accomplish specific tasks. When a user is assigned a workflow task, the task appears in the user's Inbox.

Workflows can include automatic tasks that the system performs, such as the execution of scripts. Automatic tasks allow the integration of workflows, and lifecycles for example allowing promotion of files to new lifecycle states.

When you start a workflow, you select the workflow template that includes the sequence of tasks to be performed. Multiple workflows can start simultaneously from the same template. A workflow template might allow you to direct a task to a group of users, in which case the first user who accepts the task performs it, and the task is removed from the other users' Inboxes.

When you start a workflow, you can attach files. File are available for attaching if they are already attached elsewhere, locked by another user, or in an advanced lifecycle state. Remember that when you attach files in multiple languages, a task recipient's filters might show only the files that match that user's language.

To start a workflow:

1. Do one of these:
 - To start a workflow by first selecting the type of workflow, select **Tools > Workflow > Start**.
 - If your workflow is designed to include multiple packages, select **Tools > Workflow > Start Attachments** and choose one document for each package.
2. Select the workflow template, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
3. Click **OK**.
4. On the **Info** tab, in the **Workflow Description** field, type a name for the workflow.
5. To attach a file to the workflow, do these:
 - a. On the **Info** tab, click **Add**.
 - b. To locate the files to attach, click the appropriate tab, then navigate to the files within that tab. Tabs that correspond to repository nodes are navigated in the same way as the repository nodes.
 - c. Click **Add** at the bottom of the page.
 - d. If you attached a file that has links to other files, you can add the linked files by selecting **Automatically Add Linked Objects**.
 - e. To remove an attached file, click either **Delete** or **Remove**.
6. To create, and attach a new form based on an existing form template, do these:
 - a. On the **Info** tab, click the name of the form or package, depending on what appears.
 - b. Select the form template upon which to base the new form, and click **OK**. The form's fields appear in the **Info** tab.
 - c. To remove a form, click **Remove**.
- If you remove a newly created form or cancel the workflow, the form is deleted automatically.
7. If the workflow includes the **Performers** tab, you can specify users for one or more tasks. Do these:
 - a. Click **Select** next to a task that must be performed.
 - b. In the selection dialog box, select the user or group to perform the task, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
8. In the **Comments** tab, do these:

- a. Click **Add**.
 - b. Type your comments.
 - c. Select the users to receive the comment:
 - **For subsequent recipients**
The comment is sent to all remaining users in the workflow.
 - **For next recipients only**
The comment is sent only to the users who receive the next task assignment in the workflow.
9. Click **OK**.
 10. Click **Finish**.

7.7.2 Send a quickflow

A quickflow is a single task you send to one or more users. If you send a quickflow to multiple users, you can select whether each user receives the task simultaneously or sequentially.

To send a quickflow:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Workflow > Quickflow**.
3. To select the users or groups to whom to send the quickflow, click **Select user/group**, then select the users or groups, and then click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
4. In the **Priority** drop-down list, select the priority.
5. In the **Instructions** field, type any messages for the users.
6. Select the **Return to Me** option to receive a task when a user completes the review.
7. To require each user to enter an electronic signoff when completing the review, select the **Require signoff** checkbox.
8. Click **OK**.

7.7.3 View workflows

You can view workflows through either Workflow Reporting or through My Workflows. This topic describes both.

To view workflows through Workflow Reporting

1. Select **Tools > Workflow > Workflow Reporting**.

The list of workflows appears. To reformat the list, click **Edit Workflow Report**, and choose from the available options.

2. To view more information about a workflow, select the workflow, and then select any of these:

- To view the workflow template, select **Tools > Workflow > View Details > Map**.
- To view the progress of the workflow, select **Tools > Workflow > View Details > Summary**. To narrow or broaden the list, select the appropriate filter at the top of the page.
- To view a record of events for the workflow, select **Tools > Workflow > View Details > Audit**.

To view the workflows you own via My Workflows

1. Select **Tools > Workflow > My Workflows**.

My Workflows displays the workflows you own but does not display the workflows owned by groups you belong to. To view workflows owned by a group, use the procedure “[To view workflows through Workflow Reporting](#)” on page 609.

2. To view a specific workflow, select the workflow, then select **File > View**.

7.7.4 Pause a workflow

When you pause a workflow, you temporarily stop it but expect to reinstate it at a later time. For example, you can pause a workflow to modify the workflow template. Once your changes are complete, you can resume the workflow to continue from the point at which it was paused.

To pause a workflow:

1. Select **Tools > Workflow > Workflow Reporting**

Alternately, you can select **Tools > Workflow > My Workflows**.

2. Select one or more workflows.

3. Select **Tools > Workflow > Pause Workflow**.

4. If prompted to confirm the pause, click **OK**.

7.7.5 Resume a paused workflow

When you resume a paused workflow, the workflow starts where it was paused. You can resume a paused workflow, but you cannot resume a stopped workflow.

To resume a paused workflow:

1. Select **Tools > Workflow > Workflow Reporting**
Alternately, you can select **Tools > Workflow > My Workflows**.
2. Select one or more workflows.
3. Select **Tools > Workflow > Resume Workflow**.
4. If prompted to confirm, click **OK**.

7.7.6 Stop a workflow

You can stop a workflow at any point in its progress. A stopped workflow cannot be restarted.

To stop a workflow:

1. Select **Tools > Workflow > Workflow Reporting**
Alternately, you can select **Tools > Workflow > My Workflows**.
2. Select one or more workflows.
3. Select **Tools > Workflow > Stop Workflow**.
4. To ensure that the workflow is automatically deleted from your workflows list, select the **Aborted workflow will be deleted** option.
5. If prompted to confirm, click **OK**.

7.7.7 Email the workflow supervisor or a workflow performer

To email the workflow supervisor or a workflow performer:

1. Select **Tools > Workflow > Workflow Reporting**
Alternately, you can select **Tools > Workflow > My Workflows**.
2. Select the workflow.
3. Select one of these:
 - **Tools > Workflow > Email Supervisor**
 - **Tools > Workflow > Email Performers**

Your email application opens a new email message with the email addresses filled in.

4. Type your message, and send the email.

7.7.8 Process a failed task in a workflow

If you are workflow supervisor, and receive notice that an automatic task has failed, you can perform one of the procedures here.

To retry a failed automatic task:

1. From your Inbox, open the failed automatic task.
2. Click **Rerun**.
3. Click **OK**.

To complete a failed automatic task:

1. From your Inbox, open the failed automatic task.
2. Click **Complete**.
3. Click **OK**.

7.7.9 Change the workflow supervisor

Each workflow has a workflow supervisor who can modify, pause, or stop an active workflow.

To change the workflow supervisor:

1. Select **Tools > Workflow > Workflow Reporting**.
2. Select the workflow.
3. Select **Change Supervisor**.
4. Select either **All Users** or the group to which the new supervisor belongs.
5. Select the user who will be the new supervisor for the workflow.
6. Click **OK**.

7.7.10 Save workflow information as a Microsoft Excel spreadsheet

The availability of this procedure depends on your organization's configuration of Records Client.

To save workflow information as a Microsoft Excel spreadsheet:

1. Select Tools > Workflow > Workflow Reporting.
2. Click **Save Report**.
3. Type a name for the information you are saving.
4. Select a location to which to save.
5. Click **OK**.

7.7.11 View aggregated report for workflow performance

To view reports, you must have the process_report_admin role.

To view historical reports:

1. Select one of these:
 - Tools > Workflow > Historical Report > Process
 - Tools > Workflow > Historical Report > User
2. In the **General** tab, select the duration, and other parameters for which to run the report.
3. Click **Run**.
4. Click the **Results** tab, to view the report.
5. To view additional information, click a process, instance, or user.
6. To save the report so it can be rerun, click **Save**.

7.7.12 Create a workflow template

To create a new workflow template, see the *OpenText Documentum Content Management - Workflow Designer User Guide (EDCPKL-AWF)*. Use that application's Help for instructions on creating the new workflow template.

7.8 Work queues

7.8.1 Work queue roles

Work queues hold tasks that are to be performed by available users who are assigned to the queue. Work queue users receive tasks in their Inboxes. Work queue users are assigned tasks either automatically by the server or manually by another user. Users with the queue_advance_processor role can choose to pull items from their queue regardless of their priority, and without waiting for the item to be assigned to their Inbox.

Work queue users are also referred to as *processors*.

Work queue managers monitor work queues to see which queues have overdue tasks that need to be addressed or which queues have too many tasks in the queue. They can also add, edit, and assign skill profiles to individual work queue users.

Work queue administrators create work queues, assign users to work on queue tasks, define the skill profiles that enable the application to assign tasks to the appropriate processor, and can add, edit, or assign skill profiles to the individual work queue users.

Additionally, the administrator or manager can use the Work Queue Monitor to view the tasks in the queue, the name of the processor assigned to the task, the status of the task, when the task was received, and the current priority of the task.

To access work queues, you must belong to one of the roles described in “[User roles for work queues](#)” on page 613.

Table 7-12: User roles for work queues

Role	What this role can do
Queue_processor	Works on items that are assigned by the system from one or more work queue inboxes. Queue processors can request work, suspend, and unsuspend work, complete work, and reassign their work to others. Users with the queue_processor role do not select the tasks that they work on.
Queue_advance_processor	Works on items that are assigned by the system from one or more work queue inboxes. Additionally, selects tasks to work on from one or more work queue inboxes.

Role	What this role can do
Queue_manager	<p>Monitors work queues, assigns roles to queues, and assigns users to work on queue items. Queue managers can reassign, and suspend tasks.</p> <p>Queue managers who have CREATE_GROUP privileges can create work queues.</p>
Queue_admin	<p>Creates work queues, and queue policies. Members of the queue_admin role <i>do not</i> by default have the administrator role.</p> <p>Queue administrators who have CREATE_GROUP privileges can create work queues.</p>
Process_report_admin	Runs historical workflow reports from the Workflow menu.

7.8.2 Setting up queue management

The system administrator must configure the global registry, repository, and Application server correctly to use queue management.

Queue management requires the following environment:

- Documentum CM Server and a repository designated as a global registry.
- Documentum CM Server and a repository that is designated to run queue management.
- Foundation Java API on the application server host where Documentum Webtop is deployed with connection information for the global registry repository.
- Documentum Webtop.
- BPM.dar and Form.dar or Process Engine.

A single repository can run queue management and be designated as a global registry. However, this configuration is not mandatory. Alternatively, two separate repositories can also run queue management and be designated as global registries. Ensure that Process Engine is installed in the repository running queue management and in the repository designated as a global registry.

To install queue management:

1. Designate a repository as a business objects framework global registry.



Note: Ensure that the repository is designated while creating a repository or upgrading an existing repository. For instructions about configuring the repository, see the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY-IGD)*.

2. Record the repository login credentials for the global registry user.
3. When Foundation Java API is installed as part of the Documentum Webtop deployment process, provide the login credentials for the global registry user in the `dfc.properties` file.
4. Install `BPM.dar` and `Form.dar` or Process Engine in the global registry repository.
The SBOs and TBOs required for queue management are installed.

7.8.3 Set up a new work queue

To set up your first work queue, you perform these procedures in the order listed here:

- Create the users, and groups that you will be using to process the work queues.
The chapter on user management provides more details on setting up users, and groups.
- Set up work assignment matching.
["Set up work assignment matching" on page 615](#) provides detailed information on work assignment matching.
- Create the queue policies you will need for the queue.
["Work queue policies" on page 618](#) provides more specifics on queue policies.
- Create the queue categories.
["Define a queue category" on page 621](#) explains how to create queue categories.
- Create the work queue.
["Define a work queue" on page 622](#) provides more specifics on defining work queues.
- Create override policies.
["Define work queue override policies" on page 624](#) explains the optional step of defining override policies for work queue policies.

7.8.4 Set up work assignment matching

When you are creating a work queue, your first task is to configure the work assignment matching filters by defining the skills or properties that are necessary to process tasks in the work queue. The *work assignment matching filter* lists the abilities, properties, or expertise necessary to perform tasks in a work queue. The *processor profile* lists which of these filters has been assigned to a work queue processor. When the processor pulls the next task or when a manager assigns a task, the system then uses the skills defined in the work assignment matching filter to qualify a processor based upon the skills or properties required to work on a task.

If a work assignment matching filter is *not* set up for a work queue, than any queue processor in the work queue can work on the tasks regardless of qualifications.

Once that task is created, there is no way to change the associated required skills. The system compares the skills required by the task against the skills listed for users in the work queue, and uses this comparison for both the Get Next Task and Assign Task functions.

For example, the work queue loan_underwriter_queue has three required skills defined for it: auto loans, commercial loans, and home loans. When an auto loan application comes through the workflow, the system evaluates the skill association stored in the activity template, and resolves the skill value for an auto loan. It then sends the loan application to the loan_underwriter_queue. When a supervisor assigns a task or when a processor tries to pull the task, the server ensures that this processor has auto loans listed as a skill before allowing the processor to acquire the task. A particular task associated with a queue can require one or more skills to complete. A processor may have several skills related to a work queue.

7.8.4.1 Set up skill profiles in the process template

When you create an activity that is performed by a specific work queue, you select the work queue name, and set the required skills for the activity on the Performer tab in the Activity Inspector. You can use process data to map to the values of the required skill. When you map a skill, it is added to the task, and at runtime the system uses it to qualify a processor for the task.

7.8.4.2 Define work assignment matching filters

Each work assignment matching filter contains the skill definitions that enable the system to match a processor with a task based on the skills required by the task, and the abilities or expertise of the processor. When you create the filter, you define the possible skill values, display labels, data types, and operators used by the system to compare the list of processor skills against the required job skills, and assign the task to an appropriate processor.

Users with the queue_admin role can create, delete, or modify queue matching filters. Users with the queue_manager role can view the settings of the matching filters only.

To define work assignment matching filters:

1. Navigate to **Administration > Work Queue Management > Work Assignment Matching > Matching Filters**.
2. Do one of these:
 - To create a new filter, select **File > New > Work Queue Skill Info**.
 - To edit an existing filter, select the filter, and from the right-click menu, select **Properties** or select the filter, and then select **View > Properties > Info**
3. Type a name for the filter.
4. Type a description for the filter.
5. Select the data type of the available skill values from the **Data Type** list box.

Valid values are **Integer**, **String**, and **Double**.

The value you select here determines the type of comparator that is available in the **Comparison Operator** list box.

6. Select a comparison operator from the list box.
7. Type in a **Value to be used in the comparison**, and a display label based on the data type you selected.
For example, to match work based on processing a conventional loan, type **conv** in the string column to represent a conventional loan, and type **conventional loan** as the display label.
8. Click **Insert** to add more rows to the table, as necessary to define the varying types of work matching comparison values.
9. Select **Processors can have more than one skill for this filter** to allow a processor to have more than one skill associated with this filter.
For example, a processor could have skills for processing both real estate loans, and automobile loans.
10. Click **OK**.

7.8.4.3 Add work assignment matching filters to a work queue

Add work assignment matching filters to a work queue to define the skill set for the queue, and for its users. All users in the work queue must have their skills updated each time a new filter is added to the queue. After you add the work assignment matching filter, the system prompts you to define the related skills for each processor in the queue.

When a skill is removed from the work queue, the system checks for the skill in existing tasks for this work queue, and removes them immediately.

To assign work assignment matching filters to a work queue:

1. Navigate to **Administration > Work Queue Management > Work Queues**, and select a work queue.
2. Right-click the queue, and select **Properties** or select **View > Properties > Info** to display the Work Queue Properties page.
3. Under Work Assignment Matching Filters, click **Add**.
4. Select the skills you are adding to work queue.
5. Click the add arrow to move the skills to the content selection area of the page.
6. Click **OK**.
The system prompts you to select the skills for each individual user in the queue.
7. Select the skills for each user, and click **Next**.

Note that skill profiles are not available for groups.

8. When you have selected the skills for each user, click **Finish**.

To remove work assignment matching filters from a work queue:

1. Navigate to the work queue, and select it.
2. Select **View > Properties > Info**.
3. In the Work Assignment Matching Filters table, select the filter that is related to the skills to be changed.
4. Click **Remove**.
5. Click **OK**.

When the system removes the matching filter from work queue, the corresponding skill values set up for users in the work queue are not automatically removed. The skill properties for the user remain until you remove them from the Processor Profile page for each processor.

7.8.5 Work queue policies

A work queue policy contains the logic that the system uses to track, and manage tasks in the work queue. This logic enables the system to assign an initial priority, and age the priority of the task based on different values you set up in the policy.

The queue policy contains settings for priorities, management settings, thresholds, and other management functions. When new item comes in for workflow, the server identifies the activity as a work queue item, checks the priority value in the policy, and assigns initial priority to the item. After the task is in the queue, the aging job increases the priority incrementally based upon the policy until the task is worked on.

You also set up threshold values to trigger notifications to the queue manager when high priority items are not being processed or when a specific number of tasks are waiting in a work queue.

With a work queue policy, you can define settings that move an unworked task to a higher priority level when the priority aging job runs.

You can also flag a percentage of tasks to be routed for quality checks.

7.8.5.1 Priorities of tasks

For most work queue users, work items appear in the Inbox based on their priority — the highest priority items are assigned to be worked on before lower priority work items. Priority, and aging settings are essential elements in the processing of work queue tasks. When the system creates a new work item, the server identifies the task as a work queue item, and checks for logic to enable it to assign an initial priority to the item. After the task is in the queue, an aging job increases the priority of the task based upon other logic, which moves the task higher in the Inbox until the task is worked on. Priority escalation may trigger the queue administrator to redistribute tasks or reallocate resources between work queues.

The priority level at which a task first appears, and the speed at which it increases in priority can be set either in the work queue policy or in the activity template for the task. For example, you set the initial priority for new tasks in a queue to 1, which means that all new tasks begin with a priority of 1. If you have set the Increment Priority to 10, then whenever the dm_QmPriorityAging job runs, the priority increases by a factor of ten, if the task has not been worked on. In this example, the task has remained in the queue, and the dm_QmPriorityAging job has run three times, increasing the priority to 31. The maximum priority field is set to 30, so the system sends a notification to the queue managers group, warning that the task has surpassed its maximum priority, and needs attending to.

Using a work queue policy, the queue administrator or queue manager can specify the initial priority of the task, and the frequency, and percentage at which it increments based on different values you set up in the policy. For more complex initialization, and aging scenarios, you use OpenText Documentum CM Application Builder to create a *priority module* that contains logic to dynamically calculate, and update the priority based on process data or other properties belonging to the process. A priority module can be associated with a work queue policy.

7.8.5.1.1 Set dynamic priority and aging logic for tasks

There may be situations where both the initial priority, and the amount that priority increments need to be calculated dynamically. In these cases, you create a *priority module* that the system uses instead of the work queue policy to set priority, and aging logic. A priority module can be selected when creating the work queue policy.

Process data can be used to set the initial priority, and increase the priority based on values in the workflow. For example, if a loan application belonging to a preferred customer comes through a work queue, it can be immediately placed at a higher priority value than a loan application from other customers. In addition, if the loan request is for a greater amount or comes from a preferred loan broker, then the priority can be increased at a higher rate, ensuring that the queue supervisor is alerted if the task is not completed within a specified period of time. This kind of logic can be especially useful to increase the priority of a task as it nears a deadline or some other time restriction—the priority is increased more rapidly as the deadline approaches, pushing the task up the queue at a higher rate.

7.8.5.2 Create or modify a queue policy

Each work queue can have one policy. If you associated an override policy with a document being routed in the workflow, the system uses the override policy rather than the work queue policy for that item.

Users with the queue_admin role can create or modify queue policies.

To create or modify a work queue policy:

1. Navigate to **Administration > Work Queue Management > Policies > Work Queue Policies**.
2. Navigate to the category where you want to either locate a new policy or edit an existing one.
3. Do one of these:
 - To create a new policy, select **File > New > Work Queue Policy**.
 - To edit an existing policy, select the policy, and then select **View > Properties > Info**.

You may edit the properties of a policy, but the policy name remains a read-only field. To rename the policy, you must delete the existing policy, and recreate the same policy with the new name.

4. Type a name for the policy.
5. Define these settings:

- **Threshold**

The number of unfinished tasks in the queue at which notifications are sent to the queue manager warning that the number of tasks in the queue is high. Notifications are triggered when the server runs the dm_QmThresholdNotification job.

The queue managers group is specified in the queue definition, and defines who receives the notifications.

- **Max Priority**

When a task in the work queue reaches this level, notifications are sent to the queue managers group warning that there is an important task not being processed. Notifications are triggered when the server runs the dm_QmPriorityNotification job.

- **Initial Priority**

The level of importance that is assigned to a newly created task when the work queue uses this policy. When a task remains in the queue without being worked on, the system adds the number specified in the **Increment Priority** field to this initial number each time the dm_QmPriorityAging job runs.

- **Increment Priority**

The value by which the system increments the priority level of tasks that are still in the queue each time the system runs the dm_QmPriorityAging job. It is added to the initial priority each time that the aging job runs.

- **Calculate priorities dynamically**

To use a priority module to set the initial priority, and increase its priority when the aging job runs, select the checkbox, and choose a priority module from the list-box. [“Set dynamic priority and aging logic for tasks” on page 619](#) provides more information on priority modules.

- **Percent Quality Check**

The percent used to randomly decide if the work item must be routed to another processor for a quality assurance check.

6. Click **OK**.

To delete a work queue policy:

1. Select the queue policy to delete.
2. Select **File > Delete**.

If the policy is in use, and is referenced by other work queues or work items, the system will not delete the work queue policy.

3. Click **OK**.

7.8.6 Define a queue category

Queue categories are like folders in which you organize your work queues. Categories can be designed to resemble your business model's hierarchy enabling you to drill through different categories to locate your work queue in a logical representation of your organization. Work queue categories must be created before creating the related work queues.

Users with the queue_admin or queue_manager role can create, and edit categories.

To create a queue category:

1. Navigate to **Administration > Work Queue Management > Work Queues**.
2. To nest the new category within an existing category, navigate to that existing category.
3. Select **File > New > Work Queue Category**.
4. Type the name of the new category.
5. If appropriate, type a description of the new category.
6. Click **OK**.

To delete a queue category:

1. Navigate to **Administration > Work Queue Management > Work Queues**.
2. Select the queue category to delete.
3. Select **File > Delete**.
The system warns you that this operation cannot be undone.
If the category is in use, and is referenced by other work queues, the system will not delete the work queue category.
4. Click **OK**.

7.8.7 Define a work queue

Work queues are organized, and listed under work queue categories. Before creating a work queue, you should first create a queue category, and queue policy. “[Define a queue category](#)” on page 621, and “[Work queue policies](#)” on page 618 provide more specifics on these topics.

Users with the queue_manager role, and with CREATE_GROUP privileges can create work queues.

To create a work queue:

1. Navigate to **Administration > Work Queue Management > Work Queues**.
2. Navigate to the work queue category where you want the new work queue to be located.
3. Select **File > New > Work Queue**.
The system displays the Work Queue Properties page.
4. Type the name of the new work queue using lowercase letters. Do not use quotation marks in the work queue name.
5. Type a description of the new work queue, if necessary.
6. By default, you are assigned as the queue manager. To change the queue manager, click **Edit** next to **Queue manager**, select a different user, and click **OK**.
7. Select a policy name to apply to the queue.
The settings for the queue policy appear as read-only fields on the page, except for the policy manager name.
8. To change the name of the policy manager, click **Edit**.
The name of the policy manager appears by default.
9. In the **Work Assignment Matching Filters** area, click **Add** to select skills that are required for the work queue. The system uses these skills to filter, and assign tasks to the queue.

The system displays a page where you can select specific skills to apply to the work queue.

10. Select the skills you are adding to work queue. Click the add arrow to move the skills to the content selection area of the page.
 11. Click **OK**.
 12. Assign users to the queue by clicking **Add** in the Assigned Processors table.
 13. Select the users you are adding to work queue. Click the add arrow to move the users to the content selection area of the page. Only users with roles queue_processor, and queue_advance_processor appear in the list of available users. The chapter on user management provides more details on setting up users, and groups.
 14. Click **OK**.
- The system prompts you to select the skills that it uses in matching work assignments to the individual users.
15. Select the appropriate skills for each user, clicking **Next** after you have set up each user's matching skills
 16. When you have selected the skills for each user, click **Finish**.

The system will not allow you to save the page until all assigned users have their skills selected.

By default, the new work queue is placed in the current category.

To move a work queue to another category:

1. Select the work queue.
2. Select **Edit > Add to Clipboard**.
3. Navigate to the category you want the work queue to move to.
4. Select **Edit > Move**

To delete a work queue:

1. Navigate to **Administration > Work Queue Management > Work Queues**.
2. Navigate through the categories to select the work queue to delete.
3. Select the work queue.
4. Select **File > Delete**.

The system warns you that this operation cannot be undone.

If the work queue is in use, and is referenced by other work items, the system will not delete the work queue.

5. Click **OK** to delete the work queue.

Deleting a work queue does not delete the category it was related to.

7.8.8 Define work queue override policies

A work queue override policy allows the priority, and aging of a task to be controlled based on the document properties, and lifecycle. Override policies can be used when different document types with different processing needs are routed through the workflow. For example, applications for different types of loan products might have different priorities, and different aging requirements.

To use override policies, when you apply a lifecycle to the document, you define the alias set %wq_doc_profile to the override policy that you want the system to apply to the document. If there is no override policy associated with the document, the system uses the policy associated with the work queue to set the properties of the work item.

Users with the queue_admin role can create or modify queue override policies.

To create or modify a work queue override policy:

1. Navigate to **Administration > Work Queue Management > Policies > Override Policies**.
2. Do one of these:
 - To create a new override policy, select **File > New > Work Queue Override Policy**.
 - To edit an existing override policy, select the override policy, and then select **View > Properties > Info**.
3. If creating a new policy, type a name for the override policy.
Once the override policy has been saved, the name field becomes read-only.
4. Click **Add** to view the Work Queue Policy Assignment page, where you can select a work queue, and policy.
5. Select the queue, and policy names to use as your override policies.
6. Click **OK**.
7. To remove a work queue override policy, select it, and click **Remove**.
8. Click **OK**.

7.8.9 Manage work queue users

Work queue users can be managed from within the work queue itself or from Work Queue Monitor. When you view the list of work queues within a category, clicking on the number of active users shows you the list of users, and groups that are members of the queue. You can also view the availability of the member, and if there is a delegated user for that member.

7.8.9.1 Add a user or group to a work queue

If a work queue is acquiring too many tasks, and the processing rate is too slow to meet your business needs, you can add more users to a queue.

Users with the queue_admin or queue_manager role can assign users, and groups to queues.

To add a user or group to a work queue:

1. Click the **Work Queue Monitor** node or select **Work Queue Management > Work Queues**.
2. Navigate to the active work queue.
3. Click the queue's *<number>* **users** link in the Active Users column.
4. Select **File > Add Member**.
5. Select the user or group, and click the arrow. Users must be assigned to the role queue_processor or queue_advance_processor to appear in this list.
6. Click **OK**.
7. Select skills for the processor that are used in work assignment matching.
8. Click **OK**.

7.8.9.2 Remove a user or group from a work queue

Users with the queue_admin or queue_manager can remove a user or group from a work queue.

To delete a user or group from a work queue:

1. Click **Work Queue Monitor** or select **Work Queue Management > Work Queues**.
2. Navigate to the active work queue.
3. Click the queue's *<number>* **users** link in the Active Users column.
4. Select the user or group to delete from the work queue.
5. Select **File > Remove Member**.

6. Click **Continue**.
7. Click **OK**.

If you delete a user from the queue after they have acquired a task, it remains in the user's Inbox until they have completed the task.

7.8.9.3 Add skills to work assignment processor profiles

A processor profile can include many different skills based upon the abilities, properties, or expertise of the processor. The system uses these skill profiles to match a processor to a task based on the skills or properties required to work on the task.

The queue manager, and the queue administrator assign, edit, or remove skill profiles related to work queue users, and can add or remove work queues for a processor using the processor profile.

Skills can also be added to a processor profile when a work assignment matching filter is added to an existing queue. After adding the filter, and related skills to the work queue, the system displays each processor profile, enabling you to make the updates to the skill set. Skill profiles are not defined for groups.

