

EMC® Documentum®

Documentum Administrator

Version 6.5 SP3

User Guide

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com. All other trademarks used herein are the property of their respective owners.

© Copyright 2010 EMC Corporation. All rights reserved.

Table of Contents

Preface	27
Chapter 1	Introducing Documentum Administrator	29
	Logging in to Documentum Administrator	31
	About the System Information page.....	32
	Determining the Documentum Administrator version to which you are connected	34
	How to use Documentum Administrator	34
	User privileges	35
	Creating new objects.....	35
	Modifying or viewing existing objects.....	35
	Confirming object deletion	35
	Selecting a type	36
	Selecting a user or group.....	36
	Setting the connection broker list	36
	Configuring licenses	37
	Viewing enabled licenses	37
	Enabling a feature or product.....	38
Chapter 2	Repositories	39
	Log into a repository.....	39
	Log in as an express user.....	41
	Log into another repository.....	41
	Log out of all repositories.....	41
	Set your favorite repositories.....	41
	Navigate a repository	42
	Select the columns that appear in lists	43
	Navigate categories	44
	Locate an item in a selection dialog box.....	44
	Set your preferences	45
	Open an additional repository window.....	47
	Drag-and-drop	47
	Right-click.....	47
	View messages	48
	View the status of background operations	48
	Refresh page	48
	Select HTTP or UCF content transfer.....	48
	Use modal dialogs	49
	Work with repository documents offline through My Documentum	49
	View product information.....	50

Chapter 3	Files and Folders	51
	Create a file	51
	Create a folder.....	52
	Create a cabinet	52
	Set properties	53
	Check out and edit files.....	54
	Overview of check out and edit	54
	Check out a file.....	55
	Check in a file.....	55
	Checkin information	56
	Versions	57
	Replace a repository file with a different file	58
	Cancel checkout of a file.....	58
	View currently and recently checked-out files.....	59
	View a file in read-only mode	59
	Change the format associated with a type of file	60
	Restore associated file formats to the defaults	61
	Import files to the repository	61
	Export files from the repository	62
	Deep export	63
	Delete an item from the repository.....	64
	Move an item to a new location in the repository	64
	Copy an item to a new location in the repository	64
	View your clipboard	65
	Links	65
	Link an item to another location in the repository	66
	Link an item to another repository	66
	View all locations to which an item is linked	67
	Link a repository item to your computer	67
	Add a document or folder to your browser's bookmarks or favorites	67
	Use email to send a link to a repository item.....	68
	Convert Desktop DRLs to Webtop URLs	68
	Open a link sent by email	69
	Subscriptions	69
	Receive notification when a file is read or changed.....	70
	Export the information displayed in a list.....	70
Chapter 4	Basic Configuration	73
	Repositories	73
	Viewing or modifying the docbase configuration object for a repository	74
	Modifying the synchronization settings for a repository	75
	Repository configuration properties.....	75
	Enabling Windows domain authentication for UNIX repositories	83
	Creating or modifying a domain map	84
	Defining a domain.....	84
	Modifying users for Windows domain authentication.....	85
	Content Servers	85
	Duplicating a server configuration object	86
	Creating or modifying server configuration objects	87
	Creating or modifying the server configuration object info page	88
	Creating or modifying connection broker projections	94

Modifying projection targets	95
Deleting projection targets	96
Creating, modifying, or deleting network location projections	96
Creating, modifying, or deleting application servers	97
Creating, modifying, or deleting cached types	97
Creating or modifying locations	98
Creating or modifying far stores	100
Viewing server and connection broker log files.....	100
Deleting a server configuration object	101
Configuring a server as a process engine	101
Disabling a server as a process engine	102
Federations	102
Creating or modifying federations	103
Creating federations	103
Modifying federations	105
Adding members to a federation	106
Removing member repositories from a federation.....	107
Deleting Federations.....	107
Connecting to the governing repository or a federation member	108
Choosing user subtypes	108
Modifying members of a federation	109
Choosing repository federation members	109
LDAP Servers.....	110
Understanding LDAP server configurations	112
Adding or modifying LDAP server configurations.....	113
Configuring LDAP directory and secure connection information	115
Entering directory and secure connection properties for a new LDAP server	115
Viewing or modifying directory and secure connection properties for LDAP servers	117
LDAP Server Configuration - Info page properties.....	119
Configuring synchronization and user authentication for LDAP servers	121
Configuring synchronization and user authentication for new LDAP servers	122
Viewing or modifying synchronization and user authentication properties for LDAP servers	123
LDAP Server Configuration - Sync & Authentication page properties	124
Mapping LDAP Servers	126
Adding new LDAP server mapping properties.....	127
Viewing or modifying mapping properties of existing LDAP servers	129
Using Search Builder	131
Adding or modifying repository property mapping.....	131
LDAP configuration attribute mapping examples	131
LDAP Server Configuration - Mapping page properties	132
Configuring failover settings and secondary LDAP servers	135
Understanding LDAP failover and secondary servers	136
Configuring LDAP failover when creating a new LDAP server.....	137
Viewing or modifying failover properties of existing LDAP servers	138
Configuring secondary LDAP servers	138
LDAP Server Configuration - Failover page properties.....	139
Secondary LDAP Server page properties	140
Changing the binding password.....	141
Forcing LDAP server synchronization.....	141
Duplicating LDAP configurations.....	142
Deleting LDAP configurations.....	142

Using LDAP directory servers with multiple Content Servers.....	143
LDAP Certificate Database Management.....	143
Viewing LDAP certificates	143
Importing LDAP certificates.....	144
Chapter 5 Distributed Content Configuration	145
Network locations	146
About network locations	146
Creating, copying, modifying, or viewing network locations	147
Creating network locations.....	147
Copying network locations.....	149
Modifying or viewing network locations.....	149
Deleting network locations.....	150
Deleting network location warning	151
Properties of network locations	151
ACS servers	154
About ACS servers	154
Viewing or modifying the ACS server configuration properties	155
Viewing or modifying ACS projections and stores	156
Modifying ACS server communication protocols.....	159
Designating connection brokers for an ACS server.....	160
Deleting projections or stores from an ACS server	160
Choosing network locations	162
Properties of ACS servers.....	162
ACS Server Configuration Properties - Info page	162
ACS Server Configuration Properties - Projections & Stores page.....	165
BOCS servers	168
About BOCS servers	168
Creating, modifying, or viewing BOCS servers	169
Creating BOCS servers.....	169
Setting BOCS server security	171
Setting BOCS server communication protocols	173
Viewing or modifying BOCS server properties	173
Deleting BOCS servers	174
Deleting BOCS server warning	174
Properties of BOCS servers.....	175
Configuring distributed transfer settings.....	177
Messaging server configuration	179
Chapter 6 User Management	183
User management and Documentum Collaboration Services.....	183
Users	184
Locating users	185
Setting the default permissions for the cabinet of a new user	186
Creating or modifying users.....	186
Creating users	186
Creating global users	190
User attributes.....	191
Importing users	196
Import user attributes	198
Deleting users	201
Reassigning objects to another user.....	202
Changing the home repository of a user	202
Making a user active or inactive.....	202
Modifying users	203

Viewing groups, workflows, alias sets, permission sets, and documents of a user	203
Viewing or deleting change home repository logs	203
Viewing user reassign logs	204
Reassign reports	204
Groups	204
About dynamic groups	206
Locating groups	206
Viewing where a group is used.....	206
Creating or modifying groups	207
Creating groups	207
Modifying or viewing groups.....	208
Adding users, groups, or roles to a group.....	208
Removing users from a group	209
Deleting groups.....	209
Reassigning the objects owned by a group	210
Viewing group reassign logs	210
Group attributes	210
Roles	212
Creating or modifying roles	212
Creating roles.....	213
Adding users, groups, or roles to a role	214
Modifying roles.....	214
Reassigning roles.....	215
Deleting roles	215
Role attributes	215
Module roles	217
Creating module roles.....	218
Reassigning module roles	219
Modifying module roles.....	219
Deleting module roles	219
Module role attributes	220
Sessions	221
Viewing user sessions	221
Viewing user session information	222
Viewing user session logs.....	223
Killing user sessions	223
Chapter 7 Security	225
Permissions overview	226
Object permissions	226
Folder security	228
Additional access control entries.....	229
Default alias sets.....	230
How Content Server evaluates access to an object	230
Locating a permission set	231
Viewing where a permission set is used	232
Creating or modifying permission sets	232
Creating a permission set	233
Copying a permission set	236
Setting a user's basic and extended object permissions	236
Viewing or modifying permission sets	237
Viewing or modifying a permission set	238
Adding users to permission sets	239

Deleting users from permission sets.....	241
Changing the permissions assigned to a user.....	241
Permission set properties	242
Deleting a permission set	246
Chapter 8 Audit Management	249
Managing auditing by object type.....	250
Managing auditing by object instance	252
Managing auditing by events selected for all objects in the repository	254
Modifying or removing audits for an object type	254
Modifying or removing audits for object instances.....	255
Modifying or removing audits for events	256
Searching for and viewing audit trails.....	257
Verifying audit trails.....	258
Deleting audit trails	258
Choosing a type.....	259
Selecting criteria for an audit	259
Criteria and event page	260
Audit trails.....	260
Audit policies.....	260
Creating an audit policy.....	261
Editing an audit policy.....	262
Saving a copy of an audit policy	262
Deleting an audit policy	263
Chapter 9 Job Management	265
Jobs	265
Creating jobs	268
Creating basic information for a job	270
Changing the schedule of a job	271
Setting the qualifier rules for the remove retention-expired objects job	272
Assigning a method to a job	273
Locating a method for a job	275
Creating, viewing, or modifying sysobject properties.....	275
Creating replication jobs	276
Selecting the source repository for a replication job.....	280
Selecting the target repository for a replication job	281
Setting replication job options	282
Choosing a replication folder.....	283
Choosing a replication job user	284
Choosing a permission set for replica objects	284
Choosing a storage area	284
Choosing replication and security modes	285
Creating records migration jobs	286
Setting the rules of a records migration job	289
Defining selection criteria for a records migration job.....	290
Defining version criteria for records migration job	291
Creating BOCS caching jobs	292
Setting BOCS caching rules	295
Creating job sequences.....	296
Providing repository connection and job information for a job sequence	300

Selecting repositories for a job sequence	301
Selecting jobs for a job sequence	301
Setting dependencies for a job sequence	302
Running jobs	302
Viewing the status of a running job	303
Viewing job reports	303
Setting the trace level for a job	303
Viewing job trace logs	304
Modifying jobs	304
Deleting jobs	304
Deactivating jobs on failure	305
Job descriptions	305
ACL replication (dm_ACLReplication)	306
ACL replication (dm_ACLRepl_repository)	306
Asynchronous Write (dm_AsyncronousWrite)	307
Archive (dm_DMArchive)	307
Audit management (dm_AuditMgt)	307
Consistency checker (dm_ConsistencyChecker)	308
Content replication (dm_ContentReplication)	308
Content warning (dm_ContentWarning)	309
Create full-text events (dm_FTCreateEvents)	309
Index agent startup (dm_FTIndexAgentBoot)	311
Data dictionary publisher (dm_DataDictionaryPublisher)	312
Database space warning (dm_DBWarning)	312
Distributed operations (dm_DistOperations)	312
Dmclean (dm_DMClean)	313
Dmfilescan (dm_DMfilescan)	313
Federation copy (dm_FederationCopy)	313
Federation export (dm_FederationExport)	313
Federation import (dm_FederationImport)	314
Federation status (dm_FederationStatus)	314
Federation update (dm_FederationUpdate)	314
File report (dm_FileReport)	314
Group rename (dm_GroupRename)	315
LDAP synchronization (dm_LDAPSynchronization)	315
Log purge (dm_LogPurge)	316
Queue management (dm_QueueMgt)	316
Remove expired retention objects (dm_RemoveExpiredRetnObjects)	317
Rendition manager (dm_RenditionMgt)	318
SCS log purge (dm_SCSLogPurgeJob)	318
State of repository report (dm_StateOfDocbase)	318
Swap info (dm_SwapInfo)	319
Update statistics (dm_UpdateStats)	319
User change home repository (dm_UserChgHomeDb)	319
User rename (dm_UserRename)	320
Version management (dm_VersionMgt)	320
WfmsTimer (dm_WfmsTimer)	320
Methods	321
Creating or modifying methods	321
Importing method content	324
Running methods	324
Viewing the results of a method	326
Exporting method content	326
Editing method content	326
Checking in method content	327
Deleting methods	328
Administration methods	328

	Viewing administration methods	328
	Running administration methods	329
	CAN_FETCH	330
	CLEAN_LINKS	331
	DELETE_REPLICA	331
	DESTROY_CONTENT	332
	GET_PATH	333
	IMPORT_REPLICA	334
	MIGRATE_CONTENT	334
	PURGE_CONTENT	339
	REPLICATE	340
	RESTORE_CONTENT	340
	SET_STORAGE_STATE	341
	DB_STATS	342
	EXEC_SQL	343
	MAKE_INDEX	343
	DROP_INDEX	344
	MOVE_INDEX	345
	FINISH_INDEX_MOVES	345
	GENERATE_PARTITION_SCHEME_SQL	346
	ESTIMATE_SEARCH	348
	MARK_FOR_RETRY	348
	MODIFY_TRACE	349
	GET_LAST_SQL	350
	LIST_RESOURCES	350
	LIST_TARGETS	351
	SET_OPTIONS	352
	Administration Methods Results Page	353
	Choosing a file on the server file system	354
Chapter 10	Alias Sets	355
	Locating alias sets	356
	Creating or modifying alias sets	356
	Creating alias sets	356
	Viewing or modifying alias sets	357
	Viewing alias set aliases	357
	Adding, modifying, and deleting alias set aliases	358
	Deleting alias sets	360
Chapter 11	Formats	361
	Locating formats	361
	Creating new formats	361
	Viewing or modifying a format	362
	Deleting formats	362
	Format properties	362
Chapter 12	Types	365
	Creating types	366
	Modifying types	368
	Type Properties	370
	Selecting supertypes	374
	Selecting default groups	374

Adding properties to types.....	375
Deleting types	375
Viewing assignment policies	376
Converting types to shareable object types	376
Converting types to lightweight object types	377
Converting types to shareable and lightweight object types.....	378
Chapter 13 Storage Management	379
Storage	379
Storage area types.....	382
Viewing the properties of storage areas	383
Deleting storage areas, locations, mount points, and plug-ins	383
File stores.....	383
Creating file stores.....	384
Modifying file stores	386
Properties of a file store.....	387
Linked stores.....	389
Creating linked stores	389
Modifying linked stores	390
Properties of a linked store	390
Blob stores	391
Creating blob stores	391
Viewing or modifying blob store properties	392
Properties of a blob store	392
Distributed stores	393
Creating distributed stores	393
Modifying distributed stores	394
Properties of a distributed store	395
External stores.....	396
Creating external stores.....	397
Modifying an external store.....	399
Editing a server root location.....	400
Properties of an external store	401
EMC Centera stores	402
Creating EMC Centera stores	403
Modifying an EMC Centera store.....	405
Defining the storage parameters for an EMC Centera store.....	405
Defining the content attributes saved in an EMC Centera store	407
Properties of an EMC Centera store	408
NetApp SnapLock stores.....	410
Creating NetApp SnapLock stores	411
Modifying a NetApp SnapLock store	412
Properties of a NetApp SnapLock store.....	412
Mount points	414
Creating or modifying mount points.....	414
Locations	416
Creating or modifying locations	416
Plug-ins	417
Creating or modifying plug-ins	418
Assignment policies.....	419
Creating or modifying assignment policies.....	421
Viewing a list of assignment policies	422
Creating assignment policies	422
Viewing or modifying the properties of an assignment policy.....	424
Modifying the permissions of an assignment policy	424
Properties of an assignment policy.....	424

Examples of custom assignment policy rules	427
Associating an assignment policy with an object type	427
Deleting assignment policies	428
Setting or updating a retention date or retention period for documents or other objects	428
Migration policies.....	429
Creating migration policies	430
Setting the rules of a migration policy	434
Viewing or modifying migration policies	436
Deleting migration policies	436
Chapter 14 Content Delivery	439
Locating content delivery configurations.....	441
Creating or modifying content delivery configurations	441
Creating content delivery configurations.....	442
Modifying content delivery configurations.....	446
Creating or modifying the advanced properties of a content delivery configuration.....	448
Creating or modifying replication settings for a content delivery configuration.....	450
Creating or modifying extra arguments for a content delivery configuration.....	452
Extra arguments	452
Content delivery configuration fields	463
Deleting content delivery configurations	470
Testing content delivery configurations	470
Duplicating a content delivery configuration	471
Deactivating a content delivery configuration	472
Publishing objects.....	472
Content delivery configuration results	474
Content delivery logs.....	474
Viewing content delivery logs	474
Deleting content delivery logs	474
About effective labels.....	475
Chapter 15 Indexing Management	477
Index agents and index servers.....	478
Starting and stopping index agents	479
Starting and stopping index servers	479
Suspending and resuming index servers	480
Reindexing index servers	480
Disabling index agents.....	481
Enabling index agents.....	481
Verifying indexing actions.....	482
Viewing or modifying index agent properties.....	482
Viewing index server properties	482
Viewing index server logs	483
Managing index queue items.....	483

Resubmitting individual objects	484
Resubmitting all failed queue items	485
Removing queue items by status	485
Removing queue items.....	485
Viewing queue items associated with an object.....	486
Creating a new indexing queue item	486
Chapter 16 Content Transformation Services Administration	489
Changing the CTS user	489
Configuring a CTS instance	490
Changing the polling interval	490
Changing the logging level.....	491
Changing the System Operator.....	491
Changing the notification setting	492
Changing the maximum number of queue items	492
Changing the queue item expiry	493
Viewing a CTS log file.....	493
Viewing details of a CTS instance	494
Controlling your CTS instance.....	494
Stopping the CTS service.....	495
Starting the CTS service	495
Refreshing the CTS service	495
CTS reporting.....	496
Configuring CTS reporting.....	496
Viewing archived CTS reporting data	497
Chapter 17 Content Intelligence Services	499
Understanding Content Intelligence Services.....	499
Categorizing documents	500
Choosing categorization options.....	501
Creating taxonomies and categories.....	501
Providing category evidence	502
Confidence values and document scores	502
Stemming and phrase order	504
Setting the language used for the stemming	504
Activating the stemming	505
Retaining the phrase order	505
Category links	505
Submitting documents for categorization	506
Reviewing proposed categorizations.....	506
Setting up Content Intelligence Services	506
Configuring Content Intelligence Services	507
Enabling Content Intelligence Services.....	507
Modifying Content Intelligence Services configuration.....	508
Building taxonomies	509
Defining category classes	510
Defining taxonomies.....	512
Creating subtypes for a taxonomy or for a category	514
Creating custom tab for the subtype.....	514
Creating subtype instances.....	516
Defining categories	518
Displaying object titles	520
Setting category rules.....	520
Defining property rules.....	521
Displaying attributes in Property rules.....	523

Defining simple evidence terms.....	524
Managing taxonomies.....	526
Making taxonomies available	526
Synchronizing taxonomies	527
Deleting taxonomies	528
Processing documents.....	528
Test processing and production processing.....	528
Defining document sets.....	529
Submitting documents to CIS server	531
Assigning a document manually	532
Reviewing categorized documents.....	532
Clearing assignments.....	533
Refining category definitions.....	534
Using compound terms.....	535
Selecting terms	536
Using common words as evidence terms.....	536
Modifying category and taxonomy properties	536
Defining compound evidence terms.....	537
Chapter 18 Resource Management	539
Understanding Resource Management.....	540
Managing resource agents.....	540
Adding resource agents or modifying agent properties	541
Adding resource agents	541
Viewing or modifying resource agent properties	542
Resource agent authentication failure	542
Deleting resource agents	543
Managing resource properties	543
Managing general information for resources	544
Managing resource attributes	545
Managing resource operations.....	546
Starting operations	546
Viewing resource notifications.....	547
Viewing the Notification page	547
Viewing resource logs.....	548
Monitoring resources	549
Manual configuration steps for monitoring resources.....	550
Chapter 19 Administrator Access	553
Understanding administrator access sets.....	553
Creating or modifying administrator access sets	555
Creating administrator access sets	555
Viewing or modifying administrator access sets	555
Deleting administrator access sets.....	556
Properties on the administrator access set pages	557
Chapter 20 Privileged Clients	559
Approving or denying privilege escalations	559
Selecting registered DFC clients.....	560
Deleting a DFC and its certificate	561
Chapter 21 Content Services for SAP Web Administrator	563
Understanding the Enterprise Integrations node of the WebAdmin GUI	563

Configuring Connections to SAP	564
Creating, viewing, and editing connections to an SAP server.....	565
Creating, viewing, and editing an SAP user.....	565
Configuring HTTP Archiving Services	566
Configuring, viewing, and editing archives	566
Deleting archived and linked documents	568
Configuring the repository document type.....	568
Specifying a custom filter	568
Specifying a built-in filter	569
Implementing external filters.....	569
Example: PI sheet	570
Customizing archives using service-based business objects.....	572
Customizing archives using SBOs.....	573
Managing temporary disk space in the CS SAP host	573
Configuring HTTP barcodes for archive linking.....	574
Configuring HTTP certificates for archive linking	574
Configuring HTTP repositories for archive linking.....	575
Configuring the Agent Component.....	575
Configuring queries	576
SAP queries.....	576
Creating, viewing, and editing an SAP query	576
Documentum queries	578
Creating, viewing, and editing a Documentum query	578
Restricting SAP query results by EMC Documentum query results.....	579
Testing queries with \$ARG# statements	580
Support for \$TODAY in FromDate parameter for sap_query_type_rfc query type	581
Linking objects	582
Creating, viewing, and editing SAP to Documentum links	583
Creating, viewing, and editing Documentum to SAP links	585
Automated early archiving using the Agent component.....	588
Arbitrary parameters when starting an SAP workflow	589
Checking the integrity of linked documents	589
Replication of information between Documentum and SAP	590
Replicating SAP objects.....	591
Replicating Documentum objects.....	593
Replicating custom DMS attributes from EMC Documentum to SAP	595
Configuring classification attributes for sap_query_type_plm query types	595
Replicating custom DMS attributes to SAP custom tables	597
Working with the FILTER attribute	600
Using Auto Manage to execute CS SAP actions.....	600
Creating, viewing, and editing an Agent	601
Auto Manage notification.....	602
Registering and HVP worker.....	602
Creating, viewing, and editing SAP jobs.....	602
Performing job maintenance.....	604
Configuring the Manage and View Components.....	605
Configuring the Manage component.....	605
Using the PLM interface in pre-4.7 SAP systems	608
Configuring the View component	608
Chapter 22 API and DQL	611
Running DQL queries	611
Running server APIs.....	611

Chapter 23	Search	613
	Run a simple search.....	613
	Further define search terms	614
	Run an advanced search.....	616
	Enter values for an advanced search	617
	View search results	620
	Smart navigation	621
	Monitor search results in real time	621
	Save search results from external sources	623
	View your most recent results but do not relaunch the search.....	623
	Improve your search experience	623
	How configuration can impact your search experience.....	624
	Index a repository.....	625
	Searchable items.....	625
	Saved searches	626
	Save a search to run again later.....	626
	Run a saved search	627
	View the results of a saved search but do not relaunch the search	627
	Edit a saved search	627
	Copy a saved search	628
	Search templates.....	628
	Run a search from a search template	628
	Create a search template	629
	Edit a search template	629
	Modify a search template definition.....	630
	Copy a search template	631
	Set search preferences	631
Chapter 24	Email Messages	633
	Email message archive import support.....	633
	Storing email attachments	634
	In Collaboration mode	634
	In Archive mode.....	634
	Import email messages and attachments to the repository	634
	Email conversion to EMC MF format	635
	Open an email message for viewing.....	637
	Transform an email message to HTML or PDF.....	638
	Export an email message from the repository	638
	Locate and open an email attachment	638
	Create and edit a copy of an email attachment.....	639
	Export an email attachment from the repository	639
	Locate the email to which an attachment belongs.....	640
Chapter 25	Inbox	641
	Inbox overview	641
	Open a task or notification	642
	Perform a task	642
	Complete a task.....	643
	Accept a task that has been assigned to multiple users	643
	Reject a task	644

Delegate a task	644
Repeat a task	645
Change your availability for tasks.....	645
Work queue tasks	646
Manage tasks in your queue Inbox.....	646
Get the next available task in a work queue	647
Select a task from the queue	647
Chapter 26 Workflows and Quickflows	649
Start a workflow	649
Send a quickflow	651
View workflows	651
Pause a workflow	652
Resume a paused workflow	652
Stop a workflow	652
Email the workflow supervisor or a workflow performer	653
Process a failed task in a workflow	653
Change the workflow supervisor	654
Save workflow information as a Microsoft Excel spreadsheet.....	654
View aggregated report for workflow performance.....	654
Create a workflow template	655
Chapter 27 Work Queues	657
Work queue roles.....	657
Set up a new work queue	658
Set up work assignment matching	659
Set up skill profiles in the process template	659
Define work assignment matching filters.....	660
Add work assignment matching filters to a work queue	661
Work queue policies	661
Priorities of tasks	662
Set dynamic priority and aging logic for tasks	662
Create or modify a queue policy	663
Define a queue category	664
Define a work queue.....	665
Define work queue override policies	666
Manage work queue users.....	667
Add a user or group to a work queue.....	667
Remove a user or group from a work queue	668
Add skills to work assignment processor profiles	668
Update the processor profile in a work queue.....	670
Monitor work queues.....	671
Assign or reassign a work queue task to a specific user	672
Unassign a work queue task from a user	673
Move a work queue task to another work queue.....	673
Suspend a work queue task	673
Unsuspend a work queue task.....	674
Enable users to select tasks from the queue	674
Create business calendars.....	674