If a work queue does not have any associated skill requirements, the system will not prompt you to assign skills to a processor.

To add skills to a processor profile:

1. You can add skills to a processor profile using any of these methods:
 - Navigate to **Administration > Work Queue Management > Work Assignment Matching > Processor Profile**.
 - Or navigate to **Administration > Work Queue Management > Work Queues**, select a work queue, and click the queue's **<number> users** link in the Active Users column.
 - Or from Work Queue Monitor, select a work queue, and click the queue's **<number> users** link in the Active Users column. Select the user's profile by selecting Properties from the right-click menu or by selecting **View > Properties > Info**

The Processor Profile search screen appears enabling you to see a list of all users or to search for a specific user by name or by group.

2. Access the processor to whom you are adding skills in one of two ways:
Select **Search** in the list box, and type the user name, group, or user operating system name to find the processor.
Or select **Show All Users** from the list box, and navigate to the processor name.
3. Select the user, and select either **View > Properties > Info** or select **Properties** from the right-click menu.

The Processor Profile page appears.

4. Under Skills for Work Assignment Matching, click **Add**.
5. Select a filter from the list box.
Records Client displays the skills related to that filter.
6. Select the appropriate values for the processor.
7. Click **OK**.

To change skills for a processor:

1. Navigate to **Administration > Work Queue Management > Work Assignment Matching > Processor Profile**.
The Processor Profile search screen appears enabling you to see a list of all users or to search for a specific user by name or by group.
2. Select the user, and select **View > Properties > Info**.
3. In the Skills for Work Assignment Matching table, select the filter that is related to the skills you want to change.
4. Click **Edit**.
You can add or change skills for the processor.
5. Click **OK**.

To delete skills for a processor:

1. Navigate to **Administration > Work Queue Management > Work Assignment Matching > Processor Profile**.
The Processor Profile search screen appears enabling you to see a list of all users or to search for a specific user by name or by group.
2. Select the user, and select **View > Properties > Info**.
3. In the Skills for Work Assignment Matching table, select the filter that is related to the skills you want to delete.
4. Click **Delete**.
5. Click **OK**.

If a work queue that a processor is assigned to requires a particular skill set, the system will not delete the associated filter.

7.8.9.4 Update the processor profile in a work queue

The system uses the user profile to assign tasks to a processor based on skill levels necessary for the task. You can update, add, or remove a skill for a user. You can also change work queue assignments for the user by adding or removing a work queue from the list of assigned queues.

Users with the queue_admin or queue_manager can update a user profile.

To update a processor profile:

1. Click **Work Queue Monitor** or navigate to **Work Queue Management > Work Queues**.
2. Navigate to the active work queue.
3. Click the queue's *<number>* **users** link in the Active Users column.
4. Select a user or group.
5. Select **View > Properties > Info** or select **Properties** from the right-click menu.

The Processor Profiles page shows a list of skills that the user has as well as a list of work queues that the processor is assigned to.

6. To change the processor's skill set, click **Add** in the Skills for Work Assignment Matching table.

The Processor Skill page appears with the user name, and a list box of filters associated with the assigned work queues.

7. Select a work assignment matching filter from the list box.
8. Select the skills to associate with the processor.
9. Click **OK**.

7.8.10 Monitor work queues

Although most functions of work queues can be managed from within their individual components, you can use Work Queue Monitor as a to manage work queues from one location. Use Work Queue Monitor to view the assignment status of each task, the actual task count, and the policy task count, the priority of a task, and the highest priority of the policy, as well as how many active users are assigned to each queue. If a task count or a task priority exceeds the level specified in the policy, the system displays a caution icon in the row for that queue, and displays the item in the column that exceeds the policy in bold font.

Using the controls at the top of the page, you can select different views in the monitor, depending on your access, and privileges. You can also select which columns appear on the page, and in what order they appear by clicking the column setting icon, and making your selections.

You can view all work queues in the system that you have access to by selecting **All Work Queues** from the drop down list on the page. You can also filter to show only

the work queues that you manage by selecting **My Work Queues**. The **Show Descendents** option enables you to see all work queues that are nested inside of the categories.

Use the **My Categories** link to configure which categories appear in drop-down box of the monitor screen. Only categories that you manage are available for selection.

To select a work queue category to monitor:

1. Navigate to **Work Queue Monitor**.
2. Click **My Categories**.
3. Select the categories to monitor. Click the add arrow to move the categories to the content selection area of the page.
4. Click **OK**.

To view the work queue task a single user or a group is working on:

Work queue managers, and administrators can view the inboxes of users or groups associated with their work queues.

Users with the queue_admin or queue_manager role can perform this procedure.

1. Open **Work Queue Monitor**.

You can also navigate to **Administration > Work Queue Management**, and select a work queue.

2. Click the queue's *<number>* **users** link in the Active Users column.
3. Select the user or group.
4. Select **Tools > Work Queue Management > Workload**.

The system displays that user's Inbox, and the tasks it contains.

To monitor and update active work queues:

1. Do one of these:

- In the tree pane, click the **Work Queue Monitor** node.
- Select **Tools > Work Queue Management > Work Queue Monitor**.

2. To view the tasks in the active queue, click either the queue name.

To view the users in the active queue, click the *<number>* **users** link (where *<number>* is the number of users).

3. To update queues, see the appropriate procedure:

- “[Assign or reassign a work queue task to a specific user](#)” on page 630
- “[Unassign a work queue task from a user](#)” on page 631

- “Move a work queue task to another work queue” on page 631
- “Suspend a work queue task” on page 632
- “Unsuspend a work queue task” on page 632
- “Add a user or group to a work queue” on page 625
- “Remove a user or group from a work queue” on page 625
- “Add skills to work assignment processor profiles” on page 626
- “Update the processor profile in a work queue” on page 628

7.8.10.1 Assign or reassign a work queue task to a specific user

When a work queue task is assigned or reassigned, the system matches the new performer skill to the task skill. If the new performer does not have the skills required by the task, the system will not allow the reassignment to take place.

Users with the queue_admin or queue_manager role can assign a task in a work queue to a specific user.

To assign a work queue task to a specific user:

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more tasks.
4. Select one of these:
 - If the selected tasks are not already assigned to a user, select **Tools > Work Queue Management > Assign**
 - If the selected tasks are already assigned to a user, select **Tools > Work Queue Management > Reassign**

This action is also available through the **Task Manager**.

5. Select the user to whom to assign the tasks.
6. Click **OK**.

7.8.10.2 Unassign a work queue task from a user

You can reassign a task that is already assigned to one processor, and reassign it to another processor by unassigning the task from the user. Unassigning the task moves the task back to the queue where you can assign the task to another work queue processor.

Users with the queue_admin or queue_manager role can unassign a work queue task from a user.

To unassign a work queue task from a user:

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more tasks that have already been assigned to users.
4. Select **Tools > Work Queue Management > Unassign**.

7.8.10.3 Move a work queue task to another work queue

To balance the workload between work queues, you may want to move tasks from one queue to another. When you move a task to another queue, the system compares the skills in the target work queue to the skills required by the task. Tasks can move to another queue only if the target work queue contains all of the required skills for that task. For example, if the task requires the skill attributes of western region, and jumbo loan, it can be moved to a queue with western region, southern region, and jumbo loan. It cannot be moved to a queue with only jumbo loan.

Users with the queue_admin or queue_manager role can move a task from one work queue to another work queue.

If the task is already assigned to a user, you must first unassign the task, as described in “[Unassign a work queue task from a user](#)” on page 631.

To move a task from one queue to another queue:

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more tasks.
4. Select **Tools > Work Queue Management > Move to Queue**.
5. Select the work queue to which to reassign the tasks.
6. Click **OK**.

7.8.10.4 Suspend a work queue task

Users with the queue_admin or queue_manager role can suspend a task, and specify how it should remain suspended. the application will automatically resume the task when the amount of time you specified is reached.

To suspend a task in a work queue:

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more tasks.
4. Select **Tools > Work Queue Management > Suspend**.
This action is also available through the **Task Manager**.
5. Type the time, and date when you want the application to automatically resume the task.

7.8.10.5 Unsuspend a work queue task

Users with the queue_admin or queue_manager role can unsuspend a suspended work queue task.

To unsuspend a task:

1. Click **Work Queue Monitor**.
2. Navigate to the active work queue, and click its name.
3. Select one or more suspended tasks.
4. Select **Tools > Work Queue Management > Unsuspend**.
This action is also available through the **Task Manager**.

7.8.10.6 Enable users to select tasks from the queue

Users who are assigned the queue_advance_processor role have the ability to view the work queue tasks that they are eligible to work on, and acquire them regardless of their priority. Users with the queue_advance_processor role have the additional **Work Queue** node in the directory tree that shows all of their assigned work queues displayed as separate Inboxes. From these Work Queue Inboxes, they can select any unassigned tasks that they are eligible to work on based on their skill set.

If a processor pulls only one task from the queue, the task automatically opens in Task Manager enabling them to begin working on the task immediately. To keep the system from automatically opening the task after the processor pulls it, you must change the tag `<openTaskManager>true</openTaskManager>` in the `pullqueuedtask_component.xml` file to **false**. The processor can still get the task, but must open it from the Work Queue Inbox.

7.8.11 Create business calendars

Users from various regions or business units of your organization may adhere to different work hours, and schedules. To enable workflow timers to use actual working hours, and holidays, you can create custom business calendars that reflect these different work schedules. All the timers using business days, and business hours will use the business calendar associated with the process template.

Users with the required permission sets can create calendars based on regional work schedules, country-specific holidays, or other unique time constraints.

When you create a new calendar, you can select an existing calendar, and use it as a basis for creating another calendar, making the necessary modifications to the new calendar.

You can also create different time periods within a calendar for ease of administration. For example, you can create a calendar for the Western Region for the years 2008 through 2009. The calendar can have two different periods of time on the Periods tab—a time period within 2008, and a time period in 2009. Each period of time can be edited separately, and can have its own starting, and ending times, work days, and non-working days.



Note: If you edit a calendar that is being used in a running or paused workflow, the timer expiration dates are recalculated based on the modified calendar.

To create a new calendar:

1. Select **Tools > Workflow > Calendar**.
The Calendars page appears with a list of calendars that exist within the repository.
2. Select **File > New > Business Calendar**.
3. To base the new calendar on an existing calendar, select the calendar name from the **Base calendar** list.
The default is **None**.
If the calendar is being used in a process, the system displays the process name in the Process list.
4. Type a name, and a description for the calendar.
5. Click **Next** to display the Periods page where you create separate periods of time.
6. Type a name for the group.
7. Select a **Start date**, and **End date** for this event.
8. Select a **Start time**, and an **End time** for the days that fall within the category of working days.

Select **Use same time for all checked days** to set a time for one of the working days, and use it for the selected days.

9. To identify a day as a **Non-working day**, select it from the pop-up calendar control, and click **Add**.

The date appears in the list of non-working days. To **Edit** or **Delete** the date, select it from the list, and click the link to edit or delete.

10. Click **Next** to display the Details tab, and the list of events that are associated with the calendar.

On the Details tab, you can add, edit, and delete events.

11. Click **Next** to display the Permissions tab.

Superuser or users with the bpmuser role can create or delete a business calendar. Any user can edit the calendar.

12. Click **Finish**.

The system saves the calendar to the /System/Workflow/Calendar folder.

To delete a calendar:

1. Select **Tools > Workflow > Calendar**.

The Calendars page appears with a list of calendars that exist within the repository.

2. Right-click the calendar, and select **Delete**.



Note: The system will not delete a calendar that is referenced in any process definition.

To edit a calendar:

1. Select **Tools > Workflow > Calendar**.

The Calendars page appears with a list of calendars that exist within the repository.

2. Right-click the calendar, and select **Properties**.

3. The calendar definition opens, enabling you to edit the calendar details.

7.9 Lifecycles

7.9.1 View Lifecycles

Each file in the repository has a lifecycle. A lifecycle defines a sequence of states a file experiences as it passes from creation to review to approval. For example, an employee might create a new human resources form, another employee might review it, and a third employee might give the approval necessary to make the file available to all employees. The lifecycle defines the file's state at each point in the process.

To view a file's lifecycle, and current lifecycle state, open the file's properties. If the file has no assigned lifecycle, then you can assign the lifecycle through the properties.

You also can assign a lifecycle to a file when creating, importing, or checking in the file, or by selecting the file in a file list, and using the **Apply Lifecycle** menu option. When applying a lifecycle, you can specify the initial lifecycle state for the file.

You can advance a file through its lifecycle manually by selecting the file and using the **Promote** menu option, or Records Manager Administrator can advance a file through its lifecycle automatically based on conditions specified in the lifecycle definition, if a retention policy is associated with the lifecycle. You can also demote a file to a previous lifecycle state.

See “[Common lifecycle states](#)” on page 635 for descriptions of common lifecycle states.

Table 7-13: Common lifecycle states

State	Description
WIP (Work In Progress)	The file is in draft or review.
Staging	The file is complete, and ready for testing. By default, you cannot edit a file that is in this state.

7.9.2 Assign a lifecycle to a file

To assign a lifecycle to a file:

1. Navigate to the file, and select it.

You can perform this procedure on multiple files by selecting multiple files.

2. Select **Tools > Lifecycle > Apply**.
3. In the selection dialog box, do these:

- a. Locate, and select the lifecycle, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.

- b. If the lifecycle's line item includes an option to select the lifecycle state, then select the lifecycle state in which to place the file.
- c. If the lifecycle's line item includes an option to select an alias set, then select an alias set to use with the lifecycle. The alias set determines which users have access to a file as it moves through its lifecycle.
- d. Click **OK**.

If you perform this procedure on a template, the lifecycle is assigned to all future files created from the template. The lifecycle is not assigned to files that have already been created from the template.

7.9.3 Remove a lifecycle from a file

To remove a lifecycle from a file:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Detach**.

7.9.4 Promote a file to the next lifecycle state

To promote a file to the next lifecycle state:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Promote**.
3. If prompted, select whether to promote related files.

7.9.5 Demote a file to its previous lifecycle state

To demote a file to its previous lifecycle state:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Demote**.
3. Click **Demote**.

7.9.6 Suspend a file from its current lifecycle state

Suspending a file halts the lifecycle's progress temporarily.

To suspend a file from its current lifecycle state:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Suspend**.
3. Click **Suspend**.

7.9.7 Resume a suspended file

To resume a suspended file:

1. Navigate to the file, and select it.
You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Resume**.
3. If prompted to select which state to resume to, select the state.
4. Click **Resume**.

7.10 Collaborate with other users

7.10.1 Create and edit formatted text

When you write notes, comments, replies, and other text, you often use the Rich Text Editor (RTE). You can type text directly into the RTE or add content by pasting or dragging-and-dropping from another application.

The following table describes the tools available in the RTE.

Table 7-14: Formatted text editing tools

Tool	Description
	Gives access to comment editing options, such as undo, redo, delete, and select all. With Microsoft Internet Explorer, additional choices are also available: cut, copy, paste, and remove styles.
	Adds graphics. The Insert Image dialog box opens, and provides controls for choosing, and uploading one .bmp, .gif, .jpeg, or .png image at a time, which is then shown inline in the editing area.

Tool	Description
	Creates hyperlinks. The Insert Link dialog box opens. Set the title, and URL of the hyperlink, and choose whether to have the link open in a new window.
	Checks spelling. (You will be prompted to download a plug-in.) When the spell-checker finds a possible misspelling, the word is selected, scrolled into view, and the Check Spelling dialog box opens. The word in question appears in the Change box with a suggested alternative in the To box. You can edit the text in the To box, or select a word from the list. Spelling commands are as follows: <ul style="list-style-type: none"> • Change. Changes the selected word to the one in the To box. • Change All. Changes all occurrences of the selected word in the text. • Ignore. Leaves the selected word unchanged. • Ignore All. Ignores all occurrences of the selected word in the text. • Add to Dictionary. Adds the selected word to the dictionary used to check spelling.



Note: In general, the RTE can display any HTML content that the web browser can display. However, if you paste into the RTE content that was created outside of the RTE, you might be unable to edit some elements of that content. For example, if you paste an HTML table into the RTE, it displays appropriately, and you can edit text in the table's cells, but you cannot edit the table itself.

7.10.2 Discussions

Discussions are online comment threads that facilitate collaboration around particular items. A web site production team, for example, can use discussions to share feedback about content before publishing it. Development teams can use discussions to brainstorm, debate, and reach consensus about product design, and specifications.

Most items (such as documents or rich media files) have an attached discussion page. Folder, and note pages have embedded discussions shown below the list of child items in a folder or the body of a note. You can add, edit, delete, and reply to comments in a discussion, but you cannot select or edit a discussion apart from its parent item.

Each new version of an item shares the same discussion as the immediately preceding version. A WDK setting can change this default behavior so that discussions are only shared for each new minor or branch version (while major versions have new discussions), or that no versions of an object share a discussion (every version has its own). In this manner, an object's versions can provide a sort of timeline for an object, along with the comments in each discussion. When a discussion is shared by versions, version markers for each checkin appear among the comments.

7.10.2.1 View discussions

In the optional Discussion status column of a list (indicated by the  icon), objects that have discussion comments are distinguished by one of these discussion icons:

-  means you have read all comments in the discussion.
-  means there are some comments in the discussion you have not read.

To see a discussion, with or without comments (for example, to add a comment), either click on a discussion icon, or select a single object, and pick **View > Discussion**.

To sort a list of objects according to their discussion comments (read, unread, or none), click  at the top of the Discussion status column. You can turn off the Discussion status column by using Display Setting preferences for columns.

You can mark discussions as having all read or unread comments. For example, if you want a visual reminder when only new comments are added to a particular discussion, select or open the object it is associated with, and pick **File > Mark Discussion Read**. Conversely, you can make all comments appear to be unread with **File > Mark Discussion Unread**. Selecting multiple objects applies these commands to each object in the selection.

7.10.2.2 Add and edit comments

Users with at least Write permission to an object can go to the **Properties: Info** tab for the object, and select or clear the **Show discussion** checkbox. Once a discussion is shown, users with at least RELATE permission on the discussion's primary parent can add a comment or a reply in that discussion.

To add a comment to a discussion:

1. Display the discussion by doing one of these actions:
 - Click the  or .
 - Select a single object, and pick **View > Discussion**.
2. In the discussion, below the last comment, click **add a comment**. (If there is no **add a comment** button for an object, your permission for the parent object is less than RELATE.)
3. Enter the (required) title, and (optional) body of your comment.

4. Click **OK**.

Your comment appears below the last comment, set even with the left margin of the one above it.

To reply to a particular comment:

1. Next to the title of the comment to which to respond, click .
2. In the rich-text editing window, fill in the title, and body of your comment.
Your remarks appear below the comment to which you are responding.

If there is no  icon for replying to a comment, your permission for the parent object might be insufficient. For adding or replying to comments you need at least RELATE permission.

To edit a comment:

1. Next to the title of a comment you added, click .
2. In the rich-text editing window, edit the title and/or body of your comment.
3. Click **OK** to put your changes into effect.

Unless you have administrative privileges, you can edit your comments only.

7.10.2.3 Delete comments

You can delete a comment as long as you have DELETE permission on it, and RELATE permission on the discussion. These are your permissions when you author a comment.

When you delete a comment, any replies to it (and replies to them) are also deleted, regardless of your permissions over them. If you have DELETE permission on an object, you may delete all comments in its discussion, even if you lack permission to edit those same comments.

While you cannot explicitly delete a discussion, deleting all of its parents effectively deletes the discussion as well.

7.10.2.4 Discussions in search results

The repository search index contains the rich-text content of discussions, but not their meta-content or properties. This means that discussion comments can match a search by full text, but not a search by properties like object type or creation date. You can, however, search for the names of comment authors.

When a discussion matches the search terms, the results show the parent object, not the discussion itself. You can open the discussion of any search result using the same methods as in other contexts.

7.10.3 Notes

A note is a simple page for composing, editing, and sharing information without using or requiring other users to have another application to do so. Notes can have built-in discussions, and can contain rich-text content.

Notes ( appear in Records Client only where documents are shown. They can have embedded discussions if the **Show Discussion** option is checked in the note's properties.

While you can subscribe to notes, they do not have versions or renditions. You can edit, move, copy, or link a note, but you cannot check notes in or out, or export them.

To search for notes, run an advanced search, and set the type of object field to either Sysobject (dm_sysobject) or Note (dmc_notepage).

To create a note:

1. Navigate to the location for the new note.
2. Select **File > New > Note**.

The **New Note** dialog box opens.

3. In the **Create** tab, specify the following properties:
 - **Name** (required). The name of the new note must be unique among the names of other objects in the same container.
 - **Note**. Using the RTE, specify the body of your note (this is optional). You can edit this field after the note is created.
 - To subscribe to the note, check the **Subscribe to this notepage** option (click **[+] Show options** if necessary to view the option).

You can either continue to another tab, or click **Finish** to create the note.

4. Click **Finish** to close the dialog box, and create the note.

Or, you can click **Cancel** to close the dialog box without creating a note.

To edit the body of a note:

1. Select **File > Edit**.
2. Edit the body of the note.
3. Click **OK** to put your changes into effect.

To edit the name of a note:

1. Do one of the following:
 - Right-click the note, and select **Properties** from the context menu.

- Select the note, and select **View > Properties > Info**.

The **Properties: Info** tab opens.

2. Edit the note's **Name**, and any other properties, as appropriate.
3. Click **OK** to put your changes into effect.

To delete a note, select it, and then pick **File > Delete**.

Since notes do not have versions, the **Delete** dialog box for a note differs from that for typical documents. Choices in the **Delete** dialog box are as follows:

- *Links*. Delete just the link to the location name (not selected, and disabled if the note has only one location, otherwise selected by default).
- *Note*. Permanently delete the note (selected by default if note has only one location).

7.10.4 Contextual folders and cabinets

Contextual folders, and cabinets are repository containers with optional rich-text descriptions, and built-in discussions. These features provide the ability to capture, and express the work-oriented context of a folder's hierarchy. Such contextual information might include details about project goals, tasks, roles, milestones, and so forth. Since full-text search keeps an index of all descriptions, and discussions in a repository, they are easy to find, along with the items to which they relate.

Rich-text descriptions display at the top of a contextual folder, like a room's welcome message. They can provide, for example, document summaries, instructions for using project materials, or pointers to other locations. Because they can include formatted text, pictures, and hyperlinks, folder descriptions can be informative, personalized, and appealing in order to draw users' attention.

Discussions embedded on a contextual folder page encourage team members to focus communication towards the nexus of their work (such as for document reviews) instead of using email, for example, for project correspondence. Organized in a tree of comments, these discussions help to capture, and preserve the work-related flow of information.

In some form or another, all project teams converse about a variety of topics, such as case issues, scheduling decisions, development plans, product ideas, and customer feedback. Discussions in contextual folders let teams save, and have ready access to such ad hoc but historically valuable exchanges.

To create a new contextual folder:

1. Navigate to the location for the new folder.
2. Select **File > New > Folder**.

The **New Folder** dialog box opens.

3. In the **Create** tab, specify the following properties:
 - **Name**(required). The name of the new folder.
 - **Type**. The type of folder.
 - **Description**. In the rich-text editing window, create a description that will appear below the navigation path on the folder's page (optional).
 - To subscribe to the folder, select the **Subscribe to this folder** checkbox (click **[+] Show options** if necessary to view the option).

You can either continue to another tab, or click **Finish** to create the folder.

4. Click **Finish** to close the dialog box, and create the folder.

Or, you can click **Cancel** to close the dialog box without creating a folder.

To enable a discussion for the folder, you must select the **Show Discussion** checkbox on the **Info** tab of the folder's properties dialog box.

7.10.5 Calendars

Calendars let you organize, track, and schedule events. Since calendars support the iCalendar (or iCal) standard format for exchanging calendar data over the Internet, they are well-suited for use in distributed collaborative groups.

While you can subscribe to calendars, they do not have versions or renditions. You can edit, move, copy, or link calendars, but you cannot check calendars in or out.

A calendar can be added to the clipboard, and then linked, moved or copied like a folder. A copy of a calendar includes copies of all the original's descendants. Calendars can only hold events, and only events can be copied in calendars. Events, on the other hand, can be copied in any folder location.

7.10.5.1 Create calendars and events

To create a calendar:

1. Navigate to the location for the calendar.
2. Select **File > New > Calendar**.

The **New Calendar** dialog box opens.

3. In the **Create** tab, specify the following properties:
 - **Name** (required). Enter the calendar's name, which must be unique among the names of other objects in the same container.
 - **Description**. Create a description that will appear below the navigation path on the calendar's page (optional).
 - To subscribe to the calendar, select the **Subscribe to this calendar** checkbox (click **[+] Show options** if necessary to view the option).

Either continue to another tab, or click **Finish** to create the calendar.

4. Click **Finish** to close the dialog box, and create the calendar.

Or, you can click **Cancel** to close the dialog box without creating a calendar.

To enable a discussion for the calendar, you must select the **Show Discussion** checkbox on the **Info** tab of the calendar's properties dialog box.

To create a calendar event:

1. Navigate to (or create) the calendar in which to create an event.
2. Select **File > New > Event**.

The **New Calendar Event** dialog box opens.

3. In the **Create** tab, enter information as appropriate. For field descriptions, see “[Calendar events](#)” on page 644.

Table 7-15: Calendar events

Field	Description
Name (required)	Type the name of the new event. If you select the Send mail when I finish checkbox, the event name appears in the Subject: field of the header in the email about the event.
Start Date (required)	Pick a date when the event starts.
Start Time (required unless All Day Event is selected)	Enter a time when the event starts.
All Day Event	Select this checkbox if the event is a day-long occurrence.
End Date (required)	Pick a date when the event ends.
End Time (required unless All Day Event is selected)	Enter a time when the event ends.
Organizer (required)	Pick the name of the user organizing the event if different from the (default) user creating the event. If you select the Send mail when I finish checkbox, the organizer's name appears in the CC: field of the header in the email about the event.
Attendee List	Pick the names of users attending the event. If you select the Send mail when I finish checkbox, these names appear as recipients in the To: field of the header in the email about the event.
Location	Specify the location for the event.

Field	Description
Notes	<p>Enter information about the event (optional). If you select the Send mail when I finish checkbox, these notes will appear following the default text in the body of the email message to recipients. The default text in that email is as follows:</p> <pre>You are invited to the following meeting: Topic: <i>meeting name</i> Date: <i>recurrence pattern or start date, time, duration</i> Location: <i>location</i> To view the event, point your browser to: <i>event url</i> Or open this event in your desktop calendar: <i>ICS inline attachment</i></pre>
Send mail when I finish	Select this checkbox if you want to send email notices about the event.

4. For a recurring event, open the **Recurrence** tab, and follow the guidelines in the section titled *Specifying recurring event properties* later in this chapter.
5. Click **Finish** to close the dialog box, and create the event.

If the **Send email when I finish** checkbox is selected when you click **Finish**, notification email about the event is sent to the users specified on the **Attendee List**.

Or, you click **Cancel** to close the dialog box. In this case, no event is created, and no email is sent.

7.10.5.2 Specify recurring event properties

Recurring events repeat according to a specified *frequency pattern* for a specified *duration*. You set these properties in the **Recurrence** tab of the Calendar Event properties dialog box.

Choose from the following options to specify a recurring event's frequency pattern:

- **None** (default). The event does not repeat, and event duration options are disabled.
- **Daily**. The event repeats either every day, or (if selected) **Every Other Day**.
- **Weekly**. The event repeats every week according to the following options:
 - **Every Other Week** (optional). The event repeats every other week on the selected **Days**.
 - **Days** (required when **Weekly** frequency is chosen). Pick one or more days of the week on which the event occurs. The default setting is the day of the week on which the start date falls.