Chapter 28	Lifecycles	677
	View Lifecycles	677
	Assign a lifecycle to a file	678
	Remove a lifecycle from a file	678
	Promote a file to the next lifecycle state	678
	Demote a file to its previous lifecycle state.....	679
	Suspend a file from its current lifecycle state	679
	Resume a suspended file	679
Chapter 29	Collaborate with Other Users	681
	Create and edit formatted text	681
	Discussions	682
	View discussions	683
	Add and edit comments.....	683
	Delete comments	684
	Discussions in search results	684
	Notes	685
	Contextual folders and cabinets.....	686
	Calendars.....	687
	Create calendars and events	687
	Specify recurring event properties	689
	View calendars and events	690
	Edit calendars and events.....	690
	Delete calendars and events	691
	Calendars in search results	691
	Export and import with calendars.....	691
	Data tables	692
	Create data tables and entries	692
	View data tables	695
	View data table entries.....	695
	Edit data tables.....	696
	Edit data table entries	696
	Delete data tables	697
	Import and export with data tables	697
	Rooms	697
	Visit a room	698
	Link to a room.....	698
	Objects governed by rooms	699
	Ungovern objects from a room.....	699
	Create a room.....	700
	Edit the properties of a room	701
	About room membership	702
	Copy a room	703
	Move or link to a room.....	703
	Delete a room	703
	Manage room membership	704
	Manage users as a non-administrator.....	707
	Create new users	707
	Modify users	708
	Unlist users (conceal members)	709
	Restricted folders	709
Chapter 30	My Documentum for Microsoft Outlook Administration	711

Profiles	713
Creating new profiles.....	713
The Create tab	713
The Info tab.....	714
The Target tab	715
The Import tab	716
The Permissions tab.....	718
Modifying and deleting a MyD Outlook profile	718
Overview page	720
Column Setup (Views)	720
Creating new views	721
Selecting columns	721
Modifying, duplicating and deleting views	723
Deleting views	724
Client Setup	724
Chapter 31 Taxonomies and Categories	727
Taxonomies and categories overview	727
Submitting an item for categorization	727
Chapter 32 Forms	729
Enter data in a form	729
Format text in a form	729
Create a new form	731
Save As functionality	732
Chapter 33 Records	733
Declare an item as a formal record	733
Enter values on the applicable form when declare formal record.....	734
Enter values for regular formal records	734
Enter values for Chapter 2 formal records	735
Enter values for Chapter 4 formal records	736
Link a record.....	738
Create a record relationship	738
View a record relationship	739
Remove a record relationship	739
Make library requests	739
Chapter 34 Virtual Documents	743
Virtual documents overview	743
Create a virtual document.....	744
View the structure of a virtual document	744
View the content of a virtual document.....	745
Add a descendant to a virtual document.....	745
Rearrange descendants in a virtual document.....	747
Remove a descendant from a virtual document	748
Specify that a certain version of a descendant is always used.....	749
Set a version label for a virtual document	749
Create an archive of a virtual document	749

	Convert a virtual document to a simple document.....	750
	Set your virtual document preferences	751
Chapter 35	PDF Annotations	753
	PDF annotations overview	753
	Configure PDF Annotation Service to open when user views a PDF.....	753
	Add comments to a PDF document.....	754
	View comments in a PDF document	754
Chapter 36	Relationships	755
Chapter 37	Renditions and Transformations	757
	Renditions and transformations overview	757
	Viewing renditions	758
	Dragging and dropping renditions to the desktop	758
	Importing a rendition	759
	Setting a default rendition for an object	759
	Viewing the default rendition.....	760
	Overriding an object's default thumbnail.....	760
	Resetting renditions	761
	Transforming a document to PDF or HTML format.....	761
	Creating a rendition through transformation	762
	Creating a related object through transformation	763
	Replacing a file through transformation	764
	Creating a new version through transformation.....	765
	Creating a package through transformation.....	765
	Viewing saved transformation properties.....	766
	Enabling inbox notification.....	767
Appendix A	Keyboard Shortcuts for Microsoft Windows and Mac Operating Systems	769

List of Figures

Figure 1.	System Information page	33
Figure 2.	Selection dialog box with two list boxes	45
Figure 3.	Repository Configuration Properties - Info page (1 of 2)	76
Figure 4.	Repository Configuration Properties - Info page (2 of 2)	76
Figure 5.	Repository Configuration Properties - Synchronization page	82
Figure 6.	LDAP Server Configuration Properties - Info page.....	119
Figure 7.	LDAP Server Configuration Properties - Sync & Authentication page	125
Figure 8.	LDAP Server Configuration Properties - Mapping page (1 of 2)	132
Figure 9.	LDAP Server Configuration Properties - Mapping page (2 of 2)	133
Figure 10.	LDAP Configuration - Failover page.....	139
Figure 11.	New Network Location - Info page	152
Figure 12.	ACS Server Configuration Properties - Info page	163
Figure 13.	ACS Server Configuration Properties - Projections & Stores page.....	165
Figure 14.	New BOCS Server Configuration - Security page	172
Figure 15.	BOCS Server Configuration Properties: Info page	175
Figure 16.	Distributed Transfer Settings Properties - Info page	178
Figure 17.	Messaging Server Configuration Properties - Info page	180
Figure 18.	Permission Set Properties - Permissions page.....	243
Figure 19.	New Assignment Policy - Info page	425
Figure 20.	Partial pharmaceutical taxonomy.....	502
Figure 21.	Administrator Access Set Properties - Info page.....	557
Figure 22.	WebAdmin - initial page	563
Figure 23.	Agent services	576
Figure 24.	Query test	581
Figure 25.	Linking result.....	584
Figure 26.	Linking result.....	587
Figure 27.	Integrity checking.....	590
Figure 28.	Replication result.....	592
Figure 29.	Agent services	601
Figure 30.	Real-time results in the search monitor screen	622
Figure 31.	HTML viewer for email.....	636
Figure 32.	Enhanced search.....	637
Figure 33.	Repository members in relation to room members, groups, and roles.....	702
Figure 34.	Location of Client for Outlook node in Documentum Administrator	712
Figure 35.	Create new DCO profile	713
Figure 36.	Create tab	714
Figure 37.	Info tab	714

Table of Contents

Figure 38.	Right arrow button	715
Figure 39.	Selecting target destinations for MyD Outlook profiles.....	716
Figure 40.	Profile creation Import tab.....	717
Figure 41.	The My Documentum for Microsoft Outlook Overview panel in Documentum Administrator	720
Figure 42.	The Column Setup panel.....	721
Figure 43.	Creating a new view	721
Figure 44.	Selecting columns	722
Figure 45.	Column selector drop-down menu	722
Figure 46.	Right arrow.....	722
Figure 47.	The Client Setup page	724

List of Tables

Table 1.	General preferences	45
Table 2.	Formats preferences.....	46
Table 3.	Common tabs in the Properties dialog box	53
Table 4.	Checkin information	56
Table 5.	Formats tab	60
Table 6.	Properties for imported files.....	61
Table 7.	Repository Configuration Properties - Info page properties	77
Table 8.	To change the MAC Access Protocol from NT to Ushare:.....	79
Table 9.	Repository Configuration Properties - Synchronization page properties	82
Table 10.	New Server Configuration - Info and Server Configuration Properties - Info page field definitions	88
Table 11.	Locations page properties	99
Table 12.	LDAP Server Configuration list page properties	111
Table 13.	New LDAP Server Configuration - Info and LDAP Server Configuration Properties - Info page properties.....	119
Table 14.	New LDAP Server Configuration - Sync & Authentication and LDAP Server Configuration Properties - Sync & Authentication page properties	125
Table 15.	Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example	132
Table 16.	New LDAP Server Configuration - Mapping and LDAP Server Configuration Properties - Mapping page properties	133
Table 17.	New LDAP Server Configuration - Failover and LDAP Server Configuration Properties - Failover page properties	139
Table 18.	Secondary LDAP Server page properties.....	140
Table 19.	Field properties on the network location page	152
Table 20.	Field properties on the ACS server configuration Info pages.....	163
Table 21.	Field properties on the ACS server configuration Projections & Stores page	166
Table 22.	Field properties on the BOCS server configuration Info pages.....	175
Table 23.	Attributes of a user	191
Table 24.	Default values for new users	196
Table 25.	Import user attributes	198
Table 26.	Privileges for creating or modifying groups.....	205
Table 27.	Attributes of a group	210
Table 28.	Attributes of a role.....	215
Table 29.	Attributes of a role.....	220
Table 30.	Session information	222
Table 31.	Basic permissions	226

Table 32.	Extended permissions	227
Table 33.	Permissions required under folder security	229
Table 34.	Additional access control entries.....	229
Table 35.	New Permission Set - Info and Permission Set Properties - Info page properties	243
Table 36.	New Permission Set - Permissions and Permission Set Properties - Permissions page properties	244
Table 37.	New Job - Info and Job Properties - Info page properties	270
Table 38.	New BOCS Caching Job - Caching Rules and Job Properties - Caching Rules page properties	295
Table 39.	Logs deleted by log purge job.....	316
Table 40.	Format properties	363
Table 41.	Type properties	371
Table 42.	Properties of a file store.....	387
Table 43.	Properties of a linked store.....	390
Table 44.	Properties of a blob store.....	392
Table 45.	Properties of a distributed store	395
Table 46.	Properties of external stores	401
Table 47.	Properties of an EMC Centera store	408
Table 48.	Properties of a NetApp SnapLock store	413
Table 49.	Properties of a mount point	415
Table 50.	Properties of location objects	416
Table 51.	Properties of plug-in objects	418
Table 52.	Properties of an assignment policy.....	425
Table 53.	Content delivery configuration information	446
Table 54.	Extra arguments	452
Table 55.	Content delivery fields - Info page	464
Table 56.	Content delivery fields - Advanced page	465
Table 57.	Content delivery fields - Replication page	469
Table 58.	Using effective labels	475
Table 59.	Date formats for property rules	523
Table 60.	Start Operation page properties.....	546
Table 61.	Fields on the Notification page	548
Table 62.	Administrator access sets page properties	557
Table 63.	Privileged Clients list page properties.....	560
Table 64.	Valid entries	567
Table 65.	External filters	569
Table 66.	Query types	577
Table 67.	Parameters	605
Table 68.	Parameters	609
Table 69.	Further define search terms	614
Table 70.	Common properties in an advanced search	618
Table 71.	Select a property-to-value relationship	619
Table 72.	Properties for imported email messages	635

Table 73.	User roles for work queues.....	658
Table 74.	Common lifecycle states.....	678
Table 75.	Formatted text editing tools.....	682
Table 76.	Calendar events.....	688
Table 77.	Data table field types	693
Table 78.	Editing data table field types	694
Table 79.	Descriptions of the Availability options for MyD Outlook profiles	715
Table 80.	Effect of changing availability of MyD Outlook profile to disabled.....	719
Table 81.	Icons used to format text in a form.....	730
Table 82.	Common properties for formal records	734
Table 83.	Common properties for Chapter 2 formal records.....	735
Table 84.	Common properties for Chapter 4 formal records.....	736
Table 85.	Library requests	740
Table 86.	Position of your mouse pointer when you use drag-and-drop in a virtual document.....	747
Table 87.	Virtual document preferences.....	751
Table 88.	Keyboard shortcuts.....	769

Table of Contents

Preface

The purpose of this manual is to provide the system administrator with information to install and use Documentum Administrator.

Intended Audience

Documentum Administrator is a Web-based tool used to perform most of Documentum's system administration tasks. Documentum Administrator is a superset of Webtop and incorporates Webtop's content management functionality.

The audience for Documentum Administrator consists of server administrators, Site Caching Services (SCS) administrators, Webtop administrators, Web Development Kit (WDK) administrators, Content Intelligence Services (CIS) administrators and taxonomy managers, IWS administrators, and Content Transformation Services (CTS) administrators. These are primarily experienced Documentum users who generally install and configure Documentum products and perform administrative tasks, and should have the following basic background knowledge:

- An understanding of client/server technology
- Familiarity with Web browser/application server technology
- Familiarity with relational database concepts
- Familiarity with Microsoft Office products

For additional information about concepts, instructions, and general information, please refer to the following documentation:

- *EMC Documentum Content Intelligence Services Administration Guide*
- *EMC Documentum Content Server Administration Guide*
- *EMC Documentum Content Server Full-Text Indexing System Installation and Administration Guide*
- *EMC Documentum Content Server Fundamentals*
- *EMC Documentum Content Server Release Notes*
- *EMC Documentum System Object Reference Manual*
- *EMC Documentum Distributed Configuration Guide*
- *EMC Documentum Site Caching Services User Guide*
- *EMC Documentum Site Caching Services Installation Guide*

- *EMC Documentum WDK and Applications Installation Guide*
- *EMC Documentum Web Development Kit Applications Configuration Guide*

Revision History

The following changes have been made to this document:

Revision history

Revision date	Description
March 2010	Initial publication

Introducing Documentum Administrator

Documentum Administrator enables you to monitor, administer, configure, and maintain Documentum servers, repositories, and federations located throughout your company from one system running a web browser.

For example, using Documentum Administrator you can:

- Monitor repository system and resource usage
- Configure a repository
- Create or modify repository users and groups
- Create or modify repository object types
- Create or maintain permission sets (also known as access control lists, or ACLs)
- Create or modify repository federations
- Create or modify formats
- Monitor repository sessions
- Monitor and configure Documentum system resources
- Run server APIs and issue DQL queries
- Create or modify storage areas
- Create and run methods and jobs
- Administer full-text indexing
- Administer privileged clients
- Administer EMC Documentum Site Caching Services
- Administer EMC Documentum Content Intelligence Services
- Administer EMC Documentum Content Transformation Services

For information on installing Documentum Administrator, refer to *Documentum Administrator Deployment Guide*.

For a complete discussion of Documentum Content Server administration and configuration, refer to the *Content Server Administration Guide*. For a discussion of Content Server concepts, refer to *Content Server Fundamentals*.

Click the links for information and instructions on:

- [Logging in to Documentum Administrator, page 31](#)
- [About the System Information page, page 32](#)
- [Determining the Documentum Administrator version to which you are connected, page 34](#)
- [How to use Documentum Administrator, page 34](#)
- [Confirming object deletion, page 35](#)
- [Selecting a type, page 36](#)
- [Selecting a user or group, page 36](#)
- [Setting the connection broker list, page 36](#)
- [Configuring licenses, page 37](#)

Click the links below for instructions and conceptual information on the following general subjects:

- [Chapter 4, Basic Configuration](#), including repository and server configuration, federations, and server management
- [Chapter 5, Distributed Content Configuration](#)
- [Chapter 6, User Management](#), including users, groups, roles, LDAP administration, and sessions
- [Chapter 7, Security](#), including permission sets
- [Chapter 8, Audit Management](#), including audit trails and reports on auditing
- [Chapter 9, Job Management](#)
- [Chapter 10, Alias Sets](#)
- [Chapter 11, Formats](#)
- [Chapter 12, Types](#)
- [Chapter 13, Storage Management](#), including creating and modifying storage areas of different types
- [Chapter 14, Content Delivery](#), which describes creating and modifying site publishing configurations and publishing documents using Site Caching Services.
- [Chapter 15, Indexing Management](#), which describes full-text indexing administration in repositories
- [Chapter 16, Content Transformation Services Administration](#)
- [Chapter 17, Content Intelligence Services](#)
- [Chapter 18, Resource Management](#)
- [Chapter 19, Administrator Access](#)
- [Chapter 20, Privileged Clients](#)
- [Chapter 22, API and DQL](#)

Documentum Administrator also provides general content-management functionality. The following chapters provide instructions on checking documents in and out of a repository, managing lifecycles, workflows, and virtual documents, and working with features such as forms and rooms:

- [Chapter 2, Repositories](#)
- [Chapter 3, Files and Folders](#)
- [Chapter 23, Search](#)
- [Chapter 24, Email Messages](#)
- [Chapter 25, Inbox](#)
- [Chapter 26, Workflows and Quickflows](#)
- [Chapter 27, Work Queues](#)
- [Chapter 28, Lifecycles](#)
- [Chapter 29, Collaborate with Other Users](#)
- [Chapter 31, Taxonomies and Categories](#)
- [Chapter 32, Forms](#)
- [Chapter 33, Records](#)
- [Chapter 34, Virtual Documents](#)
- [Chapter 35, PDF Annotations](#)
- [Chapter 36, Relationships](#)
- [Chapter 37, Renditions and Transformations](#)
- [Appendix A, Keyboard Shortcuts for Microsoft Windows and Mac Operating Systems](#)

Logging in to Documentum Administrator

Use these instructions to connect to a Documentum Administrator instance. Before you connect, obtain the URL to the instance, which includes the name of the host where Documentum Administrator is running and the port number on which Documentum Administrator listens.

To log in to Documentum Administrator:

1. Start a web browser on a client machine.
2. Connect to the following URL, where *host* is the host where Documentum Administrator is installed and *portnumber* is a port number provided during application server installation:
`http://host:portnumber/da/`
3. Type your login name and password on the Documentum Administrator Login page.
4. Select a repository from the list box.
If you change the repository, retype your password.
5. In the **Location** list (if available), select the location on your organization's network from which you are accessing Documentum Administrator.

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.

6. To view additional options, click **More Options**.
 - a. To connect to the repository using a particular server, select that server from the **Server** list box.
The default is **Any Running Server**.
 - b. If the repository is running in domain-required mode, type the domain name.
 - c. To set the session locale to another language, select the language from the drop-down list.
 - d. Do not select **Additional Accessibility Options** on the login page. Documentum Administrator does not support the accessibility options.
 - e. To change your password in a repository, click **Change Password**, select a repository and type your old and new passwords, then click **Change Password**.

Note:

- If LDAP user authentication is used, you cannot change your password from this page. A system administrator must change your password on the LDAP server.
- If you use Content Intelligence Services, after changing your password on the Documentum Administrator login page, click the Content Intelligence Configure link to also change and validate your password on the CIS Configuration page.

7. Click **Login**.

The **System Information** page appears with information about the system. For more information about the System Information page, refer to [About the System Information page, page 32](#).

About the System Information page

The System Information page is the first page you see when you connect to Documentum Administrator. The page displays general information about the repository and host to which you are connected.

Figure 1. System Information page

System Information		6/21/2007 5:19:57 AM
User:	dmadmin/dmadmin	Licensing: Configure
Repository		
Repository:	dad6postb7b	Content Storage Service: Enabled
Federation:	None	Content Intelligence: Enabled Configure
Global Repository:	dad6postb7b	
Content Server		
Content Server:	dad6postb7b	Hostname: pletorque-st1
Server Version:	6.0.0.059 Win32.SQLServer	Connection Broker: pletorque-st1
Trusted Mode:	Enabled	
Distributed Content		
Network Locations:	1	ACS Server: PLETORQUE-ST1ACS1
BOCS Servers:	0	ACS Write: Enabled, Synchronous
ACS Read:	Enabled	BOCS Pre-caching: Enabled
Messaging:	Enabled	
LDAP Servers		
Enabled Servers:	0	Last Sync: Not Yet Synced
Disabled Servers:	1	

The System Information page displays the following information:

- The date and time at which you connected to the repository
- **User:** The username under which you are connected
- **Licensing:** Click **Configure** to enable product licenses for the following:
 - Collaboration Services (Base or with Rooms)
 - Physical Records Management
 - Records Manager
 - Retention Policy Services
- For information on this feature, refer to [Configuring licenses, page 37](#).
- **Repository** information
 - **Repository:** The repository to which you are connected, which you selected on the login page
 - **Federation:** The name of the federation to which the current repository belongs, if any.
 - **Global Repository:** The name of the global registry.
 - **Content Storage Service:** When set to *Enabled*, indicates that Content Storage Services was enabled during Content Server installation.
 - **Content Intelligence:** When set to *Enabled*, indicates that Content Intelligence is enabled.
 - **Configure:** Click to access the **Configuration for Content Intelligence** page. This link is only available if Content Intelligence is enabled. For additional information, refer to [Understanding Content Intelligence Services, page 499](#).
- **Content Server** information
 - **Content Server:** The Content Server to which you are connected
 - **Server Version:** The Content Server version and platform
 - **Trusted Mode:** Whether Trusted Content Services is enabled in the repository to which you are connected

- **Hostname:** The name of the host on the server used to log in to the repository.
- **Connection Broker:** The connection broker used to connect to the repository
- **Distributed Content** information
 - **Network Locations:** Indicates the number of network locations associated with the repository.
 - **BOCS Servers:** Indicates the number of BOCS servers associated with the repository.
 - **ACS Read:** Indicates if users can read content in the repository through the ACS.
 - **Messaging:** Indicates if the messaging server is enabled.
 - **ACS Server:** Indicates the name of the ACS server.
 - **ACS Write:** Indicates if users can write content to the repository through the ACS and whether the write is synchronous or asynchronous.
 - **BOCS Pre-caching:** Indicates if the repository is enabled to process pre-caching requests.
- **LDAP Servers** information

This section indicates how many LDAP servers are enabled or disabled and when they were last synchronized.

Determining the Documentum Administrator version to which you are connected

From the System Information page, you can determine the Documentum Administrator version to which you are connected.

To determine the Documentum Administrator version to which you are connected:

1. Select **File > About Documentum Administrator**.
2. After you view the information, click **Close**.

How to use Documentum Administrator

This section provides some general information on the Documentum Administrator interface and how Documentum Administrator works.

Click the links below for information on:

- [User privileges, page 35](#)
- [Creating new objects, page 35](#)
- [Modifying or viewing existing objects, page 35](#)
- [Confirming object deletion, page 35](#)
- [Setting the connection broker list, page 36](#)

User privileges

Tasks performed using Documentum Administrator include creating or modifying objects, enabling auditing, and initiating site publishing jobs. Different tasks require different user privilege levels. For example, to create a site publishing configuration, you must have Superuser privileges. You must have config audit privileges to configure auditing, view audit privileges to view audit trails, and purge audit privileges to remove audit trails from a repository.

A user who connects to Documentum Administrator may not have sufficient privileges to perform administration tasks, but the user is still able to navigate Documentum Administrator and view the available administration options.

Creating new objects

To create a new object, you must first navigate to the correct list page for that object. (A list page displays all existing objects of that type in the current repository.) For example, to create a new user, navigate to the user list page by selecting **User Management > Users**. Next, select **File > New > User**.

Complete the required fields on the page, then click **Next** if there are additional pages or click **OK** if this is the last page. You must complete multiple pages to create some objects. For example, creating a new server configuration object requires completing six pages of information.

Some new objects can also be created by duplicating an existing object and giving it a new name. For example, a new server configuration object or site publishing configuration can be created using the **File > Save As** command.

Modifying or viewing existing objects

The same pages are used for viewing the properties of an existing object or modifying those properties. To view or modify an existing object, navigate to the list page for the object. Select the object name and then select **View > Properties > Info** or use the shortcut where you right-click on the object name and then select **Properties**.

Confirming object deletion

When you delete certain objects from a repository, you see a page on which you must confirm that you want to delete the object.

To confirm that you want to delete an object:

1. To delete the object, click **OK**.
The object is deleted.
2. To leave the object in the repository, click **Cancel**.
You are returned to the page from which you tried to delete the object.

Selecting a type

Use this page to select a type.

To select a type:

1. To locate the type by name, type the first few letters into the **Starts with** box and click **Go**.
2. To view additional pages of types, click the forward or back buttons.
3. To view a different number of types, select a different number from the **Show Items** list box at the top of the page.
4. To sort the items alphabetically, click **Name** or **Super Name**.
5. When you locate the correct type, select the checkbox next to the type's name and click **OK**.

Selecting a user or group

Use the Choose a group or Choose a user/group page to select a user or group.

To select a user or group:

1. Access the **Choose a group** or **Choose a user/group** page.
2. Select a user or group and then click **>** to move the selected user or group to the right side.
3. To remove a user or group on the right side, select it and then click **<**.
4. When finished, click **OK** or **Cancel**.

Setting the connection broker list

A connection broker provides repository connection information to Documentum client applications, including Documentum Administrator and Documentum Webtop. Each repository projects connection information to one or more connection brokers.

Documentum Administrator obtains connection information from the connection broker referenced in the dfc.properties file in the Documentum Administrator web application. You cannot modify dfc.properties from your browser, but if you are a System Administrator or Superuser, you can add additional connection brokers by storing connection broker information in a cookie. Click the Add Repositories link at the bottom of the tree to add a new connection broker, which will add the connection broker to the browser's cookie. This enables you to access additional repositories.

Use these instructions to modify the list of connection brokers used by Documentum Administrator.

To set the connection broker list:

1. Connect to Documentum Administrator.
2. Click **Add Repository** to access the **Add a Repository** page.

3. Select a repository and then click the **more repositories** link to access the **Connection Brokers** page.
4. To add a connection broker, type its name in the **Enter New Connection Broker** text box and then click **Add**.

If the connection broker uses a port other than 1489, use the follow format:

connection_broker_name:port_number

For example:

`mozart:1756`

5. To remove a connection broker, highlight it in the **Selected Connection Brokers** text box and click **Remove**.
6. To move a connection broker up or down in the search order, highlight the connection broker name in the **Select connection broker** text box and click **Move Up** or **Move Down**.
7. Click **OK** to save the changes or click **Cancel** to cancel the changes.

The System Information page appears.

Configuring licenses

Documentum Administrator provides a license configuration feature to enable licenses in existing repositories for the following features or products:

- Collaborative Edition
- Physical Records Management
- Records Manager
- Retention Policy Services

The following topics include information on enabling those features.

- [Viewing enabled licenses, page 37](#)
- [Enabling a feature or product, page 38](#)

Viewing enabled licenses

Use these instructions to navigate to the license list page and view which features are enabled.