- **Monthly.** The event repeats every month according to one of the following options:
 - **Same Date.** The event repeats once per month on the same date. If the date is the 29th of the month or later, this option includes the text or last day of month. For example:
Day 17.
Day 30, or the last day of the month.
 - **Same Weekday, On Alternating Weeks** (available only if start date falls on the 28th of the month, or earlier). The event repeats in a pattern similar to these examples:
The first, and third Wednesdays.
The second, and fourth Fridays.
 - **Same Weekday, Last Of Month** (available only if the day on which the event starts is one of the last seven days of the month). For example:
The last Tuesday of the month.
The last Friday of the month.
- **Annually.** The event repeats once per year on the same date each year.

If the event's frequency pattern is set to **None**, duration settings are disabled. Otherwise, choose one of the following options for a recurring event's duration:

- **Occurrences.** Specify the number of times the event occurs.
- **End Date.** Pick the date of the last time the event occurs. The default setting is the date on which the last of the specified number of **Occurrences** falls. If the **End Date** is the 29th of the month, or later, and month has no such day, the date is last day of the month.
- **Forever.** Select this option if the event has no finite number of occurrences, and no end date.

If the **Send mail when I finish** checkbox is selected when you specify recurring event properties, the notification email sent to event participants includes a description of the recurrence in the **Date** field. Here are some examples of such descriptions:

- Daily, for 5 occurrences
- Every other day, for 5 occurrences
- Weekly on Wednesday, Thursday, until September 20, 2007
- Monthly on Day 30 or last day of month, forever
- Annually, for 5 occurrences

7.10.5.3 View calendars and events

Calendars display events in a list that you can modify by changing list view preferences. Default columns in the calendar list view are as follows:

- **Event.** The name of the event.
- Attachment icon – The attachment icon is shown if attachments are available on the event. Attachments cannot be added to an event, however attachments might be added through other applications. Clicking on the attachment icon takes you to a folder view with the attachments listed in the view list.
- Exception Type icon. Indicates standalone exceptions or recurring events with exceptions.
- **Start.** The start date, and time for the event.
- **End.** The end date, and time for the event.
- **Location.** The location of the event.

7.10.5.4 Edit calendars and events

Properties of calendars, and events are the same when you view or edit them as when you create them.

Just as you can edit several objects at the same time, you can edit multiple events at once. When editing multiple events, however, only the **Info**, and **Permission** tabs are available.

When editing events, the following rules apply:

- For a recurring event, the entire series is always edited.
- For an exception to a recurring event, only the exception is changed.

Collaborative services cannot create exceptions to recurring events, but can display exceptions that another application or import creates. Such exceptions can be edited.

If you view or edit a calendar event, and you select the **Send email when I finish** checkbox, notification email is sent to event participants when you click **Finish**.

7.10.5.5 Delete calendars and events

When you delete a calendar, decide whether to delete the selected calendar only, or the selected calendar, and all events (this is similar to deleting a folder).

To delete an event, select it, and choose the **Delete** command. In this case, the following rules apply:

- For a recurring event, you must confirm that all exceptions will be deleted.
- For an exception to a recurring event, only the selected exception is deleted.

7.10.5.6 Calendars in search results

All content in a calendar (including any description and discussion comments) is indexed for full-text search. In the **Advanced Search** dialog box, Calendar, and Calendar Event are included in the list of object types for which you can search.

7.10.5.7 Export and import with calendars

Collaborative services can export events as *.ics* files, in iCal format. The **Export** command is available when one calendar or event is selected, or when a calendar or event is open. You can export an individual event or an entire calendar.

When an event is imported, its properties are handled in one of these ways:

- *Use*. If a property is supported, then it is used as follows:
 - *no change*. Keep the original value if it is supported. For example: Duration.
 - *reformat*. Reformat a value with an equivalent. For example, a start time can be expressed in more than one time zone.
 - *convert*. Convert an overly complex or unsupported value. For example, seconds are removed from times, and durations.
- *Move*. If a property is not supported, but a similar property is, the value of the former is moved to the latter. For example, a comment is moved, and combined with a description.
- *Cache*. If a property is not supported, but its presence is harmless, the property is retained in case the event is exported. For example: Free/Busy.
- *Discard*. If a property conflicts with collaborative services's object model, it is discarded. For example: Attachments.

Importing an event that was previously exported updates the original event if the exported event was changed prior to being re-imported.

7.10.6 Data tables

Use data tables to create, and manage structured collections of similar data such as lists of issues, tasks, milestones, and contacts. Information in a data table is organized as a series of entries (or records, or rows) that have a common format, or schema. Each table has just one schema, which describes the attributes of each field, including its name, and data type.

Data tables also provide an improved summary for data table fields like the traffic light. The data table entry view provides a visual and user friendly view of table entries. The entry view also supports attachments for a given entry as well as the ability to discuss the viewed entry.

While you can subscribe to data tables, they do not have versions or renditions. You can edit, move, copy, or link data tables, but you cannot check them in or out.

You can copy, move, and paste data tables. When you copy a data table with entries, the new entries have a fresh series of autonumbers, and an empty history.

Data table entries can be copied, and pasted between tables, and within the same table.

When a data table becomes governed or ungoverned, all its entries are governed or ungoverned as well. When you copy or move entries between tables with different governing, the governing is automatically changed on the copied or moved entries.

7.10.6.1 Create data tables and entries

To create a data table:

1. Navigate to the location for the new data table. Either paste a data table from the clipboard, import a data table, or perform the following steps to create one from scratch.
2. Select **File > New > Data Table**.

The **New Data Table** wizard opens.

3. In the **Create** tab, enter the following properties:
 - **Name** (required). The name of the new data table.
 - **Description** (optional). A description that appears below the navigation path on the data table's page. You can edit this field after the data table is created.

To subscribe to the data table, check the **Subscribe to this data table** option (click **[+] Show options** if necessary to view the option).

4. Click **Next** to create the data table's fields (or columns). A data table entry consists of the fields that make up a row. Each field has a name, and a data type, and one of the fields is the designated entry name. Three, unnamed, plain-text fields are initially provided for a new table. You can edit, add, or delete fields as appropriate.

For each field, choose settings as follows:

- **Field Name** (required). The name label for the field. For example, *Name*, *Date*, *Part Number*, and so on. The name must be between 1 and 128 characters in length, and it must be unique within the current table. One of the field names is designated as the entry name.
- **Field Type**. The type of data the field contains. Choose a field type, as described in “[Data table field types](#)” on page 650. You cannot change (edit) the data type of a field once the table is created.
- **Use as entry name**. The field identified as the name of the entry. Clicking the entry name in a data table row opens the entry. The following field types can be entry names: plain text, number, autonumber, date, or member. You cannot change (edit) or remove the entry name field once the table is created.

To add a field, click **Add**; to delete a field, click **Remove**.

Either continue to another tab, or click **Finish** to create the data table.

5. Click **Finish** to close the wizard, and create the data table.

Or, you can click **Cancel** to close the wizard without creating a data table.

To enable a discussion for the data table, you must select the **Show Discussion** checkbox on the **Info** tab of the create data table wizard, or the data table's properties dialog box.

Table 7-16: Data table field types

Field type	Description
Plain text	For fields displaying text with no special formatting.
Formatted text	For fields displaying text with type styles such as bold, and italic, as well as graphics, and hyperlinks.
Date	For fields displaying calendar dates. When creating a table, and defining a date field, you can (optionally) select a checkbox that specifies the field as a due date.
Number	For fields displaying fixed digits, and related characters, such as currency symbols, commas, and decimal points.
Autonumber	Numeric values created automatically, according to the sequence in which the entry is created. A data table can have only one autonumber field.
Yes/No	For fields displaying blank, yes, or no values.
Traffic light	For fields displaying blank, red, yellow, or green values, indicating the overall status of entries.

Field type	Description
Choice list	<p>For fields that display a subset of predefined values. Specify the choice values in the text box (for example: choice 1, choice 2, and choice 3, without the commas, and each on its own line).</p> <p>A choice list must have at least one choice, each choice must be unique in the list, and no line can be blank. The order of lines determines the order in which the choices appear in the list of choices when users create or edit an entry.</p> <p>To allow users to choose more than one value for this field, select the checkbox labeled Allow multiple choices.</p>
Member list	<p>For fields that display the names of members. Members can either be users or groups. Decide whether multiple users can be selected for this field or only from a list of specified users.</p>
Discussion	<p>For including a discussion field in the entry. A data table can have only one discussion field.</p>
Attachments	<p>For including an attachments field in the entry. A data table can have only one attachments field.</p>

To create a data table entry:

1. Navigate to (or create) the data table in which you want to create an entry.
2. In the data table summary view, select **File > New > Entry**.
The **New Table Entry** dialog box opens.
3. In the **Create** tab, enter data for each of the field types.
You can either continue to another tab, or click **Finish** to create the entry.
4. Click **Finish** to close the dialog box, and create the entry.
Or, you can click **Cancel** to close the dialog box without creating an entry.

Table 7-17: Editing data table field types

Field type	Description
Plain text	Edit a plain text field using a standard text box.
Formatted text	Edit a formatted text field using the RTE.

Field type	Description
Date	Edit a date field using a text box with a date picker provided for choosing a date. If the date is a due date, you can optionally select the Done? checkbox to indicate when a task is finished.
Number	Edit a number field using a text box.
Autonumber	The autonumber field is read-only.
Yes/No	Select blank, Yes , or No .
Traffic light	Select Red , Yellow , Green , or blank.
Choice list	For a choice-list field that allows one choice only, pick the value from a drop-down list of predefined choices. For a field that allows multiple choices, select from the set of predefined values.
Member list	Use the member picker to select members (either users or groups).
Discussion	You cannot edit a discussion field.
Attachments	You cannot edit an attachments field.

7.10.6.2 View data tables

When browsing in a folder, data tables appear as data table icons.

To open a data table, either select it, and pick **File > Open**, or double-click it.

The data table opens in the summary view. Entries are displayed in rows. Each row is divided into fields (or columns) of data such as name, address, and phone number, according to the table's schema.

You can sort columns, and edit column preferences the same as you do in a folder. If you delete a field, the corresponding column disappears. If you add a field, however, you must edit column preferences to make it appear in summary view.

7.10.6.3 View data table entries

To view a data table entry from the data table summary view, either select it, and pick **File > Open**, or double-click it.

If the entry belongs to a data table governed by a room, the room banner graphic (if any) appears on the page below the entry name.

If the data table schema includes an **Attachments** field, a list view appears embedded in the entry page like a folder list. The attachments area supports Records Client drag-and-drop functionality. (To use drag-and-drop, you must first enable the drag-and-drop option in your general preferences.) Folders, and folder subtypes are

not permitted in the attachments area. Attachments, if they are not already governed by a room, are governed automatically when a data table becomes governed by a room.

If the data table schema includes a **Discussion** field, the discussion appears embedded in the entry page as it does on a folder or a note page.

7.10.6.4 Edit data tables

To edit the properties of a data table, do one of the following:

- Select it, and pick **File > Edit**.
- Select it, and pick **View > Properties**.
- Right-click the data table icon, and select **Properties** from the pop-up menu.
- In summary view, click the **Edit** button at the top of the page.

When you edit a data table, the standard **Info**, **Permissions**, and **History** tabs are available, in addition to a **Fields** tab, which allows you to edit table fields.

When editing a data table's fields, you can add, rename, and delete fields, and modify certain field options. Once the data table is created, however, you cannot

- change the data type of a field
- change or remove the **entry name** field
- reorder fields

You can change the choices in a **Choice list**, and members in a **Member list**. However, you cannot change a **Date** to a **Due date**, nor a member field that allows multiple choices back to one that permits a single choice only.

If you delete a **Discussion** field, all comments in all of the data table's entries are removed.

If you delete an **Attachments** field, all attachments are removed from every entry in the data table. *This action cannot be undone.* Attachments that are linked elsewhere in the repository are unlinked. If any attachment cannot be deleted, no attachments are deleted. Until the delete operation concludes, no one can delete the data table, add or remove entries, edit the data table's properties, nor edit the data table's entries.

7.10.6.5 Edit data table entries

To edit field values in a data table entry (row), do one of the following:

- Select the entry, and pick **File > Edit**.
- Right-click the entry name, and pick **Edit** from the pop-up menu.
- On an entry page, click the **Edit** button.

The edit entry page opens, and fields appear in the same order, and with the same names, as they have in the table's schema. The name, and value of each field appear side-by-side. You edit field values the same as when you create an entry.

To edit the properties of a data table entry, do one of the following:

- Select it, and pick **View > Properties**.
- Right-click the data table entry name, and select **Properties** from the pop-up menu.
- On the entry page, click the **Edit** button at the top of the page.

When you edit the properties of a data table entry, these tabs are available:

- **Info:** standard Info tab
- **Permissions:** standard Permissions tab
- **History:** standard History tab for a data table entry

7.10.6.6 Delete data tables

In order to delete one or more data tables, you must have permissions to delete the data tables, the data table entries, and any/all attachments in the data tables. If you have delete permissions for the data table(s) but not for one or more attachments in the data table(s), the table will not be deleted.

7.10.6.7 Import and export with data tables

You can add entries to a table by importing entries from a file. To do so, open the table, and choose the **File > Import** command, which opens the **Import** dialog box. When importing entries, values are unmodified even if they conflict.

Entries in a table may be exported in *.csv* format via the **Export** command. Data is exported according to the same rules as when importing.

7.10.7 Rooms

Rooms are virtual workplaces where group interactions take place. Rooms have members, and membership is associated with both the processes, and the content in a room. Items in a room are governed by that room (that is, their permission sets are determined by the room), and non-members cannot access them.

Repository users with the appropriate permissions can create, and administer a room in Records Client, instead of relying on a system administrator. Room creators/owners, and user managers determine a room's member list.



Note: Creation, and administration of rooms are available only to WDK-based applications such as Records Client.

7.10.7.1 Visit a room

Rooms are like folders in the Records Client navigation tree.

To open the home page of a room of which you are a member:

1. In a list of items, click the room icon ().

The first time you visit a room's home page, you have the option to subscribe to it (unless you are its creator, and have already done so).

2. Choose **Yes** or **No**, and then click **Continue**.

If you choose **Yes**, the room's home page is added to your subscriptions.

The home page of a room is like the top level of a folder, with these unique aspects:

- The title is the room's, plus the words home page.
- A banner graphic (if any) appears above the room's welcome message. (A room's banner graphic also appears on the pages of governed folders, notes, and standalone discussions in that room.)
- A link to the **Membership** tab of the room properties appears at the top.
- The welcome message (if any) is like a folder's rich-text description.
- The built-in discussion is named Announcements.

7.10.7.2 Link to a room

You can add a link to a room's home page anywhere in the repository that permits links.

7.10.7.3 Objects governed by rooms

When an object is *governed by* a room, its permission set is ruled by the room, and only the room's members can access it. While a governed object may be linked to other locations in a repository, only members of the room that governs the object can access it. A room governs anything created within or imported into it, except for another room.

When an object becomes governed (is either created in or copied to the room or a governed folder), the room's default permissions are applied to the object. If the room's permission set is changed, all permission sets for governed objects are changed accordingly.

In the Room column of a list (indicated by the  icon), objects that belong to rooms are distinguished by one of the following icons, which are their *governing indicators*:

-  means the item belongs to (or is governed by) the same room as the current folder.
-  means the object belongs to a different room.

Clicking a governing indicator opens the room's home page. Click the  header icon to sort a list of objects according to whether they belong to the same room, a different room, or no room.

If you show all versions in a folder, each version of an object that is visible to you has its own governing indicator since different versions may belong to different rooms.

You can turn off the Room column by using Display Setting preferences for columns.

7.10.7.3.1 Ungovern objects from a room

A user must have Write, and Change permissions on an object in order to ungovern it. Also, a [room option on page 657](#) may limit ungoverning to owners.

When an object is ungoverned, it gets the default permission set for the repository, unless it is ungoverned from a governed folder, and the default permission set is FOLDER, in which case it gets the default permission set for the user.

The governing relationship of an object to a room can be removed in these ways:

- Moving links from inside the objects' room to anywhere outside it can lead to ungoverning those objects.
- Using the **File > Remove From Room** command.

- Copying a governed object into an ungoverned folder.
- Moving a link for a governed object out of its room via a workflow, as long as the workflow is authorized to ungovern in that room.

If you copy entries between different governed data tables, the governing on the copies is automatically changed to match the governing room's permission set.

7.10.7.4 Create a room

You can create a room anywhere in a repository that allows folders. However, it is recommended that you restrict the number of rooms in a repository to less than 250.

To create a room, users must not only have permission to create objects in the intended location, but must also belong to the Create Room role in the repository.

When you create a room, you become its owner.

To create a room:

1. Navigate to the location for the new room.
2. Do one of the following:
 - Click **New Room**.
 - Select **File > New > Room**.

The **New Room** dialog box opens.

3. In the **Create** tab, specify these properties:
 - **Name** (required). The name of the new room. The name must be unique among the names of other objects in the same cabinet.
 - **Welcome message**. Optional rich text that will appear below the navigation path on the room's home page.
 - To subscribe to the room, select the **Subscribe to this room** checkbox (click **[+] Show options** if necessary to view the option).

You can either continue to another tab, or click **Finish** to create the room.

4. Choose the room's members either now, or after the room is created.
 - The **Choose Owners** tab provides the usual Records Client controls for selecting users, groups, or roles. You can add or remove members in this role later. As the room's creator, you automatically become an Owner.
 - On the **Choose Contributors** tab, pick the repository users, groups, or roles that you want in the room's Contributors role. You can add or remove members in this role later.
5. Select the room's options either now, or after the room is created.

- **Rights to remove governing.** Decide who can remove the governing relationship that the room has over objects belonging to the room, either room Owners only, or any room member (Contributors as well as Owners).
- **Room Banner.** Decide whether your room displays a graphic at the top of all pages in the room. To specify a custom banner, select the **Use Custom Banner** checkbox. Pick the graphic file (*.gif*, *.jpg*, *.jpeg*, or *.png* format, no more than 36 pixels tall) that will upload to the room when you click **Finish**. You can remove a room's graphic by editing the room's properties, clearing the **Use Custom Banner** checkbox, and clicking **OK** to put your change into effect.
- **Accessors for newly added objects.** Set up the permissions to add to an object when it becomes governed by the room. A chart lists which permissions will be granted each local group. Each row in the chart shows the name, and current settings of one group, with an **Edit** button leading to an editing dialog. The chart initially shows the two built-in groups, **Contributors**, and **Owners**, with the following default settings:
 - **Contributors:** RELATE, Run Procedure, Change Location.
 - **Owners:** DELETE, Run Procedure, Change Location.If additional room-level groups are created after the room is created, the chart also lists these groups, with initial permission of NONE, and no extended permissions.

The room creator can change the setting for any group by clicking **Edit** in its row to open the **Set Access Permissions: For new objects added to the room** dialog box, which contains the usual controls for setting permissions.

6. Click **Finish** to close the dialog box, and create the room.
Or, you can click **Cancel** to close the dialog box without creating a room.

7.10.7.5 Edit the properties of a room

Room owners can edit the complete set of room properties. Room members who have WRITE permission on the room can edit a subset of properties inherited from the folder type. However, only room owners can change the name of the room.

To edit the properties of a room:

1. Navigate to the location that contains the room.
2. Do one of the following:
 - Select the room, and pick **View > Properties > Info**.
 - Open the room, and click the **Properties** link on the room's home page.

The **Properties: Info** tab opens.

3. Change properties, as appropriate, and click **OK** to put them into effect for the room.

Changes you make to the **Properties: Membership** tab take effect immediately (you do not need to click **OK** first).

7.10.7.6 About room membership

Room *members* are a set of repository users, groups, and roles that are on the room's member list.

Each room member has either a **Contributor** or **Owner** role in the room.

- **Contributor** role usually grants RELATE permission over room objects. Most room members are contributors.
- **Owner** role permits member list management, and usually grants DELETE permission over room objects. Room creators are room owners by default.

Local roles are in effect only for room objects, and locations; they have no meaning outside of a room.

If a member directly assigned to the **Contributor** role is also in the **Owner** role indirectly (for example, via a group), then the **Owner** role takes precedence for that member.

Room members can belong to private, *local groups* within a room. Such local groups support custom roles within the room (**Spec Approvers**, for example). The name of a local group must be unique within the room.

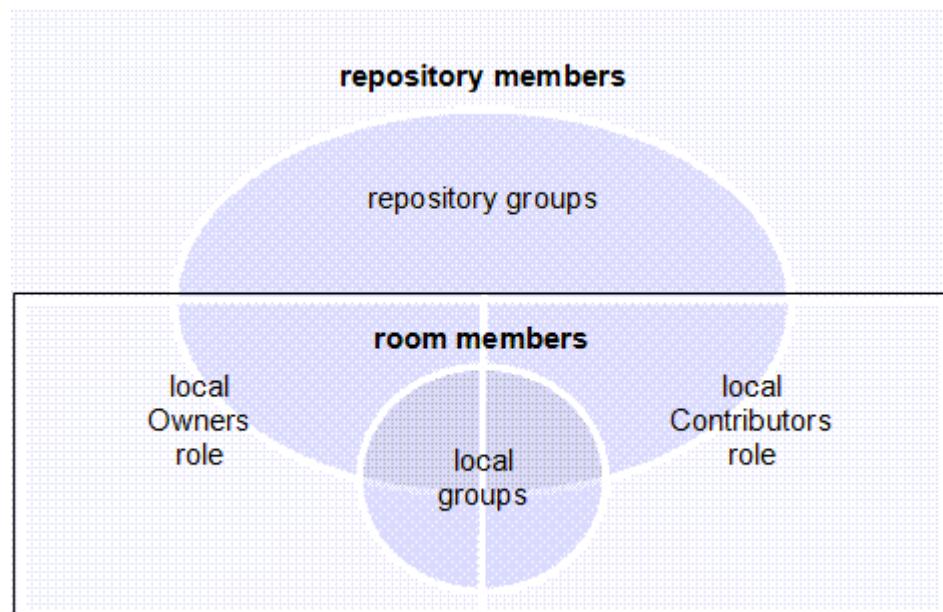


Figure 7-2: Repository members in relation to room members, groups, and roles



Note: If a repository contains more than 250 rooms, it is recommended that only users who are members of less than 250 repository groups access such repositories.

All members of a room can see the room's member list, but only room owners, and user managers can manage room membership.

To open the room member list:

- Do one of the following:
 - On the room's home page, click the **Members** link.
 - Open the **Membership** tab of room properties (**Properties: Membership**).

Columns in the room member list are as follows:

- **Name.** The name of the group or member.
- **Role.** Distinguishes owners versus contributors.
- **State.** Shows whether members have working accounts in the repository.
- **Description.** Email addresses for users, descriptions for groups.
- **Group.** Visible when the **Show Groups** checkbox is selected. If a member is not explicitly added to room, this column shows the group that grants membership to the member. (There might be multiple groups, but only the first in alphabetical order is shown.)

To see the members of a group, click the group's name. To go back up, use the navigation path above the group member list.

If you are a user manager, a button for creating a new user also appears in this dialog box.

7.10.7.7 Copy a room

You can copy a room to anywhere in a repository that a folder can be copied.

When you copy a room, the new room contains copies of everything accessible from the original. A copy of a room has the properties of the original. The local roles, and groups of the copy are duplicates of those in the original room, except that the member creating the copy is in the **Owner** role (not the owner of the original room, if different).

7.10.7.8 Move or link to a room

You can move a room anywhere in a repository that a folder can be moved.

A link to a room home page may be added anywhere in the repository that permits links.

7.10.7.9 Delete a room

Superusers, and room owners can delete a room, but any users who are *not* room members cannot delete a room, even if they have DELETE permission.

Choose one of the following options:

- **Delete just the link to[room name]** (default choice).
- **Delete the room, including its member list and local groups, and all links to it.** In this case, you must pick between deleting just the current version or all versions.

If you delete the last remaining link to a room, you are deleting the room, and must decide whether to:

- **Delete the room, its member list, and its local groups** (default choice). This action succeeds only if the home page has no links, not even hidden links to old versions, which also implies the room no longer governs anything.
- **Delete the room, its member list, its local groups, and all sub-folders and objects.** In this case, decide whether to:
 - **Delete current versions of linked objects** (default choice)
This option begins by deleting the current version of every linked object. The deletion stops, however, if the home page, and sub-folders still contain links to other versions of any of those objects, even hidden links to old versions. To be entirely deleted, the room must not have any links (not even hidden ones) to non-current versions of objects.
 - **Delete all versions of linked objects**

If you are deleting multiple objects, the deletion dialog box has multiple pages with the above choices for any room that needs it.

7.10.8 Manage room membership

Room owners, and user managers determine a room's membership. You can add members when you create or modify a room. User managers can also create new users in a room.

Once the room's members are specified, you can invite them to the room by sending an invitation. This personalizes the introduction to a room, and provides a convenient means of getting there (by clicking the link in the invitation).

To add repository users as room members:

1. On the room's **Membership** tab, click **Add**.
2. In the first dialog box, use the member picker to locate, and select the repository members, groups, and roles to add to the room's member list.
3. Click **OK** to go to the next step of assigning a role to the selected members. (Clicking **Cancel** returns to the **Membership** tab.)
4. In the second dialog box, pick the new members' role (**Contributor** or **Owner**).
5. Click **OK** to assign the role, and return to the **Membership** tab. (Clicking **Cancel** returns to the member-picking dialog box.)

To invite members to a room:

1. On the room's **Membership** tab, click **Invite**.
2. In the email dialog box that opens, click **to** and/or **cc** to select the room members you want to invite.
3. In the body of the invite, enter your message. The message initially includes a link to the rooms location.
4. Click **Send** to send the message to the specified members.
Or, click **Cancel** to close the dialog box without sending the email.

To remove members from a room:

1. On the room's **Membership** tab, click **Remove** to open the **Choose Members: Room Members** tab, which lists room members, including local groups, only.
2. In the left pane, locate, and select the room members, groups, and roles to remove from the room's member list.
3. With the members selected, click 
4. Click **OK** to remove the members from the room's member list.

The **Membership** tab opens. Members removed from a room are also removed from all local groups in the room. These members remain repository members, however, even if they are removed from a room.

To change local members' roles:

1. On the room's **Membership** tab, click **Change Role**.
2. In the first dialog box, use the standard member picker to locate, and select the room members, and groups for whom to change roles.
3. Click **OK** to go to the next step of assigning a new role to the selected members. (Clicking **Cancel** returns to the **Membership** tab.)
4. In the second dialog box, pick the members' role (**Contributor** or **Owner**).
5. Click **OK** to assign the role, and return to the **Membership** tab. (Clicking **Cancel** returns to the member-selection dialog box.)

To create a new local group:

1. On the room's **Membership** tab, click **New Group** to open the **Create New Room Group** tab.
2. Type a name for the group (required). The name must be unique among local group names in the room.
3. Optionally, type a plain text description for the group.
4. Click **OK** to create the group, and return to the room's member list.

A local group is owned by the room's Owners group (even if removed from the room). Therefore, it can be used in permission sets of governed objects only.

To edit the properties of a local group:

1. Open the room's **Membership** tab.
2. Modify group properties as appropriate, and then click **OK** to implement your changes.

To add room members to a local group:

1. On the room's **Membership** tab, click the name of the group whose membership you want to modify.
The group's member list opens.
2. On the group member list page, click **Add**.
A page for locating room members opens.
3. In the left pane, locate, and select the room members, groups, and roles to add to the group.
4. With the members selected, click .
5. Click **OK** to add the members, and return to the group's member list.

To remove a local group from a room:

1. On the room's **Membership** tab, click **Remove** to open the **Choose Members: Room Members** tab, which lists room members, including local groups, only.
2. In the left pane, locate, and select the groups to remove from the room's member list.
3. With the groups selected, click .
4. Click **OK** to remove the groups from the room's member list.

You return to the **Membership** tab.

Members removed from a room are removed from all local groups in the room, but they remain repository members. Local groups removed from a room, on the other hand, are effectively deleted from the repository.

When a local group is removed from a room, its own member list is emptied, and it no longer appears in member lists, and member pickers. It also ceases to appear on the list for setting accessors on the **Room Properties: Options** tab, under **Accessors for newly added objects**. The group remains listed on any permission sets it is already on, but its name shows that it has been deleted. It continues to be owned by the room Owners group, keeping it secure. The built-in local groups (Owners and Contributors) cannot be removed, and therefore do not appear on the Remove dialog box.