To view which licenses are enabled:

1. Connect to Documentum Administrator.
2. On the System Information page, click **Licensing: Configure Licenses**.

A list of features appears, including which licenses are enabled. For instructions on enabling a license, click the **Help** link or [Enabling a feature or product, page 38](#).

Enabling a feature or product

Use these instructions to enable the license for a particular feature or product.

To enable a product or feature license:

1. Connect to Documentum Administrator.
2. On the **System Information** page, click **Licensing: Configure Licenses**.
The **Product Licensing** page appears. The page displays a list of products and features and indicates which licenses are enabled.
3. Select the feature or product.
4. Click **Enable**.
The **Product License** page appears.
5. Type the license key for the feature or product.
6. Click **OK** to return to the Product Licensing page.
7. Click **OK** to return to the System Information page.

Chapter 2

Repositories

This chapter includes:

- Log into a repository, page 39
- Navigate a repository, page 42
- Locate an item in a selection dialog box, page 44
- Set your preferences, page 45
- Open an additional repository window, page 47
- Drag-and-drop, page 47
- Right-click, page 47
- View messages, page 48
- View the status of background operations, page 48
- Work with repository documents offline through My Documentum, page 49
- View product information, page 50
- Refresh page, page 48
- Select HTTP or UCF content transfer, page 48
- Use modal dialogs, page 49

Log into a repository

To log into a repository, you need:

- Documentum Administrator URL
- Repository name
- Your username, and password for the repository
- Documentum Administrator Network location (if applicable)
- Microsoft Windows NT domain name (if applicable)
- Language (if applicable)

To log into a repository:

1. In your web browser, type the Documentum Administrator URL.
If you use either saved credentials or an automated authentication, Documentum Administrator automatically logs you in. 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 Documentum Administrator.
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 Documentum Administrator from this computer, select **Remember my credentials for next time**.
Tip: 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**.
10. Click **Login**.

See also:

- [Log in as an express user, page 41](#)
- [Log into another repository, page 41](#)
- [Log out of all repositories, page 41](#)
- [Set your favorite repositories, page 41](#)

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 into a repository, page 39](#)

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 username, and password for the repository.
4. Click **Login**.

Log out of all repositories

To log out, select **File > Logout**.

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**.

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. Documentum Administrator 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 the items in the content pane, right-click, and choose **Select All**.

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.
Tip: To sort by lock owner, click 

To change the columns that appear, see [Select the columns that appear in lists, page 43](#).

See also:

[Navigate categories, page 44](#)

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 Step a through Step c 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 Step a through Step c 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**.

Navigate categories

Categories provide alternate ways to organize files from the way they are organized in cabinets. Categories are available if Documentum Administrator is integrated with EMC Documentum CI 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.

Tip: 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**.

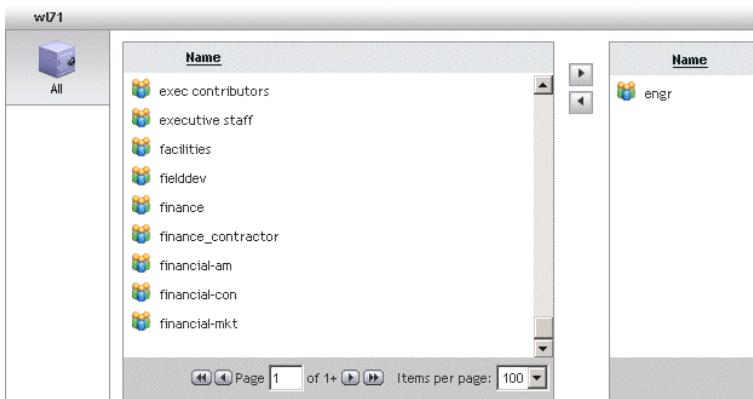
Tip: To confirm submission for all remaining files at once, click **Finish**.

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, as shown in [Figure 2, page 45](#), 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.

Figure 2. Selection dialog box with two list boxes

Set your preferences

Preferences determine your choices for how Documentum Administrator 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 Documentum Administrator, 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 [Table 1, page 45](#).

Table 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 Documentum Administrator copies files when you check them out from the repository.
Saved Credentials	Your usernames, 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.

Field	Description
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 Documentum Administrator 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 [Table 2, page 46](#).
3. Click **Add**.

You can add custom viewing, and editing applications, and set your formats preferences for viewing, and editing.

Table 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.

Field	Description
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**.

Open an additional repository window

To open an additional window that displays the repository, select **Tools > New Window**.

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, page 45](#).

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.

Tip: 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 Documentum Administrator pane.
- Navigate to the target by opening a new window. You can open a new window by selecting **Tools > New Window**.

Right-click

To perform an action on an item you can right-click the item, and select the action from the shortcut menu.

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**.

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.

Refresh page

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.

Select HTTP or UCF content transfer

Webtop 6.5x enables administrators to specify HTTP or UCF content transfer for different users within the same Webtop installation. Before Documentum ECM 6.5, all users within the same 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.

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.

Work with repository documents offline through My Documentum

My Documentum is a client application that lets you work on your documents in the offline mode when you are not logged into Documentum Administrator. My Documentum 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 keeps selected repository files available on your machine so that you can still work with the files even if you are disconnected from Documentum Administrator. When you again log in, My Documentum 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 *EMC Documentum My Documentum User Guide*.

View product information

To view the version number, and other product information, select **File > About Documentum Administrator**.

The product information includes version of Web Development Kit (WDK), upon which Documentum Administrator is built. WDK is the EMC Documentum framework used to build applications that access repositories by using web browsers.

Chapter 3

Files and Folders

This chapter includes:

- [Create a file, page 51](#)
- [Create a folder, page 52](#)
- [Create a cabinet, page 52](#)
- [Set properties, page 53](#)
- [Check out and edit files, page 54](#)
- [View a file in read-only mode, page 59](#)
- [Change the format associated with a type of file, page 60](#)
- [Import files to the repository, page 61](#)
- [Export files from the repository, page 62](#)
- [Delete an item from the repository, page 64](#)
- [Move an item to a new location in the repository, page 64](#)
- [Copy an item to a new location in the repository, page 64](#)
- [View your clipboard, page 65](#)
- [Links, page 65](#)
- [Subscriptions, page 69](#)
- [Receive notification when a file is read or changed, page 70](#)
- [Export the information displayed in a list, page 70](#)

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, page 44](#).

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 [Table 3, page 53](#) in the topic [Set properties, page 53](#).
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**.

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 [Table 3, page 53](#) in the topic [Set properties, page 53](#).
5. In the **Permissions** tab, specify the access that specific users, and groups have to the folder. For instructions, see [Permission set properties, page 242](#).
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**.

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 [Table 3, page 53](#) in the topic [Set properties, page 53](#).
6. In the **Permissions** tab, specify the access that users, and groups have to the cabinet. For instructions, see [Permission set properties, page 242](#).
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**.

Set properties

To set properties for an item:

1. Navigate to, and select an item.

Tip: To select multiple items at once, click each item while holding down **Ctrl**.

2. Select **View > Properties > Info**.

Tip: 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 [Table 3, page 53](#). 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 3. Common tabs in the Properties dialog box

Tab	Description
Info tab	<p>To edit a property, do any of these that apply:</p> <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. <p>To display additional properties, select Show More. To display all the properties, select Show All Properties.</p>
Permissions tab	Displays the access that different users have to the item. To change permissions, see Permission set properties, page 242 .
History tab	Displays a list of events that have occurred to the item, such as checkout, checkin, and promote.

Check out and edit files

This section includes these:

- Overview of check out and edit, page 54
- Check out a file, page 55
- Check in a file, page 55
- Cancel checkout of a file, page 58
- View currently and recently checked-out files, page 59

Overview of check out and edit

To edit files, you check them out to your local computer. When you check out a file, Documentum Administrator 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, Documentum Administrator either copies or streams the file to your computer, depending on the file's editing application.

If the file uses an external editing application, Documentum Administrator 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, Documentum Administrator 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.

Documentum Administrator displays a key icon next to the files that you currently have checked out. Documentum Administrator 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, Documentum Administrator 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.

Check out a file

To check out a file:

1. Navigate to the file in the repository, and select it.

Tip: 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**.

Tip: 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**.

Tip: 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.

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.

Tip: You can perform this procedure on multiple files by selecting multiple files.

2. Select **File > Check In**.

3. If Documentum Administrator 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, page 56](#).
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**.

Tip: To apply information to all remaining files at once, click **Finish**.

Checkin information

See [Table 4, page 56](#) for an explanation of common checkin fields. Some of the fields may not appear.

Table 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, page 57 .
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 Documentum Administrator scan the document for linked documents. If linked documents are found, they are checked in as descendants of the original document.
Upload options	Determines how quickly the new content is available to other users, and whether you can use Documentum Administrator while the checkin occurs. Note: If you used drag-and-drop you are not given this option. 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 Documentum Administrator.

Field	Description
	<ul style="list-style-type: none"> • Send first for local access: Updates the repository immediately for the users in your geographic area, but Documentum Administrator takes more time to update the repository for all users. This allows you to continue using Documentum Administrator while the update occurs. <p>Note: 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	<p>Retain Lock</p> <p>Make this the current version</p> <p>Keep a local copy after checkin</p> <p>Subscribe to this file</p> <p>Check in from file</p>
	<p>Saves the updated file to the repository but keeps the file checked out in your name.</p> <p>Makes the updated file the current version. For more information, see Versions, page 57.</p> <p>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.</p> <p>The file is linked to your Subscriptions.</p> <p>Replaces the repository file with a file you choose.</p>

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, Documentum Administrator 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, Documentum Administrator creates a new branch of the document, which starts with version 5.0.1.

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, page 55](#).
2. Select the checked-out file in the repository, and select **File > Check In**.
Tip: 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, page 56](#).
4. Click **OK**.

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.
Tip: 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**.
- Tip:** To confirm cancellation for all remaining files at once, click **Finish**.

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 usernames, and passwords for those repositories.

View a file in read-only mode

When you view a file, Documentum Administrator 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, Documentum Administrator 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.

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 [Table 5, page 60](#):

Table 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**.

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**.

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.

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**.
Tip: Instead of using the File menu, you can drag-and-drop the file or folder from your local computer to the location in Documentum Administrator. 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 [Table 6, page 61](#). The table describes common properties. Your installation of Documentum Administrator might include different properties.

Table 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 Documentum Administrator 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	<p>If this field appears, you can determine how quickly the imported content is available to other users, and whether you can use Documentum Administrator while the import occurs. Select one of these:</p> <ul style="list-style-type: none"> • Send for immediate global access <p>Updates the repository immediately for all your organization's users. While this occurs, you cannot perform other actions in Documentum Administrator.</p> <ul style="list-style-type: none"> • Send first for local access <p>Updates the repository immediately for the users in your geographic area, but Documentum Administrator takes more time to update the repository for all users. This allows you to continue using Documentum Administrator while the update occurs.</p>

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**.

Tip: To apply the selected properties to all remaining files at once, click **Finish**.

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, 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**.

Tip: 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**.

Tip: 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.

Deep export

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, 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 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.

Delete an item from the repository

To delete an item from the repository:

1. Navigate to the item, and select it.
Tip: 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**.

Tip: To apply selections to all remaining files at once, click **Finish**.

Move an item to a new location in the repository

You can move an item to another location within the same repository. By default, Documentum Administrator moves only the selected version of the item. Your administrator might have instead configured Documentum Administrator 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.

Tip: 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.
Tip: You can select multiple items.
2. Select **Edit > Add To Clipboard**.
Tip: 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**.
Tip: 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**.

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.

Tip: You can select multiple items.

2. Select **Edit > Add To Clipboard**.

Tip: 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, page 41](#).
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**.

Tip: 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, Documentum Administrator adds **Copy** to the name of the copied item.

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**.

Links

This section includes these:

- [Link an item to another location in the repository, page 66](#)
- [Link an item to another repository, page 66](#)
- [View all locations to which an item is linked, page 67](#)
- [Link a repository item to your computer, page 67](#)
- [Add a document or folder to your browser's bookmarks or favorites, page 67](#)
- [Use email to send a link to a repository item, page 68](#)
- [Open a link sent by email, page 69](#)

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.

Tip: You can select multiple items.

2. Select **Edit > Add To Clipboard**.

Tip: 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**.

Tip: 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**.

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, Documentum Administrator performs the operation on original item in the original repository. For example, when you check out the shortcut, Documentum Administrator 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 Documentum Administrator window, open the repository to which to link.

4. Navigate to the location in the new repository.

5. Select **Edit > Link Here**.

The Content Server uses automated jobs to synchronize shortcuts, and originals.

Note:

- 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.

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**.

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.

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**.

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.
Tip: 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.

Convert Desktop DRLs to Webtop URLs

The Documentum Desktop client has been phased out. As a result, Desktop users will no longer be able to access desktop DRLs (links to repository documents) embedded in e-mail messages. Documentum Webtop 6.5 SP2 provides existing Documentum Desktop client users with the DRLInvoker application (DRLInvoker.exe) that converts desktop DRLs to 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 2.0 platform is required to ensure that the conversion of Desktop URLs to 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 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. Based on your operating system, perform the relevant steps:

On Windows XP/XP Home:

1. Right-click the file and select the option **Open With**.
2. Select **Choose Program**. The Open With dialog box is displayed.
3. Locate the **DRLInvoker.exe** as the program to open files of this type.
4. Select the checkbox **Always use the selected program to open this kind of file**.
5. Click **OK**.

On other versions of Windows:

1. Select the file.
2. Hold down the Shift key and right-click the file.
3. Select the option **Open With**. The Open With dialog box is displayed.
4. Locate the **DRLInvoker.exe** as the program to open files of this type.
5. Select the checkbox **Always use this program to open files of this type**.
6. Click **OK**.

Subsequently, you can double-click .drl files to open linked documents.

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.

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.

To subscribe yourself to a repository item:

1. Navigate to the item, and select it.
2. Select **Tools > Subscribe**.

Tip: 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, page 44](#).

To cancel your subscription to an item:

1. Navigate to the item, and select it.
2. Select **Tools > Unsubscribe**.

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.
Tip: 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 Documentum Administrator inbox, and your email inbox.

Tip: You can later turn notification off by selecting the file, and selecting either **Tools > Turn off read notification** or **Tools > Turn off change notification**.

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.

Chapter 4

Basic Configuration

The basic configuration section provides information and instructions for the following configuration areas:

- **Repositories**

The Repositories section is where you configure the docbase config object for a repository. Docbase configuration objects contain information on the underlying database, security levels, folder security, and other operating configuration parameters.

Note: Docbases are called repositories in Documentum 6 and later, except where the term *docbase* is used in the name of an object or property (for example, docbase config object).

- **Content Servers**

The Content Servers section is where you create, modify, or delete server configuration objects.

- **Federations**

Federations are sets of repositories that share users, groups, permission sets, and objects.

- **LDAP (Lightweight Directory Access Protocol)**

The LDAP section is where you create, modify, or delete LDAP configuration objects.

Use LDAP servers to manage users and groups or for user authentication. The mapping between the LDAP person or group entries and Documentum user or group attributes is stored in Documentum as an LDAP configuration object.

Click the links for information and instructions on:

- [Repositories, page 73](#)
- [Content Servers, page 85](#)
- [Federations, page 102](#)
- [LDAP Servers, page 110](#)

Repositories

Use the Administration > Basic Configuration > Repository navigation to configure the docbase configuration object for a repository. Each repository contains one docbase configuration object. The docbase configuration object defines the name of the underlying RDBMS, security levels for the

repository, whether folder security is enabled, the Macintosh access protocol, and other operating configuration parameters.

You can modify the existing docbase configuration object; however, you cannot create additional docbase configuration objects or delete the existing docbase configuration object. You must be a Superuser to view or modify the properties of the docbase configuration object.

The Repository list page lists the docbase configuration object for the current repository, the database for the repository, the federation to which the repository belongs, if any, and the effective date of the repository configuration object. The effective date is used to manage client query caches. Refer to the *Content Server Administration Guide* for more information on query caching.

The docbase configuration object has two tabs: Info and Synchronization. The fields on the Info tab display basic information about the repository. The Synchronization tab defines the behavior of Offline Client when accessing the repository. The Synchronization tab is displayed for repositories in which the Offline Client DocApp is installed. The release notes for Documentum Desktop provide information on configuring Offline Client.

Click the links below for instructions and information on:

- [Viewing or modifying the docbase configuration object for a repository, page 74](#)
- [Modifying the synchronization settings for a repository, page 75](#)
- [Repository configuration properties, page 75](#)
- [Enabling Windows domain authentication for UNIX repositories, page 83](#)

Viewing or modifying the docbase configuration object for a repository

You can modify some, but not all, of the docbase configuration object values.

To view or modify the docbase configuration object Info page:

1. Connect as a Superuser to the repository whose docbase configuration object you want to modify.
2. Navigate to **Administration > Basic Configuration > Repository** to access the **Repository list** page.
3. Select the repository name and then select **View > Properties > Info**.
The **Repository Configuration Properties - Info** page appears.
4. Modify the values that you want to change.
For information on the properties of the docbase configuration object, refer to [Repository configuration properties, page 75](#).
5. To enable Windows domain authentication on a UNIX repository, use the instructions in [Enabling Windows domain authentication for UNIX repositories, page 83](#).
6. To modify the synchronization settings, click the **Synchronization** tab.
The **Repository Configuration Properties - Synchronization** page appears.
7. Click **OK** to accept the changes or **Cancel** to return to the Repository list page.

Modifying the synchronization settings for a repository

The synchronization settings control the behavior of the Documentum Offline Client.

To modify the synchronization settings for a repository:

1. Connect as a Superuser to the repository whose docbase configuration object you want to modify.
2. Navigate to **Administration > Basic Configuration > Repository** to access the **Repository** list page.
3. Select the repository name and then select **View > Properties > Info**.
The **Repository Configuration Properties - Info** page appears.
4. Click the **Synchronization** tab.
The **Repository Configuration Properties - Synchronization** page appears.
5. Modify the values that you want to change.
For information on the properties of the docbase configuration object, refer to [Repository configuration properties, page 75](#).
6. Click **OK** to accept the changes or **Cancel** to return to the Repository list page.

Repository configuration properties

This section shows the Repository Configuration Properties - Info and Repository Configuration Properties - Synchronization pages and describes the fields on these pages.

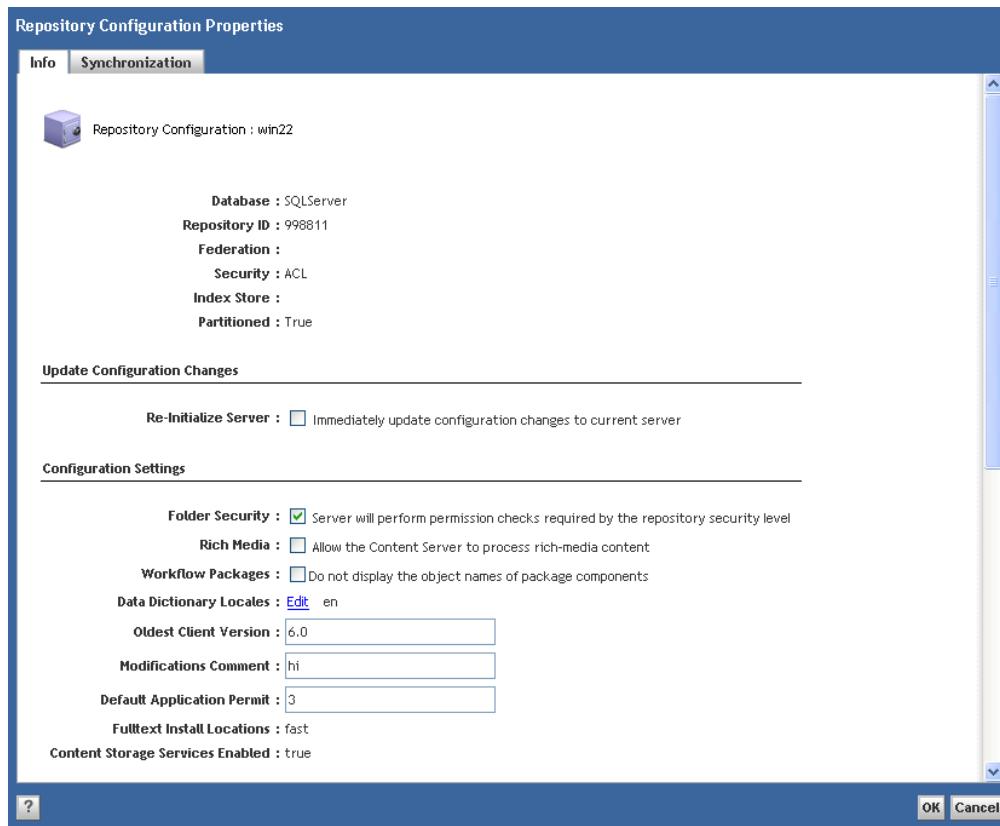
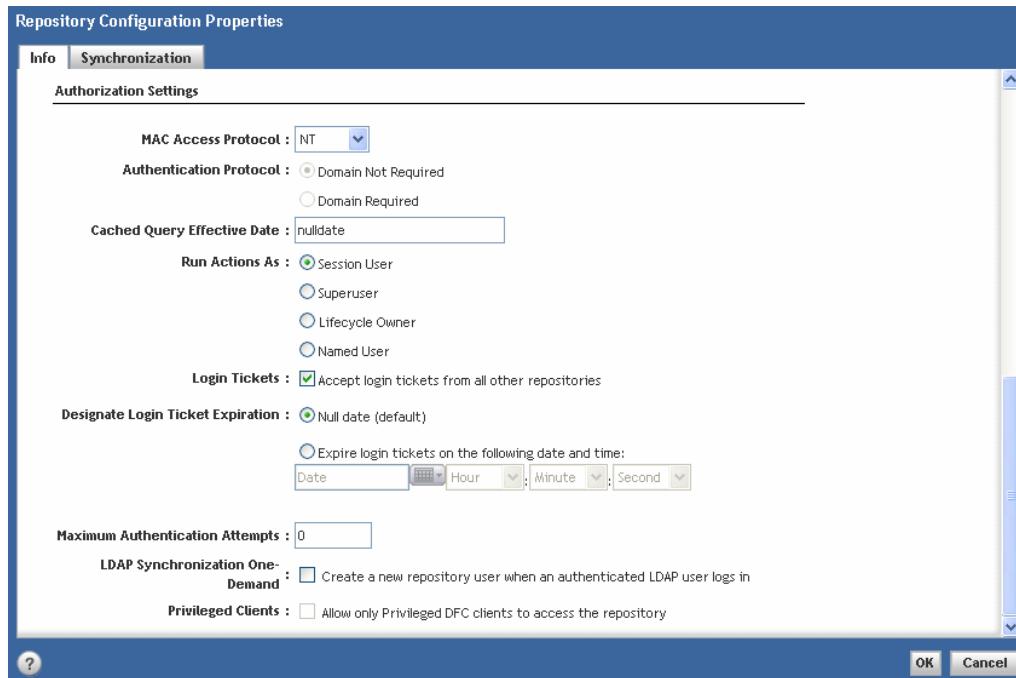
Figure 3. Repository Configuration Properties - Info page (1 of 2)**Figure 4. Repository Configuration Properties - Info page (2 of 2)**

Table 7. Repository Configuration Properties - Info page properties

Field label	Value
Database	The name of the RDBMS vendor. Read-only.
Repository ID	The repository ID number assigned during installation. Read-only.
Federation	Indicates if the repository is a member of a federation. Read-only.
Security	The security mode of the repository. ACL and None are valid values. None means repository security is disabled. ACL means access control lists (permission sets) are enabled. Read-only.
Index Store	Name of the tablespace or other storage area where type indexes for the repository are stored.
Partitioned	If True, indicates that the repository is partitioned. When a repository is created or updated with partitioning enabled, the Content Server sets the flag to True. The Partitioned field is: <ul style="list-style-type: none">• not selectable or changeable.• available only in 6.5 repositories.• not available for DB2 or Sybase repositories.
Re-Initialize Server	Select to reinitialize the server to which you are connected. This is necessary for changes to objects to take effect.
Folder Security	Boolean. Select to enable folder security. When folder security is enabled, the server performs the permission checks required by the repository security level and for some operations, also checks and applies permissions on the folder in which an object is stored or on the objects primary folder. For more information on folder security, refer to Turning Folder Security On and Off in the <i>Content Server Administration Guide</i> .
Rich Media	Boolean. Select to indicate that Media Server is installed in the repository and Content Server can process rich-media content. Requires the server to be reinitialized for changes to take effect.

Workflow Packages	Boolean. The default cleared (FALSE). When selected (TRUE), the object names of package components are not displayed. For more information, refer to the documentation for workflows.
Data Dictionary Locales	Repeating property. The locales enabled in the data dictionary. The server must be reinitialized for any changes to be visible.
Oldest Client Version	Determines how XML documents are chunked by DFC. The default is not set. The value must be changed manually. If the value is not set, DFC is compatible with client versions earlier than the current DFC version. If the value is set, DFC stores data in a format that older clients cannot use. Set the property value to the client version number in the format XX.YY, where X is the major version and Y is the minor version.
Modifications Comment	Optionally, add a comment.
Default Application Permit	Default user permission level for application-controlled objects accessed through an application that does not own the object. Valid values are: <ul style="list-style-type: none">• 1: None permission• 2: Browse permission• 3: Read permission• 4: Relate permission• 5: Version permission• 6: Write permission• 7: Delete permission The default value is 3, for Read permission. In pre-5.3 repositories, the Verity versions installed and their locations.
Fulltext Install Locations	
Content Storage Services Enabled	When set to TRUE, indicates that Content Storage Services was enabled during Content Server installation.