7.10.9 Manage users as a non-administrator

Collaborative projects sometimes involve repository users working with external users such as clients, auditors, or suppliers. External users typically do not have user accounts administered centrally in the repository. Such mixed groups might perform confidential or proprietary work, and can benefit from membership in the same room.

External users typically do not have user accounts administered centrally in the repository, like LDAP users do, for instance.

To address these cases, system administrators can delegate some user-management tasks to non-administrators by assigning them to the role of user Manager (**dce_user_manager**). User managers can perform a variety of user management tasks without being a system administrator. Specifically, user managers can:

- **Browse users and groups.** User managers can access a node in the repository tree called *Administration*, which contains a link to *User Management*, which links to pages for *Users*, *Groups*, and *Roles*.
- **Create new users.** In the *Administration* area, and on room member pages, user managers have access to a dialog box for creating new users.
- **Modify users.** User managers can unlist certain users, or prevent their names from appearing in the repository user list in a user picker. They can also restrict certain users' access to content.

In addition to this overview topic, the following topics describe managing users as a non-administrator:

- “Create new users” on page 665
- “Modify users” on page 666
- “Unlist users (conceal members)” on page 667
- “Restricted folders” on page 667

7.10.9.1 Create new users

User managers can create new users at the repository level in the Administration area, or in a room for which they are an owner.

To create a new user:

1. Open the **New User** dialog box in one of these ways:
 - Navigate to **Administration > User Management > Users**. Select **File > New > User**.
 - Navigate to the room to which to add a new user. Open the room's **Properties: Membership** tab by either clicking the **Members** link on the room's home page, or accessing the room's properties. Click the **New User** button.

Controls in the **New User** dialog box are disabled for user managers, except as noted in this procedure.

2. In the **Name** field, type the user's name.
3. The **User Source** property is set to **Inline Password**, and user managers cannot change it. This setting means that the user must provide a password that is stored only in the repository. There is no external authentication.
4. In the **Password** field, type the user's password. The password is encrypted, and stored in the repository.
5. In the **Password Verify** field, type the user's password again.
6. Type a **Description** for the new user (optional).
7. Type the user's **E-Mail Address**.
This is the address to which notifications for workflow tasks, and registered events are sent.
8. In the **User OS Name** field, type the user's operating system user name.
This is the user's repository user name.
9. Select a **Home Repository** for the user.
10. To prevent the user's name from being included in repository member lists, select the **Is Unlisted** checkbox. Otherwise, the user's name appears in

repository member lists, as usual. For more information on this setting, see [Unlisting users](#), later in this chapter.

11. To restrict the user's access to specific folders, cabinets, or rooms, click **Select Folder** to locate, and select them in the repository. For more information on this setting, see [Restricted folders](#), later in this chapter.



Note: To remove some containers from the restricted folder list, open it, select the folders, and click **Remove**. To remove all containers from the list, click **Clear**.

12. Select one of the following choices for the user's default folder:
 - **Choose existing folder.** Click **Select Folder** to pick a folder, cabinet or room other than the default folder */Temp*.
 - **Choose/Create folder with the user name.** This is the default choice.
13. The **Privileges**, and **Extended Privileges** settings are set to **None**. User managers cannot change these settings.
14. The user's client capability is set to **Consumer**, and user managers cannot change it.
15. Click **OK** to create the new user.

7.10.9.2 Modify users

An administrator can modify any user. A user manager can modify only those users created by someone who was, at the time, a user manager but not also an administrator. (When a user manager who is also an administrator creates a user, that user is considered to have been created by an administrator rather than a user manager.)

The user manager role (**dce_user_manager**) must be present in the repository's list of roles so that collaborative services can detect which users can be modified by user managers.

Members can be modified via the User Properties dialog, accessed in the usual manner, either at the repository level or at the room level. All controls that user managers can edit in the New User dialog, they can also edit in the User Properties dialog, with these provisions:

- Modifying a user's name does not take effect until a job is run on the server.
- To change a user's password, replace the masked-input characters (usually bullets or asterisks) with a new value in both the **Password**, and **Verify Password** fields.
- The list of folders in the **Restrict Folder Access To** list might include folders for which a user manager lacks BROWSE permission. These folders are indicated in the list by a message stating that a folder cannot be listed. To eliminate such folders from the list, a user manager can click **Clear**. Such folders do not appear in the folder picker.

7.10.9.3 Unlist users (conceal members)

An unlisted user's name does not appear to regular users in the repository user list. While a user is unlisted, the only places their names appear are:

- User lists in the Administration area.
- User list for adding people to a room (in the **New Room** dialog box or **Add Member** dialog) when viewed by a user manager.
- Member lists of rooms in which user is a member.
- Contexts where the user is already picked for some purpose, such as an permission set entry for an object, the Owner attribute of an object, a member field in a table, or a performer assignment in a Quickflow.

Unlisted users appear in user lists with [unlisted] after their names, except in room lists.

A group for unlisted users, called **dce_hidden_users**, is created at the root of the repository user list. This group is visible to administrators, and to user managers in the Administration area, and administrators should avoid renaming or deleting it. The group's description states that it is managed by collaborative services, and its child list should not be modified directly. If a group with the same name already exists, that group is used instead of a new one. If a group with the correct name cannot be found, it is created. Administrators, and user managers can open the group to view its children, but they cannot manually add users to or remove users from this group.

Unlisting affects lists, not objects. Content created by an unlisted user is unaffected. Unlisting takes effect as soon as the user manager saves the dialog box.

7.10.9.4 Restricted folders

When users have anything on their restricted folder list, their access to repository content is limited to objects that are descendants of the listed item. If the restricted folder list is empty, the user has access to all folders, and cabinets in the repository, subject to the permissions on those cabinets, and folders subject to folder security.

Folder restriction never applies to:

- Rooms in which the user is a member
- System cabinets required for participation in the repository, such as */System*, */Templates*, and */Resources*

7.11 Forms

7.11.1 Enter data in a form

A form provides fields for you to enter, and retrieve data. You open a form from a file list or from a task. When a form is attached to a task, it appears either as an attached file or as fields within the task. When you enter data in a form, the data is saved as content, properties, or both. If data is saved as properties only, the form will have a file size of zero.

To enter data in a form:

1. If the form opens automatically in a task, go to [step 3](#).
2. Navigate to the form, select it, and then select **File > Edit**.
3. Enter information as needed. For additional instructions, see “[Format text in a form](#)” on page 668.
4. To clear your changes, click **Reset**.
5. When you are done entering information, click either **Save** or **Submit**.
6. If prompted to confirm, click **Yes**.

7.11.2 Format text in a form

To format text in a form, use the buttons described in “[Icons used to format text in a form](#)” on page 668. Some of the buttons may not appear.

Table 7-18: Icons used to format text in a form

Button	Description
	Moves the selected text to your clipboard, and deletes it from the current location. In certain browsers, the browser security setting might disable this button. To move text to your clipboard, press <i>Ctrl-X</i> .
	Copies the selected text to your clipboard. In certain browsers, the browser security setting might disable this button. To copy text, press <i>Ctrl-C</i> .
	Pastes the text from your clipboard to the selected location. In certain browsers, the browser security setting might disable this button. To paste text, press <i>Ctrl-V</i> .

Button	Description
	Bolds the selected text.
	Italicizes the selected text.
	Underlines the selected text.
	Aligns the current block of text to the left margin.
	Centers the current block of text.
	Aligns the current block of text to the right margin.
	Aligns the current block of text to both the left, and right margins.
	Indents the current block of text.
	Removes the indent on the current block of text.
	Formats the selected text as subscript text.
	Formats the selected text as superscript text.
	Formats the selected text as a numbered list.
	Formats the selected text as a bulleted list.
	Changes the color of the selected text.
	Changes the background color of the selected text.
	<p>Undoes the previous action.</p> <ul style="list-style-type: none"> • Undo does not apply to actions taken by using the right-click menu. • Undo does not apply to changes made to tables. • Some browsers might not let you undo the modification of background color.
	Restores the action that had been undone.

Button	Description
	Inserts an image.
	Turns the selected text into a hyperlink.
	Inserts a table from your clipboard. The table can be in HTML, RTF, or Microsoft Word format.
	Checks spelling.
	Displays the HTML source for the text.

7.11.3 Create a new form

When you create a new form, the form is based on a template that determines the form's fields. Developers create form templates by using Documentum Forms Builder. To use form functionality, you must be assigned the user role of `form_user`, which is defined by the Forms DocApp.

When creating forms, make sure that the form does not store the metadata. If metadata is stored, then if the formal folder/cabinet inherits a retention policy, no one can modify the metadata (as the content of the form is protected). This applies to a formal folder (which normally inherits retention from the file plan).

To create a form:

1. Navigate to where the form will be created.
2. Select **File > New > Form**.
3. In the **Form Name** field, enter a name for the new form.
4. In the **Template** field, select the form template used to create the form.
5. Click **Next**.
6. To enter data in the form, see “[Enter data in a form](#)” on page 668.

7.11.4 Save As functionality

The **File > Save As** functionality in Documentum Webtop is enabled only when you work with Forms. This functionality allows you to save a new Form instance with the same set of permissions.

7.12 Virtual documents

7.12.1 Virtual documents overview

A virtual document is a file that contains one or more files nested within it. The virtual document is also called the parent document, and the files within it are called descendants or children.

For example, you could create a virtual document for a book, and populate the virtual document with the files that comprise the book's chapters. Each chapter is a separate file that is nested within the parent document.

The files nested in a virtual document can themselves be virtual documents. This means you can have multiple levels of nesting.

When you check out a virtual document, you can select whether to check out only the parent document, or check out the parent document, and its descendants.

When you view a virtual document, you can select whether to view the document's structure or its content. When you view its structure, Virtual Document Manager (VDM) opens to display the virtual document's descendants.

A virtual document can contain descendants of different file formats. For example, a Microsoft Word file could be the parent file, and its descendants could be an Excel spreadsheet, and TIFF image.

You can add, remove, and rearrange descendants in a virtual document. You can convert a virtual document back to a simple document that contains no descendants.

Virtual documents are designated by this icon:



7.12.2 Create a virtual document

To create a virtual document, you convert a simple document to a virtual document. This document becomes the parent document, to which you can add descendants.

To create a virtual document:

1. Navigate to, and select the file to be converted.
2. Select **Tools > Virtual Document > Convert to Virtual Document**.
3. Add descendants, as described in “[Add a descendant to a virtual document](#)” on page 673.

7.12.3 View the structure of a virtual document

When you view the structure of a virtual document, Virtual Document Manager (VDM) opens to display the virtual document's descendants. From VDM, you can add, remove, or change the location of descendants within the virtual document. You can also perform standard file operations on descendants by using the procedures you would use for any file in the repository.

To view the structure of a virtual document:

1. Navigate to the virtual document.
2. Select the virtual document.
3. Select **Tools > Virtual Document > View Virtual Document**.
4. To display the descendants in the navigation pane, do one of these:
 - To display the next level of descendants, click the plus sign (+) next to the virtual document.
If a descendant is itself a virtual document, view its descendants by clicking its plus sign (+).
 - To display all descendants, select the virtual document, and then select **Display > Expand selection**
5. To simultaneously display both the repository directory structure, and the virtual document structure, select **Display > Show all**.
To hide the repository directory structure, select **Display > Show virtual document**.

7.12.4 View the content of a virtual document

When you view the content of a virtual document, the content opens in an editing application.

If the repository includes XML functionality, and if you view an XML-based virtual document, you can view both the parent, and descendants in a single, read-only file. If there is no content in a virtual document, then Virtual Document Manager (VDM) automatically displays the virtual document's structure.

To view the content of a virtual document in read-only mode:

1. Navigate to the virtual document, and select it.
2. Select **File > Open (Read Only)**.
Records Client does one of three things, depending on how your opening options are set in your virtual documents preferences, as explained in “[Set your virtual document preferences](#)” on page 679.
3. Do one of these:

- If Records Client displays the document's content, skip the rest of this procedure.
- If Records Client prompts you to select between content, and structure, select **Open the content of the document**, and then click **OK**.
- If Records Client displays the document's structure through VDM (instead of displaying its content through an editing application), then select the document name within the header of VDM, and then select **File > Open (Read Only)**.

7.12.5 Add a descendant to a virtual document

To add a descendant, you must have adequate permissions for accessing the parent document. You can add the same document to a virtual document more than once.

To add a descendant to a virtual document:

1. Do one of these:
 - To select the descendant now, navigate to the descendant, and add it to your clipboard.
 - To select the descendant later or to create a new file as the descendant, skip this step. You will select the descendant later in this procedure.
2. Navigate to the parent document, and view its structure. For instructions on viewing the structure, see ["View the structure of a virtual document" on page 672](#).
3. Do one of these:
 - To use a descendant from your clipboard, select **Tools > Virtual Document > Add Child > From Clipboard**, then select the descendant, and then click **OK**.
 - To navigate to the descendant in the repository, select **Tools > Virtual Document > Add Child > From File Selector**, select the descendant, and click **OK**. For detailed steps see ["Locate an item in a selection dialog box" on page 543](#).
 - To create a new file to be used as the descendant, select **Tools > Virtual Document > Add Child > Using New Document**.

If the parent document is not already checked out to your computer, Records Client checks it out. If the intended parent is not a virtual document, the system automatically converts the document to a virtual document.

4. If you chose to create a new file to be used as the descendant, then create the new file by using the standard procedure for creating a new file. Otherwise, skip this step.
5. Check in the parent document as follows:

- a. Select the parent document.
- b. Select **Tools > Virtual Document > Save Changes**.
- c. Click **OK**.
- d. Select checkin options, and click **OK**.

The new descendant is added as the last descendant in the parent document.

To add descendants by drag-and-drop:

1. Navigate to the parent document, and view its structure in the navigation pane.
2. In either the content pane or a new window, navigate to the files to add as descendants.



Note: To open a new window, select **Tools > New Window**.

3. Drag-and-drop the files from **step 2** to the appropriate location in the parent, dropping the files by positioning your mouse pointer either high, low, or midway on an existing descendant, as described in “Position of your mouse pointer when you use drag-and-drop in a virtual document” on page 675.

A shortcut menu appears.

4. In the shortcut menu, select **Add here**.

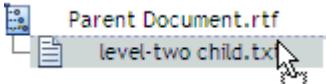
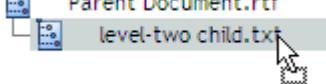
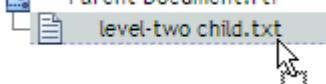
The file is added to the parent document. If you did not select a specific location within the descendants, the file is added as the last descendant in the document. If the intended parent is not a virtual document, the system automatically converts the document to a virtual document.

If the parent document is not already checked out to your computer, Records Client checks it out.

5. Check in the parent document as follows:

- a. Select the parent document.
- b. Select **Tools > Virtual Document > Save Changes**.
- c. Click **OK**.
- d. Select checkin options, and click **OK**.

Table 7-19: Position of your mouse pointer when you use drag-and-drop in a virtual document

Mouse pointer	Result
Position the mouse pointer high on the target file, as shown here. 	The added files become the descendants that come before the target file in the order of descendants.
Position the mouse pointer midway on the target file, as shown here. 	The added files become descendants of the target file. If the target file is a simple document, Records Client converts it to a virtual document.
Position the mouse pointer low on the target, as shown here. 	The added files become the descendants that come after the target file in the order of descendants.

7.12.6 Rearrange descendants in a virtual document

To reorder descendants in a virtual document:

1. Navigate to the virtual document, and view its structure, as described in “[View the structure of a virtual document](#)” on page 672.)
2. Select the parent document.
3. Select **Tools > Virtual Document > Reorder Children**.
4. Select the descendant.
5. Click **Up** or **Down** to move the descendant up or down in the list.
6. Repeat step 4, and step 5 for each descendant to be reordered.
7. Click **OK**.
If the parent document is not already checked out to your computer, Records Client checks it out.
8. Select the parent document.
9. Select **Tools > Virtual Document > Save Changes**.
10. Click **OK**.
11. Select your checkin options, and click **OK**.

To move descendants to other locations in a virtual document:

1. Navigate to the virtual document, and view its structure, as described in “[View the structure of a virtual document](#)” on page 672.
2. In either the tree pane or a new window, navigate to the descendant.



Note: To open a new window, select **Tools > New Window**.

3. Drag-and-drop the descendants to the appropriate location in the parent, dropping the descendants by positioning your pointer either high, midway, or low on another descendant, as described in “[Position of your mouse pointer when you use drag-and-drop in a virtual document](#)” on page 675.

A shortcut menu appears.

4. In the shortcut menu, click **Reposition**.

If the parent document is not already checked out to your computer, Records Client checks it out.

5. Check in the parent document as follows:

- a. Select the parent document.
- b. Select **Tools > Virtual Document > Save Changes**.
- c. Click **OK**.
- d. Select your checkin options, and click **OK**.

7.12.7 Remove a descendant from a virtual document

When you remove a descendant from a virtual document, the descendant's parent document will be checked out for you if it is not already checked out. Removing descendants does not delete the files from the repository. It only removes the files from the virtual document structure.

To remove a descendant from a virtual document:

1. Navigate to the virtual document, and view its structure, as described in “[View the structure of a virtual document](#)” on page 672.

2. Select the descendants to remove.

3. Select **Tools > Virtual Document > Remove Child**.

If the parent document is not already checked out to your computer, Records Client checks it out.

4. Check in the parent document as follows:

- a. Select the parent document.
- b. Select **Tools > Virtual Document > Save Changes**.

- c. Click **OK**.
- d. Select your checkin options, and click **OK**.

7.12.8 Specify that a certain version of a descendant is always used

You can specify that a particular version of a descendant is always used when a virtual document is opened or exported. Typically, a virtual document always uses the CURRENT version of a descendant. But you can set a binding rule that specifies that another version is used.

If the version of the descendant is missing, then the virtual document has a *broken binding*. In your preferences, you select whether to have Virtual Document Manager (VDM) display or ignore broken bindings. See “[Set your virtual document preferences](#)” on page 679.

To specify that a certain version of a descendant is always used:

1. Navigate to, and select a descendant document in a virtual document. You can navigate to a descendant by viewing the structure of the virtual document, as described in “[View the structure of a virtual document](#)” on page 672.
2. Select **Tools > Virtual Document > Fix to Version**.
If the parent document is not already checked out to your computer, Records Client checks it out.
3. In the **Always Use** field, select the version to fix to the virtual document.
4. Click **OK**.
5. Check in the parent document as follows:
 - a. Select the parent document.
 - b. Select **Tools > Virtual Document > Save Changes**.
 - c. Click **OK**.
 - d. Select your checkin options, and click **OK**.

7.12.9 Set a version label for a virtual document

To set a version label for a virtual document:

1. Navigate to the virtual document, and select it.
2. Select **Tools > Virtual Document > Modify Version Labels**.
3. Enter a version label.
4. To apply the version label to all descendants of the virtual document, check **apply to all descendants**.
5. Click **OK**.

7.12.10 Create an archive of a virtual document

A archived of a virtual document is called a snapshot.

To view a list of snapshots created for a virtual document:

1. Navigate to the virtual document, and select it.
2. Select **View > Snapshots**.

To create a snapshot:

1. Navigate to the virtual document, and select it.
2. Select **Tools > Virtual Document > New Snapshot**.
3. In the **Create** tab, do these:
 - a. Enter a name for the snapshot.
 - b. Select a location for the new snapshot.
 - c. Select the type of snapshot.
 - d. To freeze the snapshot, make sure **Freeze Snapshot** is checked. This should be checked by default. By freezing the snapshot, you ensure that the frozen version of the document, and frozen version of each descendant cannot be changed without creating a new version.
4. On the **Info** tab, set properties as described in “[Common tabs in the Properties dialog box](#)” on page 551 in the topic “[Set properties](#)” on page 550.
5. Set information in any remaining tabs as appropriate. For information on the functionality affected by those tabs, see the topic in this guide that covers that functionality.
6. Click **Finish**.

To freeze or unfreeze a snapshot:

1. Navigate to the snapshot, and select it.

2. Select one of these:

- **Tools > Virtual Document > Freeze Snapshot**

Freezing a snapshot blocks users from editing the frozen version of the document or the frozen version of each descendant. Any changes a user makes to the document or a descendant can be saved only as a new version of the document or descendant.

- **Tools > Virtual Document > Unfreeze Snapshot**

Unfreezing a snapshot lets users again edit the document, and descendants without versioning. However, if a descendant is part of multiple frozen snapshots, then you must unfreeze all the snapshots to edit the descendant.

7.12.11 Convert a virtual document to a simple document

You can convert a virtual document to a simple document only if the virtual document has no descendants.

To convert a virtual document to a simple document:

1. Navigate to the virtual document.
2. If you have not already done so, remove all descendants from the virtual document. See “[Remove a descendant from a virtual document](#)” on page 676.
3. Select the virtual document.
4. Select **Tools > Virtual Document > Convert to Simple Document**.

7.12.12 Set your virtual document preferences

To set your virtual document preferences:

1. Select **Tools > Preferences**.
2. Select the **Virtual Documents** tab, and complete the fields in “[Virtual document preferences](#)” on page 680.

Table 7-20: Virtual document preferences

Property	Description
Opening options	<p>Select what happens when you open a virtual document by clicking its name. This does not apply if the virtual document is already opened in Virtual Document Manager (VDM):</p> <ul style="list-style-type: none"> • View structure: When you click the virtual document's name, the first level of nested files appears. • View content: When you click the virtual document's name, a read-only copy of the content appears. • Prompt each time: When you click the virtual document's name, you are prompted to select to display the structure or the read-only content. <p>If there is no content in a virtual document, then VDM automatically displays the virtual document's structure, regardless of how you set this preference.</p>
Bindings	<p>Select whether VDM shows broken bindings. A binding is broken if VDM cannot find the version of a component specified by the component's binding rule</p>
Copy	<p>Select what happens when you copy a virtual document to your clipboard. You can select one of these:</p> <ul style="list-style-type: none"> • Root only: Copies the content, and properties of the parent file only. • Root and descendants: Copies the parent file, and all the descendants nested in the parent file, including descendants of descendants, and so on. • Root and link to existing descendants: Copies the parent file, and references the descendants. • Prompt me each time: Prompts you to select what to copy.
Checkout	<p>Select what happens when you attempt to check out an item that is locked by another user:</p> <ul style="list-style-type: none"> • Download as read-only: Downloads a copy of the item as read-only. • Prompt me each time: Prompts you to select whether to download as read-only.

3. To save your changes, click **OK**.

7.13 PDF annotations

7.13.1 PDF annotations overview

If your organization has installed the OpenText Documentum CM PDF Annotation Service, then you can store comments created in Adobe Acrobat or Reader into a repository. You can view, and enter comments in PDFs directly from Records Client.

Comments are associated with a specific version of a document. If a document is versioned, the comments on the previous version are not migrated to the new version.

Example: If you check out a 1.0 CURRENT version of a document, and then a second user adds comments to the document, the comments are associated with the 1.0 version. If you then check in, and change the version number to 1.1, then when you view the 1.1 CURRENT version, you will not see the comments from the 1.0 version.

To use PDF Annotation Services, you must configure Records Client to open PDF Annotation Service when you view a PDF.

7.13.2 Configure PDF Annotation Service to open when user views a PDF

To configure PDF Annotation Service to open when a user views a PDF:

1. Select **Tools > Preferences**.
2. Select the **Formats** tab.
3. In the **Choose object type** list, select **Document (dm_document)**.
4. In the **Object's primary format** list, select **Acrobat PDF (pdf)**.
5. In the **Application for viewing** list, select **Comment**.
6. If appropriate, repeat **step 3** to **step 5** for documents of other formats (such as Microsoft Word). If doing so, do not select **Acrobat PDF (pdf)** in **step 4**. Instead, select the appropriate format.

7.13.3 Add comments to a PDF document

To add comments to a PDF document:

1. Navigate to a PDF document.
2. Select the document, and then select **File > Open (Read Only)**.

The PDF opens in read-only mode in a separate window, with its comments.

If you use Internet Explorer, then the browser also launches an extra blank page. To avoid this, select the Internet Explorer **Tools > Internet Options** menu option, then select the **Advanced** tab, and make sure the **Reuse windows for launching shortcuts** option is specified.

3. To add comments, use the Acrobat commands for doing so. For more information, see your Acrobat documentation.
4. To save your comments to the repository, click Adobe's **Send and Receive Comments** button.

Comments that are saved in a repository have the Acrobat .XFDF format.

7.13.4 View comments in a PDF document

To view comments in a PDF document:

1. Navigate to a PDF document.
2. Select the document, and then select **File > Open (Read Only)**.

The PDF opens in a separate window, with its comments.

If you use Internet Explorer, then the browser also launches an extra blank page. To avoid this, select the Internet Explorer **Tools > Internet Options** menu option, then select the **Advanced** tab, and ensure that the **Reuse windows for launching shortcuts** option is specified.

7.14 Relationships

A relationship is a connection between two items in a repository. Relationships allow Records Client to process the items together. Relationships also allow users to access certain items by first accessing other related items. For example, if a document has been annotated by several reviewers, and if each annotation has a relationship to the original document, a user can access the annotations by viewing the document's relationships.

To view an item's relationships:

1. Navigate to the item, and select it.
2. Select **View > Relationships**.

To create a relationship between two items:

1. Navigate to the item to be the parent, and select it.
2. Right-click the item, and select **Add Relationship**.
3. In the selection area, select the item to relate to this item, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
4. Click **Next**.
5. In the **Relationship** list, select the type of relationship.
6. Click **Finish**.

To create a relationship between two items by drag-and-drop:

1. Navigate to either of the items.
2. If the other item is in a different location, open an additional browser window by selecting **Tools > New Window**, and then navigate to the other item.
3. Drag-and-drop the child item to the parent item.
4. In the **Relationship** list, select the type of relationship.
5. Click **Finish**.

To remove a relationship between two items:

1. Navigate to either of the items, and select it.
2. Select **View > Relationships**.
3. Select the relationship to remove.
4. Click **File > Remove Relationship**.
5. Click **OK**.

7.15 Renditions and transformations

7.15.1 Renditions and transformations overview

A rendition is an alternate copy of a file or an alternate file that is associated with an original file. For example, a rendition can be a copy of an image in a different file format or in a different resolution.

You can display all of a file's renditions by selecting the menu option **View > Renditions**.

You can create renditions outside the repository, and import them in, or you can generate renditions within Records Client, through transformation.

Transformations let you automatically transform the look, and format of an existing file in order to create a new rendition associated with the original file.

When transforming a file, you choose a preset transformation task, and enter any applicable transformation parameters. The transformation profiles that are available for a given file depend on the file's format, and the OpenText Documentum CM products installed, and configured for the repository.

Transformations occur on one item at a time, and are processed asynchronously, meaning that transformed items, and renditions might not be immediately available. You receive a notification when a transformation is completed or if a transformation fails.

When a file is versioned, its renditions, including any thumbnail renditions, are not carried forward with the new version of the file automatically. If you create a new version of the file, the renditions remain with the previous version. However, Records Client may automatically generate new renditions when you check in, and version a file if it was selected during rendition creation. See [“Creating a rendition through transformation” on page 686](#) for more information on automatically updating a rendition upon versioning.



Notes

- Some rendition, and transformation functionality is available only on repositories that are configured with OpenText™ Documentum™ Content Management Transformation Services products. Without the presence of these products, some rendition, and transformation functions described in this guide may not be available.
- Records Client does not allow multiple renditions of the same format. Therefore, for any new renditions created, Records Client replaces any existing renditions of the same format. For example, a Microsoft Word document can only have one Acrobat PDF rendition at any time.

7.15.2 Viewing a list of the different renditions of a file

To view a list of the different renditions of a file

1. Navigate to, and select a file.
2. Select **View > Renditions**.

Records Client shows all of the renditions for the file.

7.15.3 Importing a rendition

To import a file from outside the repository to use as a new rendition for an existing repository file

1. Navigate to, and select a file for which to import a rendition.
2. Select **File > Import Rendition**.
3. In the **File to Import** field, enter the file to import. You can type the path to the file, or you can browse to locate the file.
4. In the **Format** field, select the rendition's file format if the correct format does not appear automatically.
5. Click **OK**.