MAC Access Protocol	<p>The file-sharing software type in use for Macintosh clients. Valid values are:</p> <ul style="list-style-type: none"> • None • NT • Ushare • Double <p>The default value when the server is installed is None.</p> <p>If you change the value from NT, Ushare, or Double to None, existing resource forks will no longer be accessible.</p> <p>To change the value from or to NT, Ushare, or Double, you must first change the value to None, save the docbase config, and then change it from None to the new value. For example:</p>
Authentication Protocol	<p>Defines the authentication protocol used by the repository.</p> <ul style="list-style-type: none"> • On Windows, if set to Domain Required, it indicates that the repository is running in domain-required mode. • On UNIX platforms, choose between UNIX authentication or Windows domain authentication. <p>If you choose Windows domain authentication, use the instructions in Enabling Windows domain authentication for UNIX repositories, page 83 to complete the process.</p>
Cached Query Effective Date	Used to manage the client query caches. The default is NULLDATE.

Run Actions As	The user account that is used to run business policy (document lifecycle) actions. Options are: <ul style="list-style-type: none">• Session User (default)• Superuser• Lifecycle Owner• Named User If selected, click the Select User link to access the Choose a user page to select a user.
Login Tickets	If selected, Allow login tickets from repositories is disabled. If selected, all other repositories are trusted and login tickets from all repositories are accepted by the current repository.
Allow login tickets from repositories	Visible and enabled only if Allow all login tickets is not selected.
Expire all login tickets in <i>N</i> minutes	Click Select to access the Choose Repositories page to designate repositories whose login tickets are permitted in the current repository (the trusted repositories).
Designate Login Ticket Expiration	5.3 and 5.3 SP1 repositories only. Defines the earliest possible creation date for valid login tickets. Tickets issued before the designated date are not valid in the current repository. The default value is NULLDATE, meaning that there is no cutoff date for login tickets. Use in case of a security breach or other emergency by setting this to a time and date in the future. Login tickets created before that time and date cannot be used to establish a connection. Currently-connected users are not affected by setting the time and date.
	5.3 SP2 repositories and later, replacing the Expire all login tickets in <i>N</i> minutes field. This defines the earliest possible creation date for valid login tickets. Tickets issued before the designated date are not valid in the current repository. The radio buttons allow you to select one of the following: <ul style="list-style-type: none">• Null date: Select if there is no cutoff date for login tickets in the current repository. This is the default value.• Expire login tickets on the following date and time: Select to define the earliest possible

	creation date for valid login tickets, then use the calendar control to choose the correct date and time.
Maximum Authentication Attempts	Use in case of a security breach or other emergency by setting this to a time and date in the future. Login tickets created before that time and date cannot be used to establish a connection. Currently connected users are not affected by setting the time and date.
	The number of times user authentication can fail for a user before that user is disabled in the repository. Authentication attempts are counted for logins and API methods requiring the server to validate user credentials, including the Changepassword, Authenticate, Signoff, Assume, and Connect methods.
	By default, the installation owner's account is not subject to the failure threshold and is not disabled when it reaches the maximum number of attempts. You can modify the installation owner account from the User pages.
	A value of zero (0) means that the feature is not enabled.
LDAP Synchronization On-Demand	Requires the server to be reinitialized for changes to take effect. 5.3 SP1 and later repositories. Used to synchronize LDAP directory users with the repository between scheduled runs of the LDAP synchronization job: <ul style="list-style-type: none">• When cleared, LDAP directory users who do not exist in the repository cannot log in.• When selected, if an LDAP directory user attempts to log in and is found not to exist in the repository, Content Server searches all active directory connections for the user. If the user is found and can be authenticated, the user is created in the repository.
Privileged Clients	Boolean. If selected, indicates that the repository is accessible to privileged clients only. This checkbox is available only if a DFC client exists in the repository and is approved to perform privilege escalations. Approving or

denying privilege escalations is discussed in [Chapter 20, Privileged Clients](#).

Figure 5. Repository Configuration Properties - Synchronization page

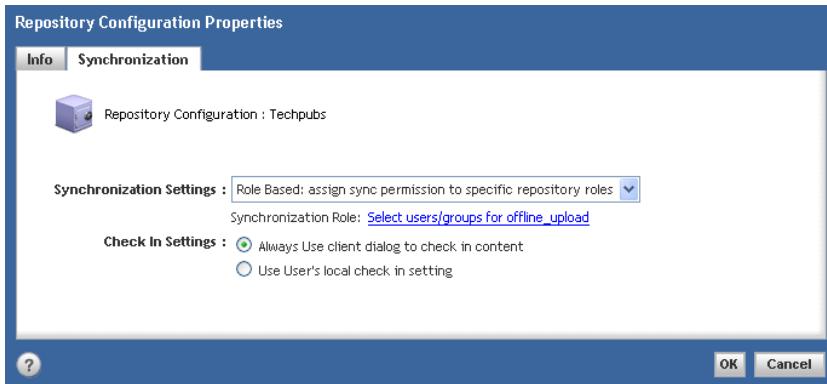


Table 9. Repository Configuration Properties - Synchronization page properties

Field label	Value
Synchronization Settings	<p>For repositories where Offline Client is enabled. Options are:</p> <ul style="list-style-type: none"> None: no content synchronization to local machine. Basic: 1-way download to local machine as read only. Role-Based: assign sync permissions to specific repository roles. <p>No content is synchronized to the local machine. This is the default setting for a repository.</p> <p>Content is downloaded to the local machine and marked read-only. No content is uploaded from the local machine.</p> <p>Synchronization permissions are based on specific user roles. Synchronization is enabled and users can download content. Whether content can be uploaded depends on a particular user's role. If selected, you must designate the synchronization roles and check-in settings.</p>

Field label	Value
Synchronization Role	If you selected role-based synchronization where Offline Client is enabled, you must designate the roles. Click the Select users/groups for offline upload link to access the Choose a user/group page to select users who you want to use offline upload.
Check In Settings	Select to use the client dialog or the user's local settings to check content into the repository. Options are: <ul style="list-style-type: none"> • Always Use client dialog to check in content • Use User's local check in setting

Enabling Windows domain authentication for UNIX repositories

A repository on a UNIX host can use Windows domain authentication to authenticate repository users. First, you must modify the repository configuration object by selecting Windows domain authentication on the Repository Configuration Properties - Info page of the docbase configuration object. Next, define a domain map and add Windows domains to it.

The following topics discuss creating the domain map and modifying users:

- [Creating or modifying a domain map, page 84](#)
- [Defining a domain, page 84](#)
- [Modifying users for Windows domain authentication, page 85](#)

There are two other tasks associated with using Windows domain authentication:

- Modifying the `dm_check_password` program to work with Windows domain authentication.
For instructions, refer to Managing User Authentication, in the *Content Server Administration Guide*.
- Modifying the `user_source` property in the user object for each user in the UNIX repository.

Each user in a UNIX repository must have the `user_source` property set to domain only, UNIX first, or domain first. You can do this with Documentum Administrator on the User page.

Note that UNIX users who are authenticated against a Windows domain cannot execute methods under their own accounts. All methods executed by such users must be run with `run_as_server` set to TRUE.

Creating or modifying a domain map

Use these instructions to create or modify a domain map for Windows authentication on a UNIX repository.

To create or modify a domain map:

1. Connect as a Superuser to the repository whose docbase configuration object you want to modify.
2. Navigate to **Administration > Basic Configuration > Repository** to access the **Repository** list page.
3. Select the repository name and then select **View > Properties > Info**.
The **Repository Configuration Properties - Info** page appears.
4. In the **Authentication Protocol** section, select **Windows Domain Authentication**.
5. Click **Define Domain Map** to access the **Domain Map** page.
The Define Domain Map link does not appear on the Repository Configuration Properties - Info page unless Windows Domain Authentication is selected.
6. On the Domain Map page:
 - To add a domain, click **Add** to access the **Domain Entry** page.
On the Domain Entry page, enter information in the **Domain**, **Primary Controller**, and **Backup Controller** fields, then click **OK** to return to the Domain Entry page.
 - To modify a domain, select it and click **Edit**.
 - To delete a domain, select it and click **Remove**.
7. Click **OK** to return to the Repository Configuration Properties - Info page.

Defining a domain

The Domain Entry page defines a Windows domain that is used for Windows domain authentication of users in a UNIX repository. To define a domain, you must know the names of the domain's primary controller and any backup controllers. Under Windows NT 4.0 and earlier, the primary domain controller is the computer that authenticates domain logins and maintains the directory database for a domain. A backup domain controller is a computer that receives a copy of the domain's directory database.

To define a domain:

1. Type a domain name.
This is a required field.
2. Type the domain's primary controller.
This is a required field.
3. Type the domain's backup controller.
This is an optional field.
4. Click **OK**.

Modifying users for Windows domain authentication

After the domain map is set up, configure users in the repository.

To modify users for Windows domain authentication:

1. Navigate to **Administration > User Management > Users**.
The **Users** list page appears.
2. For each user, select **View > Properties > Info** to access the **User Properties - Info** page.
3. For each user, modify the **User Source** field:
 - **Domain Only**
The user is authenticated only against the Windows domain.
 - **UNIX First**
The server attempts to authenticate the user first using default UNIX authentication. If that fails, the server attempts to authenticate the user against the Windows domain.
 - **Domain First**
The server attempts to authenticate the user first against the Windows domain. If that fails, the server attempts to authenticate the user using UNIX authentication.
4. Click **OK** to save the changes and return to the Users list page.

Content Servers

Use the **Administration > Basic Configuration > Content Servers** navigation to access pages to create new servers or create, modify, or delete server configuration objects.

A server configuration object is a template for a server. A server's configuration is defined by the properties in its server configuration object and the parameters in the server.ini file read during server startup.

The default server installation process creates a repository with one server. You can configure additional servers to run against a particular repository. Each server has a server configuration object in the repository against which the server is running.

The Server Configuration list page lists the server configuration objects for the current repository. The columns list the server name, the host on which it is running, the server's current status (unknown, running), and the version of the server configuration object.

Server configuration objects are stored in the repository System cabinet. You can create multiple server configuration objects as long as they are uniquely named. You can also modify a server configuration object and save it as a new object.

Note: Creating, starting, and stopping a remote Content Server from the Content Server list page has been removed from Documentum Administrator. As of Content Server 5.3 SP1, an installation program is now used to create remote servers. Refer to the *Content Server Installation Guide* and *Distributed Configuration Guide* for more information.

Click the links for instructions and information on:

- Duplicating a server configuration object, page 86
- Creating or modifying server configuration objects, page 87
 - Creating or modifying the server configuration object info page, page 88
 - Creating or modifying connection broker projections, page 94
 - Modifying projection targets, page 95
 - Deleting projection targets, page 96
 - Creating, modifying, or deleting network location projections, page 96
 - Creating, modifying, or deleting application servers, page 97
 - Creating, modifying, or deleting cached types, page 97
 - Creating or modifying locations, page 98
 - Creating or modifying far stores, page 100
- Viewing server and connection broker log files, page 100
- Deleting a server configuration object, page 101
- Configuring a server as a process engine, page 101
- Disabling a server as a process engine, page 102

Duplicating a server configuration object

Use these instructions to create a new server configuration object using an existing server configuration object as a template. Create a new server configuration object when you run additional servers against a repository, whether on the same host or a different host. The chapter Servers in the *Content Server Administration Guide* provides information on how and when to start additional servers.

To duplicate a server configuration object:

1. Navigate to **Administration > Basic Configuration > Content Servers**.
The **Content Server Configuration** list page appears.
2. Select the server name to copy and then select **File > Save As**.
The **Server Configuration Properties - Info** page appears.
3. In the **Name** field, type the name of the new server configuration object.
4. Modify any properties that you want to change.
Refer to [Creating or modifying server configuration objects, page 87](#) for information on modifying the other properties.
5. Click **OK** to save the new server configuration object or **Cancel** to exit.

Creating or modifying server configuration objects

Accessing the server configuration object pages checks out the server configuration object. Click **OK** to check in the server configuration object as a new version or click **Cancel** to cancel the checkout.

You must select the reinit box for changes that you made to take effect.

The Server Configuration Properties pages are organized into tabbed pages as follows:

- Info

The New Server Configuration - Info or Server Configuration Properties - Info page contains information on the server host, the platform on which the server is running, code pages and locales, and other general information. For instructions, refer to [Creating or modifying the server configuration object info page, page 88](#).

- Connection Broker

The Server Configuration Properties - Connection Broker page contains information on connection broker projection. Use this page to set up or modify connection broker projection targets. For instructions, refer to [Creating or modifying connection broker projections, page 94](#).

- Network Location

In 5.3 SP1 and later repositories, the New Server Configuration - Network Location or Server Configuration Properties - Network Location page contains information on the network locations associated with a particular Content Server. Use this page to set up or modify the proximity values for the associated network locations. For instructions, refer to [Creating, modifying, or deleting network location projections, page 96](#).

- App Servers (application servers)

The New Server Configuration - App Servers or Server Configuration Properties - App Servers page contains information on application servers. Use this page to optionally add an application server for Java method execution. For instructions, refer to [Creating, modifying, or deleting application servers, page 97](#).

- Cached Types

The New Server Configuration - Cached Types or Server Configuration Properties - Cached Types page allows you to specify which user-defined types are to be cached at server startup. For instructions, refer to [Creating, modifying, or deleting cached types, page 97](#).

- Locations

The New Server Configuration - Locations or Server Configuration Properties - Locations page lists the locations of certain files and programs that exist on the server host's file system and of certain objects in the repository, including the assume user program, change password program, log file, and Verity location. (The Verity location applies to pre-5.3 repositories only.) For instructions on creating or modifying locations, refer to [Creating or modifying locations, page 98](#).

- Far Stores

The New Server Configuration - Far Stores or Server Configuration Properties - Far Stores page lists storage areas a server has access to and allows you to designate which storage areas are far stores for that server. A server cannot store content in a far store. For more information on far stores, refer to the *Documentum Distributed Configuration Guide*. For instructions on creating or modifying far stores, refer to [Creating or modifying far stores, page 100](#).

If you are creating a new server configuration object, start with the Server Configuration Properties - Info page and proceed sequentially through the tabs. However, the easiest way to create a new server configuration object is to copy an existing server configuration object and then modify the new server configuration object's properties. To create a copy of a server configuration object, use the instructions in [Duplicating a server configuration object, page 86](#).

If you are viewing or modifying the properties of an existing server configuration object, view the pages in succession or modify and save information on individual pages. On each page, click a tab to navigate to the other pages.

Creating or modifying the server configuration object info page

Use these instructions to create or modify the server configuration object information on the New Server Configuration - Info or Server Configuration Properties - Info page. If creating a new server configuration object, it is recommended that you copy an existing server configuration object and modify the properties of the new object. Use the instructions in [Duplicating a server configuration object, page 86](#).

To create or modify the server configuration object Info page:

1. Navigate to **Administration > Basic Configuration > Content Servers**.
The **Content Server Configuration** list page appears.
2. To create a server configuration object, select **File > New > Server Config** to create a server configuration object.
The **New Server Configuration - Info** page appears.
3. To modify an existing server configuration object, select a server configuration object, then select **View > Properties > Info**.
The **Server Configuration Properties - Info** page appears.
4. Enter or modify the server configuration object properties.
5. If creating a new server configuration object, click **Next** to proceed to the **New Server Configuration - Connection Broker** page. Refer to [Creating or modifying connection broker projections, page 94](#) for information about this page.
Click **OK** to save any changes or click **Cancel** to reject any changes.
The system displays the Content Server Configuration list page.

Table 10. New Server Configuration - Info and Server Configuration Properties - Info page field definitions

Field label	Value
Name	The name of the initial server configuration object created. By default, the server configuration object has the same name as the repository. When you create a new server configuration object, you assign it a new name.
Host Name	The name of the host on which the server is installed. Read-only.

Field label	Value
Server Version	The version, operating system, and database of the server defined by the server configuration object. Read-only.
Process ID	The server's process ID on its host. Read-only.
Install Owner	The Documentum installation owner. Read-only.
Install Domain	On Windows, the domain in which the server is installed and running. Read-only.
Trusted Mode	Indicates whether Trusted Content Services is enabled. Read-only.
Re-Initialize Server	When selected, the server is re-initialized after the server configuration object is saved. Some changes to the server configuration object require restarting the server rather than re-initializing the server.
Web Server Port	Identifies the port the web server uses. The default is 80.
Web Server Location	The name of the web server host and its domain. Used by client applications for creating DRLs.
Agent Launcher	Defines the method that launches the agent exec process. The default value is agent_exec_method. The agent_exec_method is created when you install Content Server. Its name is stored in the agent_launcher property of the server configuration object. It polls jobs that contain scheduling information for methods. Jobs are launched by the agent_exec process. To disable all job execution, leave this field empty. Click the Select Agent Launcher Method link to access the Choose a method page.

Field label	Value
Operator Name	The name for the repository operator if the repository operator is not explicitly named on the dmarchive.bat command line or in the Archive or Request method. This must be manually configured. The default is the owner of the server configuration object (the repository owner). The repository operator is the user whose Inbox receives all archive and restore requests.
	Click the Select Operator link to access the Choose a user page.
Server Cache Size	The maximum number of objects allowed in the server cache. The default is 200.
Client Cache Size	The maximum permitted size of the client cache, expressed as the number of objects. The default is 50.
Network File Share	Indicates whether the server is using Network File Share for file sharing.
Checkpoint Interval	Defines the interval at which the server broadcasts service information to connection brokers. The unit of measurement is seconds. The default is 300 seconds.
Keep Entry Interval	Specifies how long each connection broker keeps a server entry if the connection broker does not receive checkpoint broadcasts from the server. This time limit is included in the server's broadcast information. By default, the value is 1,440 minutes (24 hours).
Locale Name	Indicates the server's locale. The value is determined programmatically and is set during server installation. In general, do not change this value. For more information on locales, review the Internationalization Summary appendix in <i>Content Server Fundamentals</i> .

Field label	Value
Default Client Codepage	<p>The default codepage for clients. The value is determined programmatically and is set during server installation. In general, it will not need to be changed. Do not change this without reviewing the Internationalization Summary appendix in <i>Content Server Fundamentals</i>.</p> <p>Options are:</p> <ul style="list-style-type: none"> • UTF-8 • ISO_8859-1 • Shift_JIS • EUC-JP • EUC-KR • US-ASCII • ISO_10646-UCS-2 • IBM850
Server OS Codepage	<p>The code page used by the operating system of the machine on which the server resides. The value is determined programmatically and is set during server installation. In general, do not change this value. For more information on locales, review the Internationalization Summary appendix in <i>Content Server Fundamentals</i>.</p> <p>Options are:</p> <ul style="list-style-type: none"> • UTF-8 • ISO_8859-1 • Shift_JIS • EUC-JP • EUC-KR • US-ASCII • ISO_10646-UCS-2 • IBM850

Field label	Value
Turbo Backing Store	The name of the file store storage area where the server puts renditions generated by indexing blob and turbo content. The default is filestore_01.
Rendition Backing Store	The name of the file store storage area where the server will store renditions generated by full-text indexing operations.
Modifications Comments	Remarks on changes made to the server configuration object in this version.
SMTP Server	The name of the computer hosting the SMTP Server that provides mail services to Content Server.
	The value is provided during server installation.
Workflow Agent Worker Threads	The number of workflow agent worker sessions. The maximum value is 1000. The default value is 3. Setting this to 0 disables the workflow agent.
Secure Connect Mode	<p>Options are:</p> <ul style="list-style-type: none"> • Dual: Uses encrypted and unencrypted connections. • Native: Uses unencrypted connections only. • Secure: Uses encrypted connections only.
	If you change the mode, you must restart the server. Re-initializing the server does not suffice.
Maximum Content Migration Threads	<p>Defines a valid value range for the argument PARALLEL_DEGREE for parallel content migration when running MIGRATE_CONTENT administration method or setting up a migration policy rule. Valid values are between 1 and 128. This option:</p> <ul style="list-style-type: none"> • Is available only for 6.5 repositories • Requires a Content Storage Services license that is enabled on the Content Server. • Works in conjunction with the Content Migration Threads field on the MIGRATE_CONTENT - Parameters or Job Properties - Rules pages.
	The value entered in the Content Migration Threads field cannot exceed the Maximum Content Migration Threads value.

Field label	Value
Inherit Permission Set From	<p>The permission set the server uses for new objects if a user fails to specify a permission set for an object or fails to specify that no default permission set is wanted. Options are:</p>
	<p>A User permission set is defined for a user when a system administrator, Superuser, or repository owner creates a user. This permission set can be used as the permission set for any object created by the user. Because user objects are not subtypes of SysObject, the permission set is not used to enforce any kind of security on the user. A User permission set can only be used as a default permission set.</p>
	<p>A Type permission set is associated with the type definition for a SysObject or SysObject subtype. For example, you can define a default permission set for all objects of type dm_document or type dm_process. Because type objects are not subtypes of SysObject, the permission set is not used to enforce any kind of security on the user. A Type permission set can only be used as a default permission set.</p>
	<p>A Folder permission set is associated with a folder or cabinet. If a user wants to change a folder or cabinet's properties, modify the folder or cabinet object itself, or move, copy, or link an object to the folder, the server uses the permissions in the associated permission set to determine whether the user can perform the requested operation.</p>
Default Alias Set	<p>The default alias set for new objects. Click the Select Alias Set link to access the Choose an alias set page.</p>
Enabled LDAP Servers	<p>The LDAP configuration objects for LDAP servers used for user authentication and synchronization.</p>
Maximum Login Ticket Expiration Time	<p>Click the Select link to access the Choose LDAP Server Configurations page to add LDAP servers.</p>
	<p>The maximum length of time, in minutes, that a login ticket generated by the current server can remain valid. The minimum value is 1 minute. The maximum value is 43200 minutes (30 days). The default value at server installation is 43200.</p>

Field label	Value
Default Login Ticket Expiration Time	The default length of time, in minutes, that a login ticket generated by the current server can remain valid. The value must always be less than or equal to the maximum login ticket expiration time. The default value is 5 minutes.
Application Access	Application access control (AAC) tokens are encoded strings that may accompany connection requests from applications. The information in a token defines constraints on the connection request. If selected, a connection request received by this server from a non-Superuser must be accompanied by a valid application access control token and the connection request must comply with the constraints in the token.
Superuser Access	When selected, a user with Superuser privileges cannot connect to the server using a global login ticket.
Next	Click to continue to the New Server Configuration - Connection Broker page. The Next and Previous buttons appear only when creating a new server configuration object.
OK	Click to save changes to the server configuration object and return to the Content Server Configuration list page.
Cancel	Click to exit the Server Configuration Properties - Info page without saving changes and return to the Content Server Configuration list page.

Creating or modifying connection broker projections

Use the New Server Configuration - Connection Broker or Server Configuration Properties - Connection Broker page to define the connection brokers to which the server projects. You can add, modify, or delete projection targets.

The Documentum connection broker is a process that provides client sessions with server connection information. Each server broadcasts information to connection brokers at regular intervals. The broadcast contains the information maintained by connection brokers about the server and the repository accessed by the server.

The New Server Configuration - Connection Broker or Server Configuration Properties - Connection Broker page lists the host where there are connection brokers to which the current server projects, the port number used by each connection broker, and the proximity value of each connection broker. It also lists a note for each connection broker and indicates whether or not the server is projecting to each connection broker.

To create or modify connection broker projection targets:

1. Access the **New Server Configuration - Connection Broker** or **Server Configuration Properties - Connection Broker** page.
2. To add a new projection target, click **Add** to access the **Connection Broker Projection for ACS Server** page.
3. To edit an existing projection target, select a target host and then click **Edit** to access the **Connection Broker Projection for ACS Server** page.
4. Enter information on the **Connection Broker Projection for ACS Server** page:
 - a. **Target Host:** Type the name of the host on which the connection broker resides.
 - b. **Port:** Type the port number on which the connection broker is listening.
 - c. **Proximity:** Type the correct proximity value for the connection broker.
Local connection brokers usually have a proximity of 1. If using Content Servers in a distributed environment, assign connection brokers a prefix of 9, in the format 9xxx, where a value such as 9001 is close and a value such as 9200 is far.
 - d. **Note:** Type a note about the connection broker.
 - e. **Status:** Select **Enabled** to enable projection to the connection broker.
 - f. Click **OK** to save the new projection target or **Cancel** to exit without saving the changes.
The **New Server Configuration - Connection Broker** or **Server Configuration Properties - Connection Broker** page appears.
5. To delete an existing connection broker, select a connection broker and then click **Remove**.
6. If creating a new server configuration object, click **Next** to proceed to the **New Server Configuration - Application Server** page.
7. To enable the changes, reinitialize the server. Restarting the server is not required.

Modifying projection targets

Use these instructions to modify connection broker projections for a server.

To modify projection targets:

1. On the **Server Configuration Properties - Connection Broker** page, select the projection target host to modify.
2. Click **Edit**.
The **Connection Broker Projection for ACS Server** page appears.
3. Change any values that you want to change.
4. Click **OK** to save the changes or **Cancel** to cancel the changes.
The **Server Configuration Properties - Connection Broker** page appears.

Deleting projection targets

Use these instructions to delete connection projection targets for a server.

To delete projection targets:

1. On the **Server Configuration Properties - Projection Broker** page, select the projection targets to delete.
2. Click **Remove**.
3. Click **OK** to delete the project targets or **Cancel** to cancel the deletions.

Creating, modifying, or deleting network location projections

A network location identifies locations from which end users connect to Documentum web clients. Network locations can optionally define specific IP address ranges where the users are located. Content Servers use network locations to determine the content storage location from which a content file is provided to web client users.

Use the New Server Configuration - Network Location or Server Configuration Properties - Network Location page to define the network locations used by a server. You can add, modify, or delete network location projections and define proximity values for each network location. The proximity value describes the server's approximate distance from a network location.