The file is imported as a rendition of the primary rendition.

7.15.4 Transforming a document to PDF or HTML format

Records Client uses Transformation Services products to provide the functionality to transform documents to PDF or HTML format. When a document is selected for transformation to PDF or HTML format, the request is sent to a queue where it awaits processing by the Transformation Services product. The default transformation parameters are used for that document type. When processing is complete, a new file in either PDF or HTML format is stored in the original's list of renditions.

It may also be possible, depending on what other OpenText Documentum CM products are installed on your system, to transform a document to PDF or HTML formats with options. See “[Creating a rendition through transformation](#)” on page 686, and “[Creating a related file through transformation](#)” on page 687 for more information.

To transform a document to PDF or HTML

1. Navigate to, and select a document to transform to PDF or HTML.
You can transform a parent file or another rendition. (Locating renditions is described in “[Viewing a list of the different renditions of a file](#)” on page 684.)
2. Select **Tools > Transform > PDF Rendition** or **Tools > Transform > HTML Rendition**.
The transformation request is immediately sent to the appropriate queue for processing, and appears in the renditions list for the parent file when it is completed.

7.15.5 Creating a rendition through transformation

Records Client uses Transformation Services products to transform a file using a set of properties in order to create a new rendition.

Transformations to create new renditions occur on one item at a time, and requests are processed asynchronously, meaning that new renditions may not be available immediately. You receive a notification in your Inbox when a transformation is completed or if a transformation fails.



Caution

Not all features mentioned in the following procedure are available for all file formats, and some file formats cannot be transformed. Format availability depends on the Content Transformation Services products installed, and any special configuration on your system.

To create a new rendition through transformation

1. Navigate to, and select the file to transform to create a new rendition.

Note: You can transform a parent file or another rendition. (Locating renditions is described in “Viewing a list of the different renditions of a file” on page 684.)
2. Select **Tools > Transform > More Formats**.
3. The **Transform** wizard appears. Do the following:
 - a. Select a transformation profile, and click **Next**.
 - b. If the **Transformation Details** screen appears, enter any information necessary for setting the parameters of the transformation, and click **Next**.
 - c. In the **Save As** screen, select **Create a New Rendition**, and click **Next**.
 - d. In the **Rendition Definition** screen, complete the fields as required. At this time, you may choose to save the transformation so that it is performed each time the file is versioned.
 - e. If you have selected multiple files for this transformation, click **Next**. Alternatively, if you wish to apply the selected parameters to all of the files selected for the transformation, or if you have selected only one file to transform, click **Finish**.

The transformation request is immediately sent to the appropriate server queue for processing. When the transformation is complete, a notification is sent to your Inbox.

7.15.6 Creating a related file through transformation

Records Client uses Transformation Services products to transform a file using a set of properties in order to create a new related file.

Transformations to create new related files occur on one item at a time, and requests are processed asynchronously, meaning that new files may not be available immediately. You receive a notification in your Inbox when a transformation is completed or if a transformation fails.



Caution

Not all features mentioned in the following procedure are available for all file formats, and some file formats cannot be transformed. Format availability depends on the Content Transformation Services products installed, and any special configuration on your system.

To create a new related file through transformation

1. Navigate to, and select the file to transform to create a new related file.
You can transform a parent file or a rendition. (Locating renditions is described in ["Viewing a list of the different renditions of a file" on page 684](#).)
2. Select **Tools > Transform > More Formats**.
The **Transform** wizard appears.
3. Select a transformation profile, and click **Next**.
4. If the **Transformation Details** screen appears, enter any information necessary for setting the parameters of the transformation, and click **Next**.
5. In the **Save As** screen, select **Create a New Object**, and click **Next**.
6. The **New Object Definition** screen enables you to enter or apply properties for the new files. This includes name, title, permission set, lifecycle, and location. The only required property is the name. This screen also enables you to choose whether to perform this transformation every time these new files are versioned.

Do the following:

- a. Enter a name for the new file. The file name is entered by default.
- b. If you wish, enter a title for the file.
- c. If you wish, select an alternate object type for the file.
- d. Click **Edit** to enter an alternate permission set to the file.
- e. To apply a lifecycle to the files, click **Edit**.
- f. Select the location for the new file. You have two options:
 - **Same as parent file**

- Places the new file in the same cabinet or folder location as the original.
 - **New location**
 - Requires you to select a new location in an edit window.
- g. To perform this transformation each time the original file is versioned, click **Save Transformation**.
7. If you have selected multiple files for this transformation, click **Next**. Alternatively, if you wish to apply the selected parameters to all of the files selected for the transformation, or if you have selected only one file to transform, click **Finish**.
- The transformation request is immediately sent to the appropriate server queue for processing. When the transformation is complete, a notification is sent to your Inbox.

7.16 Presets

7.16.1 Presets overview

A preset determines the selections or actions available in particular situations. Creating a preset offers a way to reduce screen options to those options that are relevant to the user's task in the particular situation.

A preset is assigned to a particular item or set of items. For example, a preset could be assigned to a particular user group. Or a preset could be assigned to a particular user group when combined with a particular folder location. The item or set of items is called the preset's *scope*. The scope assigned to each preset must be unique.

A preset comprises one or more rules. Each rule determines the selections or actions available within a specific functional area. For example, a rule can determine available lifecycles, available actions, or available autocomplete text. For a list of the functional areas for which you can create rules, see "[Preset rules](#)" on page 690:

When you create a preset for a folder, the rules apply not only to files that are created in the folder, but also to files that are imported into the folder. For example, after importing a file into a folder that allows only LifecycleA to be applied, the user would not be able to apply LifecycleB to that file. In addition, Preset rules descend to subfolders.

The default order of precedence for applying presets is as follows: a preset for a location takes first precedence; then a preset for a user; then a preset for a role; then a preset for an object type. Customized installations might vary.

To access presets, navigate to **Administration / Presets**.

It is important to note that presets are not used to provide security.

7.16.2 Create a preset

To create a new preset:

1. Navigate to **Administration / Presets**.
 2. Select **File > New > Preset**. The Presets:Setup page is displayed.
 3. Enter a name and description for the preset.
 4. Select the user, role, or group to apply the preset to, by clicking **Select** in the **Apply to a User/Role/Group** field, selecting the relevant user, role, or group, and clicking **OK**. For more information, see the [Locate an item in a selection dialog box](#) section.
 5. Select the repository location to apply the preset on, by clicking **Select** in the **Apply to existing location** field, selecting the relevant repository location, and clicking **OK**. For more information, see the [Locate an item in a selection dialog box](#) section.
 6. Select the type of item the preset is to apply to by clicking **Select** next to the **Apply to specific type** field, selecting the relevant item, and clicking **OK**. For more information, see the [Locate an item in a selection dialog box](#) section.
 7. Select whether the new preset applies to all repositories or just to the current repository by clicking **Select** in the **Apply to specific repository** field, selecting the relevant repository, and clicking **OK**. For more information, see the [Locate an item in a selection dialog box](#) section.
 8. Click **Next**.
- The **Rules** tab is displayed.
9. Optionally, you can use an existing preset as a template for the new preset. To use an existing preset as a template for the new preset, click **Select** next to the **Start with another preset** option, select the existing preset, and click **OK**.
 10. To define preset rules, see “[Edit preset rules](#)” on page 690.

7.16.3 Edit an existing preset

To edit a preset:

1. Navigate to **Administration / Presets**, and select the preset.
2. Select **File > Edit**.
3. To edit the **Rules** tab, see “[Edit preset rules](#)” on page 690.

7.16.4 Edit preset rules

This procedure assumes you have opened a preset by either creating a new preset or editing an existing one.

To edit preset rules:

1. In the **Rules** tab, in the first list, select the type of rule. For rule descriptions, see “[Preset rules](#)” on page 690.
2. In the **Available** list, do one of these:
 - For the **Actions** rule: Select the action to exclude, and click the arrow to move your selection to the **Excluded** list box. To display additional actions, use the fields above the list.
 - For the **Attributes** rule: Select an object type, then select an property, then type in the values to be available as auto-attributes for that property, and then click **Apply**.
 - For the **Navigation** rule: Select the repository nodes available when a user logs in, and in the **Section to start in** field, select which node is the first node that opens when the user logs into a repository.
 - For all other rules: Select the item to which to give access, and click the arrow to move your selection to the **Selected** list box. To display additional values, use the fields above the list.

The rules you have selected for this preset appear in the summary at the bottom of the page.

3. To select another rule or another rule value, return to [step 1](#)
4. Click **Finish**.

7.16.5 Preset rules

See “[Preset rules](#)” on page 690 for an explanation of the functions you can assign to a preset.

Table 7-21: Preset rules

Preset rule	Description
Permissions	The permission sets that can be assigned to an item.
Formats	The file formats that can be assigned to new, imported, or checked in files. Additional formats based on the file's extension might also be available.

Preset rule	Description
Types	<p>The repository object types that can be assigned to new or imported files.</p> <p>Each item in a repository has an associated object type. The object type defines the characteristics of the item. For example, there is an object type for documents, an object type for folders, and an object type for email messages. Your organization can create customized object types.</p>
Groups	The filters available for narrowing a list of users or groups in a selection list for a permission set or quickflow.
Workflows	The workflow templates available for starting a new workflow.
Lifecycles	The lifecycles available to assign to a file. Note that when a user assigns a lifecycle to a file, the list of available lifecycles might be narrowed further by the file's object type.
Templates	The templates available for creating new files. Note that when a user selects a template for creating a new file, the list of templates might be narrowed further by the type, and format of the file the user is creating.
Actions	The menu items, tool buttons, action links, and action buttons available.

Preset rule	Description
Attribute	<p>The default values available for a property when a file is created or linked. This setting follows these rules:</p> <ul style="list-style-type: none"> • If a property is single-valued, and the value is already set, the existing value is not overridden. • If the property is multi-valued, the specified value is added. • If the data dictionary does not allow the value, the value is not set. <p>If the auto-attribute set of values gets out of synchronization with the data dictionary, the data dictionary set of values is presented to the user.</p> <ul style="list-style-type: none"> • If this setting is applied to a folder, it is applied to all files imported into the folder. When a preset is modified, the changes apply only to newly created items. • If this setting is applied to a user, role, or group, it is applied to all files created by that user or the users in that role or group. • These cannot have preset values: the object_name attribute, the a_content_type attribute, read-only attributes. If an attribute is read-only because of an item's current lifecycle, and state, the auto-attribute value is not set. • Preset attributes are limited to these types: string, integer, double. • For import, if all mandatory attribute values are set by the auto-attribute preset, the import is silent after the user selects files for import.
Navigation	<p>The repository nodes available. This applies only when the preset is assigned to a user, group, or role. When you select this rule, you choose the repository nodes available, and you also designate which node is the first node that opens when a user logs in.</p>

7.16.6 Remove a preset from an item

To remove a preset from an item:

1. Navigate to **Administration / Presets**, and select the preset.
2. Select **File > Edit**.
3. Click **Select** next to the type of item the preset applies.
4. In the selection dialog box, clear the item by selecting it, and clicking the remove arrow.

7.16.7 Delete a preset

When you delete a preset, it is removed from all the items that use it.

To delete a preset:

1. Navigate to **Administration / Presets**.
2. Select the preset.
3. Select **File > Delete**.
4. To view technical information, click **Help**.
5. At the warning prompt, click **Continue**.

7.16.8 The Documentum Webtop Express preset

The Records Client Express preset governs repository access for users who are given the express_user role. The Records Client Express preset is intended for users who need only limited access to repositories. “[Express user capabilities](#)” on page 693 describes the access granted by the Records Client Express preset.

Administrators who belong to the dmc_wdk_presets_coordinator role can edit the Records Client Express preset. To edit the Records Client Express preset, use the usual procedure for editing a preset.

Table 7-22: Express user capabilities

Preset	Values
Formats	None Text PDF all MS Office formats
Types	dm_document dm_folder
Templates	Displays templates that correspond to formats

Preset	Values
Actions	Document: Content transfer, subscriptions, email, quickflow, Properties, clipboard actions, create, delete Excluded: Relationships, export to CSV, favorites, notifications, lifecycle, and virtual document actions, tools (most); new workflow template, room, form, cabinet
Locations	My Home Cabinet Cabinets Subscriptions Recent Files Inbox (not Searches, Categories, Administration)

7.17 Permission sets

7.17.1 Permission sets overview

Each item in the repository has a permission set that determines who can access the item. The permission set lists the users, and groups who have access to the item, and specifies the level of access given to each. For example, a permission set might give one user permission only to view an item, while it gives another user additional permissions to edit, and delete the item.

The permission set specifies the level of access by assigning each user or group basic permissions, and extended permissions. For descriptions see “[Basic permissions](#)” on page 694, and “[Extended permissions](#)” on page 695.

When you create a new item in the repository, you choose the permission set that is assigned to the item. If you do not choose a permission set, Records Client automatically assigns the permission set specified in your user properties as your default permission set.

To access permission sets, navigate to **Administration / Security**.

7.17.2 Basic permissions

When adding a user or group to a permission set, you assign the user or group one of the permission levels described in “[Basic permissions](#)” on page 694.

Table 7-23: Basic permissions

Permission level	Permissions
None	No access is permitted to the item.
Browse	User can view the item's properties but not the item's content.
Read	User can view both the properties, and content of the item.

Permission level	Permissions
Relate	User can add annotations to the item.
Version	User can modify the item's content, and they can check in a new version of the item (with a new version number). The user cannot overwrite an existing version or edit the item's properties.
Write	User can edit item properties, and check in the item as the same version.
Delete	User can delete items.

7.17.3 Extended permissions

You can add one or more extended permission to a user or group's basic permission level in a permission set. Extended permissions are described in “[Extended permissions](#)” on page 695.

Table 7-24: Extended permissions

Extended permission	Description
Execute Procedure	User can change the owner of an item, and can run external procedures on certain item types.
Change Location	User can move the item.
Change State	User can change the item's lifecycle state.
Change Permission	User can modify the item's permissions.
Change Ownership	User can change the owner of the item
Extended Delete	User can delete the item.

7.17.4 Create or edit a permission set

To create or edit a permission set:

1. Navigate to **Administration / Security**.
2. Do one of these:
 - To create a new permission set, select **File > New > New Permission Set**.
 - To edit an existing permission set, navigate to, and select the permission, and then select **View > Properties > Info**.
3. Enter or edit the name of the permission set.

4. To change who owns the permission set, click **Select Owner**, select the new owner, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
5. In the **Class** field, select one of these:
 - **Regular**
The permission set can be used only by the user or group that creates it. Any user or group in the repository except the repository owner can create a regular permission set.
 - **Public**
The permission set can be used by anyone in a repository. Any user or group in the repository can create a public permission set. Public permission sets can be modified or deleted only by the permission set owner, a superuser, a system administrator, or the repository owner. If the repository owner is the owner of a particular permission set, it is called a system permission set.
6. Click **Next** to open the **Permissions** tab.
By default, a permission set includes the **dm_owner** user, and the **dm_world** group. The **dm_owner** user is the user who is the owner of the permission set. The **dm_world** group is the group that contains all repository users.
7. To edit the **Permissions** tab, see “[Edit permissions](#)” on page 696.

7.17.5 Edit permissions

To edit permissions:

1. If already viewing the **Permissions** tab, go to [step 2](#). If you are not already viewing the **Permissions** tab, select a file or permission set, and then select **View > Properties > Permissions**.
You can edit permissions for multiple items at once by selecting multiple items, and selecting **View > Properties > Permissions**. The **Permissions** tab displays only the values that are common to all the items selected.
2. To assign a different permission set, click **Select**, select the permission set, and click **OK**. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
3. To change the assigned permission levels, do these in the **Additional Permissions** or **Additional Common Permissions** area (depending on which is displayed):
 - a. To add users or groups, and assign them permissions, click **Add**, select the users or groups, and click **OK**. Go to [c](#) on page 697.
 - b. To edit permissions for users or groups, select the users or groups, and click **Edit**.

- c. In the **Basic Permissions** list, select the permission level for the user or group. For descriptions of basic permissions, see “[Basic permissions](#)” on page 694.
 - d. In the **Extended Permissions** list, select any extended permissions to give the user or group. For descriptions of extended permissions, see “[Extended permissions](#)” on page 695.
 - e. Do one of these:
 - If you did one of these, click **Finish**:
 - Selected just one user or group.
 - Selected multiple users or groups but will apply the same level to all remaining ones.
 - If you selected multiple users or groups, and will apply a different level to the next one, click **Next**, and return to [c on page 697](#).
 - f. To make more changes to permission levels, repeat [a on page 696](#) through [e on page 697](#).
 - g. To remove users or groups from the permission set, select the users or groups, and click **Remove**.
4. To restrict users or groups from access in repositories where Trusted Content Services is enabled, do these in the **Restrictions** or **Common Restrictions** area (depending on which is displayed):
 - a. To add restrictions to additional users or groups , click **Add**, select the users or groups, and click **OK**. Go to [c on page 697](#).
 - b. To edit restriction on users or groups, select the users or groups, and click **Edit**.
If validation conflicts are displayed, do one of these:
 - To continue despite the conflicts, click **OK**.
 - To resolve the conflicts, click **Cancel**, and select new users or groups.
 - c. In the **Basic Permissions** list, select the permission level to deny the user or group. For descriptions of basic permissions, see “[Basic permissions](#)” on page 694.
 - d. In the **Extended Permissions** area, select the extended permissions to deny the user or group. For descriptions of extended permissions, see “[Extended permissions](#)” on page 695.
 - e. Do one of these:
 - If you did one of these, click **Finish**:
 - Selected just one user or group.
 - Selected multiple users or group but will apply the same restrictions to all remaining ones.

- If you selected multiple users or groups, and will apply different restrictions for the next one, click **Next**, and return to [c on page 697](#).
- f. To make more changes to restrictions, repeat these substeps.
 - g. To remove users or groups from having restrictions, select the users or groups, and click **Remove**.
5. To edit required groups or required group sets in repositories where Trusted Content Services is enabled, do these in the **Advanced Permissions** area:
 - a. In either the **Required Groups** area or the **Required Groups Sets** area, do one of these:
 - To add users or groups, click **Add**, select the users or groups, and click **OK**.
 - To edit users or groups, select the users or groups, and click **Edit**.
 - To remove users or groups, select the users or groups, and click **Remove**. Skip to [e on page 698](#).
 - b. In the **Basic Permissions** list, select the permission level to deny the user or group. For descriptions of basic permissions, see [“Basic permissions” on page 694](#).
 - c. In the **Extended Permissions** area, select the extended permissions to deny the user or group. For descriptions of extended permissions, see [“Extended permissions” on page 695](#).
 - d. Do one of these:
 - If you did one of these, click **Finish**:
 - Selected just one user or group.
 - Selected multiple users or group but will apply the same level to all remaining ones.
 - If you selected multiple users or groups, and will apply a different level to the next one, click **Next**, and return to [b on page 698](#).
 - e. To make more changes to required groups or required group sets, repeat these substeps.
6. When you are done editing permissions, do one of these:
 - To save your changes, click **OK**.
 - To go to another tab, click the tab.

7.18 Users, groups, and roles

7.18.1 Users

7.18.1.1 Locate a user

To locate a user:

1. Navigate to **Administration / User Management / Users**.
2. Do one of these:
 - Click **Show All Users**.
 - In one or more search fields, type information about the user, and then click **Search**.

A list of users appears.

To display the search fields again, click **More Options**.

3. Locate the user in the list using standard navigation. For instructions, see “[Navigate a repository](#)” on page 540

7.18.1.2 Create or edit a user

You must have adequate privileges to create or edit users.

- If the server authenticates users against the operating system, each user must have an account on the server host.
- If you create users who will be managed by an LDAP server, the `user_name`, and `user_login_name` properties of the `dm_user` object must have unique, non-null values, and the `user_address` property of the `dm_user` object must have a non-null value.

To create or edit a user:

1. Navigate to **Administration / User Management / Users**.
2. Do one of these:
 - To create a new user, select **File > New > User**.
 - To edit an existing user, locate and select the user, and then select **View > Properties > Info**. For instructions on locating a user, see “[Locate a user](#)” on page 699.
3. Enter values to define the new user. For an explanation of user properties, see “[User properties](#)” on page 700.
4. Click **OK**.

7.18.1.3 User properties

See “[User properties](#)” on page 700 for descriptions of user properties that might require further explanation, beyond their field names.

Table 7-25: User properties

Field	Description
State	Determines whether the user can connect to the repository. An active user can connect to the repository. An inactive user cannot.
Name	The user's name as it appears on the user's home cabinet, and on items the user creates or modifies.
User Login Name	The name with which the user logs in to the repository.
User Source	The authentication source. Select None if the user is authenticated in a Windows domain or if the user has an account on the Documentum CM Server host, and is authenticated by the operating system.
E-Mail Address	The address to which notifications are sent for workflow tasks, and registered events.
User OS Name	The login name for authenticating the user on an operating system or on an LDAP server.
Windows Domain	The user's Windows domain, to be used if the repository is on a Windows host or on a Linux host with a domain map for Windows domain authentication.
Home Repository	The repository where the user receives notifications, and tasks.
Restrict Folder Access To	Restricts the user's repository access to particular repository locations.
Default Folder	The location for storing items the user creates.
Default Group	The group assigned to items the user creates.
Default Permission Set	The permission set assigned to items the user creates.
Db Name	The user's name in an RDBMS. This is used if the user is a repository owner or registers RDBMS tables.

Field	Description
Privileges	<p>This authorizes the user to perform certain activities.</p> <p>When setting this, if you grant superuser privileges to a user after installing or upgrading a repository or after manually running the toolset.ebs script, add that user manually to the group called admingroup.</p> <p>If you <i>revoke</i> a user's superuser privileges, remove the user from the admingroup.</p>
Alias Set	The user's default alias set.
Workflow Disabled	Indicates that the user is not available to receive workflow tasks.
Propagate changes to members	<p>If creating a global user, this propagates your changes to members of the repository federation. A global user is a user who is found in all members of a repository federation, and whose property values are the same in all of the repositories. Global users are managed through the governing repository. Global users can also have local properties, which you can modify in a local repository.</p> <p>For more information on global users, see the <i>OpenText Documentum Content Management - Administrator User Guide (EDCAC-UGD)</i>.</p>
Turn off authentication failure checking	Allows the user more login attempts than the limit set in the repository config object.

7.18.1.4 Import users from information contained in an input file

To import a user from information contained in an input file:

1. Determine what type of authentication the repository uses. If the server authenticates users against the operating system, each user must have an account on the server host before you create the users.
2. Create the input file. See “[Input file for new users](#)” on page 702.
3. In Records Client, do these:
 - a. Navigate to **Administration / User Management / Users**.
 - b. Click **File > Import User**.
 - c. In the **Input File Path** field, click **Browse**, and select the location of the input file for creating the new users.

- d. As appropriate, enter additional values that apply to all the users you are importing. Values specified in the input file override values specified on this page. For an explanation of user properties, see “[User properties](#)” on page 700.
- e. Click **Finish**.

7.18.1.4.1 Input file for new users

You import users from information contained in an input file.

Before you create the users, determine what type of authentication the repository uses. If the server authenticates users against the operating system, each user must have an account on the server host.

If the server uses an LDAP directory server for user authentication, the users do not need to have operating system accounts.

If you specify the attributes `user_group` (the user's default group), and `acl_name` (the user's default permission set), any groups, and permission sets must already exist before you import the users.

If you are creating a user who is authenticated using a password stored in the repository, the password cannot be assigned in the input file. You must assign the password manually.

Each user to be imported starts with the header `object_type:dm_user`. Follow the header with a list of `attribute_name:attribute_value` pairs. The attributes `user_name`, and `user_os_name` are required. In addition, the default values in “[Default values for new users](#)” on page 702 are assigned when the file is imported.

Table 7-26: Default values for new users

Argument	Default
<code>user_login_name</code>	<i>user name</i>
<code>privileges</code>	0 (None)
<code>folder</code>	<i>/user name</i>
<code>group</code>	docu
<code>client_capability</code>	1

Each `attribute_name:attribute_value` pair must be on a new line. For example:

```
object_type:dm_user
user_name:Pat Smith user_group:accounting acl_domain:smith acl_name:Global
User Default ACL object_type:dm_user user_name:John Brown
```

If the file contains umlauts, accent marks, or other extended characters, store the file as a UTF-8 file, or users whose names contain the extended characters are not imported.

The attributes you can set through the input file are:

```
user_name user_os_name user_os_domain user_login_name
user_login_domain user_password user_address user_db_name user_group_name
user_privileges (set to integer value) default_folder user_db_name
description acl_domain acl_name user_source (set to integer value)
home_docbase user_state (set to integer value) client_capability (set
to integer value) globally_managed (set to T or F) alias_set_id (set
to an object ID) workflow_disabled (set to T or F) user_xprivileges
(set to integer value) failed_auth_attempt (set to integer value)
```

You can specify as many of the above attributes as you wish, but the attribute_names must match the actual attributes of the type.

The attributes may be included in any order after the first line (object_type:dm_user). The Boolean attributes are specified using T (for true) or F (for false). Use of true, false, 1, or 0 is deprecated.

Any permission sets that you identify by acl_domain, and acl_name must exist before you run the file to import the users. Additionally, the ACLs must represent system permission sets. They cannot represent private permission sets.

Any groups that you identify by user_group_name must exist before you run the file to import the users.

Documentum CM Server will create the default folder for each user if it does not already exist.

7.18.1.5 Make a user active or inactive

To make a user active or inactive:

1. Locate, and select the user. For instructions, see “[Locate a user](#)” on page 699.
2. Select **View > Properties > Info**.
3. To make a user active, click **Active**.
4. To make a user inactive, click **Inactive**.
5. Click **OK**.

7.18.1.6 Change the home repository of a user

The home repository is where the user receives Inbox tasks, and notifications.

To change the home repository of a user:

1. Locate, and select the user. For instructions, see “[Locate a user](#)” on page 699.
2. Click **Tools > Change Home Repository**.
3. Select the new home repository.
4. Select when to run the job that assigns the new home repository.
5. Click **OK**.

7.18.1.7 View the groups to which a user belongs

To view the groups to which a user belongs:

1. Locate, and select the user. For instructions, see ["Locate a user" on page 699](#).
2. Select **View > Locations**.

7.18.1.8 Reassign one user's items to another user

This procedure is useful if you are deleting a user from the repository, and want to reassign the user's files, and objects to another user.

To reassign one user's items to another user:

1. Locate, and select the user. For instructions on locating a user, see ["Locate a user" on page 699](#).
2. Click **Tools > Reassign User**.
3. Click **Select User**, and select the new user to which to reassign items. For detailed steps see ["Locate an item in a selection dialog box" on page 543](#).
4. Complete the remaining fields:
 - **Run the Re-name job**
Select whether the items are reassigned immediately.
 - **Checked Out Objects**
Select whether to unlock items that the previous user had locked.
5. Click **OK**.

7.18.1.9 Delete a user

OpenText strongly recommends making users inactive rather than deleting them from the repository.

It is important to know that if you delete a user, the Documentum CM Server does not delete the references to that user in other repository objects, such as groups, and permission sets. This means that if you delete a user, you must do one of these:

- Reassign the user's objects to another user. See ["Reassign one user's items to another user" on page 704](#).
- Create a user with the same name. If you create a user with the same name, the new user inherits the group membership, and object permissions belonging to the deleted user.

You cannot delete the repository owner, installation owner, or yourself.

7.18.1.10 View user management logs

To view user logs:

1. Navigate to **Administration / User Management / Users**.
2. Select one of these:
 - **View > Reassign Logs**
 - **View > Change Home Repository Logs**

7.18.2 Groups

A group is a collection of users, other groups, and roles. A group can own sysobjects, and permission sets. By default, a group is owned by the user who creates the group.

To locate groups, navigate to **Administration / User Management / Groups**.

To open a group, double-click the group.

7.18.2.1 Create or edit a group

To create or modify a group, you must have adequate privileges. See “[Privileges for groups](#)” on page 705.