The New Server Configuration - Network Location and Server Configuration Properties - Network Location pages list the network locations with which the server is associated, the proximity value for each network location, and whether projection to that network location is enabled. If projection to the network location is enabled, the server can serve content to users connecting from that network location. For more information about network locations, refer to [About network locations, page 146](#).

To create, modify, or delete network location projections:

1. Access the **New Server Configuration - Network Location** or **Server Configuration Properties - Network Location** page.

2. To add network locations, click **Add**.

The **Choose Network Locations** page appears.

- a. Select the network locations to add.

The network locations displayed are in the global registry known to DFC on the Documentum Administrator host.

- b. Click **Add**.

The network locations move to the right-hand column.

- c. Click **OK** to save the change or **Cancel** to exit without saving.

The system displays the **New Server Configuration - Network Location** or **Server Configuration Properties - Network Location** page.

3. To change the proximity values for a network location, edit the **Proximity** field.

4. To enable or disable the server's projection to a network location, select or clear the **Enabled** checkbox.
5. To delete network locations from the server, select a network location and click **Remove**.
6. Click **OK**.

Creating, modifying, or deleting application servers

Use these instructions to create or modify application server entries in the server configuration object. You can also delete an application server using these instructions.

To create, modify, or delete application servers:

1. Access the **New Server Configuration - App Servers** or **Server Configuration Properties - App Servers** page.
2. To add an application server, click **Add** to access the **Application Server** page.
3. To modify an application server, select an existing application server and then click **Edit** to access the **Application Server** page.
4. Add or modify information on the Application Server page:
 - a. **Name:** Type the application server name.
 - b. **URI:** Type the URI to the application server, in the format:
`http://host_name:port_number/servlet_path`
 - c. Click **OK** to add the application server or **Cancel** to exit without saving changes.
 The New Server Configuration - App Servers or Server Configuration Properties - App Servers page appears.
5. To delete an application server, select the application server name and then click **Remove**.
6. Click **OK** to save changes or **Cancel** to exit without saving any changes. The system displays the Content Server Configuration page.
 To proceed to the **New Server Configuration - Cached Types** or **Server Configuration Properties - Cached Types** page, click **Next** or click the **Cached Types** tab.

Creating, modifying, or deleting cached types

The New Server Configuration - Cached Types and Server Configuration Properties - Cached Types pages lists names of all user-defined object types to cache on server startup. By default, no user-defined objects are cached.

To create, modify, or delete cached types:

1. Access the **New Server Configuration - Cached Types** or **Server Configuration Properties - Cached Types** page.
2. To add a cached type, click the **Add** link.

The **Choose a type** page appears.

- a. Select the object types to cache.
- b. Click **Add**.
- c. Click **OK**.

You must click **OK** at the bottom of any page on which you checked object types to cache. If you view another page before clicking **OK**, the previously selected types are not saved as cached types.

The New Server Configuration - Cached Types or Server Configuration Properties - Cached Types page appears.

3. To delete a cached type, select its name and then click **Remove**.
4. Click **OK** to save changes or **Cancel** to exit without saving any changes. The **Content Server Configuration** page appears.

To proceed to the **New Server Configuration - Locations** or **Server Configuration Properties - Locations** page, click **Next** or click the **Locations** tab.

Creating or modifying locations

Use the **New Server Configuration - Locations** and **Server Configuration Properties - Locations** pages to modify the locations where files and programs on the server host's file system are found and objects in the repository are found, including the assume user program, change password program, and log file.

To view or modify locations:

1. Access the **New Server Configuration - Locations** or **Server Configuration Properties - Locations** page.
2. To change a location, click the **Select Location** link next to the object or file whose location you want to change.
3. The **Choose a Location** page appears.
 - a. Select a **Location** and **File System Path**.
 - b. Click **OK** to return to the **New Server Configuration - Locations** or **Server Configuration Properties - Locations** page.
4. Click **OK** to save changes or **Cancel** to exit without saving any changes. The **Content Server Configuration** page appears.

To proceed to the **New Server Configuration - Far Stores** or **Server Configuration Properties - Far Stores** page, click **Next** or click the **Far Stores** tab.

The following locations can be changed:

Table 11. Locations page properties

Field label	Value
Assume User	The location of the directory containing the assume user program. The default is assume_user.
Change Password	The location of the directory containing the change password program. The default is change_password.
Common	The location of the common directory. The default is common.
Events	The location of the events directory. The default is events.
Log	The location of the logs directory. The default is temp.
Nls	The location of the NLS directory. The default is a single blank.
Secure Writer	The location of the directory containing the secure writer program. The default is secure_common_area_writer.
System Converter	The location of the directory containing the convert.tbl file and the system-supplied transformation scripts. There is no default for this field.
Temp	The location of the temp directory.
User Converter	The full path for the user-defined transformation scripts. The default is convert.
User Validation	The full path to the user validation program. The default is validate_user.
Verity	5.3 and later repositories, contains a dummy value for compatibility with Webtop 5.2.x. The default value is verity_location.
Signature Check	The location of the directory that contains the signature validation program. The default is validate_signature.
Authentication Plugin	The location of an authentication plugin, if used. The default is auth_plugin in \$Documentum/dba/auth.

Creating or modifying far stores

In a distributed content environment, a far store is a storage area remote or inaccessible from the current Content Server, in which the server cannot store content. Use the New Server Configuration - Configuration Properties and Server Configuration Properties - Far Store pages to designate which storage areas are far stores. For more information on distributed content environments, refer to the *Distributed Configuration Guide*.

To designate a store as a far store or remove its far store designation:

1. To add a far store:
 - a. Click the **Add** link.
The **Choose a storage** page appears.
 - b. Select the storage areas that must be designated as far stores.
 - c. Click **Add**.
 - d. Click **OK** to save the far stores or **Cancel** to exit from the Add page.
2. To remove a far store:
 - a. Select the far stores to remove.
 - b. Click the **Remove** link.
3. Click **OK** to save the changes or **Cancel** to exit without saving.

Viewing server and connection broker log files

The server log file records server activities. Server logs provide valuable information for troubleshooting server or repository problems.

Connection broker logs record information about connection brokers, which provide connection information to clients.

If you are connected to a secondary server, you see only the server and connection broker logs for that server.

Use these instructions to view server or connection broker logs.

To delete server log files, run the Log Purge tool. For more information on the tool, refer to [Log purge \(dm_LogPurge\), page 316](#).

To view logs:

1. Navigate to **Administration > Basic Configuration > Content Servers**.
2. To view server logs:
 - a. Select the server configuration object of the server whose log you want to view.
 - b. Select **View > Server Log**.
The **Select Server Log** page displays a list of log files.
 - c. Select the log to view and click **View Log**.

- The log is displayed.
- d. Click **Close**.
3. To view connection broker logs:
- a. Select **View > Connection broker Log**.
A list of log files is displayed.
 - b. Select the log to view and click **View Log**.
The log is displayed.
 - c. Click **Close**.

Deleting a server configuration object

Use these instructions to delete a server configuration object.

Do not delete the CURRENT version of the server configuration object of a server that is in use. You can safely delete the CURRENT version of the server configuration object of a server that is shut down and not in use, or old versions of an in-use server's server configuration object. To display old versions of server configuration objects, select the **All Versions** filter from the list box on the server configuration object page.

To delete a server configuration object:

1. Navigate to **Administration > Basic Configuration > Content Servers**.
The **Server Configuration** list page appears.
2. Select the server configuration objects to delete.
3. Select **File > Delete**.
The **Delete Object** page appears.
4. Click **OK** to delete the server configuration objects or **Cancel** to leave the server configuration objects in the repository.
The Server Configuration list page appears.

Configuring a server as a process engine

If the Business Process Manager (BPM) DocApp is installed in a repository and you have a license for process engines, a server for that repository may be configured as a process engine. Ensure that the license key is available.

Note:

- There is no interface for reversing this process. Use the instructions described in [Disabling a server as a process engine, page 102](#) to disable a server as a process engine.
- The Configure Process Engine option is not available for Documentum version 6 and later repositories. Installing the BPM DocApp on a version 6 or later repository automatically configures the server to be a process engine.

To configure a server as a process engine:

1. Connect to the repository whose server you are configuring as a process engine.
2. Navigate to **Administration > Basic Configuration > Content Servers**.
3. Select a server.
4. Select **Tools > Configure Process Engine**.
5. Type the license key and click **OK**.
The system displays a confirmation page.
6. Click **OK** or **Cancel**.
The server is now able to run workflows.

Disabling a server as a process engine

There is no interface for reversing the process described in [Configuring a server as a process engine, page 101](#). Use these instructions to disable a server as a process engine.

To disable a server as a process engine:

1. Using any client, connect to the repository whose server you are disabling as a process engine.
2. Navigate to the /System/Workflow/Process Engine folder.
3. Ensure that all objects in the folder are displayed.
For example, in Documentum Administrator or Webtop, select **Show All Objects and Versions** from the list box.
4. Delete the object corresponding to the name of the server that is configured as a process engine.

Federations

The Federations list page displays all federations known to the connection brokers in your preferences list.

A federation is a set of two or more repositories bound together to facilitate the management of a multi-repository distributed configuration. Federations share a common name space for users and groups and project to the same connection brokers. Global users, global groups, and global permission sets are managed through the governing repository, and have the same property values in each member repository within the federation.

For example, if you add a global user to the governing repository, that user will be added to all the member repositories by a federation job that synchronizes the repositories.

One enterprise can have multiple repository federations, but each repository can belong to only one federation. Repository federations are best used in multi-repository production environments where users share objects among the repositories. We do not recommend creating federations that include production, development, and test repositories, because object types and format definitions change

frequently in development and test environments, and these must be kept consistent across the repositories in a federation.

The repositories in a federation can run on different operating systems and database platforms. Repositories in a federation can have different server versions; however, the client running on the governing repository must be version-compatible with the member repository in order to connect to it.

To create or modify federations, you do not have to be connected to a repository in the federation. To add a repository to a federation, your Documentum Administrator connection broker list must include a connection broker to which the particular repository projects.

Before you set up a repository federation, refer to the appropriate chapters in the *Distributed Configuration Guide*.

Click the links below for instructions and information on:

- [Creating federations, page 103](#)
- [Modifying federations, page 105](#)
- [Adding members to a federation, page 106](#)
- [Removing member repositories from a federation, page 107](#)
- [Deleting Federations, page 107](#)
- [Connecting to the governing repository or a federation member, page 108](#)
- [Choosing user subtypes, page 108](#)
- [Modifying members of a federation, page 109](#)
- [Choosing repository federation members, page 109](#)

Creating or modifying federations

Click the links below for instructions on creating or modifying federations:

- [Creating federations, page 103](#)
- [Modifying federations, page 105](#)

Creating federations

Use these instructions to create a federation. Before you create a federation, obtain the user name and password of a Superuser in each repository.

All repositories in a federation must project to the same connection brokers. When you create a federation, Documentum Administrator updates the connection broker projection information in the server configuration object for each member repository. No manual configuration is necessary.

The repositories in a federation can run on different operating systems and database platforms. Repositories in a federation can have different server versions; however, the client running on the governing repository must be version-compatible with the member repository in order to connect to it.

For more information on federations, refer to the *Distributed Configuration Guide*.

To create a federation:

1. Navigate to **Administration > Basic Configuration > Federation**.

The **Federations** list page appears.

2. Select **File > New > Federation**.

The New Federation Configuration page appears on which you select the governing repository for a new federation. Click the headings to sort the list by repository name or connection broker, click the headings.

If you do not see a particular repository on the page, either it is already a member of a federation or no connection broker to which it projects appears in your connection broker list.

3. Select the governing repository of the new federation and click **Next** to access the login page.
4. Type the name and password of a user who has Superuser privileges in the governing repository and click **Next** to access the **New Federation Configuration - Info** page.

5. Enter information on the New Federation Configuration - Info page.

- a. **Name:** Type the name of the new federation.

- b. **Make All Governing Repository Users & Groups Global:** Select to make all users and groups in the governing repository global users and global groups.

- c. Click **Next** to continue to the **New Federation Configuration - User Subtypes** page.

6. Enter information on the New Federation Configuration - User Subtypes page.

On this page, designate the user subtypes to propagate to member repositories.

- a. Click **Add**.

If there are user subtypes in the repository, a list of user subtypes is displayed on the Choose a user subtype page.

- b. Select the user subtypes to propagated to member repositories.

- c. Click **Add**.

The subtypes move to the **Selected** list.

- d. Click **OK** to accept the user subtypes or **Cancel** to return to the New Federation Configuration - User Subtypes page.

7. Click **Next** to access the **New Federation Configuration - Members** page.

8. Add member repositories on the New Federation Configuration - Members page.

- a. Click **Add**.

The system displays the **Choose Member Repositories** page.

- b. Select the repositories that you want to be member repositories.

- c. Click **Add**.

The repositories move to the **Selected** list.

- d. To remove any member repositories from the **Selected Items** list, select them and then click **Remove**.

- e. Click **OK** to accept the member repositories or **Cancel** to exit to the Members page.

- f. Provide login information for the member repositories.

- g. Click **Finish**.
The federation is created and the Federations list page appears.
9. Ensure that all repositories project to the same connection brokers.

Modifying federations

Use these instructions to modify an existing repository federation.

To modify a federation:

1. Connect to a repository using the same connection broker as at least one of the member repositories.
2. Navigate to **Administration > Basic Configuration > Federations**.
The **Federations** list page appears.
3. Select the federation to modify and then select **View > Properties > Info**.
The **Federation Configuration Properties** login page appears.
4. Enter information on the Federation Configuration Properties login page.
 - a. **Name and Password**: Type the name and password for the federation.
 - b. **Domain**: Optionally, type the domain.
 - c. Click **Next**.
The **Federation Configuration Properties - Info** page appears.
5. Modify information on the Federation Configuration Properties - Info page.
 - a. To change the federation's status, select or clear the **Active** checkbox.
 - b. Click **Next** or click the **User Subtypes** tab.
The **Federation Configuration Properties - User Subtypes** page appears.
6. Enter or modify information on the Federation Configuration Properties - User Subtypes page.
 - a. To add a subtype, click **Add**.
If there are user subtypes in the repository, the system displays a list of user subtypes on the **Choose a user subtype** page.
 - i. Select the subtypes to propagate to member repositories.
 - ii. Click **Add**.
The subtypes move to the **Selected** list.
 - iii. Click **OK** to accept the user subtypes or **Cancel** to return to the Federation Configuration Properties - User Subtypes page.
 - b. To delete a subtype, select it and then click **Remove**.
 - c. Click **Next** or click the **Members** tab to access the **Federation Configuration Properties - Members** page.
7. Enter or modify member repositories on the Federation Configuration Properties - Members page.

- a. To add a member, click **Add**.
If there are members in the repository, a list of members is displayed on the **Choose Member Repositories** page.
 - i. Select a repository and then click **Add**.
 - ii. Click **OK**.
 - iii. Type a Superuser's name and password.
 - iv. Click **OK**.
- b. To remove a federation member, select it and then click **Remove**.
The repository is removed from the member list.
- c. To edit a federation member, select it and click **Edit**.
 - i. Type a Superuser's **Name** and **Password** for the member repository.
 - ii. Optionally, select or clear the **Skip this member and continue authentication** checkbox.
 - iii. Click **OK**.
- d. Click **Finish** or **Cancel**.
The system displays the **Federations** list page.

Adding members to a federation

Use these instructions to add member repositories to a federation.

To add members to a federation:

1. Access the **Federation Configuration Properties - Members** page:
 - a. Connect to a repository using the same connection broker as at least one of the member repositories.
 - b. Navigate to **Administration > Basic Configuration > Federations**.
The **Federations** list page appears.
 - c. Select the federation to modify and then select **View > Properties > Info**.
The **Federation Configuration Properties** login page appears.
 - d. Enter information on the **Federation Configuration Properties** login page.
 - i. **Name and Password**: Type the name and password for the federation.
 - ii. **Domain**: Optionally, type the domain.
 - iii. Click **Next**.
The **Federation Configuration Properties - Info** page appears.
- e. Click the **Members** tab to access the **Federation Configuration Properties - Members** page.
The federation members are listed.
2. Click the **Add** link to access the **Choose Member Repositories** page.
3. Locate the repository that you want to add and select the checkbox next to the repository name.

You can sort the repositories by clicking the **Repository Name** or **Connection Broker Name** columns. To view a different number of repositories, select a number from the list box. You can also type in the repository name or part of the name, or you can click the arrow buttons to jump to the next page of repositories.

4. Click the **Add** button and then click **OK**.
5. Type the name and password of a user who has Superuser privileges in the new member repository and click **OK**.
6. Click **Finish**.

The system displays the Federation list page.

Removing member repositories from a federation

Use these instructions to remove member repositories from a federation.

To delete member repositories from a federation:

1. Access the Federation Configuration Properties - Members page:
 - a. Connect to a repository using the same connection broker as at least one of the member repositories.
 - b. Navigate to **Administration > Basic Configuration > Federations**.
The **Federations** list page appears.
 - c. Select the federation to modify and then select **View > Properties > Info**.
The **Federation Configuration Properties** login page appears.
 - d. Enter information on the Federation Configuration Properties login page.
 - i. **Name and Password**: Type the name and password for the federation.
 - ii. **Domain**: Optionally, type the domain.
 - iii. Click **Next**.
The **Federation Configuration Properties - Info** page appears.
 - e. Click the **Members** tab to access the **Federation Configuration Properties - Members** page.
The federation members are listed.
2. Select the checkbox next to any members that you want to remove and click the **Remove** link.
The members are removed.
3. Click **OK**.
The system displays the Federations list page.

Deleting Federations

Use these instructions to delete a federation. Alternatively, you can make a federation inactive by accessing the Info page of the federation and clearing the **Active** checkbox.

To delete a federation:

1. Navigate to **Administration > Basic Configuration > Federations**.
2. Select the federation to delete.
3. Select **File > Delete**.
4. Type the user ID and password of a Superuser in the governing repository.
5. Click **OK**.

The federation is deleted.

Connecting to the governing repository or a federation member

On this page, provide the login information for the governing repository or a federation member.

To connect to a federation member:

1. Type the user name and password of a Superuser in the repository.
2. If required, type in the domain where the user is authenticated.
3. Click **Next** or **OK**.

Choosing user subtypes

On the New Federation Configuration - User Subtypes or Federation Configuration Properties - User Subtypes page, choose user subtypes to be propagated to all members of the federation. The type itself must be created in each repository in the federation. This page ensures that users of that particular subtype are propagated to the member repositories.

To choose user subtypes:

1. Click **Add** to access the **Choose a user subtype** page to designate the user subtypes to propagate to member repositories.
If there are user subtypes in the repository, the system displays a list of user subtypes.
2. To jump to a subtype or group of subtypes, type the first few letters of the type name in the **Starts with** field and click **Go**.
To view more pages, click the forward and back buttons.
To view more subtypes on one page, select a different number from the **Show items** list box.
3. Select the subtypes and then click **Add**.
4. To deselect subtypes, select them in the right-hand column and click **Remove**.
5. Click **OK** to accept the user subtypes or **Cancel** to return to the New Federation Configuration - User Subtypes or Federation Configuration Properties - User Subtypes page.

Modifying members of a federation

The New Federation Configuration - Members or Federation Configuration Properties - Members page lists the members of a repository federation. From these pages, you can add, modify, and remove member repositories.

You can sort the members by clicking the Member, Active, Status, and Refresh Date links. If a repository is Active, it is active in the federation. The Status indicates whether or not the repository is initialized. The Refresh Date is the date of the last federation update.

To modify the members of a federation:

1. To add a member to the federation:
 - a. Click **Add**.
A list of repositories who are not members of a federation are displayed. (A repository can belong to only one federation.)
 - b. Select the checkboxes corresponding to the repositories that you want to add to the federation.
 - c. Click **Add**.
 - d. Click **OK**.
 - e. Provide the user name and password of a Superuser for each new repository.
 - f. Click **OK**.
2. To edit a member:
 - a. Select the checkbox next to the member repository's name.
 - b. Click **Edit**.
 - c. Provide the user name and password of a Superuser.
 - d. Click **OK**.
3. To remove a repository from a federation:
 - a. Select the checkboxes corresponding to the repositories that you want to remove from the federation.
 - b. Click **Remove**.
The member is removed.
4. Click **OK**.

Choosing repository federation members

On this page, select the members of a repository federation. The repositories listed are all repositories not already in a federation that are known to all the connection brokers in your preferences. You can sort the list of repositories by repository name or connection broker.

To select the members of a repository Federation:

1. To jump to a particular repository or group of repositories, type the first few letters of the repository name in the **Starts with** field and click **Go**.
2. To view more pages, click the forward and back buttons.
3. To view more repositories on one page, select a different number from the **Show items** list box.
4. To select members, select the checkboxes next to their names and click **Add**.
5. To deselect members, select them in the right-hand column and click **Remove**.
6. Click **OK**.

LDAP Servers

An LDAP (Lightweight Directory Access Protocol) directory server is a third-party product that maintains information about users and groups. Documentum Content Servers use LDAP directory servers to authenticate users and manage users and groups from a central location.

If your organization uses LDAP directory servers for user authentication or to manage users and groups, use the pages under the **Administration > Basic Configuration > LDAP Servers** node in Documentum Administrator to configure and map your existing LDAP configuration to Documentum.

Superusers can create, view, modify, or delete LDAP configuration objects. You can also configure primary LDAP servers with failovers, so that content server can use failovers for authentication in case primary server is unavailable. Changes from the directory server are automatically propagated to all the repositories using the directory server by the dm_LDAPSynchronization job.

When you navigate to the LDAP Server Configuration list page (**Administration > Basic Configuration > LDAP Servers**), Documentum Administrator displays all the primary LDAP servers that are configured to the repository. If there are no LDAP servers configured to the repository, Documentum Administrator displays the message *No LDAP Server Configurations*.

Note: Using an LDAP directory server has the following constraints:

- The `changePassword` method is not supported for users managed through an LDAP directory server.
- Dynamic groups are supported only on Sun Java System directory servers.

From the LDAP Server Configuration list page, you can navigate to other pages to:

- Add new LDAP servers
- View or modify existing LDAP server properties
- Synchronize LDAP servers
- Duplicate an existing LDAP server configuration
- Delete existing LDAP servers configurations

Click the links below for information and instructions for:

- [Understanding LDAP server configurations, page 112](#)
- [Adding or modifying LDAP server configurations, page 113s](#)
- [Configuring LDAP directory and secure connection information, page 115](#)
- [Configuring synchronization and user authentication for LDAP servers, page 121](#)
- [Mapping LDAP Servers, page 126](#)
- [Configuring failover settings and secondary LDAP servers, page 135](#)
- [Changing the binding password, page 141](#)
- [Forcing LDAP server synchronization, page 141](#)
- [Duplicating LDAP configurations, page 142](#)
- [Deleting LDAP configurations, page 142](#)
- [Using LDAP directory servers with multiple Content Servers, page 143](#)

Table 12. LDAP Server Configuration list page properties

Field label	Value
Name	The name of the LDAP configuration object. Set up the name of the LDAP server on the LDAP Server Configuration Properties - Info page.
Hostname	The name of the host on which the LDAP directory server is running. Set up the hostname on the LDAP Server Configuration Properties - Info page.
Port	The port number where the LDAP directory server is listening for requests. Set up the port on the LDAP Server Configuration Properties - Info page.
SSL Port	The SSL port for the LDAP directory server. Set up SSL Port on the LDAP Server Configuration Properties - Info page.
Directory Type	The directory type used by the LDAP directory server. Set up the directory type on the LDAP Server Configuration Properties - Info page.
Import	Indicates if users and groups, groups and member users, or users only are to be imported. Set up the import option on the LDAP Server Configuration Properties - Sync & Authentication page.
Sync Type	Indicates if synchronization is full or incremental. Set up the synchronization type on the LDAP Server Configuration Properties - Sync & Authentication page.

Field label	Value
Failover	Indicates if failover settings have been established for the primary server. Set up failover settings on the LDAP Server Configuration Properties - Failover page.
Enabled	Indicates whether the LDAP server is active or not. Enable or disable the server on the LDAP Server Configuration Properties - Info page.

Understanding LDAP server configurations

If your organization currently uses Lightweight Directory Access Protocol (LDAP) to manage users and groups or for user authentication, use the pages under the **Administration > Basic Configuration > LDAP Servers** node to map your existing LDAP configuration to Documentum. Using an LDAP server provides a single place where you make additions and changes to users and groups. Using the dm_LDAPSynchronization job, the changes from the directory server are automatically propagated to all the repositories using the directory server. Using an LDAP directory server to manage users and groups in the Documentum system ensures that:

- The users and groups defined in the directory server are in each repository using the directory server.
- The values of the mapped properties for the users are the same in each participating repository.

To configure an LDAP server in SSL mode, you must first properly initialize the certificate database on Content Server by downloading and installing certutil utility. Refer to the *Content Server Administration Guide* for complete instructions.

To create a new LDAP configuration, you need the following information about the LDAP directory server:

- The name of the host where the LDAP directory server is running
- The port where the LDAP directory server is listening
- The type of LDAP directory server
- The binding distinguished name and password for accessing the LDAP directory server
- The person and group object classes for the LDAP directory server
- The person and group search bases
- The person and group search filters
- The Documentum attributes that you are mapping to the LDAP attributes

For 5.3x repositories, only user attributes can be mapped from an LDAP directory server to Documentum attributes using Documentum Administrator. If you need to map group attributes, use IAPI.

For examples of LDAP configuration attribute mapping under Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory, refer to [LDAP configuration attribute mapping examples, page 131](#).

The mapping between the LDAP person or group entries and Documentum user or group attributes is stored in Documentum as an LDAP configuration object. A 5.3 or later server can use multiple LDAP servers and configuration objects.

There are two ways in which repositories in federation can be configured for synchronization. Refer to the LDAP White Paper in Powerlink website for more information.

An LDAP server may be used with external password checking. Refer to the chapter called Managing User Authentication in the *Content Server Administration Guide* for information on the required setup in such a configuration. You must properly configure SSL for the LDAP server and download and install the certutil utility and CA certificates.

For 5.3x repositories, only user attributes can be mapped from an LDAP directory server to Documentum attributes using Documentum Administrator. If you need to map group attributes, use IAPI.

When you create users who will be managed by an LDAP server:

- The user_name, and user_login_name attributes of the dm_user object must have non-null values.
- The user_name and user_login_name attributes of the dm_user object must have unique values.

For more information about using LDAP with Documentum repositories, refer to the chapter called Managing User Authentication in the *Content Server Administration Guide*. For information on which LDAP servers are certified for use with Content Server, refer to the *Content Server Release Notes* for your Content Server version.

Adding or modifying LDAP server configurations

When adding an LDAP directory server to an existing Documentum installation, the users and groups defined in the LDAP directory server are given precedence. The user or group entry in the directory server matches a user or group in the repository, the repository information is over written by information in directory server in case synchronization type is set to full synchronization on Sync and Authentication tab.

When you add a new LDAP server configuration, you access the New LDAP Server Configuration pages. When you view or modify existing LDAP server configurations, you access the LDAP Server Configuration Properties pages. The New LDAP Server Configuration pages and the LDAP Server Configuration Properties pages have four tabs: Info, Sync & Authentication, Mapping, and Failover. (The Failover tab is available only for Documentum 6 repositories.) The field properties on each tab are the same, regardless if you are in add, view, or modify mode; however, some fields may be read-only. For example, the field properties on the New LDAP Server Configuration - Info page are the same field properties on the LDAP Server Configuration Properties - Info page.

To add a new LDAP server configuration:

1. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the **LDAP Server Configuration** list page.
2. Select **File > New > LDAP Server Configuration** to access the **New LDAP Server Configuration - Info** page where you enter information such as directory type and IP address for the new LDAP directory.

For information on the field properties for this page, refer to [LDAP Server Configuration - Info page properties, page 119](#).

3. Click the **Sync & Authentication** tab.

The system displays the **New LDAP Server Configuration - Synch & Authentication** page where you enter synchronization and user authentication information.

For information on the field properties for this page, refer to [LDAP Server Configuration - Sync & Authentication page properties, page 124](#).

4. Click the **Mapping** tab.

The system displays the **New LDAP Server Configuration - Mapping** page where you enter user and group mapping information.

For information on the field properties for the New LDAP Server Configuration: Mapping page, refer to [LDAP Server Configuration - Mapping page properties, page 132](#).

From New LDAP Server Configuration: Mapping page, you can access the Map Property page by clicking **Add** in the Property Mapping grid.

5. Click the **Failover** tab. (The Failover tab is available only for Documentum 6 repositories.)

The system displays the **New LDAP Server Configuration - Failover** page where you configure the Content Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down.

For information on the field properties for the New LDAP Server Configuration - Failover page, refer to [LDAP Server Configuration - Failover page properties, page 139](#).

From the New LDAP Server Configuration - Failover page, you can access the Secondary LDAP Server page by clicking **Add** in the Secondary LDAP Servers grid.

6. Click **Finish** when you have completed configuring the new LDAP server.

To view or modify properties of existing LDAP servers:

1. Navigate to **Administration > Basic Configuration > LDAP Servers**.

The system displays the **LDAP Server Configuration** list page.

2. Select the LDAP server that you want to view or modify and then select **View > Properties > Info**.

The system displays the **LDAP Server Configuration Properties - Info** page where you view or modify information such as directory type and IP address for the LDAP directory.

For information on the field properties for this page, refer to [LDAP Server Configuration - Info page properties, page 119](#).

3. Click the **Sync & Authentication** tab.

The system displays the **LDAP Server Configuration Properties - Synch & Authentication** page where you view or modify synchronization and user authentication information.

For information on the field properties for this page, refer to [LDAP Server Configuration - Sync & Authentication page properties, page 124](#).

4. Click the **Mapping** tab.

The system displays the **LDAP Server Configuration Properties - Mapping** page where you view or modify user and group mapping information.

For information on the field properties for this page, refer to [LDAP Server Configuration - Mapping page properties, page 132](#).

From the LDAP Server Configuration Properties - Mapping page, you can access the Map Property page by clicking **Add** in the Property Mapping grid.

5. Click the **Failover** tab. (The Failover tab is available only for Documentum 6 repositories.)
The system displays the **LDAP Server Configuration Properties - Failover** page where you view or configure the Content Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down.
For information on the field properties for the LDAP Server Configuration Properties: Failover page, refer to [LDAP Server Configuration - Failover page properties, page 139](#).
From the LDAP Server Configuration Properties - Failover page, you can access the Secondary LDAP Server page by clicking **Add** in the Secondary LDAP Servers grid.
6. Click **OK** when you have completed viewing or modifying the LDAP server configuration properties.

Configuring LDAP directory and secure connection information

This section discusses configuring LDAP directory and secure connection information on the New LDAP Server Configuration - Info and LDAP Server Configuration Properties - Info pages, which contain the same field properties.

Click the links for information or instructions on:

- [Entering directory and secure connection properties for a new LDAP server, page 115](#)
- [Viewing or modifying directory and secure connection properties for LDAP servers, page 117](#)
- [LDAP Server Configuration - Info page properties, page 119](#).

Entering directory and secure connection properties for a new LDAP server

Use these instructions to enter LDAP directory and secure connection properties for a new LDAP server.

To enter directory and connection properties for a new LDAP server:

1. Navigate to the New LDAP Server Configuration - Info page.
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select **File > New > LDAP Server Configuration**.
The system displays the New LDAP Server Configuration - Info page where you enter information such as directory type and IP address for the new LDAP directory.
2. Enter the name and status for the new LDAP configuration object:
 - a. **Name:** Enter the name of the new LDAP configuration object.

- b. **Status:** Select the **Enable this LDAP Configuration** checkbox to enable the LDAP configuration.
3. Enter information in the **LDAP Directory** section:
 - a. **Directory Type:** Refer to the Release Notes for your version of Documentum Content Server to see which LDAP server versions are supported. Options are:
 - Sun One/Netscape/iPlanet Directory Server (default)
 - Microsoft Active Directory
 - Microsoft ADAM
 - Oracle Internet Directory Server
 - IBM Directory Server
 - Novell eDirectory
 - b. **Hostname / IP Address:** Type the name of the host on which the LDAP directory server is running.
 - c. **Port:** Type the port number where the LDAP directory server is listening for request. The default is 389.
 - d. **Binding Name:** Type the binding distinguished name used to authenticate requests to the LDAP directory server by Content Server or the check password program.
 - e. **Binding Password:** Type the binding distinguished password used to authenticate requests to the LDAP directory server by Content Server or the check password program.
 - f. **Confirm Password:** Re-enter the binding password for verification.
4. Enter information in the **Secure Connection** section:
 - a. **Use SSL:** Select to connect to the directory using SSL.
If selected, the system:
 - Sets the SSL port to 636.
 - Sets the Certificate Location field to *ldapcertdb_loc* and enables the Select link.
 - Displays the Validate SSL Connection button.
 - b. **SSL Port:** If you selected Use SSL, the system automatically sets the port number to 636.
 - c. **Certificate Location:** If you selected Use SSL, the system sets this field to *ldapcertdb_loc* and enables the Select link.
 - d. **Select:** Click to access the Location Chooser page to select a different value for the certification location.
 - e. **Validate SSL Connection:** Click to validate that a secure connection can be established with the LDAP server on the specified port. If the validation fails, the system displays an error message and you cannot proceed further until valid information is provided.
5. Click **Next** or click the **Sync & Authentication** tab to continue.

Before continuing to the New LDAP Server Configuration - Sync & Authentication page, the system validates the information entered on the New LDAP Server Configuration - Info page:

- **Name** must be a valid entry.
 - **Hostname / IP Address** and **Port** must be a valid and connected directory.
 - **Binding Name** and **Binding Password** must be a valid authentication for the named directory.
 - **Binding Password** and **Confirm Password** values must match.
 - **SSL Port** and **Certificate Location** must be valid to establish a secure connection to the LDAP server.
6. Click **Cancel** to discard changes and return to the LDAP Server Configuration list page.

Viewing or modifying directory and secure connection properties for LDAP servers

Use these instructions to view or modify LDAP directory and secure connection properties for existing LDAP servers.

To view or modify directory and secure connection properties for LDAP servers:

1. Navigate to the LDAP Server Configuration Properties - Info page:
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select an LDAP server to view or modify and then select **View > Properties > Info**.
The system displays the LDAP Server Configuration Properties - Info page where you view or modify information such as directory type and IP address for the new LDAP directory.
2. View the name or modify the status of the LDAP configuration object:
 - a. **Name**: The name of the new LDAP configuration object. This field is read-only.
 - b. **Status**: Select the **Enable this LDAP Configuration** checkbox to enable the LDAP configuration.
3. View or modify information in the **LDAP Directory** section:
 - a. **Directory Type**: Refer to the Release Notes for your version of Documentum Content Server to see which LDAP server versions are supported. Options are:
 - Sun One/Netscape/iPlanet Directory Server (default)
 - Microsoft Active Directory
 - Microsoft ADAM
 - Oracle Internet Directory Server
 - IBM Directory Server
 - Novell eDirectory
 - b. **Hostname / IP Address**: View or modify the name of the host on which the LDAP directory server is running.

- c. **Port:** View or modify the port number where the LDAP directory server is listening for request. The default is 389.
 - d. **Binding Name:** View or modify the binding distinguished name used to authenticate requests to the LDAP directory server by Content Server or the check password program.
 - e. **Binding Password:** View or modify the binding distinguished password used to authenticate requests to the LDAP directory server by Content Server or the check password program.
 - f. **Set:** Click to access the LDAP Server Configuration Properties page to change the binding password.
4. View or modify information in the **Secure Connection** section:
 - a. **Use SSL:** Select to connect to the directory using SSL. If selected, the system:
 - Sets the SSL port to 636.
 - Sets the Certificate Location field to *ldapcertdb_loc* and enables the Select link.
 - Displays the Validate SSL Connection button.
 - b. **SSL Port:** If you selected Use SSL, the system automatically sets the port number to 636.
 - c. **Certificate Location:** If you selected Use SSL, the system sets this field to *ldapcertdb_loc* and enables the Select link.
 - d. **Select:** Click to access the Location Chooser page to select a different value for the certification location. **Password** and **Confirm Password** values must match.
 - e. **Validate SSL Connection:** Click to validate that a secure connection can be established with the LDAP server on the specified port. If the validation fails, the system displays an error message and you cannot proceed further until valid information is provided.
 5. To view or modify other properties for the LDAP server:
 - Click the **Sync & Authentication** tab to access the LDAP Server Configuration Properties - Sync & Authentication page to view or modify synchronization and user authentication information.
 - Click the **Mapping** tab to access the LDAP Server Configuration Properties - Mapping page to view or modify user and group mapping information.

From this page, you can access the Map Property page by clicking **Add** in the Property Mapping grid.
 - Click the **Failover** tab to access the LDAP Server Configuration Properties - Failover page to view or modify the Content Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down. (The Failover tab is available only for Documentum 6 and later repositories.)

From this page, you can access the Secondary LDAP Server page by clicking **Add** in the Secondary LDAP Servers grid.
- The system validates the information on the LDAP Server Configuration Properties - Info page before continuing:
- **Name** must be a valid entry.
 - **Hostname / IP Address** and **Port** must be a valid and connected directory.

- **Binding Name** and **Binding Password** must be a valid authentication for the named directory.
 - **SSL Port** and **Certificate Location** must be valid to establish a secure connection to the LDAP server.
6. Click **OK** when done viewing or modifying the LDAP server or click **Cancel** to return to the LDAP Server Configuration list page.

LDAP Server Configuration - Info page properties

This section defines the field properties on the New LDAP Server Configuration - Info and LDAP Server Configuration Properties - Info pages. The field properties on both pages are the same, regardless if you are in add, view, or modify mode; however, some fields may be read-only.

Figure 6. LDAP Server Configuration Properties - Info page

The screenshot shows the 'LDAP Server Configuration Properties' dialog box. The 'Info' tab is selected. The main area displays the following fields:

- Name:** test
- Status:** Enable this LDAP Configuration
- LDAP Directory** section:
 - Directory Type:** Sun One/Netscape/iPlanet Directory Server
 - Hostname / IP Address:** 11.22.333.44
 - Port:** 389
 - Binding Name:** cn=Directory Manager
 - Binding Password:** [Set](#)
- Secure Connection** section:
 - Use SSL:** Connect to directory using SSL
 - SSL Port:** 636
 - Certificate Location:** [Select](#) ldapcertdb_loc
 - Validate SSL Connection:** [Test](#)

A red message at the bottom states: Please check that the certificate database is present on the content server at the specified location. For more details refer Content Server Administration guide.

At the bottom right are 'OK' and 'Cancel' buttons.

Table 13. New LDAP Server Configuration - Info and LDAP Server Configuration Properties - Info page properties

Field	Description
Name	The name of the new LDAP configuration object. This field is read-only if you are viewing or modifying the LDAP configuration object.

Field	Description
Status	Select the Enable this LDAP Configuration checkbox to enable the LDAP configuration.
Directory Type	Refer to the Release Notes for your version of Documentum Content Server to see which LDAP server versions are supported. Options are: <ul style="list-style-type: none">• Sun One/Netscape/iPlanet Directory Server (default)• Microsoft Active Directory• Microsoft ADAM• Oracle Internet Directory Server• IBM Directory Server• Novell eDirectory
Hostname / IP Address	The name of the host on which the LDAP directory server is running.
Port	The port number where the LDAP directory server is listening for requests. The default is 389.
Binding Name	The binding distinguished name used to authenticate requests to the LDAP directory server by Content Server or the check password program.
Binding Password	The binding distinguished password used to authenticate requests to the LDAP directory server by Content Server or the check password program. The Binding Password field only appears on the New LDAP Server Configuration - Info page.
Confirm Password	If adding a new LDAP server configuration, re-enter the binding password for verification. The Confirm Password field only appears on the New LDAP Server Configuration - Info page.
Set	Click to access the LDAP Server Configuration Properties page to set the password. This link appears only on the LDAP Server Configuration Properties - Info page.

Field	Description
Use SSL	<p>Select to connect to the directory using SSL.</p> <p>If selected, enter 636 for the SSL port. If selected the system:</p> <ul style="list-style-type: none"> • Sets the SSL port to 636 • Sets the Certificate Location field to <i>ldapcertdb_loc</i> • Enables the Select link • Displays the Validate SSL Connection button
Certificate Location	<p>If you selected Use SSL, the system sets this field to <i>ldapcertdb_loc</i> and enables the Select link.</p> <p>Click the Select link to access the Location Chooser page to select a different value for the certification location.</p>
Validate SSL Connection	<p>If you selected Use SSL, click to validate that a secure connection can be established with the LDAP server on the specified port. If the validation fails, the system displays an error message and you cannot proceed further until valid information is provided.</p>
Next	<p>Click to continue to the New LDAP Server Configuration - Sync & Authentication page.</p>
Cancel	<p>Click to discard changes and return to the LDAP Server Configuration list page.</p>
OK	<p>Click to save changes on all pages and return to the LDAP Server Configuration list page.</p>

Configuring synchronization and user authentication for LDAP servers

This section discusses configuring synchronization and user authentication properties on the New LDAP Server Configuration - Sync & Authentication and LDAP Server Configuration Properties - Sync & Authentication pages, which contain the same field properties.

Click the links for information or instructions on:

- [Configuring synchronization and user authentication for new LDAP servers, page 122](#)
- [Viewing or modifying synchronization and user authentication properties for LDAP servers, page 123](#)
- [LDAP Server Configuration - Sync & Authentication page properties, page 124](#)

Configuring synchronization and user authentication for new LDAP servers

Use these instructions to configure synchronization and user authentication properties for new LDAP servers.

To configure synchronization and user authentication properties for a new LDAP server:

1. Navigate to the New LDAP Server Configuration - Sync & Authentication page:
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select **File > New > LDAP Server Configuration**.
The system displays the New LDAP Server Configuration - Info page where you enter information such as directory type and IP address for the new LDAP directory.
 - c. Click the **Sync & Authentication** tab.
The system displays the New LDAP Server Configuration - Sync & Authentication page where you enter synchronization and user authentication properties.
2. Enter information in the **Synchronization** section.
 - a. **Import:** Options are:
 - *Users and groups* (default)
 - *Users only*
If selected:
 - The **Update group names in repository** checkbox is disabled.
 - b. **Sync Type:** Options are:
 - *Full: Import all based on user/group mappings* (default)
 - *Incremental: import only new/updated user/groups*
 - c. **Deleted Users:** Options are:
 - *set to inactive* (default)
 - *unchanged*
 - d. **Update Names:** Select to **Update user names in repository** or **Update group names in repository**.
The Update group names in repository checkbox is not enabled if Users Only is selected in the Import field.
 - e. **User Type:** Select a user type. The default is *dm_user*.
3. Enter information in the **User Authentication** section.
 - a. **Bind to User DN:** Options are:
 - *Search for DN in directory using user's login name*
 - *Use DN stored with user record in repository* (default)

- b. **External Password Check:** Select to use external password check to authenticate users to the directory.
4. Click **Next** or click the **Mapping** tab to continue to the New LDAP Server Configuration - Mapping page.
5. Click **Cancel** to return to the LDAP Server Configuration list page.

Viewing or modifying synchronization and user authentication properties for LDAP servers

Use these instructions to view or modify synchronization and user authentication properties for existing LDAP servers.

To view or modify synchronization and user authentication properties for LDAP servers:

1. Navigate to the LDAP Server Configuration Properties - Sync & Authentication page:
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select the LDAP server to view or modify and then select **View > Properties > Info**.
The system displays the LDAP Server Configuration Properties - Info page.
 - c. Click the **Sync & Authentication** tab.
The system displays the New LDAP Server Configuration - Sync & Authentication page where you enter synchronization and user authentication properties.
2. View or modify information in the **Synchronization** section.
 - a. **Import:** Options are:
 - *Users and groups* (default)
 - *Users only*
If selected:
 - The **Update group names in repository** checkbox is disabled.
 - *Groups and member users*
 - b. **Sync Type:** Options are:
 - *Full: Import all based on user/group mappings* (default)
 - *Incremental: import only new/updated user/groups*
 - c. **Deleted Users:** Options are:
 - *set to inactive* (default)
 - *unchanged*
 - d. **Update Names:** Select to **Update user names in repository** or **Update group names in repository**.

The Update group names in repository checkbox is not enabled if Users Only is selected in the Import field.

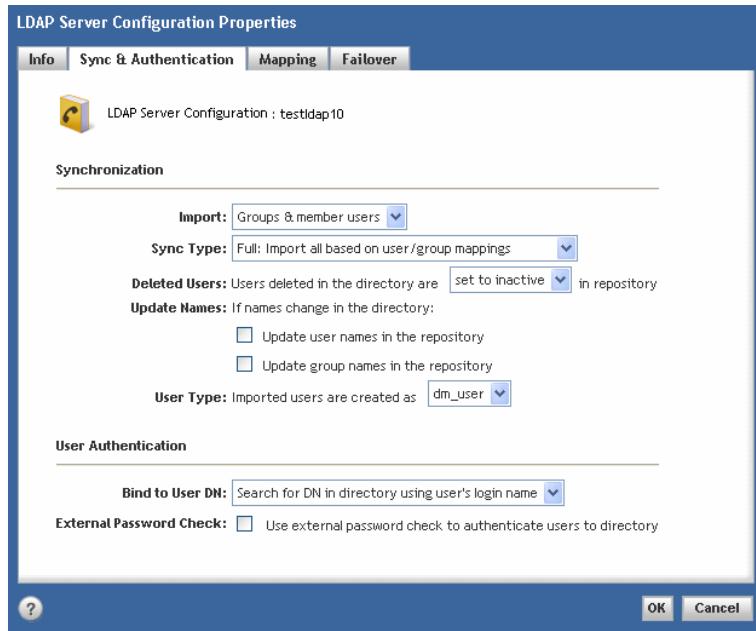
- e. **User Type:** Select a user type. The default is *dm_user*.
3. View or modify information in the **User Authentication** section.
 - a. **Bind to User DN:** Options are:
 - *Search for DN in directory using user's login name*
 - *Use DN stored with user record in repository (default)*
 - b. **External Password Check:** Select to use external password check to authenticate users to the directory.
4. To view other properties for the LDAP server:
 - Click the **Info** tab to access the LDAP Server Configuration Properties - Info page to view or modify information such as directory type and IP address for existing LDAP directories.
 - Click the **Mapping** tab to access the LDAP Server Configuration Properties - Mapping page to view or modify user and group mapping information.

From this page, you can access the Map Property page by clicking **Add** in the Property Mapping grid.
 - Click the **Failover** tab to access the LDAP Server Configuration Properties - Failover page to view or modify the Content Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down.

From this page, you can access the Secondary LDAP Server page by clicking **Add** in the Secondary LDAP Servers grid.
5. Click **OK** when you have completed viewing or modifying the LDAP server configuration properties or click **Cancel** to return to the LDAP Server Configuration list page.

LDAP Server Configuration - Sync & Authentication page properties

This section defines the field properties on the New LDAP Server Configuration - Sync & Authentication and LDAP Server Configuration Properties - Sync & Authentication pages. The field properties on both pages are the same, regardless if you are in add, view, or modify mode.

Figure 7. LDAP Server Configuration Properties - Sync & Authentication page**Table 14. New LDAP Server Configuration - Sync & Authentication and LDAP Server Configuration Properties - Sync & Authentication page properties**

Field	Description
Import	<p>Options are:</p> <ul style="list-style-type: none"> • Users and groups (default) • Users only. If selected: <ul style="list-style-type: none"> — The Update group names in repository checkbox is disabled on the New LDAP Server Configuration - Sync & Authentication and LDAP Server Configuration Properties - Sync & Authentication pages. • Groups and member users.
Sync Type	<p>Options are:</p> <ul style="list-style-type: none"> • Full: Import all based on user/group mappings (default) • Incremental: Import only new/updated user/groups

Field	Description
Deleted Users	Options are: <ul style="list-style-type: none">• set to inactive (default)• unchanged
Update Names	Select to Update user names in repository or Update group names in repository . The Update group names in repository checkbox is not enabled if Users Only is selected in the Import field.
User Type	Select a user type. The default is <i>dm_user</i> .
Bind to User DN	Options are: <ul style="list-style-type: none">• <i>Search for DN in directory using user's login name</i>• <i>Use DN stored with user record in repository</i> (default)
External Password Check	Select to use external password check to authenticate users to directory.

Mapping LDAP Servers

This section discusses mapping LDAP server properties on the New LDAP Server Configuration - Mapping and LDAP Server Configuration Properties - Mapping pages, which contain the same field properties.

LDAP directory servers allow you to define attribute values for user and group entries in the directory server. Content Server supports mapping those directory server values to user and group properties in the repository. Using mapping automates setting user and group properties.

Mappings between LDAP attributes and repository properties are defined when you create the ldap config object in Documentum Administrator. You can map the LDAP values to system or user-defined properties. You can map a single directory value to a repository property or you can map multiple directory values to a single repository property.

For example, you can map the LDAP attribute homepage to a custom property called *web_page*. A common use of the ability is to map the LDAP attributes *givenname* and *sn* (surname) to the *dm_user.user_name* property.

To map multiple LDAP properties to a single repository property, you use an expression. For example, the following expression uses the LDAP attributes *sn* and *givenname* to generate a *user_address* value:

```
 ${sn}_${givenname#1}@company.com
```

If the user's sn (surname) is Smith and the givenname is Patty, the expression above resolves to smith_p@company.com. The 1 at the end of givenname directs the system to only use the first letter of the given name.

Note: You can specify an integer at the end of an LDAP attribute name in an expression to denote that you want to include only a substring of that specified length in the resolved value. The integer must be preceded by a pound (#) sign. The substring is extracted from the value from the left to the right. For example, if the expression includes \${sn#5} and the surname is Anderson, the extracted substring is Ander.

Values of repository properties that are set through mappings to LDAP attributes may only be changed either through the LDAP entry or by a user with Superuser privileges.

Note: Changing mappings for the user_name, user_login_name, or group_name after the user or group is synchronized for the first time is not recommended. Doing so may cause inconsistencies in the repository.

Click the links for information and instructions on:

- [Adding new LDAP server mapping properties, page 127](#)
- [Viewing or modifying mapping properties of existing LDAP servers, page 129](#)
- [Using Search Builder, page 131](#)
- [Adding or modifying repository property mapping, page 131](#)
- [LDAP configuration attribute mapping examples, page 131](#)
- [LDAP Server Configuration - Mapping page properties, page 132](#)

Adding new LDAP server mapping properties

Use these instructions to add mapping properties for new LDAP servers.

To add mapping properties when creating a new LDAP server:

1. Navigate to the New LDAP Server Configuration - Mapping page:
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select **File > New > LDAP Server Configuration**.
Enter information on the New LDAP Server Configuration - Info page.
 - c. Click the **Sync & Authentication** tab.
Enter information on the New LDAP Server Configuration - Sync & Authentication page.
 - d. Click the **Mapping** tab.
The system displays the New LDAP Server Configuration - Mapping page where you can enter user and group mapping information.
2. Enter information in the **User Mapping** section:
 - a. **User Object Class:** Type the user object class to use for searching the users in the directory server.