Table 7-27: Privileges for groups

Privilege	Description
Create Group	Can create a group with yourself as the owner. Can modify groups to which you belong.
System Administrator	Can modify any group.
Superuser	Can create a group, and assign a different user as the owner.

To create or edit a group:

1. Navigate to **Administration / User Management / Groups**.
2. Do one of these:
 - To create a new group, select **File > New > Group**.
 - To edit an existing group, locate, and select the group, and then select **View > Properties > Info**.

For instructions on locating a group, see “[Groups](#)” on page 705.

3. Enter the appropriate information to define the group. For an explanation of group properties, see “[Group properties](#)” on page 706.
4. Click **OK**.

7.18.2.2 Group properties

See “[Group properties](#)” on page 706 for descriptions of fields that might require further explanation, beyond their field names.

Table 7-28: Group properties

Field	Description
Name	The name of the group. The name must consist of characters that are compatible with Documentum CM Server's server OS code page.
Group Native Room	Available in repositories with Collaborative Services is enabled. If you select a room, the group is considered a private group in the room.
Class	Distinguishes between groups, and roles. Select Group . The server does not enforce the value of this property, and does not set the property to any value other than group.
E-Mail Address	The email address for the group. This is typically the email address of the group's owner. If no value is entered in this field, the group email address defaults to the group name.
Owner	The owner of the group. The user you select has the Create Group privilege. If you are a superuser, you can select the owner. Otherwise, you can set this to a group of which you are a member.
Administrator	The administrator for the group. The administrator can modify the group. If this is null, only a superuser, and the group owner can modify the group. The Administrator cannot add users to the roles that require super user privilege.
Alias Set	The alias set for the group.
Global Group	If you are connected to the governing repository of a federation, this makes the group a global group.

Field	Description
Private Group	Makes the group a private group. Otherwise, the group is public. By default, groups created by users with system administrator or superuser privileges are public, and groups created by users with a lower privileges are private.
Dynamic Group	<p>Makes the group a dynamic group. A dynamic group is a group comprised of potential members, any of whom can be made actual members at runtime.</p> <p>The default membership setting for a dynamic group is Treat users as non-members. This means that at runtime, the potential members do not automatically become actual members.</p> <p>At runtime, however, the application from which a user accesses the repository can request that the user be made an actual member.</p> <p>You can use dynamic groups to model role-based security. For example, suppose you define a dynamic group called EngrMgrs. Its default membership behavior is to assume that users are not members of the group. The group is granted the privileges to change ownership, and change permissions. When a user in the group accesses the repository from a secure application, the application can issue the session call to add the user to the group. If the user accesses the repository from outside your firewall or from an unapproved application, no session call is issued, and Documentum CM Server does not treat the user as a member of the group. The user cannot exercise the change ownership or change permissions permits through the group.</p>

7.18.2.3 Add or remove members in a group

To add or remove members:

1. Navigate to **Administration / User Management / Groups**, and double-click the group.
2. To add members:
 - a. Select **File > Add Members**
 - b. Select the members. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
 - c. Click **OK**.
3. To remove a member:
 - a. Select the member.
 - b. Click **File > Remove Members**.

7.18.2.4 Reassign one group's items to another group

To reassign one group's items to another group:

1. Navigate to **Administration / User Management / Groups**, and select the group.
2. Select **Tools > Reassign**.
3. Click **Select**, and select the new group to which to assign items. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
4. Complete the remaining fields:
 - **Run the Re-name job**
Select whether the items are reassigned immediately.
 - **Checked Out Objects**
Select whether to unlock items that the previous user had locked.
5. Click **OK**.

7.18.2.5 View the groups to which a group belongs

To view the groups to which a group belongs:

1. Navigate to **Administration / User Management / Groups**, and select the group.
2. Select **View > Locations**.

7.18.2.6 Sort Groups and members within groups

With Documentum Webtop 6.6, an Administrator can sort Groups, and members within a Group using the column header. This functionality enables you to manage large number of groups and members within the group.

To sort Groups using the column header:

1. Navigate to the **Administration** node.
2. Select **User Management > Groups**.
A list of existing groups is displayed.
3. Click the column header to sort the groups in ascending or descending order.

To sort members within a Group using the column header:

1. Navigate to the **Administration** node.
2. Select **User Management > Groups > Users**.
A list of existing users in the selected group is displayed.
3. Click the column header to sort the members within a group in ascending or descending order.

7.18.2.7 Delete a group

It is recommended that you do not delete groups. Instead, remove all members of the group, and leave the group in the repository.

7.18.3 Roles

A role is a group that contains the users, and groups assigned particular duties within a client application domain.

To locate roles, navigate to **Administration / User Management / Roles**.



Note: A role that has been created as a domain is listed in the groups list, not the roles list.

To open role, double-click the role.

7.18.3.1 Create or edit a role

If you create a role as a domain, it is listed on the groups list, not the roles list.

To create or edit a role:

1. Navigate to **Administration / User Management / Roles**.
2. Do one of these:
 - To create a new role, select **File > New > Role**.
 - To edit an existing role, locate, and select the role, and then select **View > Properties > Info**.
3. Enter values to define the role. For an explanation of properties, see “[Role properties](#)” on page 710.
4. Click **OK**.

7.18.3.2 Role properties

See “[Role properties](#)” on page 710 for descriptions of fields that might require further explanation, beyond their field names.

Table 7-29: Role properties

Field	Description
Class	Select Role . This lets your applications distinguish between groups, and roles. The server does not enforce the value of this property, and does not set the property to any value other than group.
E-Mail Address	The email address of the role's owner. If no value is entered, the email address defaults to the role name.
Owner	The role owner can modify the role.
Administrator	A user or group, in addition to a superuser or the role owner, who can modify the role. If this is null, only a superuser, and the role owner can modify the role.
Private Group	Creates the role as a private role. Otherwise the role is a public role. By default, roles created by users with system administrator or superuser privileges are public, and roles created by users with a lower user privilege level are private.
Create role as domain	If you create a role as a domain, it is listed on the groups list, not the roles list.

Field	Description
Dynamic Group	Creates the role as a dynamic group. For more information on dynamic groups, see “ Group properties ” on page 706.

7.18.3.3 Add or remove members in a role

To add or remove members:

1. Navigate to **Administration / User Management / Roles**, and double-click the role.
2. To add members:
 - a. Select **File > Add Members**.
 - b. Select the members. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
 - c. Click **OK**.
3. To remove a member:
 - a. Select the member.
 - b. Click **File > Remove Members**.

7.18.3.4 Reassign one role's items to another role

To reassign one role's items to another role:

1. Navigate to **Administration / User Management / Roles**, and select the role.
2. Click **Tools > Reassign**.
3. Click **Select**, and select the new role to which to assign items. For detailed steps see “[Locate an item in a selection dialog box](#)” on page 543.
4. Complete the remaining fields:
 - **Run the Re-name job**
Select whether the items are reassigned immediately.
 - **Checked Out Objects**
Select whether to unlock items that the previous user had locked.
5. Click **OK**.

7.18.3.5 View the groups to which a role belongs

To view the groups to which a role belongs:

1. Navigate to **Administration / User Management / Roles**, and select the role.
2. Select **View > Locations**.

7.18.3.6 Delete a role

It is recommended that you do not delete roles. Instead, remove all members of the role, and leave the role in the repository.

Appendix A. Records Troubleshooting Tips, Limitations and FAQs

Before proceeding to troubleshoot any problems, always make sure 1) that the client you are working from, whether Records Client or Documentum Webtop (for core OpenText Documentum CM functionality) is approved for Privileged DFC and 2) that the person accessing any records functionality (performing a records operation) is a member of the correct role. All functionality in all of the records products is role-based. Administrators and end users therefore, must be a member of the role that allows them to execute the operation.

A.1 Applying a retention policy using our public API

First:

1. Select one of the items that you think might be up for disposition and view applied retention. Verify that there is a qualification date and also check what phase the retainer is in.
2. Verify that the qualification date is not in the future.
3. Are the jobs running correctly? From Documentum Administrator, you can view the results and you can check the messages in the job report.
4. Run promotion manager and see if any items are eligible (this would help us determine if items could be promoted). Similarly for disposition manager we could do a search and see what is up for disposition.

Reasons for why items cannot be promoted to final phase:

1. Freeze markup applied
2. No qualification date. This can be caused by:
 - a. Item was disqualified from promotion manager.
 - b. Retainer does not age if an individual retention policy is on a folder.
 - c. A suspend record relation was applied between the two retained items (the child is the one that gets suspended and does not have a qualification date).
 - d. Events are mandatory and they have not been fulfilled.
3. Qualification date in future.

Reasons for why items do not get disposed:

1. Did you specify all of the parameters correctly on the job for the Disposition Manager? Each time the Dar is installed, the method parameters need to be re-entered.
2. Is the item under a hold or a permanent retention markup? Items under hold or permanent will not be processed during a disposition run. They will not be disposed: exported, transferred, or destroyed.

3. Is the item checked out? Items that are checked out will not get disposed.
4. Items are not in the final phase, yet.

Remedies for no qualification date:

- Did you apply an individual retention policy to a folder? These items will never show up in Promotion Manager or Disposition Manager as they never age (the items inside the folder will age independently).
- Verify that you have a valid authority specified on the retention policy for each phase.
- If you are using a conditional retention policy, confirm that an event date has been set for each retainer.

Whenever disposition is run a work order is created. Using the work order reports, you can now filter on the operation origin and select the Automated field, if you are only interested in work orders initiated by the jobs (set the Operation filter to Disposition as well to only get the disposition job work orders).

A.2 Special characters

To avoid unexpected results against search or report queries, avoid naming administrative components, created for Records Manager and Retention Policy Services, using the following special characters:

- !
- @
- \$
- %
- (
-)
- The accent character on the keyboard below tilde
- +
- _
- -
- ,

A.3 Why can I no longer log in to a repository using my Privileged DFC instance

This problem impacts users who lose their ability to log in to a OpenText Documentum CM repository that they were able to log in to previously. Stated otherwise, this problem impacts users if the IP address (or host name) of the host to which their client connects is changed or if their instance of Privileged DFC is disabled. Instructions to enable or disable Privileged DFC, and other Foundation Java API related information, is documented in the *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS-AGD)*. If the IP address of the Application server changes, you will not be able to log in to the repository. The reason for this behavior is that OpenText Documentum CM has a security feature to prevent someone from reusing someone else's identity. Once a client tries to connect to a repository, the global registry stores information about where the client was running from. To fix this, you will need to perform the following procedure.

1. Stop the Application server.
2. Remove the dfc.keystore file that is in the web applications' WEB-INF/classes directory.
This will cause a new identity to be created.
3. Start the Application server and logon to the repository. As a result a new identity is generated.
4. Using Documentum Administrator you need to register the new identity for privilege. Refer to the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)* for procedures.
5. Restart the Application server.
6. Log in as a Records Manager and try to create a contact to ensure that Privileged DFC is set up correctly.

A.4 How to identify your Privileged DFC instance from other instances on the same host

This problem impacts users trying to identify their privileged client among other privileged clients listed on Documentum Administrator.

Users may have difficulties identifying their client, as the default values for all clients listed looks similar. Users can take extra steps to run a command to identify their client or they can modify the dfc.properties file to tag their instance of the client. Once tagged they will always be able to identify their instance of the client when it is listed. Users will not have to take extra steps to run a command once their client is tagged.

Figure A-1 illustrates a list of privileged clients as they would appear, when their respective dfc.properties is not modified.

Client Name	Client ID	Host Name	Approved
dfc_OTT2QALAB10.dctmlabs.com_BUM...	dfc_cvzHIO3reHPZUPN0PX3F6BUMIJa	OTT2QALAB10.dctmlabs.com	Yes
dfc_OTT2QALAB10.dctmlabs.com_zgx...	dfc_P1pYtn1k6DEPPWoIpuAQoxzgx98a	OTT2QALAB10.dctmlabs.com	Yes
dfc_OTT2QALAB10.dctmlabs.com_VJC...	dfc_9gpK233QJnlv7M5Jn71oVJC50a	OTT2QALAB10.dctmlabs.com	Yes
dfc_OTT2QALAB10.dctmlabs.com_ZGY...	dfc_PAkfoYxuRxfD1ATe9jwrzYZGYqJa	OTT2QALAB10.dctmlabs.com	Yes

Figure A-1: List of privileged clients in Documentum Administrator

A user could have difficulties identifying their client unless they run the following command, from a command shell on their client:

```
C:\Program Files\Apache Software Foundation\Tomcat <version>\webapps\da\WEB-INF\classes>
C:\Program Files\Java\jdk-<version>\bin\keytool -list -v -keystore dfc.keystore -
storepass dfc
```

Follow these steps to modify the dfc.properties for your privileged client.

To tag your instance of Privileged DFC, edit the dfc.properties file as follows:

1. Add the following line dfc.name = dfc whereby dfc can be substituted with the a string that will identify that instance of Privileged DFC. For example, if Documentum Webtop and Records Client are running on the same host set dfc.name to Documentum Webtop for the Documentum Webtop instance and Records Client for the Records Client instance.

Note: This step is not required if the Foundation Java API instances share the same dfc.keystore file.

2. Delete the dfc.keystore file. The location of this file is determined by the dfc.security.keystore.file entry in dfc.properties. If this property is not specified, the default is for the dfc.keystore to be created in the same directory as the dfc.properties file.
3. Start the application and log in to the repository. A new dfc.keystore file should be generated (and of course, privilege needs to be registered for this new identity).

If you have not modified the dfc.properties file, as suggested, follow these steps to determine your client id and use it to identify your client.

To determine the client id for a Foundation Java API instance:

1. Ensure that the keytool file (deployed as part of the JDK for Java) is in your classpath.
2. From a command shell, navigate to the location of the dfc.keystore file location.



Note: The location should be defined within the dfc.properties file. If not, navigate to the same folder the dfc.properties file is in.

3. Run this command (make sure to update the Java path appropriately beforehand):

```
C:\Program Files\Java\jdk1.5.0_13\bin\keytool -list -v -keystore dfc.keystore -storepass dfc
```

The output would appear as in the sample provided under the screenshot at the top of this section. Scan the output for the client id and use it to identify the client in the screenshot.

A.5 Why my Privileged DFC instance does not show up in Documentum Administrator

This problem impacts users who would like to affect their Privileged DFC instance in Documentum Administrator. Users for example cannot enable or disable their Privileged DFC instance if they cannot list it in Documentum Administrator. Users are not able to list their Privileged DFC instance in Documentum Administrator if the global repository is not or is incorrectly configured. A global repository is a mandatory requirement for the Records Client or any other WDK-based application. Global repository implies that a OpenText Documentum CM repository is enabled as a global registry. Both the global repository and the OpenText Documentum CM repository can be configured on the same host or separately on different hosts. For further details, refer to *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*. To enable a repository as a global registry refer to *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS-AGD)*.

A.6 How to test that your instance of Privileged DFC is properly configured

This test can benefit users experiencing problems performing standard operations on their client. Although this test can be performed at any time if there are concerns, it is best to perform this test after a fresh installation or upgrade of the product.

To complete the test:

1. Navigate to a folder already under retention or create a folder if necessary and apply retention.
2. Link a document or record to the folder under retention.

Your instance of Privileged DFC is properly configured if the operation completes successfully.

A.7 Digital shredding

Digital shredding is available for file store storage areas. Digital shredding is a process that removes objects in shredding-enabled storage areas and renders them irretrievable. For information on digital shredding, refer to *OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS-GGD)*.

Digital shredding removes deleted content files and their associated content objects, then overwrites the file's addressable locations with a character, then its complement, and finally a random character.

The interface for DA displays the **Enable Digital Shredding** checkbox for all file stores. Uncheck the checkbox to disable Digital Shredding.

A.8 Auditing

Turn on Auditing using DA to gather audit information. Auditing, for records is turned off by default. Once auditing is enabled, use the Audit Trail Report to report .

A.9 Why is Declare Formal Record disabled?

Use this checklist to determine why the option to Declare Formal Record is disabled on the Records menu item:

- Is Records Manager installed and is the user entitled for Records Manager?
- Have you updated the repository with the dar file that was built with that load? All Records Manager functionality is disabled if the appropriate dar file is not installed.
- Is the user in the dmc_rm_recordscontributor role? Make sure that the user is explicitly specified in that role.
- Did you select a folder? Declare Formal Record is disabled if a folder (or cabinet) is selected. All it takes is one folder to be selected for the menu item to be disabled if multiple objects are selected.
- Did you select a formal record? We don't allow formal records to be declared as formal records. All it takes is one formal record to be selected for the menu item to be disabled if multiple objects are selected.

A.10 Why is the node for Records Manager, Retention Policy Services, Physical Records Manager, or Records Manager Commonwealth Edition missing?

There are many reasons why functionality for a particular node Records Manager, Retention Policy Services, Physical Records Manager, or Records Manager Commonwealth Edition may be disabled. Follow this checklist to troubleshoot the problem.

- Is the user allocated the license of the Records product in OTDS?
- Have you updated the repository with the respective dar file that was built with that load? All functionality for a particular node is disabled if the respective dar file is not installed. Each application has its own dar file.



Note: When upgrading from a previous version, make sure to update the respective dar file.

- Is the user in the appropriate role? For Retention Policy Services node to be shown, the user needs to be in at least one of the following roles:
 - dmc_rps_retentionmanager
 - dmc_rps_poweruser
 - dmc_rps_complianceofficer
 - dmc_rps_vitalrecordadministrator

For the Records Manager node to be shown, the user needs to be in at least one of the following roles:

- dmc_rm_recordsmanager
- dmc_rm_class_guide_admin
- dmc_rm_security_architect
- dmc_rm_record_rel_admin
- dmc_rm_csl_admin
- dmc_rm_security_officer



Note: 1. The records manager role is automatically a member of the retention manager role, so records managers should see both nodes.

2. If you update the DAR file, you need to restart the Application server for the changes to go into effect.

If you are still not seeing the node, in the `TraceProp.properties` file (located in `$WEBROOT/classes/com/documentum/debug`) turn on the RECORDSMANAGER trace flag and restart the Application server. All trace flags are turned off by default. There may now be additional information in the Application server's log file that may explain why it is disabled.

A.11 Creating formal records, cabinets, and folders

Regardless of the role a user is in or the client the user uses, the user also needs to be in the `form_user` group to create formal records, formal cabinets, and formal folders. The menu options for **Declare Formal Record**, **File > New > Formal Cabinet**, and **File > New > Formal Folder** will not be enabled for the user if the user is not in the `form_user` group.

A.12 Why can I not create new objects in a folder after I upgrade Records (only if Security Policy is applied)

After upgrading, the members of `dmc_rps_contributor` role need to be added to the `dmc_rm_recordscontributor` role to create new objects in a folder.

Though users are specified specifically on the security policy, they need to be in the `dmc_rm_security_user` role as well. Users in the `dmc_rm_security` role are automatically granted the `dmc_rps_contributor` privileges.

Appendix B. Keyboard Shortcuts for Microsoft Windows and Mac Operating Systems

You can use keyboard shortcuts to select menus and buttons using your keyboard instead of your mouse. “[Keyboard shortcuts](#)” on page 721 describes the default keyboard shortcuts. Customized installations might vary.

Table B-1: Keyboard shortcuts

Action	Microsoft Windows shortcut	Mac OS shortcut
Create a new document	Shift-N	Shift-N
Check out	O	O
Edit	E	E
Check in	I	I
View	V	V
Open in read-only mode	Enter	Enter
View properties	P	P
Import	Shift-I	Shift-I
Export	Shift-E	Shift-E
Save as	A	A
Search	Shift-S	Shift-S
Subscribe	U	U
Add to clipboard	Shift-C	Shift-A
Copy here	Shift-V	Shift-C
Move here	Shift-M	Shift-M
Link here	Shift-L	Shift-L
Delete	Delete	Delete
Start a quickflow	Q	Q
Apply a lifecycle to a document	L	L
Promote a document to its next lifecycle state	R	R
Demote a document to its previous lifecycle state	D	D
Declare a record	Shift-R	Shift-R
Create a discussion	Shift-U	Shift-U

Action	Microsoft Windows shortcut	Mac OS shortcut
Convert a simple document into a virtual document	Shift-T	Shift-V
Email	M	M
Select all the items on the page	Ctrl-A	Cmd-A
Select the next item	Right arrow	Right arrow
Select the previous item	Left arrow	Left arrow
Select the item above	Up arrow	Up arrow
Select the item below	Down arrow	Down arrow
Go to the next field or button	Tab	Tab
Go to the previous field or button	Shift-Tab	Shift-Tab
Help	Shift-H	Shift-H
Log out	Shift-O	Shift-O

Appendix C. Records Manager and Department of Defense functionality

C.1 Overview of Department of Defense functionality

This appendix describes all of the Records Manager functionality included for the Department of Defense. Department of Defense functionality is therefore optional unless it is necessary to work with Department of Defense records. This means Department of Defense functionality is available only if one or more of the Department of Defense dar files are installed.

There are two versions of Department of Defense records functionality, each associated to its own set of dar files:

- The newer DoD5015 Version 3 for declaring standard and classified records.
- The older DoD5015 Version 2 for declaring chapter 2 and chapter 4 records, whereby chapter 2 is similar to standard and chapter 4 is similar to classified.

Customers planning to install Department of Defense functionality for the first time are recommended to install the latest version, DoD5015v3. Existing customers working with the older version are recommended to upgrade to the latest version.

Total Department of Defense functionality is available when both of the Department of Defense dar files, of the respective version, are installed. Functionality is otherwise available or limited as follows, depending on the installed version:

- *On DoD Version 3 installations:* Only Department of Defense standard records and email records can be declared if only the Department of Defense standard dar file is installed. Department of Defense classified records can also be declared if the Department of Defense classified dar file is installed on top of the standard dar.
- *On DoD Version 2 installations:* Only Department of Defense Chapter 2 records and email records can be declared if only the Department of Defense Chapter 2 dar file is installed. Department of Defense Chapter 4 records can also be declared if the Department of Defense Chapter 4 dar file is installed on top of the Chapter 2 dar.

If you can declare Department of Defense standard records but not Department of Defense classified records, it means the Department of Defense classified dar is not installed. If you can declare Department of Defense Ch2 records but not Department of Defense Ch4 records, it means the Department of Defense Ch4 dar is not installed. For complete installation details, refer to the latest version of the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)*.

Department of Defense features include:

- Declaring standard and classified records or chapter 2 and chapter 4 records, depending on the installed version.

Both the standard and chapter 2 dars support functionality for declaring email records.

- classification guides
- reporting...declassification report, confirming purge of classified records from the report
- disposition run bundles
- NARA transfers

C.2 Classification guides

Topics include:

- “About classification guides” on page 724
- “Creating classification guides for classified records” on page 725

C.2.1 About classification guides

Classification Guides is an optional Department of Defense feature used specifically to facilitate the declaration of Department of Defense version 2 Chapter 4 records or of Department of Defense version 3 classified records. Classification fields on the classification form that an end user would normally have to fill in are instead pre-populated when the end user selects a classification guide. Records Manager privileged users and administrators in the Records Manager role can create classification guides.

Classification Guides are only available under the Records Manager node if either the Classified dar file or the Chapter 4 dar file is installed. Chapter 2 and Chapter 4 dar files are provided for customers using the previous version of Department of Defense functionality. The Classified dar file is dependent on the Standard dar file and similarly the Chapter 4 dar file is dependent on the Chapter 2 dar file. If the Classification Guides node is not displayed and you would like to use it to declare classified records, refer to the latest version of the *OpenText Documentum Content Management - Records Client Deployment Guide (EDCRM-IGD)* to install the two optional dars.

Classified records extend standard records, therefore, all functionality available in standard records functionality is also available in classified records functionality. Although a classification guide can be used to pre-populate mandatory classification fields on a classification form, you still have to manually enter values for the other mandatory fields that appear above the classification fields. For example, the following mandatory attributes have fields for which you manually enter values common to all formal records declared:

- Record Name
- Subject
- Media Type

- Format
- Authors

It is the mandatory classification attributes which appear below these attributes that are pre-populated.

C.2.1.1 Creating classification guides for classified records

Classification guides predefine values for declaring classified records, in particular the security level. Values for attributes on the classification form used to declare classified records are pre-populated only if you specify a classification guide. Values missing against attributes on a classification guide leave matching fields empty on the classification form for the same attributes.

To create a classification guide:

1. Navigate to the **Security Levels** administration node to determine if any security levels are available. If not, create a security level. To create a security level , refer to “[Creating security levels](#)” on page 396.



Note: A classification guide can only be created when at least one security level is available.

2. Navigate to **Records Manager > Classification Guides**.

Classification guides are displayed in the content pane according to one of two options in the filter setting located in the upper right corner under the menu bar. The two options are:

- **Enabled Classification Guides**
- **All Classification Guides**



Note: Classification guides that are *disabled* are not displayed when the filter is set to **Enabled Classification Guides**, which is the default setting unless you change the filter option to **All Classification Guides**. Disabled classification guides are displayed in the content pane as being *False* or if enabled as being *True*.

3. Click **File > New > Dod5015v3 Classification Guide** or click the other option, **Classification Guide**, depending on the version you want to create it for. For example, click **Classification Guide** if you need to create it for the older version, Chapter 4 records. If both options are available, it means both dars, the one for the older version and the one for the new version, are installed.

The **New Classification Guide** screen displays the **Create** tab.



Note: **File >New** is not available if no security levels are displayed on the **Security Levels** administration page.

4. Type a unique name in the mandatory **Name** field and click **Next**.

The **Info** tab is displayed only if the name provided is unique.

5. Select a security option from the list box for the mandatory **Classification** field.
6. Click either **Finish** to create a partially completed classification guide or continue to enter values for the remaining optional fields and then click **Finish**. ["Optional attributes on the New Classification Guide Info tab" on page 726](#) describes the optional attributes.

The new classification guide is created and listed in the content pane under Classification Guides. Make sure that you change the default filter setting in the upper right corner from *Enabled Classification Guides* to *All classification Guides*.



Note: The security level options displayed in the **Classification** list box are available only when they are enabled.

Table C-1: Optional attributes on the New Classification Guide Info tab

Attribute	Description
Title	The value for this attribute is automatically populated according to the mandatory value entered on the Create tab.
Classification	<p>Select the desired security level. Whatever levels are created in the Security Levels will be displayed here, for example:</p> <ul style="list-style-type: none"> • Unclassified • Confidential • Secret • Top Secret <p>If a security level is not displayed in the list box, navigate to Records Manager > Security Levels and make sure the Is Enabled attribute on their Properties is selected.</p>
Remarks	Specify any comments or instructions for the classification guide you feel are needed.
Supplemental Marking	The attribute marking set called Supplemental Marking will display all of its attribute marking values from this menu option. Add supplemental markings to add additional security to the object.
Project Name	The attribute marking set called Project Name will display all of its attribute marking values from this menu option. Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.