- b. **User Search Base:** Type the user search base. This is the point in the LDAP tree where searches for users start. For example:
cn=Users,ou=Server,dc=sds,dc=inengvml1lc,dc=corp,dc=emc,dc=com
 - c. **User Search Filter:** Type the person search filter. This is the name of the filter used to make an LDAP user search more specific. The typical filter is cn=*.
 - d. **Search Builder:** Click to access the Search Builder page. This page enables you to build and test a user search filter. When finished, the User Search Filter field is populated with the resulting filter.
3. Enter information in the **Group Mapping** section:
 - a. **Group Object Class:** Type the group object class to use for searching the groups in the directory server.. Typical values are:
 - For Netscape and Oracle LDAP servers: groupOfUniqueNames
 - For Microsoft Active Directory: group
 - b. **Group Search Base:** Type the group search base. This is the point in the LDAP tree where searches for groups start. For example:
cn=Groups,ou=Server,dc=sds,dc=inengvml1lc,dc=corp,dc=emc,dc=com
 - c. **Group Search Filter:** Type the group search filter. This is the name of the filter used to make an LDAP group search more specific. The typical filter is cn=*.
 - d. **Search Builder:** Click to access the Search Builder page. This page enables you to build and test a group search filter. When finished, the Group Search Filter field is populated with the resulting filter.
 4. Add, edit, or delete information in the **Property Mapping** section.

When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.

 - a. **Add:** Click to access the Map Property page to add an attribute.
 - i. Select a repository property to map.
 - ii. In the **Map To** section, select the LDAP property to which the repository property maps or type a custom value. Options are:
 - **Single LDAP Attributes:** If selected, select an LDAP attribute from the drop-down list.
 - **Fixed Value:** If selected, type a custom value.
 - **Expression:** If selected, type an expression and select an LDAP attribute reference from the drop-down list. This is only available for Documentum 6 repositories.

Click the **Test Expression** button to test.
 - iii. In the **Reject User/Group** section, select to reject synchronization of any LDAP user or group. This is only available for Documentum 6 repositories.

- Options for when to reject synchronization are:
- Is empty or has insufficient characters
 - Is empty
 - Never reject any user/group
- iv. Click **OK** to return to the New LDAP Server Configuration - Mapping page.
- b. **Edit:** Select an attribute and then click Edit to access the Map Property page.
- i. Edit the attribute properties.
 - ii. Click **OK** to return to the New LDAP Server Configuration - Mapping page.
- c. **Delete:** Select an attribute and then click Delete to remove an attribute. The system displays the Delete Confirmation page.
5. Click **Next** or click the **Failover** tab to continue to the New LDAP Server Configuration - Failover page.
6. Click **Finish** when you have completed entering user and group mapping information for the new LDAP server or click **Cancel** to return to the LDAP Server Configuration list page.

Viewing or modifying mapping properties of existing LDAP servers

Use these instructions to view or modify mapping properties for existing LDAP servers.

To view or modify mapping properties of existing LDAP servers:

1. Navigate to the LDAP Server Configuration Properties - Mapping page.
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select the LDAP server to view or modify and then select **View > Properties > Info**.
The system displays the LDAP Server Configuration Properties - Info page.
 - c. Click the **Mapping** tab.
The system displays the LDAP Server Configuration Properties - Mapping page
2. Enter information in the **User Mapping** section:
 - a. **User Object Class:** Type the user object class to use for searching the users in the directory server.
 - b. **User Search Base:** Type the user search base. This is the point in the LDAP tree where searches for users start. For example:
`cn=Users,ou=Server,dc=sds,dc=inenegvm1llc,dc=corp,dc=emc,dc=com`
 - c. **User Search Filter:** Type the person search filter. This is the name of the filter used to make an LDAP user search more specific. The typical filter is `cn=*`.
 - d. **Search Builder:** Click to access the Search Builder page. This page enables you to build and test a user search filter. When finished, the User Search Filter field is populated with the resulting filter.

3. Enter information in the **Group Mapping** section.
 - a. **Group Object Class:** Type the group object class to use for searching the groups in the directory server. Typical values are:
 - For Netscape and Oracle LDAP servers: groupOfUniqueNames
 - For Microsoft Active Directory: group
 - b. **Group Search Base:** Type the group search base. This is the point in the LDAP tree where searches for groups start. For example:
cn=Groups,ou=Server,dc=sds,dc=inengvml1llc,dc=corp,dc=emc,dc=com
 - c. **Group Search Filter:** Type the group search filter. This is the name of the filter used to make an LDAP group search more specific. The typical filter is cn=*.
 - d. **Search Builder:** Click to access the Search Builder page. This page enables you to build and test a group search filter. When finished, the Group Search Filter field is populated with the resulting filter.
4. Add, edit, or delete information in the Property Mapping Section.

When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.

 - a. **Add:** Click to access the Map Property page to add an attribute.
 - i. Select a repository property to map.
 - ii. In the **Map To** section, select the LDAP property to which the repository property maps or type a custom value. Options are:
 - **Single LDAP Attributes:** If selected, select an LDAP attribute from the drop-down list.
 - **Fixed Value:** If selected, type a custom value.
 - **Expression:** If selected, type an expression and select an LDAP attribute reference from the drop-down list. This is only available for Documentum 6 repositories.

Click the **Test Expression** button to test.
 - iii. In the **Reject User/Group** section, select to reject synchronization of any LDAP user or group. This is only available for Documentum 6 repositories.

Options for when to reject synchronization are:

 - Is empty or has insufficient characters
 - Is empty
 - Never reject any user/group
 - iv. Click **OK** to return to the LDAP Server Configuration Properties - Mapping page.
 - b. **Edit:** Select an attribute and then click **Edit** to access the Map Property page.
 - i. Edit the attribute properties.
 - ii. Click **OK** to return to the LDAP Server Configuration Properties - Mapping page.
 - c. **Delete:** Select an attribute and then click Delete to remove an attribute. The system displays the Delete Confirmation page.

5. Click **OK** when you have completed viewing or modifying user and group mapping information for the LDAP server or click **Cancel** to return to the LDAP Server Configuration list page.

Using Search Builder

Access the Search Builder page by clicking the Search Builder button on the New LDAP Server Configuration - Mapping or LDAP Server Configuration Properties - Mapping page.

The Search Builder page enables you to build and test a user or group search filter. You can enter up to ten lines of search criteria. When finished, the User Search Filter or Group Search Filter field is populated with the resulting filter.

Adding or modifying repository property mapping

Access the Map Property page from the New LDAP Server Configuration - Mapping or LDAP Server Configuration Properties - Mapping page.

To add or modify repository property mapping:

1. Access the Map Property page.
2. Select a repository property to map.
3. In the **Map To** section, select the LDAP property to which the repository property maps or type a custom value. Options are:
 - **Single LDAP Attributes:** If selected, select an LDAP attribute from the drop-down list.
 - **Fixed Value:** If selected, type a custom value.
 - **Expression:** If selected, type an expression and select an LDAP attribute reference from the drop-down list. Click the **Test Expression** button to test.
4. In the **Reject User/Group** section, select to reject synchronization of any LDAP user or group. Options for when to reject synchronization are:
 - Is empty or has insufficient characters
 - Is empty
 - Never reject any user/group
5. Click **OK** to save the changes or click **Cancel**.

The system displays the New LDAP Server Configuration - Mapping or LDAP Server Configuration Properties - Mapping page.

LDAP configuration attribute mapping examples

The tables below contain examples of how the Attribute Map page for LDAP configurations is typically completed for Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory LDAP servers.

Table 15. Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example

DM attribute	DM type	LDAP attribute	Type
user_name	dm_user	cn	A
user_login_name	dm_user	uid	A

LDAP Server Configuration - Mapping page properties

This section defines the field properties on the New LDAP Server Configuration - Mapping and LDAP Server Configuration Properties - Mapping pages. The field properties on both pages are the same, regardless if you are in add, view, or modify mode.

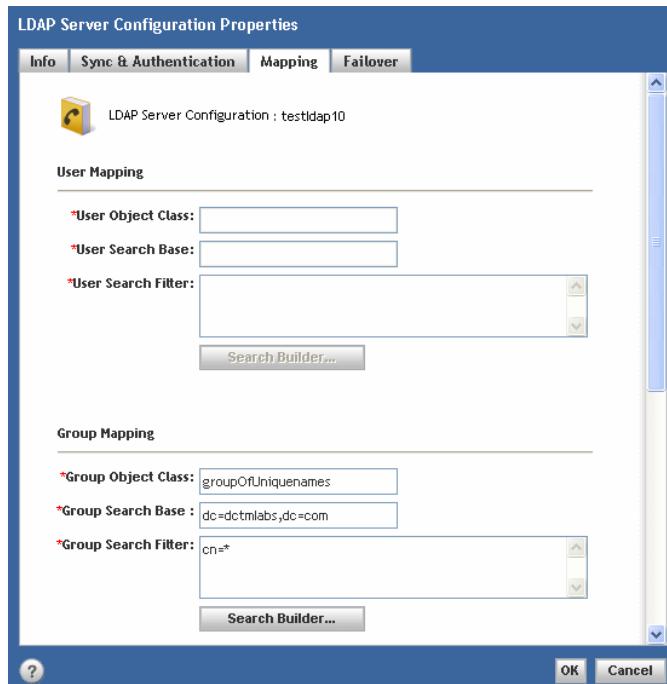
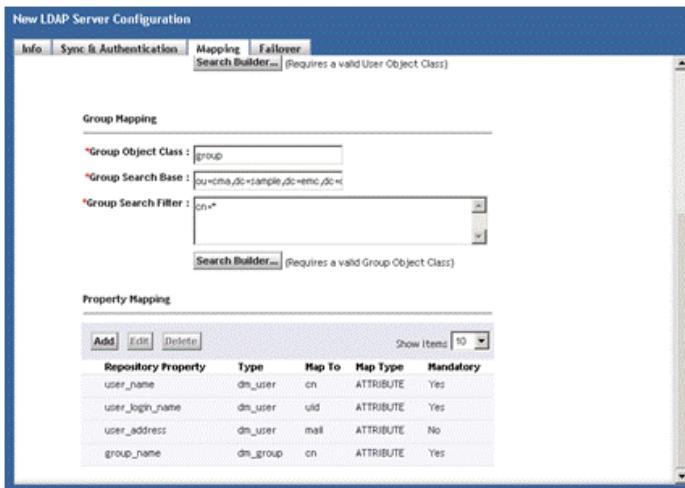
Figure 8. LDAP Server Configuration Properties - Mapping page (1 of 2)

Figure 9. LDAP Server Configuration Properties - Mapping page (2 of 2)**Table 16. New LDAP Server Configuration - Mapping and LDAP Server Configuration Properties - Mapping page properties**

Field	Description
User Object Class	Type the user object class to use for searching the users in the directory server.
User Search Base	Type the user search base. This is the point in the LDAP tree where searches for users start. For example: cn=Users,ou=Server,dc=sds,dc=inengvml1lc,dc=corp,dc=emc,dc=com.
User Search Filter	Type the person search filter. This is the name of the filter used to make an LDAP user search more specific. The typical filter is cn=*
Search Builder	Click to access the Search Builder page. This page enables you to build and test a user search filter. When finished, the User Search Filter field is populated with the resulting filter.
Group Object Class	Type the group object class to use for searching the groups in the directory server. Typical values are: <ul style="list-style-type: none"> • For Netscape and Oracle LDAP servers: groupOfUniqueNames • For Microsoft Active Directory: group

Field	Description
Group Search Base	Type the group search base. This is the point in the LDAP tree where searches for groups start. For example: cn=Groups,ou=Server,dc=sds,dc=ingeniumllc,dc=corp,dc=emc,dc=com
Group Search Filter	Type the group search filter. This is the name of the filter used to make an LDAP group search more specific. The typical filter is cn=*
Search Builder	Click to access the Search Builder page. This page enables you to build and test a group search filter. When finished, the Group Search Filter field is populated with the resulting filter.
Property Mapping	When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.
Add	Click to access the Map Property page to add an attribute. From there, select a Documentum attribute, then select the LDAP attribute to which the Documentum attribute maps or type in a custom value.
Edit	Select an attribute and then click Edit to access the Map Property page. On the Map Property page, edit the attribute properties.
Delete	Select an attribute and then click Delete to remove an attribute. The system displays the Deletion Confirmation page.
Repository Property	Displays the repository property that is the target of the mapping.
Type	Identifies the source of the property: User or Group.
Map To	Displays which attributes on LDAP that the property is mapped to.

Field	Description
Map Type	Identifies the type of data: LDAP attribute, expressions, or a fixed constant.
Mandatory	Indicates if the mapping is mandatory for the attribute.
	<p>Content Server requires three properties to be defined for a user and one property to be defined for a group. The mandatory properties are:</p> <ul style="list-style-type: none"> • <code>user_name</code> • <code>user_login_name</code> • <code>group_name</code> <p>When you define an LDAP configuration object in Documentum Administrator, default mapped values are provided for these properties. You can change the defaults, but you must provide some value or mapping for these properties. Users cannot be saved to the repository without values for these three properties, nor can a group be saved to the repository without a group name.</p>

Configuring failover settings and secondary LDAP servers

This section discusses configuring failover settings and secondary LDAP servers on the New LDAP Server Configuration - Failover and LDAP Server Configuration Properties - Failover pages, which contain the same field properties. Configuring failover settings and secondary LDAP server functionality is only available for Documentum 6 repositories.

Click the links for information and instructions on:

- [Understanding LDAP failover and secondary servers, page 136](#)
- [Configuring LDAP failover when creating a new LDAP server, page 137](#)
- [Viewing or modifying failover properties of existing LDAP servers, page 138](#)
- [Configuring secondary LDAP servers, page 138](#)
- [LDAP Server Configuration - Failover page properties, page 139](#)
- [Secondary LDAP Server page properties, page 140](#)

Understanding LDAP failover and secondary servers

You can configure Content Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down. By default, the primary LDAP server handles all user authentication requests. However, if Content Server fails to bind to the primary LDAP directory server, you can define a way for it to bind to secondary LDAP servers, authenticate users, and then reattempt the connection with the primary LDAP directory server.

This feature is controlled by five properties in the dm_ldap_configuration object that you configure for the primary LDAP server using Documentum Administrator:

- retry_count, which configures the number of times Content Server attempts to contact the LDAP directory server before reporting that the connection attempt has failed.
- retry_interval, which holds the value for time in seconds that elapses before Content Server attempts to contact the LDAP directory server again.
- failover_ldap_config_id, a repeating property that points to the ldap_configuration objects of the secondary LDAP directory servers.
- failover_use_interval, which holds the value for the interval in seconds during which Content Server uses the secondary LDAP directory server for user authentication before attempting to contact the primary LDAP directory server again.

Initially, if Content Server fails to bind to the primary LDAP directory server, it waits the number of seconds specified in the retry_interval property before attempting to bind to the primary LDAP directory server again. Content Server repeats this pattern of waiting and attempting the connection for the number of times specified in the retry_count property. If retry_count property is set to 0, Content Server immediately reports that it failed to contact the primary LDAP directory server.

If the binding attempts to the primary server fail the specified number of times, Content Server attempts to contact the secondary LDAP directory servers in the order they are configured in the repeating property failover_ldap_config_ids. After it binds to a secondary LDAP directory server, Content Server uses it to authenticate users for the duration of time that is configured in the failover_use_interval property. When the specified time period has elapsed, Content Server attempts to contact the primary LDAP directory server for user authentication.

If the secondary LDAP directory server is down or goes down within the specified use interval, Content Server contacts the remaining secondary LDAP directory servers in the order that they are configured. If all attempts to contact the secondary LDAP directory servers fail, Content Server contacts the primary LDAP server again.

If all LDAP servers are down, user authentication fails. Failover details, including information on the switches between LDAP servers, are captured in the authentication trace in the Content Server log.

Content Server only contacts the secondary LDAP directory servers that are configured for the primary LDAP directory server. Each secondary LDAP directory server can be associated with only one primary LDAP directory server.

Note: LDAP failover is supported for user authentication and on-demand user synchronization only. LDAP failover is not supported for user or group synchronization.

Configuring LDAP failover when creating a new LDAP server

This section provides instructions to configure failover settings for a new LDAP server:

To configure LDAP failover when creating a new LDAP server:

1. Navigate to the New LDAP Server Configuration - Failover page:
 - a. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
 - b. Select **File > New > LDAP Server Configuration**.
The system displays the New LDAP Server Configuration - Info page where you enter information such as directory type and IP address for the new LDAP directory.
 - c. Click the **Sync & Authentication** tab.
Enter information on the New LDAP Server Configuration - Sync & Authentication page where you enter synchronization and user authentication information.
 - d. Click the **Mapping** tab.
The system displays the New LDAP Server Configuration - Mapping page where you enter user and group mapping information.
 - e. Click the **Failover** tab.
The system displays the New LDAP Server Configuration - Failover page where you can configure the Content Server to user other LDAP directory servers for user authentication in the event that the first LDAP directory server is down.
2. Enter information in the **Failover Settings** section:
 - a. **Retry Count**: Enter a number of times to try to connect to the primary LDAP server before failover to a designated secondary LDAP server. The default is set to 3 attempts.
 - b. **Retry Interval**: Enter an interval number and select a duration (seconds, minutes, or hours) between retries. The default is set to 3 seconds.
 - c. **Reconnect**: Enter an interval number and select a duration (seconds, minutes, or hours) after a failover for the system to try to connect to the primary LDAP server. The default is set at 5 seconds.
3. Add, edit, or delete secondary LDAP servers in the **Secondary LDAP Servers** section. The system contacts the secondary LDAP servers in the order they are listed in this table.
 - a. **Add**: Click to access the Secondary LDAP Server page to add a secondary LDAP server.
 - b. **Edit**: Select a secondary LDAP server and then click Edit to access the Secondary LDAP Server page to edit it.
 - c. **Delete**: Select a secondary LDAP server and then click Delete to delete it.
 - d. **Move Up and Move Down**: Click to reorder the list of secondary LDAP servers.
4. Click **Finish** when you have completed configuring failover properties for the new LDAP server.

Viewing or modifying failover properties of existing LDAP servers

Use these instructions to view or modify failover properties for existing LDAP servers.

To view or modify failover properties of existing LDAP servers:

1. Navigate to **Administration > Basic Configuration > LDAP Servers**.
The system displays the LDAP Server Configuration list page.
2. Select the LDAP server to view or modify and then select **View > Properties > Info**.
The system displays the LDAP Server Configuration Properties - Info page.
3. Select **Properties > Failover** from the submenu.
The system displays the LDAP Server Configuration Properties - Failover page where you can configure the Content Server to user other LDAP directory servers for user authentication in the event that the first LDAP directory server is down.
For information on the field properties for the LDAP Server Configuration Properties - Failover page, refer to [LDAP Server Configuration - Failover page properties, page 139](#)
Note: The Properties option is not available if you select more than one server.
4. Click **Finish** when you have completed configuring the failover properties for the LDAP server.

Configuring secondary LDAP servers

Use the Secondary LDAP Server page to configure secondary LDAP servers.

To configure secondary LDAP servers:

1. Type the **Name** of the new secondary LDAP server.
2. Add information in the **LDAP Directory** section:
 - a. **Hostname / IP Address:** Type the name of the host on which the secondary LDAP directory server is running.
 - b. **Port:** The port information is copied from the primary LDAP server.
 - c. **Binding Name:** The binding name is copied from the primary LDAP server.
 - d. **Binding Password:** Type the binding distinguished password used to authenticate requests to the secondary LDAP directory server by Content Server or the check password program.
 - e. **Confirm Password:** Re-enter the binding password for verification.
 - f. **Bind to User DN:** The bind to user DN information is copied from the primary LDAP server.
3. Enter information in the **Secure Connection** section:
 - a. **Use SSL:** The SSL information is copied from the primary LDAP server.
 - b. **SSL Port:** The SSL port number is copied from the primary LDAP server.
 - c. **Certificate Location:** The certificate location is copied from the primary LDAP server.

- d. **Select:** Click to access the Location Chooser page to select a different value for the certification location.

LDAP Server Configuration - Failover page properties

This section defines the field properties on the New LDAP Server Configuration - Failover and LDAP Server Configuration Properties - Failover pages.

Figure 10. LDAP Configuration - Failover page

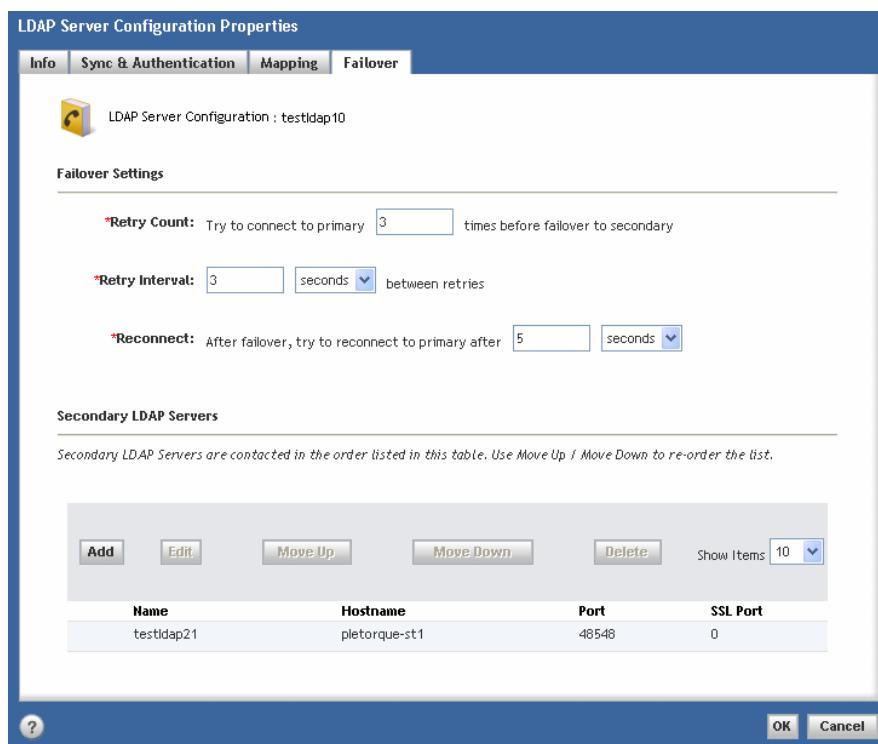


Table 17. New LDAP Server Configuration - Failover and LDAP Server Configuration Properties - Failover page properties

Field	Description
Failover Settings	Use this section to enter settings for the primary LDAP server.
Retry Count	Enter a number of times to try to connect to the primary LDAP server before failover to a designated secondary LDAP server. The default is set at 3.
Retry Interval	Enter an interval number and select a duration (seconds, minutes, or hours) between retries. The default is set at 3 seconds.

Field	Description
Reconnect	Enter an interval number and select a duration (seconds, minutes, or hours) after a failover for the system to try to reconnect to the primary LDAP server. The default is set at 5 minutes.
Secondary LDAP Servers	<ul style="list-style-type: none"> To add a new secondary LDAP server, click Add. The Secondary LDAP Server page is displayed. To modify an existing secondary LDAP server, select the checkbox next to the name and click Edit. The Secondary LDAP Server page is displayed. To delete an existing secondary LDAP server, select the checkbox next to the name and click Delete. To reorder the list of LDAP servers, click Move Up or Move Down.
Name	Name of the secondary LDAP server.
Hostname	The name of the host on which the secondary LDAP directory server is running.
Port	The port information.
SSL Port	The SSL port number.

Secondary LDAP Server page properties

This section defines the field properties on the Secondary LDAP server page.

Table 18. Secondary LDAP Server page properties

Field	Description
Name	Enter the name of the secondary LDAP server.
Hostname / IP Address	Type the name of the host on which the secondary LDAP directory server is running.
Port	The port information is copied from the primary LDAP server.
Binding Name	The binding name is copied from the primary LDAP server.

Field	Description
Binding Password	Type the binding distinguished password used to authenticate requests to the secondary LDAP directory server by Content Server or the check password program.
Confirm Password	Re-enter the binding password for verification.
Bind to User DN	The bind to user DN information is copied from the primary LDAP server.
Use SSL	The SSL information is copied from the primary LDAP server.
SSL Port	The SSL port number is copied from the primary LDAP server.
Certificate Location	The certificate location is copied from the primary LDAP server.

Changing the binding password

Change the binding password for LDAP directories on the LDAP Server Configuration Properties page. Access this page by clicking the Change link on the LDAP Server Configuration Properties - Info page.

To change the binding password

1. In the **Password** field, type the binding distinguished name used to authenticate requests to the LDAP directory server by Content Server or the check password program.
2. In the **Confirm Password** field, re-enter the binding password for verification.
3. Click **OK** to save the changes or click **Cancel**.

The system displays the LDAP Server Configuration Properties - Info page.

Forcing LDAP server synchronization

Use the instructions in this section to synchronize LDAP servers.

The Synchronize Now option calls the SBO API to synchronize the LDAP configuration. The type of synchronization is determined by the first_time_sync flag on the LDAP configuration object.

To synchronize LDAP servers:

1. Select **Administration > Basic Configuration > LDAP Servers** to access the LDAP Server Configuration list page.
2. Select the LDAP servers to synchronize and then select **File > Synchronize Now** to force synchronization of the selected servers.

Duplicating LDAP configurations

Use the instructions in this section to duplicate LDAP configurations.

Use the Save As option to create a copy of an LDAP configuration. The new LDAP configuration contains all the details of the original configuration object except for the secondary, or failover, servers. Secondary servers cannot be shared by the primary server.

To duplicate LDAP servers:

1. Select **Administration > Basic Configuration > LDAP Servers** to access the LDAP Server Configuration list page.
2. Select the LDAP server to duplicate and then select **File > Save As**.

The system opens a new LDAP server dialog with attributes copied from the selected LDAP Server configuration object.

Note: The Duplicate option is not available if you select more than one server.

Deleting LDAP configurations

Use the instructions in this section to delete an LDAP configuration. You must be a Superuser to delete an LDAP configuration.