Attribute	Description
Classified By	<p>This field becomes mandatory when creating a classified record when the Current Classification is higher than <i>Unclassified</i>. It is otherwise optional when creating unclassified records.</p> <p>Select the radio button next to the means by which to specify a valid user for this value. You can choose to select from a list or type in a value.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Publication Date	<p>The value you type or select from the date control button could be the publication date of the document. The value you select from the date control button populates the left field with the date and the right field with a default time set to 12:00 AM. You can also position the cursor in either field to change the values manually.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Originating Organization	<p>The value you type for this field should identify the official name or code of the office responsible for the creation of the document being declared.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>

Attribute	Description
Declassify On	<p>Use this field to prevent automatic declassification or to initiate automatic declassification of a classified record. One of the five options for this attribute is empty and comes up as the default value to prevent running any de-classification job. The other four options represent the different de-classification jobs that will be run if specified:</p> <ul style="list-style-type: none"> • Exemption Category • Date • Event • Date and Event <p>A classified record is exempt from declassification according to the exemption category selected for Exemption Categories.</p> <p> Note: De-classification of a classified record implies that the classified record would be turned into an unclassified record with a security level equal to 0 (Unclassified). Downgrading of a classified record is typically done to reduce the security level though it could be reduced if necessary to the point of being a declassified record. Declassifying a record is normally done when the latter is made public and is no longer subject to security controls.</p>
Declassify On Date (Conditional attribute displayed only if Date or Date and Event is the selected value for Declassify On.)	<p>This attribute is displayed only when a date driven job is specified for Declassify On. The date driven jobs are Date and Date and Event.</p> <p>Specify a date on which to run a date driven de-classification job.</p>
Reasons for Classification	<p>The value selected for this attribute identifies why the record is classified.</p>
Exemption Categories	<p>Select a value for this attribute only if the value selected for Declassify On specifies Exemption Category.</p>

Attribute	Description
Enabled	<p>This attribute is enabled by default and can be disabled by deselecting the checkbox. The classification guide is listed in the content pane when you finish the procedure to create one as <i>True</i> or <i>False</i>. You will NOT see the classification guide in the listing if it is enabled False, that is if you change the default setting for this option by deselecting the checkbox. Change the default filter setting in the upper right corner from Enabled Classification Guides to All Classification Guides.</p> <p> Note: Any classification guide that is not enabled (disabled or otherwise displayed as being <i>False</i>) cannot be added from the Choose an item screen when you select <i>Classification Guides</i> as the value for Derived From on the classified record form.</p>

C.3 Disposition run bundles

Related topics outside of this section:

- “About disposition run bundles” on page 314
- To enable disposition run bundles, refer to “Disposition configuration option settings” on page 124

C.3.1 Overview of disposition run bundles

A disposition run bundle, or simply bundle for discussion purposes here, captures all of the disposition details that are associated with a disposition run. Strategy runs and transfer runs are created in the bundle based on disposition strategies. A disposition run could involve processing transfer runs or strategy runs or both. Because a transfer run requires confirmation, 2 work orders will always be created, one against disposition processing and another one against confirmation processing. Failure of disposition processing, against either a strategy or transfer run, can be recovered when you right-click the bundle itself or if you open the bundle and right-click the work order inside the bundle. Recovery of confirmation processing can be done from the transfer run inside the bundle or from the work order created by the confirmation. If the transfer run in the bundle shows an error, that is Error = Yes, and the Status = Confirmed, fix the error (remove the hold from the affected documents for example) and then recover. When recovery finishes, the expected result should be Error = No and Status = Confirmed and Disposed, unless another error occurs.

 **Note:** Transfer runs are protected from being deleted if they have not been confirmed and disposed, or rejected. Disposition of a transfer run cannot be

finished if someone, a Retention Manager for example, deletes the transfer run, before it has been confirmed. Confirm transfer runs as soon as possible.

Disposition run bundles:

- Are optional unless Department of Defense functionality is required. Disposition run bundles functionality as a result, is automatically enabled when the Department of Defense Standard dar (RM-DoD5015v3-Standard-Record.dar) is installed. Although Department of Defense functionality may not be required, disposition run bundles functionality can always be manually enabled (or disable) when desired, from the Disposition Configuration object `dmc_rps_disp_configuration_object`, by setting the value for `enable_run_bundle` to True (or False).
- Are created whether disposition is run manually using Disposition Manager or run automatically by the Disposition Job.
- Listed in the navigation pane under Retention Policy Services > Disposition Run Bundles.
- Are colored red, green, or black, that is the name (which is system generated) is red if the run encountered any errors, green if confirmation is required, or otherwise black if no errors or no confirmation is required. All run bundles *Active* and *Inactive* are displayed in this example. The filter setting in the upper right-hand corner of the UI is set to *Active* by default. *Active* run bundles are green if no errors or red if there are errors whereas, the *Inactive* ones are black.

A Yes in the Action Required column means that user action is required, either to confirm a transfer or to recover if there is an error. Only transfer runs, as opposed to strategy runs, require confirmation. Transfer runs are associated with the two NARA transfer disposition strategies:

- NARA transfer, Destroy content
- NARA transfer, Destroy all

Strategy runs are associated with the other disposition strategies:

- Export All, Destroy All
- Destroy All
- Export All
- Export All, Destroy Content
- Destroy Content



Note: A manifest of the items transferred is included with only transfer runs.

The details on the Transfer Info tab, when selected from the Properties of a transferred object, are described as follows:

- No, represents the number of transfers.

- Status, can consist of the following values: Transferred or Confirmed.
- Receiving Organization, represents the entity to which the object is transferred.
- Date, identifies the date and time the object was exported.
- Machine Name, is the name of the Records Queue Manager server from which the object was exported.
- Disk Path, identifies the export location on the Records Queue Manager server specified.

 **Note:** This is the export location from which NARA objects are transferred, either by FTP or on CD, to the receiving organization.

- Notes, available space for including user notes when necessary.

C.3.2 To open a disposition run bundle and view the details, and when necessary to view the details of the work order and perform recovery actions

1. Navigate to **Retention Policy Services > Disposition Run Bundles**. To view both *Active* and *Inactive Disposition Run Bundles*, change the default setting from *Active* to *All*. Details against any run bundle listed include the Name (which is system generated), Disposition Status, Error, Disposition Start Time, Disposition End Time, and Action Required.
2. Right-click a disposition run bundle and select **Open**. Details against the selected run bundle include the Name (of the disposition strategy), Creation Date, Error, Accession, PDF Included, Status, Modified Date, Export Location, and Receiving Organization.

NARA transfers are grouped together and are identified with this icon  and are referred to as transfer runs. All other objects in the manifest processed again  disposition strategies other than NARA transfers are identified with this icon  and are referred to as strategy runs. It is only the transfer runs in disposition run bundles that require you to take action and provide confirmation. Strategy runs do not require any action or confirmation.

 **Note:** The two items below the transfer (or strategy) run identify the master work orders that processed the operation. The first master work order listed, processed the transfer whereas the second one processed the confirmation.

3. Optionally, you can right-click a master work order and perform any of the work order actions:
 - **View Input**
 - **View Results**
 - **View Breakdown**
 - **View Items**

- Recover
4. Click **Close**.
- The status of a retainer on a transfer run becomes waiting after it is successfully disposed the first time. Disposition resumes only after confirmation is provided.

C.3.3 To confirm or to reject a NARA transfer run



Note: Transfer confirmation is required only when a disposition run involves a NARA transfer. These instructions are intended for transfer runs only. A transfer of objects can also be rejected if the items transferred are not what was expected or requested. Other reasonThe objects being transferred can only be rejected if they have not already been confirmed.

1. Navigate to **Retention Policy Services > Disposition Run Bundles**. To view both *Active* and *Inactive Disposition Run Bundles*, change the default filter setting, in the upper right-hand corner of the screen, from *Active* to *All*.
2. Right-click a disposition run bundle, one that was based on a NARA transfer, and select **Open**.

The **Disposition Run Bundle** content page is displayed.

3. Right-click the transfer run item and select the desired option to either **Confirm Transfer** or **Reject Transfer**. Select the **Confirm Transfer** action if confirmation from the receiving organization has been received. Otherwise, select **Reject Transfer** if there is a problem with the transferred items, so that the retainers are returned to the *Open* status, for another disposition attempt.

All transfer runs have one of the following names:

- NARA Transfer and Destroy content
- NARA Transfer and Destroy all

The possible values that can be displayed for the **Status**:

- *Initialized*
- *In Progress*
- *Transferred*
- *Confirmed*
- *Confirmed and Disposed*
- *Rejected*
- *Completed*

Note the following behavior regarding the transfer menu options and the **Confirmation of Transfer** dialog:

- The **Confirm Transfer** menu option: Is available only when the **Status** displays *Transferred*.

Is not available if a *Transferred* status is associated with an error.

- The **Recover** option is displayed instead of **Confirm Transfer** if a *Confirmed* status is associated with an error.
- The **Reject Transfer** menu option is available only when the **Status** displays *Initialized*, *In Progress*, or *Transferred*.
- *Initialized* means the transfer run is created. It appears only briefly before shifting to *In Progress*.
- *Transferred* means data has been exported to disk and is being shipped to the receiving organization. Information must be entered for the **Receiving Organization Name** and the **Receiving Organization Contact**, once the receiving organization has acknowledged receiving the items, to allow disposition to continue.
- *Confirmed* means values for the **Receiving Organization Name** and for the **Receiving Organization Contact** were specified. Disposition however against the objects in the transfer run has not been finished. Therefore, if a user chooses to recover the disposition after confirmation has been provided, the information provided previously will be used and the text field and the **Browse** button as a result are grayed out. User has only to click **Ok** to continue the disposition.



Note: Because NARA transfers (transfer runs) involve disposition processing and confirmation processing, the goal is to obtain the *Confirmed and Disposed* Status. If only *Confirmed* is displayed, it means the disposition processing part of the transfer run encountered an error, possibly a document with a hold. A *Confirmed* status should prompt you to fix the error, remove the hold for example, and then perform recovery.

- *Confirmed and Disposed* implies that the transfer run, both disposition processing and confirmation processing, have completed successfully. This is the final status of a transfer run.
- *Completed* is displayed for strategy runs only. This is the final status of a strategy run.

4. If **Confirm Transfer** is selected, enter the values for the **Receiving Organization Name** and for the **Receiving Organization Contact** on the **Confirmation of Transfer** screen, and then click **OK** to start the confirmation and to continue disposition. The input information as a result is recorded on the transfer run and on each object that was transferred.

If **Reject Transfer** is selected, all transfer information attached to the transfer objects for this run will be cleared. The **Status** of the transfer run is therefore set to *Rejected*. As a result, the disposition status of the corresponding retainers will be returned to the *Open* status so that the user can start a new disposition run to repeat the transfer.

A message is displayed at the bottom of the content pane, once the processing is done. The **Operation Origin** on the **Work Order Report** indicates *External* for a *Disposition* operation that requires confirmation.

5. Optionally, if there are errors in any run in the run bundle, refer to “[To open a disposition run bundle and view the details, and when necessary to view the details of the work order and perform recovery actions](#)” on page 731.

C.3.4 To view the last transferred item list



Note: Follow this procedure to determine if any objects in a disposition run were previously transferred. Objects can be transferred more than once. For example, if the retainer being disposed of is owned by a retention policy that specifies a rollover. The retainer could in fact rollover many times before it rolls over to a retainer that is associated to a retention policy that destroys both its content and metadata. All retainers in other words, that acted on the object, including the last retainer that destroyed all (content and metadata), could have all involved a transfer. **No last transferred items** is displayed if the object has never been transferred before the current disposition run.

1. Navigate to **Retention Policy Services > Disposition Run Bundles**. To view both *Active* and *Inactive Disposition Run Bundles*, change the default setting from *Active* to *All*.
2. Right-click a disposition run bundle and click **Open**, then select the transfer run and click **Properties**.
3. On the **Properties** page, select the **Last Transferred Item List** tab.
4. Click **OK** or **Cancel** to close the **Properties** page. The **OK** button is used to commit changes made, if any, on the **Info** or **Permissions** tabs.

C.3.5 To view the manifest of a transfer run or, to export the manifest or declare it as a formal record



Note: A **Transfer Manifest** is created whenever a disposition run is performed against a NARA transfer. The **Transfer Manifest** is created for transfer runs only, not strategy runs. These instructions are intended for transfer runs only.

1. Navigate to **Retention Policy Services > Disposition Run Bundles**. To view both *Active* and *Inactive Disposition Run Bundles*, change the default setting from *Active* to *All*.
2. Right-click a disposition run bundle, one that was based on a NARA transfer, and select **Open**.

The **Disposition Run Bundle** page is displayed.

3. Right-click the transfer run item and select **Open Manifest**. The **Transfer Manifest** page is displayed.

The **Transfer Manifest** displays the following details about the disposition run bundle selected:

- Disposition Strategy

One of the two NARA transfer strategies would be displayed.

- Transfer Time
- Machine Name
- PDF Included
- Accession

Accession is Department of Defense terminology. No means that metadata still exists. The entity or organization who transferred the content still manages its metadata. Therefore, when rolled over retention on the metadata is ready for disposition, the receiving organization will have to be notified at that time to perform the expected disposition action against the content. Yes means that both content and metadata have been destroyed. Receiving organization assumes full responsibility for managing both the metadata and the content.

- Transferred by
- Export Root Directory
- All Items Exported

Details against the items listed in the manifest include:

- Object Name
- Export Path
- Audit Export Path
- Retention Policies
- Last Receiving Org
- Last Receiving Org Contact

4. Click **Close**, unless you want to export the manifest or declare it as a formal record or both, then click **Close**.

If you click **Export All to CSV**, click the desired button **Open** or **Save** on the **File Download** dialog. Although the .csv file is captured by default in Excel format it can also be view in other formats if you right-click the file and select **Open With**.

	A	B	C	D	E	F	G	H	I	J	K
1	Transfer Manifest for 'NARA Transfer, Destroy content' in 'DRB20121120134701_0900001880007645'										
2											
3	Disposition Strategy: NARA Transfer, Destroy content										
4	Accession: No										
5	Transfer Time: Nov 20, 2012 1:47:59 PM										
6	Transferred By: Administrator										
7	Machine Name: ott2eng1357.ddmlabs.com										
8	Export Root Directory: C:\temp\Transfer\DRB20121120134701_0900001880007645\NARA Transfer, Destroy content										
9	PDF Include: No										
10	All Items Exported: Yes										
11											
12	Object No Export Pat Audit Expi Retention Last Recel Last Receiving Org Contact										
13	Full page C:\temp\1C:\temp\1NARA Traaaaaa Administrator										
14											
15											
16											
17	Transfer Manifest for 'NARA Tra										

Figure C-1: Manifest example

Declare Formal Record is not displayed if Records Manager is not installed. The manifest is automatically and transparently exported to .csv format once you click **Declare Formal Record**. If you click **Declare Formal Record**, follow the instructions for declaring formal records, “[Declaring electronic or physical documents as formal records](#)” on page 340. When following the instructions, make sure the **Form Template** you select is a Department of Defense form template, *Record DoD 5015 V3 Standard* or *Record DoD 5015 V3 Classified*. The .csv file is automatically assigned a unique name which is displayed by default next to the **Name** attribute on the selected **Form Template**. For example, *Transfer Manifest for 'NARA Transfer, Destroy Content' in 'DRB20121120134701_0900001880007645'.csv*.

C.4 Declaring Department of Defense formal records

There are four formal record types to choose from if all DoD functionality is available: *formal*, *DoD standard*, *DoD classified*, and *DoD email*. All formal record types are associated to a form. The following list represents the forms displayed when you select Records > Declare Formal Record for an object that is selected in the content pane.

- Formal Record (dmc_rm_formal_record)

Select this form to declare a record that does not have to be Department of Defense compliant.

This form is available (listed) when Records Manager is installed.

- Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec)

Select this form to declare a record as a standard DoD record.

This form is available (listed) if the Department of Defense standard dar is installed.

- Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec)

Select this form to declare a record as a classified DoD record.

This form is available (listed) if the Department of Defense classified dar is installed.

- Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec)

This form is automatically selected when email records are declared. This form prompts you for email.

This form is available (listed) if the Department of Defense standard dar is installed.

The instructions to declare any of the formal record types are the same. Refer to “Declaring electronic or physical documents as formal records” on page 340 to follow the instructions and then refer to “Entering values on the applicable Department of Defense form when declaring Department of Defense formal records” on page 738 for the attribute descriptions on the three Department of Defense forms.



Note: The Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_class_rec) form template available out-of-the-box defines Unclassified as the lowest security level, ranking = 0. You must manually update the classified form template, according to the following four steps, for systems which do not use Unclassified as the lowest security level.

Classified records can be:

- upgraded to a higher security level
- downgraded to a lower security level
- declassified to the lowest security level of Unclassified.

To specify the lowest security level instead of Unclassified on the classified form template:

1. Log in to Documentum Webtop or the Records Client. You must be in the Form Designer role, form_designer, to edit a form template.
2. Navigate to *Cabinets/System/Forms/Record DoD 5015 V3 Classified*.
3. Edit the *Record DoD 5015 V3 Classified* (Format: XForms) xml content, by replacing all occurrences of **Unclassified** with the lowest security level object name in your docbase.
4. Check in the object as *Same Version*.

There is no need to restart the docbase service nor the Application server after the changes are made.

Contact your Records Administrator (the Records Manager) if the form(s) you need are not displayed as values in the list box on the form for the form type that was selected. You cannot select a Form Template unless the appropriate dar(s) is/are installed. You might only need to declare formal records in which

case you would not need the Department of Defense dars installed, only the Default dar would be needed.

C.4.1 Entering values on the applicable Department of Defense form when declaring Department of Defense formal records

This section describes the attributes on the forms used to declare Department of Defense formal records. The button at the end of each form Create Record Relationship is available to create a record relationship with other objects whenever it is necessary. You can, when necessary, immediately relate the formal record being declared to another object, without having to follow a separate process. Select the applicable section for the Department of Defense record type you are declaring:

- “[Entering values on the Department of Defense standard records form](#)”
on page 738, Department of Defense compliant form without classification attributes
- “[Entering values on the Department of Defense email records form](#)”
on page 743, Department of Defense compliant form for email
- “[Entering values on the Department of Defense classified records form](#)”
on page 747, Department of Defense compliant form with classification attributes

Though custom forms could be listed among the choices, only those forms available out-of-the-box are described.

All mandatory and optional fields for each attribute are described in the applicable section depending on the form you are using to declare a formal record.



Note: Although entries are required in the mandatory fields to process the form, the optional fields can be addressed later from the Properties of the form.

C.4.1.1 Entering values on the Department of Defense standard records form

Refer to this section if you are declaring standard formal records. Attributes on the sample form, as shown in the following image, are described in “[Attributes for standard records \(Record DoD 5015 V3 Standard \(dmc_rm_dod5015v3_std_rec\)\)](#)” on page 740.

Info : AAa(2).doc (File 1 of 2)

Record DoD 5015 V3 Standard

* Record Name: AAa(2).doc

* Subject:

* Media Type:

* Application Format:

* Originating Organization:

Date Filed: Nov 30, 2009 4:04 PM

Received Date: Date 12:00 AM

* Publication Date: Nov 30, 2009 4:04 PM

* Unique Record Identifier: 090133c28000-572

Record Category Identifier: Items per page: 10

No items

Vital Record:

Authors:

Insert Delete

* Authors

Keywords:

Insert Delete

Keywords

Primary Addressees:

Insert Delete

Primary Addressees

Other Addressees:

Insert Delete

Other Addressees

Locations:

Insert Delete

Physical Locations

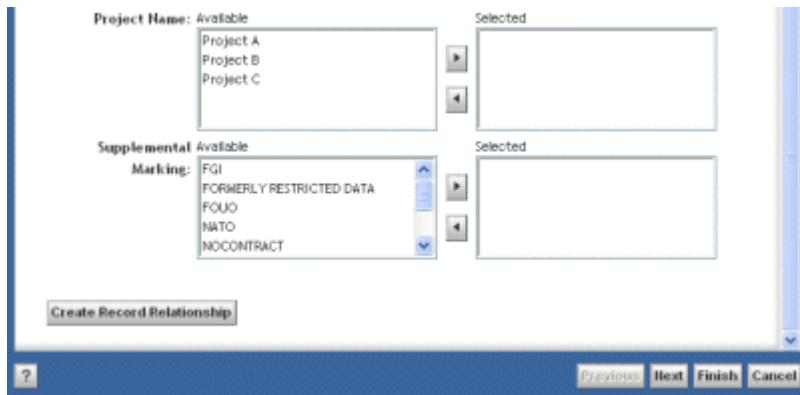
This screenshot shows the 'Info' screen for a document named 'AAa(2).doc'. The document is identified as 'File 1 of 2'. The form is based on the 'Record DoD 5015 V3 Standard'. The following fields are populated:

- Record Name: AAa(2).doc
- Subject: (empty)
- Media Type: (dropdown menu)
- Application Format: (dropdown menu)
- Originating Organization: (empty)
- Date Filed: Nov 30, 2009, 4:04 PM
- Received Date: Date, 12:00 AM
- Publication Date: Nov 30, 2009, 4:04 PM
- Unique Record Identifier: 090133c28000-572
- Record Category Identifier: (empty)

The 'Vital Record' checkbox is unchecked.

Below the main form, there are four sections with 'Insert' and 'Delete' buttons:

- Authors: One item listed: 'Authors'
- Keywords: One item listed: 'Keywords'
- Primary Addressees: One item listed: 'Primary Addressees'
- Other Addressees: One item listed: 'Other Addressees'
- Locations: One item listed: 'Physical Locations'



Next is displayed at the bottom of the form only when you select more than one item to be declared as **Individual records**. You do not have to click **Next**. You can click **Finish** to apply the same metadata to the remaining records. You only click **Next** if you want each individual record to have different metadata when filing.

All mandatory fields require entries to proceed with filing. Any field that is incorrectly addressed prevents the form from being processed. Unaccepted entries are clearly described in red text at the bottom of the form when processing is prevented. Make sure to provide entries for all the mandatory fields and that all the entries are valid.

Table C-2: Attributes for standard records (Record DoD 5015 V3 Standard (dmc_rm_dod5015v3_std_rec))

Attribute (*) indicates mandatory attributes	Description
* Record Name	The name of the document is populated in this field automatically if a single document was selected for the record. If multiple documents were selected for a single record, Please Enter Record Name is displayed for this value.
* Subject	Any value you type for this field is acceptable. The principal topic addressed in a document could be used. Confirm with your Records Administrator how this field is defined in your organization.

Attribute (*) indicates mandatory attributes	Description
*Media Type	<p>The value you select identifies the material or environment on which information is inscribed (microfiche, electronic, and paper for example).</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Application Format	<p>The value you select identifies the format based on the application used to create the document being declared a record.</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Originating Organization	<p>The value you type for this field should identify the official name or code of the office responsible for the creation of the document being declared.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Date Filed	<p>The value for this field is automatically populated when a document is declared a formal record.</p>
Received Date	<p>The value you type or select from the date control button could be the date you received the document. The value you select from the date control button populates the left field with the date and the right field with a default time set to 12:00 AM. You can also position the cursor in either field to change the values manually.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>

Attribute (*) indicates mandatory attributes	Description
*Publication Date	<p>The value you type or select from the date control button could be the publication date of the document. The value you select from the date control button populates the left field with the date and the right field with a default time set to 12:00 AM. You can also position the cursor in either field to change the values manually.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Unique Record Identifier	Read-only field, pre-populated (system generated) to identify the record object.
Record Category Identifier	This field is automatically populated based on the applied naming policy.
Vital Record	The checkbox is Read Only and indicates if the document being declared was marked as a Vital record using the retention markup feature of Retention Policy Services. This is set when a retention markup with the Vital designation is applied.
*Authors	<p>Type in the name of the person(s) who authored the document that is being declared a formal record.</p> <p>You can click Insert to insert another value and all inserted values are saved.</p>
Keywords	<p>Type in text that can be used to facilitate searching. The metadata on a form associated to a particular record can be used for keywords.</p> <p>You can click Insert to insert another value and all inserted values are saved.</p>
Primary Addressees	<p>Type in the primary name of individual or individuals who authored the document.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Other Addressees	<p>Type in the names of anyone else responsible who can address questions if necessary.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>

Attribute (*) indicates mandatory attributes	Description
Locations	Type in the name of the location to indicate where the record is kept. Confirm with your Records Administrator how this field is defined in your organization.
Project Name	Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.
Supplemental Marking	Add supplemental markings to add additional security to the object.
Create Record Relationship	Displays a page that allows you to choose the record relationship type. On this page there is also a locator that allows you to connect the record being declared to another as a child or as a parent using the selected relationship type. For further details about record relationships, refer to “Record relations” on page 405.

C.4.1.2 Entering values on the Department of Defense email records form

Refer to this section if you are declaring email formal records. The information here is applicable only if you are declaring email records directly from Records Activator for Microsoft Outlook. Attributes on the sample form are described in “[Attributes for email records \(Record DoD 5015 V3 Email \(dmc_rm_dod5015v3_email_rec\)\)](#)” on page 744. Administrators can customize email optional mappings, if necessary, according to instructions in “[About customized email optional mappings](#)” on page 310.

The email messages can be declared as Department of Defense Email Records only through Records Activator for Microsoft Outlook client. To declare an email message as an email record through Records Activator for Microsoft Outlook, the shouldParseMsgFile property must be set to true in mailapp.properties file on the Application server where records, to which records activator is pointing, is deployed. If you select Include Attachments while declaring an email message as an email record through Records Activator for Microsoft Outlook, but the attachment extraction is disabled in mailapp.properties by setting shouldSeparateAttachments to false, then you will receive a confirmation message asking if you want to declare the email message alone as a record without including attachments. Depending upon the option selected for this prompt, either email message alone is declared as an email record without including its attachments or email record declaration operation is canceled.

The source email message, which is declared as an email record, is imported into repository in its native outlook message format (.msg format) as an object of dm_email_message type or any of its sub-types. The import of source email message in EMCMF format as an object of dm_message_archive type or its subtypes is not supported. The object type of the source email message imported into repository while declaring the email record is decided based on the value set for the 'Source Email Type For Filing Email Records' attribute in Records Manager Docbase Configuration object. The supported object type values for this attribute include dm_email_message and its subtypes. The default value for this attribute is dm_email_message.

Records Activator for Microsoft outlook prompts you to select file plan location to save the email record while declaring it and also displays the Department of Defense Email Record form to allow to enter the values for different fields of Department of Defense Email Record form.

Next is displayed at the bottom of the form only when you select more than one item to be declared as **Individual records**. You do not have to click **Next**. You can click **Finish** to apply the same metadata to the remaining records. You only click **Next** if you want each individual record to have different metadata when filing.

All mandatory fields require entries to proceed with filing. Any field that is incorrectly addressed prevents the form from being processed. Unaccepted entries are clearly described in red text at the bottom of the form when processing is prevented. Make sure to provide entries for all the mandatory fields and that all the entries are valid.

Table C-3: Attributes for email records (Record DoD 5015 V3 Email (dmc_rm_dod5015v3_email_rec))

Attribute (*) indicates mandatory attributes	Description
*Record Name	The name of the document is populated in this field automatically if a single document was selected for the record. If multiple documents were selected for a single record, Please Enter Record Name is displayed for this value.
*Subject	Any value you type for this field is acceptable. The principal topic addressed in a document could be used. Confirm with your Records Administrator how this field is defined in your organization.

Attribute (*) indicates mandatory attributes	Description
*Media Type	<p>The value you select identifies the material or environment on which information is inscribed (microfiche, electronic, and paper for example).</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Application Format	<p>The value you select identifies the format based on the application used to create the document being declared a record.</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Originating Organization	<p>The value you type for this field should identify the official name or code of the office responsible for the creation of the document being declared.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Date Filed	<p>The value for this field is automatically populated when an email is declared a formal record.</p>
Received Date	<p>The value for this is mapped to the Received date of the email.</p>
*Publication Date	<p>The value for this is mapped to the Sent date of the email.</p>
*Unique Record Identifier	<p>Read-only field, pre-populated (system generated) to identify the record object.</p>
Record Category Identifier	<p>This field is automatically populated based on the applied naming policy.</p>

Attribute (*) indicates mandatory attributes	Description
Vital Record	The checkbox is Read-Only. The checkbox is selected if the folder to which you are declaring the record has Vital on it, which means that this record will inherit it. You cannot select or deselect this box, it only displays if a vital marking (applied directly or indirectly) is on the object.
*Authors	Read-Only value that is mapped to the From field of the email. You can click Insert to insert another value and all inserted values are saved.
Keywords	Type in text that can be used to facilitate searching. The metadata on a form associated to a particular record can be used for keywords. You can click Insert to insert another value and all inserted values are saved.
Addressee(s)	Read-Only value that is mapped to the To field of the email.
Other Addressees	Read-Only value that is mapped to the CC field of the email.
Hidden Addressees	Read-Only value that is mapped to the BCC field of the email.
Location	Type in the name of the location to indicate where the record is kept. Confirm with your Records Administrator how this field is defined in your organization.
Project Name	Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.
Supplemental Marking	Add supplemental markings to add additional security to the object.

Attribute	Description
(*) indicates mandatory attributes	
Create Record Relationship	Displays a page that allows you to choose the record relationship type. On this page there is also a locator that allows you to connect the record being declared to another as a child or as a parent using the selected relationship type. For further details about record relationships, refer to “Record relations” on page 405.

C.4.1.3 Entering values on the Department of Defense classified records form

Refer to this section if you are declaring a document as a classified record. Attributes on the sample form, are described in “Attributes for classified records (Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_classified_rec))” on page 750.

The screenshot shows a Microsoft Word document window with the title bar 'Info : AAA(2).doc (File 1 of 2)'. The content area contains a form for entering record information. The fields include:

- Record Name: AAA(2).doc
- Unique Record Identifier: 090103c280004b74
- Record Category Identifier: No items
- Items per page: 10
- Subject: [empty]
- Media Type: [dropdown menu]
- Format: [dropdown menu]
- Originating Organization: [empty]
- Date Filed: Nov 30, 2009 4:35 PM
- Received Date: Date 12:00 AM
- Publication Date: Nov 30, 2009 4:35 PM
- Vital Record Indicator: [checkbox]
- Authors: [button] Insert [button] Delete
- Authors: [list box]

Figure C-2: Default settings on a form for classified formal records

Appendix C. Records Manager and Department of Defense functionality

Keywords:

Addressees:

Other Addressees:

Locations:

Derived From:

- Classification Guide
- Original Classified Record
- none

Classification Guide:

Title	Initial Classification	Declassify On	Classified By	Publication Date	Supplemental Marking	Project Name	Originating Organization	Exemption Category	Reason for Classification
-------	------------------------	---------------	---------------	------------------	----------------------	--------------	--------------------------	--------------------	---------------------------

bold column means attribute value will be automatically copied into form

Other Sources:

Project Name: Available
Project A
Project B
Project C

Supplemental Marking: Available
FGI
FORMERLY RESTRICTED DATA
FOUO
NATO
NOCONTRACT

Downgrade on Schedule: Upgrade Review

Classification: Initial Current

Classifying Agency:

Classified By: Available
Anne Ly
author1
author10
author2
author3

The screenshot shows a Windows-style application window titled 'Classification'. It contains several dropdown menus and lists:

- Reasons for Classification:** Available items include 1.4(a) Military plans, weapons systems; 1.4(b) Foreign government, informal; 1.4(c) Intelligence activities (including counterintelligence); 1.4(d) Foreign relations or foreign policy; 1.4(e) Scientific, technological, or engineering.
- Declassify On:** Available items include Date (dropdown menu), Declassify On Date (Date picker set to 12:00 AM), and Declassify On Event (dropdown menu).
- Exemption Category:** Available items include X1. Reveal an intelligence source, method, or technique; X2. Reveal information that would compromise the国家安全 of the United States; X3. Reveal information that would compromise the security of the military; X4. Reveal United States military plans; X5. Reveal foreign government information.
- Declassified On:** Available items include (Extend): 25K1. Reveal the identity of a confidential informant; 25K2. Reveal information that would compromise the国家安全 of the United States; 25K3. Reveal information that would compromise the security of the military; 25K4. Reveal information that would compromise the safety of the public; 25K5. Reveal actual U.S. military weapons systems.
- Declassified By:** This section is currently empty.

At the bottom of the form are buttons for 'Create Record Relationship', '?', and 'Previous', 'Next', 'Finish', 'Cancel'.

Note: Update the classified form template if your system does not use **Unclassified** as the lowest security level. *Record Dod 5015 V3 Classified* (*dmc_rm_dod5015v3_classified_rec*) out-of-the-box supports **Unclassified** as the lowest security level. Instructions to complete the update are provided in the note at the top of the section for “[Declaring electronic or physical documents as formal records](#)” on page 340.

Next is displayed at the bottom of the form only when you select more than one item to be declared as **Individual records**. You do not have to click **Next**. You can click **Finish** to apply the same metadata to the remaining records. You only click **Next** if you want each individual record to have different metadata when filing.

All mandatory fields require entries to proceed with filing. Any field that is incorrectly addressed prevents the form from being processed. Unaccepted entries are clearly described in red text at the bottom of the form when processing is prevented. Make sure to provide entries for all the mandatory fields and that all the entries are valid.

Classified Records all have a security level, of which the lowest level is **Unclassified**. A default security level or ranking of 0 represents a classification of **Unclassified** for declassified records. Classified records can be downgraded from Top Secret to Secret for example; the downgrade feature however does not allow downgrading to **Unclassified**. A classified record that is downgraded to Unclassified must be declassified using Declassify On, Declassify On Date, and Declassify On Event. Classified and unclassified records can also be upgraded when necessary.

The form makes it possible for you to:

- create a classified record while deriving values from a classification guide or from another classified record already present in the system

- change classification settings to upgrade or downgrade the record
- schedule downgrades and declassification
- declassify classified records or turn unclassified records into classified records
- identify reviewers if needed



Note: Values required to create classified records can be derived from classification guides which act as a template to facilitate the process. If no classification guides are available, end users must contact their Records Administrator.

Some optional attributes are conditional and become mandatory only when classified records are declared. The **Classifying Agency** for example, is optional if the security ranking for the **Current Classification** is set to *Unclassified*. A value other than *Unclassified* makes the **Classifying Agency** mandatory.

All mandatory fields require entries to proceed with filing. Any field that is incorrectly addressed prevents the form from being processed. Unaccepted entries are clearly described in red text at the bottom of the form when processing is prevented. Make sure to provide entries for all the mandatory fields and that all the entries are valid.

Table C-4: Attributes for classified records (Record DoD 5015 V3 Classified (dmc_rm_dod5015v3_classified_rec))

Attribute (*) indicates mandatory attributes	Description
*Record Name	The name of the document is populated in this field automatically if a single document was selected for the record. If multiple documents were selected for a single record, Please Enter Record Name is displayed for this value.
Record Category Identifier	This field is automatically populated based on the applied naming policy.
*Subject	Any value you type for this field is acceptable. The principal topic addressed in a document could be used. Confirm with your Records Administrator how this field is defined in your organization.

Attribute (*) indicates mandatory attributes	Description
*Media Type	<p>The value you select identifies the material or environment on which information is inscribed (microfiche, electronic, and paper for example).</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Format	<p>The value you select identifies the format based on the application used to create the document being declared a record.</p> <p>The values are created by your Records Administrator.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Originating Organization	<p>The value you type for this field should identify the official name or code of the office responsible for the creation of the document being declared.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
Date Filed	<p>The value for this field is automatically populated when a document is declared a formal record.</p>
Received Date	<p>The value you select could be the date you received the document.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Publication Date	<p>The value you select could be the publication date of the document.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p>
*Unique Record Identifier	<p>Read-only field, pre-populated (system generated) to identify the record object.</p>

Attribute (*) indicates mandatory attributes	Description
Vital Record Indicator	Read-Only checkbox. If checked it means that the document being declared has an applied retention markup with the Vital designation.
*Authors	<p>Type in the name of the person(s) who authored the document that is being declared a formal record.</p> <p>You can click Insert to insert another value and all inserted values are saved.</p>
Keywords	<p>Type in text that can be used to facilitate searching. The metadata on a form associated to a particular record can be used for keywords.</p> <p>You can click Insert to insert another value and all inserted values are saved.</p>
Addressees	<p>Type in the primary name of individual or individuals who authored the document.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p> <p>Click Insert if you need to specify additional values for this attribute. Delete removes the field which has its radio button selected. Though you can insert more than one field to create a list of possible choices, only one radio button can be selected.</p>
Other Addressees	<p>Type in the names of anyone else responsible who can address questions if necessary.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p> <p>Click Insert if you need to specify additional values for this attribute. Delete removes the field which has its radio button selected. Though you can insert more than one field to create a list of possible choices, only one radio button can be selected.</p>

Attribute (*) indicates mandatory attributes	Description
Locations	<p>Type in the name of the location to indicate where the record is kept.</p> <p>Confirm with your Records Administrator how this field is defined in your organization.</p> <p>Click Insert if you need to specify additional values for this attribute. Delete removes the field which has its radio button selected. Though you can insert more than one field to create a list of possible choices, only one radio button can be selected.</p>
Derived From	<p>Classification fields for a classified record can be derived, that is populated automatically from a Classification Guide or from an Original Classified Record. They can also be populated manually if the radio button for none is selected. In either case, whether you select the radio button for a Classification Guide or for an Original Classified Record, you must select an item from the respective list box.</p> <p>The following classification fields will copy their values to the form:</p> <ul style="list-style-type: none"> • Initial Classification • Declassify On • Declassify On Date • Classified By • Supplemental Marking • Project Name • Exemption Category • Reason For Classification <p>All of these populate the form in both cases, using a Classification Guide or an Original Classified Record.</p>
Other Sources	<p>The text box for this attribute lets you describe other sources you might use or reference to obtain values if you do not derive them from a classification guide or from an original classified record. You can Insert and Delete text boxes as necessary to define more than one other source.</p>

Attribute (*) indicates mandatory attributes	Description
Project Name	Select the attribute marking(s) from this attribute marking set that provides the amount of security needed to access the record by those members in the group tied to a particular attribute marking.
Supplemental Marking	Select the attribute marking(s) from this attribute marking set if you need additional security on top of existing security.
Downgrade on Schedule	<p>The following options are added to the bottom of the form when you select the checkbox for this attribute:</p> <ul style="list-style-type: none"> • Downgrade On • *Downgraded On Date • *Downgraded On Event • Target Downgrade Level • *Downgrade Instructions • Downgraded On • Downgraded By <p> Note: Fields identified with an asterisk are conditional, which can be optional or mandatory based on the trigger selected for Downgrade On.</p> <p>Downgrade is not applicable to unclassified records (which already have the lowest security ranking of Unclassified equal to 0).</p>
Downgrade On	<p>Use this option to identify the trigger that will be used to start the downgrade. Though there are 3 triggers (<i>Date</i>, <i>Event</i>, and <i>Date and Event</i>) in the list, a fourth item in the list is left <i>blank</i> to allow for a manual downgrade.</p> <p> Note: Though some of the options are conditional depending on the trigger selected, only those options that become mandatory need to be filled.</p>
Downgrade On Date	<p>Specify the date you want the downgrade to be done on if the trigger includes a date.</p> <p>This field is conditional, it becomes mandatory only if you select Date or Date and Event for the trigger.</p>

Attribute	Description
(*) indicates mandatory attributes	
Downgrade On Event	<p>Specify the event you want the downgrade to be done on if the trigger includes an event.</p> <p>This field is conditional, it becomes mandatory only if you select Event or Date and Event for the trigger.</p>
Target Downgrade Level	<p>You can only downgrade to any level lower than the current security level but not all the way to Unclassified as this is declassifying which is done differently on the form.</p>
Downgrade Instructions	<p>Specify instructions for the downgrade.</p> <p>This field is conditional, it becomes mandatory regardless of the trigger selected unless no trigger is specified.</p>
Downgraded On	<p>Read-Only field that is automatically populated when the downgrade is processed.</p>
Downgraded By	<p>Select any user from the list.</p>
Upgrade	<p>The following options are added to the bottom of the form when you select the checkbox for this attribute:</p> <ul style="list-style-type: none"> • Upgraded On • Upgraded By • Reasons for Upgrade
Upgraded On	<p>The value for this field is automatically populated when the upgrade is processed.</p>
Upgraded By	<p>Add the name of the user.</p>
Reasons for Upgrade	<p>Choose the radio button next to the preferred method to specify the value and complete the entry.</p>
Review	<p>The following options are added to the bottom of the form when you select the checkbox for this attribute:</p> <ul style="list-style-type: none"> • Reviewed On • Reviewed By <p> Note: Reviewed By is mandatory only when a date is specified for Reviewed On.</p>
Reviewed On	<p>Specify the date and time the review was completed, if a review was involved.</p>

Attribute (*) indicates mandatory attributes	Description
Reviewed By	Enter the name of the reviewer(s). This field is mandatory only if a review date is specified.
*Initial Classification	The value for this field is automatically populated if values are derived from a source such as <i>Classification Guides</i> or <i>Original Classified Records</i> . Regardless of the source that values are derived from, you can reset the value as needed.
*Current Classification	The value for this field is automatically populated if values are derived from a source such as <i>Classification Guides</i> or <i>Original Classified Records</i> . Regardless of the source that values are derived from, you can reset the value as needed.
Classifying Agency	Type the name of the classifying agency when you are creating a classified record. Confirm with your Records Administrator how this field is defined in your organization.
Classified By	This field becomes mandatory when creating a classified record when the Current Classification is higher than <i>Unclassified</i> . It is otherwise optional when creating unclassified records. Select the radio button next to the means by which to specify a valid user for this value. You can choose to select from a list or type in the value. Confirm with your Records Administrator how this field is defined in your organization.
Reasons for Classification	Select from a list of valid values the reason for creating a classified record if a classification guide is not specified for Derived From or if one is selected but has no value specified to automatically populate this field. You can change the default value set by the classification guide if necessary.

Attribute (*) indicates mandatory attributes	Description
Declassify On	<p>Select from the list of triggers the trigger needed to initiate declassification for classified records. Although a blank is included among the options in the list box, the other 4 options for the triggers are:</p> <ul style="list-style-type: none"> • Exemption Category and Date • Manual Date • Event • Date and Event • Auto Calculated Date <p>Auto-calculated date takes the Publication Date entered on the form and adds the Declassification threshold to generate the declassification date.</p> <p>Classified records at some point in time should be declassified. A blank is included among the triggers as the value to be selected for unclassified records when the Current Classification specifies <i>Unclassified</i>.</p> <p>The value for this field could be automatically populated according to a classification guide if one is selected for Derived From. You can change the value as needed.</p> <p>This field cannot be automatically populated if Declassify On on the classification guide selected is not given a value.</p>
*Declassify On Date	<p>This field is mandatory if the declassifying trigger selected for Declassify On is set to the <i>Date</i> or the <i>Date and Event</i>.</p>
Declassify On Event	<p>This field is mandatory if the declassifying trigger selected for Declassify On is set to the <i>Event</i> or the <i>Date and Event</i>.</p>

Attribute (*) indicates mandatory attributes	Description
Exemption Category	<p>Select from a list of valid values the exemption category if a classification guide is not specified for Derived From or if one is selected but has no value specified to automatically populate this field.</p> <p>The exemption category is required if you select a declassification date that exceeds the declassification threshold (in other words the records would normally be declassified by a certain date but you are asking for an extension).</p> <p>You can change the default value set by the classification guide if necessary.</p> <p>A value other than classification guides selected for Derived From makes this field read-only.</p>
Declassified On	Read-Only value that displays the time and date that the record was declassified on (either manually or automatically by the declassification job).
Declassified By	Read only that identifies the person who performed the declassification or the account associated with the job.
Create Record Relationship	Displays a page that allows you to choose the record relationship type. On this page there is also a locator that allows you to connect the record being declared to another as a child or as a parent using the selected relationship type. For further details about record relationships, refer to “Record relations” on page 405.

C.5 Running the Department of Defense declassification report

The declassification report is used to report on all classified records in the system and gives administrators the capability to report on all classified records that have been declassified. It includes an action button that allows administrators to purge declassified records. There are several filters that enable administrators to query by declassification date or to query for records that are on hold or permanent status. This report is available only if the Department of Defense Classified dar file is installed and if the user is in the dmc_rm_security_officer role.

Records when they are declassified are automatically exported to a specific location C:\Documentum\RM\Declassification Export and can be purged using the declassified report. Once exported, declassified records can then be imported as a Department of Defense record into a declassified (for example, public) file plan or repository.

To run the declassification report:

1. Select **Records > Reports > Declassification Report**. The **Declassification Report** is displayed.

You can click **Report** against the default settings or change the default settings to narrow the results. Reporting against the default filter settings returns results showing only declassified records. All declassified records are displayed if the default **Declassification Date** value is not changed. Filters can be set to show only declassified records that have Hold and Permanent retention markups or only declassified records. Filters can also be set to show all classified records that have Hold and Permanent retention markups or all records regardless of any retention markups.

2. Select a date range for the **Declassification Date** and click **Report** to obtain results based on default settings or the desired settings.

Only declassified records can be purged. Attempts to purge classified records will be prevented. *To purge declassified records:*

- a. Select one or more declassified records in the results returned and click **Purge Declassified**.

The **Declassified Records Purge Authorization Check** screen is displayed to confirm the action.

- b. Enter your **User Name, Password**, and a reason for the **Justification** and click **OK** to continue.

The **Declassified Records Purge Warning** screen is displayed.

- c. Click **OK** to complete the action.

C.6 Records - XML export and XML import operations

Department of Defense records (Department of Defense email records, Department of Defense standard records, or Department of Defense classified records) and Department of Defense folders stored in a repository can be recreated in other repositories by importing an XML file that is generated from the Department of Defense Schema. The Department of Defense schema supports the following three export scenarios:

- Exporting manually using Records > Export to XML and selecting Department of Defense Schema to generate an XML file
- Declassification whereby declassified records are automatically exported and processed through the Department of Defense Schema to generate an XML file
- Disposition whereby NARA transfers are automatically exported and processed through the Department of Defense Schema to generate an XML file

The XML file generated according to any one of the export scenarios can then be selected, at anytime, using Import From XML to recreate the Department of Defense records in another location.



- Note:**
- 1) Import of records does not use retention information. Records imported into the new location inherit policies from the new folder.
 - 2) The child record in a Department of Defense record relation must be imported first to recreate the relation in the new location. A record relation is then recreated in the new location when the parent record is imported.
 - 3) Both the parent and child must be imported into the same folder to recreate the record relation.
 - 4) Any information not encoded in the Department of Defense Schema is not exported or imported.

To manually export Department of Defense record or Department of Defense folder objects from a repository:

1. Navigate to a Department of Defense record or Department of Defense folder in the repository and select it in the content pane. For example, **doc-01**.
2. Select **Records > Export To XML** and click **DoD Schema**.
3. Select an export location from the **Select Folder** screen displayed.
4. Click **Yes** on the **Yes/No** screen displayed to continue, or **No** to abort if necessary.

An **Export successful** message appears at the bottom of the content pane when the operation is completed.

The XML file exported can now be imported to recreate Department of Defense records or Department of Defense folders objects in other locations.

5. Optionally, you can navigate to the export location to see the XML file that now represents the Department of Defense record and/or records selected.

For example, **0909ade98000464c_doc-01_0909ade980004649_doc-01_2.xml**.



Note: Records supports Export to XML in Department of Defense Schema functionality for new Department of Defense email records, whose source email messages are imported in their native Microsoft Outlook message format (.msg format).

To import Department of Defense record or Department of Defense folder objects exported to XML:

The XML file generated as a result of any of the export scenarios described at the top of this section must be available for this procedure. The Department of Defense record or Department of Defense folder object is recreated in the new location from the XML file when it is imported.

1. Select **Records > Import From XML**.
2. Click **Add Files** on the **Import XML Files** screen.
3. Navigate to the XML file created from the export operation to add it.

For example click **0909ade98000464c_doc-01_0909ade980004649_doc-01_2.xml**, then click **OK**.

The screen refreshes so you can select a File Plan location. The **Finish** button however is unavailable until a valid folder location for the File Plan is selected. A valid folder location is a managed folder that has at least one record policy or a retention policy applied to it.

4. Click **Select** to add a **File Plan** location from the resulting locator screen.
 5. Click **OK** on the locator screen to accept the selected location.
 6. Click **Finish** to complete the process.
- A confirmation message is displayed at the bottom of the content pane.
7. Optionally, you can navigate to the File Plan location selected for the formal record or records to see them in their new file plan location.



Note: To recreate a Department of Defense Email Record by importing XML files in Department of Defense Schema, the `shouldParseMsgFile` property must be set to true in `mailapp.properties`. During recreation of Department of Defense email record using the XML file in Department of Defense Schema, the source email message is imported into repository in its native outlook message format (.msg format) as an object of `dm_email_message` type or any of its sub-types. The import of source email message in EMCMF format as an object of `dm_message_archive` type or its subtypes is not supported. The object type of

the source email message imported into repository during this operation is determined based on the value set for the attribute 'Source Email Type For Filing Email Records' in Records Manager Docbase Configuration object. The supported object type values for this attribute include `dm_email_message` and its subtypes. The default value for this attribute is `dm_email_message`.

Appendix D. XML Report examples against View Input and View Results

View Input and View Results are menu options that are displayed against the Work Order Report and the Work Order Breakdown Report when you right-click a work order in the list of results returned. The input parameters and the results parameters are captured in XML schemas which are the XML work order reports. A Work Order Report Summary XML schema is also available, which captures input parameters from the work order input. The XML tags are labeled to indicate what parameter is represented.

The XML report generated against View Input is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<wOInput xmlns="http://documentum.emc.com/records/WorkOrderInput" xmlns:ns2="http://documentum.emc.com/records/RecordsPolicy">
    <inputSource>
        <items>
            <item>0900167f80003307</item>
        </items>
    </inputSource>
    <inputParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="GenericParameters">
        <genericParameter>
            <key>apply_markup_reason</key>
            <values>
                <value></value>
            </values>
        </genericParameter>
        <genericParameter>
            <key>apply_markup_ids</key>
            <values>
                <value>0800167f80003313</value>
            </values>
        </genericParameter>
        <genericParameter>
            <key>operation_mode</key>
            <values>
                <value>DIRECT</value>
            </values>
        </genericParameter>
    </inputParameters>
    <processedItems>
        <processedItem>0900167f80003307</processedItem>
    </processedItems>
    <failedItems/>
</wOInput>
```

The XML report generated against View Results is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<OperationReport xmlns:ns2="http://documentum.emc.com/records/ProcessedItem" xmlns:ns3="http://documentum.emc.com/records/ProcessedItemResult" xmlns:ns4="http://documentum.emc.com/records/ActionItems" xmlns:ns5="http://documentum.emc.com/records/FailureItems" xmlns:ns6="http://documentum.emc.com/records/SkippedItems" xmlns:ns7="http://documentum.emc.com/records/WarningItems" xmlns:ns8="http://documentum.emc.com/records/SuccessItems" xmlns:ns9="http://documentum.emc.com/records/ReportSummary">
    <ns9:ReportSummary>
        <ns9:processor_host></ns9:processor_host>
        <ns9:operation>APPLY_REMOVE_MARKUP</ns9:operation>
        <ns9:Parameters>
            <ns9:parameter>
                <ns9:name>apply_markup_reason</ns9:name>
                <ns9:value></ns9:value>
```

```
</ns9:parameter>
<ns9:parameter>
    <ns9:name>apply_markup_ids</ns9:name>
    <ns9:value>0800167f80003313</ns9:value>
</ns9:parameter>
<ns9:parameter>
    <ns9:name>operation_mode</ns9:name>
    <ns9:value>DIRECT</ns9:value>
</ns9:parameter>
</ns9:Parameters>
<ns9:initiated_by>dcmbao3</ns9:initiated_by>
<ns9:status>SUCCEEDED</ns9:status>
<ns9:start_time>2012-09-19T13:52:59.000-04:00</ns9:start_time>
<ns9:last_update_time>2012-09-19T13:53:10.251-04:00</ns9:last_update_time>
<ns9:terminated>false</ns9:terminated>
<ns9:total_processed>1</ns9:total_processed>
<ns9:total_skipped>0</ns9:total_skipped>
<ns9:total_success>1</ns9:total_success>
<ns9:total_failure>0</ns9:total_failure>
<ns9:total_actions>0</ns9:total_actions>
<ns9:total_warned>0</ns9:total_warned>
</ns9:ReportSummary>
<ns8:SuccessItems>
    <ns3:ProcessedItemResult>
        <ns2:ProcessedItem>
            <ns2:object_id>0900167f80003307</ns2:object_id>
            <ns2:object_name>a2</ns2:object_name>
            <ns2:version>1.0,CURRENT</ns2:version>
            <ns2:object_type>dm_document</ns2:object_type>
            <ns2:content_type>msw12</ns2:content_type>
            <ns2:folder_location>/b3cab/misc</ns2:folder_location>
        </ns2:ProcessedItem>
        <ns3:message>[Successfully applied Retention Markup ids, 0800167f80003313
to item with object id, 0900167f80003307.]</ns3:message>
        <ns3:result_time>2012-09-19T13:53:09.940-04:00</ns3:result_time>
    </ns3:ProcessedItemResult>
</ns8:SuccessItems>
</OperationReport>
```

Appendix E. Optional attributes

The list of attributes described hereunder are those that are not displayed by default on the Column Preferences dialog for a particular piece of functionality. For example, columns not displayed by default for the Retention Report, or any other report or manager, and so forth, are described here.

Table E-1: Optional attributes to display as a column (column headings)

Column Heading	Description
Acknowledged By Me	This relates to Retention Policy Services notifications and indicates that the notification has been acknowledged by the current user.
Action Name	Retention policies can have actions that need to be done when either entering or leaving a phase. The action name is an identifier that the Retention Manager has to specify to help understand what the action is supposed to do. For example, if you want to send an inbox notification to all of the Retention Managers when entering the final phase, the user may want to enter the name Notify Retention Managers when entering final phase.
All Events	The choose an event locator has a filter to display either: All Events, System Events, or Custom Events.
Applied Markup Id	All applied retention markups will have a unique object id.
Approved On	This is the Retention Markup Approved Date from the Retention Markup. This date is per markup not per application of the markup.
Approvers	This is the Approvers found on the Contacts tab from a retention markup. The approvers are per markup not per application of the markup.
Assembled From Id	Object id of the virtual document that is the source of the assembly, formal record for example, associated with a document.
Cascade Rule	Indicates the value that is set for the Cascade Rule under the Policy Rules of a retention policy. Possible values: Cascade To Everything, Cascade To Subcategories, Cascade To Subfolders, Do Not Cascade.

Column Heading	Description
Completed Disposition On	The date when disposition last completed. This could be due to either a rollover, a reset, or if disposition completed resulting in either a terminal retainer being applied or the objects destruction.
Created	
Current Events	
Current State Number	
Disposition Strategy Id	
Format	
Fulfilled Events	
Future Events	
Has Frozen Assembly	
Inherited	If the markup was applied directly, then the value was not inherited. Markups are inherited because of folder hierarchies and if the document is part of a snapshot.
Container Aging	
Final Phase	
Is Replica	
Is Virtual Document	
Link Count	
Linked Strategy Type	Indicates whether a linked retention policy is structural or not. <i>Structural</i> is displayed when the Retention Strategy is set to <i>Linked</i> and the checkbox for the Structural Retention Type is selected. <i>Nonstructural</i> is displayed when the Retention Strategy is set to <i>Linked</i> and the checkbox for the Structural Retention Type is deselected. Otherwise, a blank (nothing) is displayed when the Retention Strategy is set to <i>Individual</i> .
Markup Id	Object id of the markup.
Notification Id	The object id of a work order notification.
Notification Type	Indicates whether a work order notification was sent as an Email or Inbox notification.
Number of Resets	Folders, with structural retention, that have been emptied after a disposition run are reset to restart the aging process. Structurally retained folders cannot be deleted.

Column Heading	Description
Number Sent	Indicates the number of work order notifications that were sent to obtain acknowledgement.
Object Id	Object ID of the folder or document that has the markup applied.
Past Events	
Phase	The name assigned to the phase of a lifecycle.
Phase Authorities	The authorities specified for each phase of a lifecycle that is selected for a retention policy.
Previous Receiving Organization	
Requestors	Entities in the list of requestors on the Contacts tab of a retention markup.
Retained Object Id	The ID of the object that is under retention.
Retainer Id	The object ID of a retainer.
Retention Strategy	Any of the retention strategies could be displayed, either for transfer runs or strategy runs.
Retention Type	Either linked or individual retention could be specified for a retention policy.
Review Date	The value entered for the Retention Markup Review Date on a retention markup.
Reviewed On	The actual date and time the review was done on.
Rollover Policy Id	The object id assigned to the rollover retention policy specified for a retention policy. A rollover retention policy must be specified for any retention policy that is non-terminating.
State Change User Id	The id of the user responsible for the state change in a close folder operation, that is a close, re-open, or revert action.
Type	The retention markup report returns results under this column heading. Identifies the object type: dm_folder, dm_cabinet, dm_document, and so forth.
Version	