Before deleting an LDAP configuration object, note the following potential consequences:

- If you delete an LDAP configuration object that is referenced by a Content Server's server configuration object, the Content Server cannot use that LDAP server to authenticate users and there will be no default LDAP object referenced in the server configuration object.
- If you delete an LDAP configuration object that is referenced by a Content Server's server configuration object and by user or group objects, the server cannot use the LDAP server to authenticate users, no default LDAP object will be referenced in the server configuration object, and user and group objects referencing the LDAP object cannot be updated correctly.

If you delete the LDAP configuration object, you must manually update user and group objects referencing the LDAP object so that the users and groups can be authenticated with a different authentication mechanism. To locate users referencing the LDAP configuration object, click **User Management > Users** and search by typing the LDAP Config object name in the **User Login Domain** field.

To delete an LDAP server configuration:

1. Select **Administration > Basic Configuration > LDAP Servers** to access the LDAP Server Configuration list page.
2. Select the LDAP servers to delete and then select **File > Delete**.
The system displays the Delete confirmation page.
3. Click **OK** to delete the LDAP server configuration or **Cancel** to return to the LDAP list page without deleting the configuration.

Using LDAP directory servers with multiple Content Servers

If multiple Content Servers are running against a particular repository, you must perform some additional steps to enable LDAP authentication regardless of the particular Content Server to which a user connects.

To enable LDAP authentication with multiple Content Servers:

1. Using Documentum Administrator, connect to one of the nonprimary Content Servers.
2. Navigate to the existing ldap configuration object.
3. Re-enter the Binding Name and Binding Password for the LDAP directory server.
4. Save the ldap configuration object.
5. Perform steps 1 to 4 for each nonprimary Content Server.

LDAP Certificate Database Management

The LDAP Certificate Database Management system enables administrators to:

- Import certificates into the LDAP certificate database on the Content Server.
- View certificate information in the LDAP certificate database.

The certificate database is automatically created on the Content Server at the LDAP certificate database location. The system creates a certificate database when an administrator attempts to view the LDAP Certificate Database List page for the first time and the certificate database is not present at the location specified in the ldapcertdb_loc location object.

Only an administrator who is the installation owner can access the LDAP Certificate Database Management node.

This section discusses:

- [Viewing LDAP certificates, page 143](#)
- [Importing LDAP certificates, page 144](#)

Viewing LDAP certificates

Use the instructions in this section to view LDAP certificate information.

To view LDAP certificates:

1. Navigate to **Administration > Basic Configuration > LDAP Certificate Database Management**.
The **LDAP Certificate Database List** page appears and displays a list of certificates that are available in the LDAP certificate database.
2. Select a certificate and then click **View > Properties**.

The **Certificate Info** page is displayed.

3. View the information on the **Certificate Info** page:
 - **Nickname:** The unique name for the certificate.
 - **Valid From:** The date from which the certificate is valid.
 - **Valid To:** Date up to which the certificate is valid.
 - **Signature Algorithm:** The certificate signature algorithm.
 - **Serial Number:** The serial number for the certificate.
 - **Version**
 - **Issuer DN:** The distinguished name of the issuer.
 - **Subject DN:** The distinguished name for the subject.
4. Click **OK** or **Cancel** to return to the LDAP Certificate Database List page.

Importing LDAP certificates

Use the instructions in this section to import new certificates.

To import LDAP certificates:

1. Navigate to **Administration > Basic Configuration > LDAP Certificate Database Management**.
The **LDAP Certificate Database List** page appears and displays a list of certificates that are available in the LDAP certificate database.
2. Select **File > Import > LDAP Certificate**.
The **Import Certificate** page appears.
3. Enter the path and filename of the certificate in the **Certificate File Name** field.
4. Click **OK**.
The system imports the certificate to the certificate database. The system displays an error message if it fails to import the certificate.

Chapter 5

Distributed Content Configuration

The distributed content configuration chapter provides information and instructions for the following configuration areas:

- Network locations, which represent places or portions of a network's topography and may be used to define one or more IP addresses or ranges that are in that location.

Network locations are a basic building block of a single-repository distributed environment for web-based clients. For more information about network locations, refer to the *Distributed Configuration Guide*.

- ACS (accelerated content services) servers, which are light-weight servers that handle read and write content operations for web-based client applications.

ACS servers are automatically created when the Content Server software is installed and the first Content Server is configured. For more information about ACS servers, refer to the *Distributed Configuration Guide* and the *Content Server Administration Guide*.

- BOCS (Branch Office Caching Services) servers, which are caching servers that cache content locally. Caching content allows users to obtain frequently accessed content very quickly.

BOCS servers are installed independently of the Content Server and ACS server. BOCS servers communicate only with ACS servers and DMS servers. They do not communicate directly with Content Servers. For more information, refer to the *Branch Office Caching Services Release Notes* and the *Distributed Configuration Guide*.

- Distributed Transfer Settings, which are parameters on a repository that control reading and writing content through the distributed infrastructure.
- Messaging Server, which is the Documentum Messaging Services (DMS) server, an intermediary process that provides messaging services between an ACS or BOCS server and a web application server. A DMS server's services are used for:
 - Content pre-caching operations
 - Asynchronous write operations

The messaging server configuration object (dm_dms_config) also contains the DMS server URL information for communications with BOCS servers in push and pull modes. For more information about the messaging server, refer to the *Distributed Configuration Guide*.

Click the links for information and instructions on:

- [Network locations, page 146](#)
- [ACS servers, page 154](#)

- BOCS servers, page 168
- Configuring distributed transfer settings, page 177
- Messaging server configuration, page 179

Network locations

Network locations identify locations on a network, and optionally a range of IP addresses, from which users connect to Documentum web clients.

Use the **Administration > Distributed Content Configuration > Network Locations** navigation to access the Network Locations list page. From the Network Locations list page, you can create, copy, view, modify, and delete network locations.

This section provides conceptual information about network locations and instructions for creating, copying, modifying, viewing, and deleting network locations. It contains the following topics:

- About network locations, page 146
- Creating network locations, page 147
- Copying network locations, page 149
- Modifying or viewing network locations, page 149
- Deleting network locations, page 150
- Deleting network location warning, page 151
- Properties of network locations, page 151

For additional information about network locations and their use in distributed content models, refer to the *Distributed Configuration Guide*.

Note: If the repository to which you are connected is not a global registry or is not the global registry known to DFC on the Documentum Administrator host, the following message appears when you navigate to the **Network Locations** list page:

Network locations can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have Superuser privileges to create network locations.

Click **Global Registry Login** and a login page is displayed for the repository known to DFC as a global registry.

About network locations

Network locations are a basic building block of a single-repository distributed environment for web-based clients. Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to Documentum web clients. For example, a Documentum installation might include network locations called San Francisco, New York, London, Athens, Tokyo,

and Sydney, corresponding to users in those cities. A network location may also identify specific offices, network subnets, or even routers.

Network locations are associated with server configuration objects and acs configuration objects. The server configuration objects and acs configuration objects contain information defining the proximity of a Content Server or ACS Server to the network location. Content Server uses the information in the server configuration objects and acs configuration objects and their associated network locations to determine the correct content storage area from which to serve content to a web client end user and to determine the correct server to serve the content.

Network locations can be created only in a repository designated as a global registry, and the name of each location must be unique among the set of network locations in the global registry. Create network locations only in the global registry repository defined when DFC is installed on the Documentum Administrator host. If multiple global registry repositories exist on your network, a particular Documentum Administrator instance recognizes only one as a global registry: the global registry designated during DFC installation on the Documentum Administrator host. You may be able to connect to a global registry repository without being able to create network locations in that global registry.

It is strongly recommended that your installation contain only one global registry.

You must have Superuser privileges in the global registry repository to create network locations.

Creating, copying, modifying, or viewing network locations

Click the links for help on the following topics:

- [Creating network locations, page 147](#)
- [Copying network locations, page 149](#)
- [Modifying or viewing network locations, page 149](#)
- [Properties of network locations, page 151](#)

Creating network locations

Network locations can be created only in repositories designated as global registries. Create them only in the global registry repository known to the DFC installation on the host of that particular Documentum Administrator instance. You must have Superuser privileges in the global registry repository to create network locations. The *Distributed Configuration Guide* and [About network locations, page 146](#) provide additional information on network locations.

Note: When **localhost** is in the URL used from a browser on the application server host to access an application server, it resolves to 127.0.0.1. Unless 127.0.0.1 is included in a network location, the correct network location is not selected automatically. You are most likely to encounter this situation if you are troubleshooting an application directly from the application server host. Therefore, when

you create network locations, include the IP address 127.0.0.1 in a network location if all three of these conditions are met:

- Running a browser on the application server host where a WDK application is located
- Using **localhost** in the URL when accessing the application
- Wanting the correct network location automatically selected

To create network locations:

1. Connect to the global registry repository known to DFC as a user with Superuser privileges.
2. Select **Administration > Distributed Content Configuration > Network Locations**.

The Network Locations list page appears. You will not see any network locations listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the Network Locations list page:

Network locations can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create network locations.

3. Select **File > New > Network Location**.

The **New Network Locations - Info** page appears.

4. Enter general information about the network location:

- **Unique ID:** Type a unique identifying label for use by the system and network administrators.
- **Description:** Optionally, type a description about the new network location.

5. Type information in the **User Selectable Network Location** section:

- **User Selectable:** Select to display the network location to users whose IP address is not mapped to a particular network location.

At login time, an end user whose IP address is not mapped to a network location sees a set of possible network locations. When selected, this network location is on the list from which the user selects. If there is only one network location with this checkbox selected, that network location is used automatically and the user does not see the list.

- **Display Name:** Type a user-friendly name to identify the network location.

This is the label the system displays to users who must select the correct network location when connecting to a Documentum web client. It is recommended that you use unique names.

6. Enter information in the **IP Address Ranges** section.

- a. Click **Add**.

- b. Type the IP address range in one of the following formats:

- IPV4 address range can be entered by separating the two IP addresses with a hyphen(-).

For example: x.x.x.x-x.x.x.x where x can be from 0 to 255

- IPV6 address range can be entered by separating the two IP addresses with a hyphen(-).

For example: x:x:x:x:x:x:x-x:x:x:x:x or x:x:x::y (ipv6-address/prefix-length) where the x's are the hexadecimal values of the eight 16-bit pieces of the address and y is a

- decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.
- c. Repeat steps *a* through *b* until you have entered all the IP address ranges that comprise this network location.
 7. Click **OK** to save the changes or **Cancel** to exit without saving.

Copying network locations

To save time retying information that already exists, you can copy a network location file using the **Save As** option. To copy a network location, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges.

To copy a network location:

1. Connect to the global registry repository known to DFC as a user with Superuser privileges.
2. Select **Administration > Distributed Content Configuration > Network Locations**.
The Network Locations list page appears. You will not see any network locations listed if you are not connected to the global registry.
Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the Network Locations list page:
Network locations can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create network locations.
3. Select a network location and then select **File > Save As**.
The Network Location Properties - Info page appears. The fields display the values copied from the selected network location; however, the **Name** and **Display Name** fields display *Copy [x] of [name]/[display name]* to keep the network location and display names unique.
4. Modify the properties on the Network Location Properties - Info page.
For information on network location properties, refer to [Properties of network locations, page 151](#).
5. Click **OK** to save the changes or **Cancel** to exit without saving.

Modifying or viewing network locations

Use the instructions in this section to modify or view network locations. To modify or view network locations, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges.

To modify or view a network location:

1. Connect to the global registry repository known to DFC as a user with Superuser privileges.

2. Select **Administration > Distributed Content Configuration > Network Locations**.

The Network Locations list page appears. You will not see any network locations listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the Network Locations list page:

Network locations can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create network locations.

3. Select a network location and then select **View > Properties > Info**.

The **Network Location Properties - Info** page appears.

4. Modify the properties on the Network Location Properties - Info page.

For information on network location properties, refer to [Properties of network locations, page 151](#).

5. Click **OK** to save the changes or **Cancel** to exit without saving.

Deleting network locations

Use the instructions in this section to delete network locations. You must have Superuser privileges to delete a network location. Users who connect from a location that was mapped to a deleted network location are not automatically mapped when they connect to a web client. If you selected any network locations to be displayed to users who are not automatically mapped, the users see that list when they log in.

When you delete network locations, references to the network locations in existing server configuration objects, acs configuration objects, bocs configuration objects, and BOCS caching jobs are not automatically removed. You must manually remove any references to the deleted network locations.

To delete network locations:

1. Connect to the global registry repository known to DFC as a user with Superuser privileges.

2. Select **Administration > Distributed Content Configuration > Network Locations**.

The Network Locations list page appears. You will not see any network locations listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the Network Locations list page:

Network locations can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create network locations.

3. On the Network Location list page, select the network location to delete.

4. Note the **Display Name** and **Unique ID** for the network location.

5. Select **File > Delete**.

The Network Location object Delete page appears.

6. Click **OK** to delete the selected network location or **Cancel** to retain the network location.
If deleting multiple network locations, select **Next** or **Finish**.
7. Delete references to the network location from existing server configuration objects, acs configuration objects, bocs configuration objects, and BOCS caching jobs in the current repository and any other repositories.

Deleting network location warning

You have asked to delete a network location object. Network locations are used to determine which server provides content files to end users. If the network location that you are deleting is associated with any BOCS or ACS servers, users at those locations may not receive content in the most efficient manner possible.

On the **Network Location object Delete** page, click **OK** to delete the selected objects or **Cancel** to retain the objects. If deleting more than one network location, select **Next** or **Finish**.

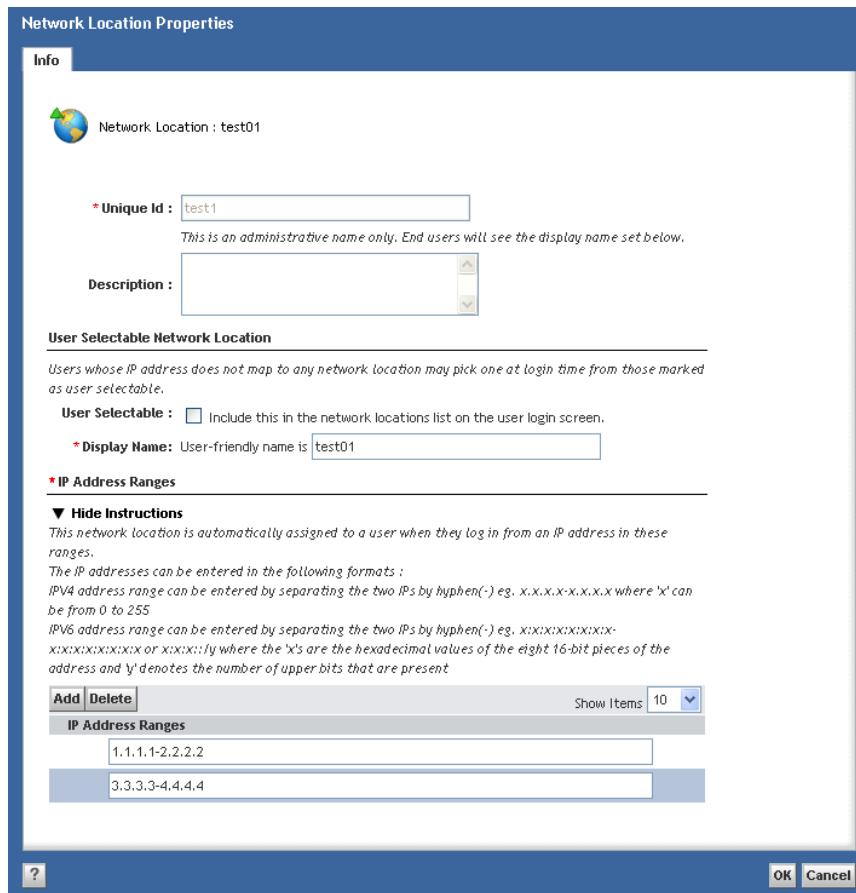
When you delete network locations, references to the network locations in existing server configuration objects, acs configuration objects, bocs configuration objects, and BOCS caching jobs are not automatically removed. You must manually remove any references to the deleted network locations.

Properties of network locations

This section:

- Shows the Network Location Properties - Info page
- Lists the properties on the New Network Location - Info and Network Location Properties - Info pages

To create, copy, view, or modify network locations, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges.

Figure 11. New Network Location - Info page**Table 19. Field properties on the network location page**

Field label	Value
Unique ID	A description intended for use by system and network administrators. For example, this may identify network locations by network subnets. This field cannot be edited after the network location is created.
Description	A description of the network location.
User Selectable	Select to display the network location to users whose IP address is not mapped to a particular network location.
	At log-in time, an end user whose IP address is not mapped to a network location sees a set of possible network locations. When selected, this network location is on the list from which the user selects. If there is only one network location with this checkbox selected, that network

Field label	Value
Display Name	location is used automatically and the user does not see the list.
IP Address Ranges	<p>A description of the network location that is easy for end-users to understand. (For example, Paris, San Francisco, Chicago, or Tokyo.) This is displayed on the login page for Documentum web clients, such as Webtop, when users must choose a network location. The display name is not the object name. The display name is editable after the network location is created.</p>
IP Address Ranges	<p>The IP address range identified by the network location. Each range must conform to standard IP address conventions. A network location may have multiple IP address ranges. It is recommended that each IP address is mapped to a single network location, but if an IP address maps to multiple physical locations, you may need to map that address to multiple network locations.</p>
IP Address Ranges	<p>Type the IP address in one of the following formats:</p>
	<ul style="list-style-type: none"> • IPv4 address range can be entered by separating the two IP address with a hyphen(-). For example: x.x.x.x-x.x.x.x where x is from 0 to 255.
	<ul style="list-style-type: none"> • IPv6 address range can be entered by separating the two IP addresses with a hyphen(-). For example:
	<p>x:x:x:x:x:x-x:x:x:x:x:x::y (ipv6-address/prefix-length) where the x's are the hexadecimal values of the eight 16-bit pieces of the address and y is a decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.</p>
OK	Click to save changes and return to the Network Locations list page.
Cancel	Click to exit without saving any changes and return to the Network Locations list page.

ACS servers

This section provides conceptual information and instructions about Accelerated Content Services (ACS) servers. An ACS server is a light-weight server that handles read and write content operations for web-based client applications. ACS servers do not interact with metadata but they can interact with Content Servers to write content to storage areas.

Use the **Administration > Distributed Content Configuration > ACS Servers** navigation to access the ACS Servers Configurations list page.

This section discusses the following topics:

- [About ACS servers, page 154](#)
- [Viewing or modifying the ACS server configuration properties, page 155](#)
- [Viewing or modifying ACS projections and stores, page 156](#)
- [Modifying ACS server communication protocols, page 159](#)
- [Designating connection brokers for an ACS server, page 160](#)
- [Deleting projections or stores from an ACS server, page 160](#)
- [Choosing network locations, page 162](#)
- [Properties of ACS servers, page 162](#)

About ACS servers

Accelerated Content Services (ACS) servers use the HTTP and HTTPS protocols to quickly handle read and write content operations for web-based client applications. Each Content Server host installation has one ACS server. That ACS server communicates with one Content Server per repository installed on the host installation. It also communicates with the Documentum Message Services (DMS) server. A single ACS server can serve content from multiple repositories. ACS servers do not write metadata.

An ACS server is created when the first Content Server or remote Content Server is configured in a Content Server software installation. An ACS server is represented in each repository by an acs configuration object, which is created during repository configuration. No additional ACS servers are created in a particular server installation.

ACS must be enabled in the app.xml file of all WDK-based applications in order for the ACS server to be used by that application.

Some ACS server properties can be modified using Documentum Administrator. Some ACS server behavior is controlled by settings in the acs.properties file, which is located on the ACS server host and cannot be modified by Documentum Administrator.

An ACS server may be in server configuration mode or in acs configuration mode:

- In server configuration mode, an ACS server uses the connection broker projections and network locations already configured in the associated server configuration object. Local stores are stores defined as far from the Content Server.

In this mode, the connection broker projections, network locations, and local stores are displayed in read-only form on the ACS Server Configuration Properties - Projections & Stores page.

- In **acs** configuration mode, an ACS server uses the connection broker projections, network locations, and local stores configured in the **acs** configuration object.

In this mode, you must manually enter the connection broker projections, network locations, and local stores on the ACS Server Configuration Properties - Projections & Stores page.

The *Distributed Configuration Guide* provides information on modifying the **acs.properties** file and additional information about the ACS server.

Viewing or modifying the ACS server configuration properties

Use these instructions to view or modify information on the ACS Server Configuration Properties - Info page. The section [About ACS servers, page 154](#) and the *Distributed Configuration Guide* provide additional information about ACS servers.

To view or modify ACS servers configuration properties:

1. Connect as a Superuser to the repository in which you want to view or modify the ACS server.
2. Select **Administration > Configuration > ACS Servers**.
The **ACS Servers Configurations** list page appears.
3. Select the ACS server to view or modify and then select **View > Properties > Info**.
The **ACS Server Configuration Properties - Info** page appears.
4. View or modify properties in the **ACS Server Configuration** section:
 - **Name:** Read only. The value assigned when the ACS server is installed and the **acs** configuration object is created.
 - **Associated Content Server:** Read only. Displays the name of the Content Server the ACS server is associated with.
 - **Description:** Add or modify a description of the ACS server.
 - **ACS Server Version:** Read only. Displays the major and minor version of the ACS server that the distributed content infrastructure uses to determine what its capabilities are. For example, 2.1 designates that the ACS server is bundled with a Documentum 6.5 repository, while 1.0 designates that the ACS server is bundled with a 5.3 SPx repository.
 - **Content Access:** Select an access type.
 - If using a Documentum 6 or later repository, the options are **Read and Write**, **Read from local stores only**, **Read from all stores**, and **None (disabled)**.
 - If using a 5.3 SPx repository, the options are **Read from local stores only**, **Read from all stores**, and **None (disabled)**.

Refer to [Properties of ACS servers, page 162](#) for additional information about the Content Access options.

5. The **ACS Server Connections** section displays the protocol used by the ACS server (HTTP and HTTPS protocols are supported) and the base URL for the ACS server. The base URL is in the format:
protocol://host:port/ACS/servlet/ACS
 - To add a new protocol for an ACS server connection, click **Add** to access the ACS Server Connection page.
 - To change the protocol or modify the base URL for the ACS server, select the ACS server connection and then click **Edit** to access the ACS Server Connection page.
 - To delete an existing protocol and base URL for the ACS server, select the ACS server connection and then click **Delete**.
6. Exit from the ACS Server Configuration Properties - Info page.
 - Click the **Projections & Stores** tab to view or modify the connection broker projections, network locations, and local stores information for the ACS server.
 - Click **OK** to save the ACS server configuration and return to the ACS Servers Configurations list page.
 - Click **Cancel** to exit without saving any changes and return to the ACS Servers Configurations list page.

Viewing or modifying ACS projections and stores

This section discusses the ACS Server Configuration Properties - Projections & Stores page and provides instructions for viewing or modifying ACS connection broker projections, network location projections, and local stores. This page also designates where the projection and store information comes from:

- If **Associated content server** is selected as the source, then the values in the associated Content Server's configuration object are displayed for the ACS server in read-only mode. This is referred to as server configuration mode.
- If **Settings entered here** is selected as the source, then you can manually add, modify, and delete projections and stores. This is referred to as acs configuration mode.

The ACS Server Configuration Properties - Projections & Stores page consists of three sections:

- **Connection Broker Projections**

The Documentum connection broker is a process that provides client sessions with server connection information. Each ACS server broadcasts information to connection brokers at regular intervals. The broadcast contains the information maintained by connection brokers about the ACS server and the repositories accessed by the ACS server.

The Connection Broker Projections section on the ACS Server Configuration Properties - Projections & Stores page lists the host where there are connection brokers to which the current ACS server projects, the port number used by each connection broker, and if the connection broker is enabled to receive projections from Content Servers and ACS servers.

If in server configuration mode, then the values in the associated Content Server's configuration object are displayed for the ACS server in read-only mode. To change the values, you must modify the server configuration object itself.

If in acs configuration mode, you can manually enter the connection brokers to which you want the ACS server to project.

Note that in acs configuration mode, connection brokers are used only to provide client connection information. The ACS server uses network location proximity values to determine the end users to which it serves content.

- **Network Location Projections**

Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to Documentum web clients. For example, a Documentum installation might include network locations called San Francisco, New York, London, Athens, Tokyo, and Sydney that correspond to users in those cities. A network location may also identify specific offices, network subnets, or even routers.

The Network Location Projections section on the ACS Server Configuration Properties - Projections & Stores page defines the network locations with which an ACS server is associated and to which it serves content, the proximity value for each network location, and whether an ACS server can project to that network location. For more information about network locations, refer to [About network locations, page 146](#).

On the ACS Server Configuration Properties - Projections & Stores page you can add, modify, or delete network location projections if the ACS server is in acs configuration mode. When an ACS server is in server configuration mode, the ACS server uses the projection values defined in the server's configuration object to project to the network locations. You cannot add, modify, or delete network location projects from the ACS Server Configuration Properties - Projections & Stores page.

- **Local Stores**

The information displayed in the Local Stores section on the ACS Server Configuration Properties - Projections & Stores page is determined by the selected configuration mode:

- If the ACS server is in acs configuration mode, use this section to configure near stores the ACS server can access.

You can select from all storage areas for the repository, excluding distributed stores.

- If the ACS server is in server configuration mode, the stores displayed in this section are the near stores that are near to the associated Content Server. The stores displayed in this section are calculated by the server to be near stores.

For more information about acs configuration mode and server configuration mode, refer to [About ACS servers, page 154](#).

To view or modify ACS projections and stores:

1. Access the ACS Server Configuration Properties - Projections & Stores page:
 - a. Connect as a Superuser to the repository in which you want to view or modify the ACS projections and stores.
 - b. Select **Administration > Configuration > ACS Servers**.
- The **ACS Servers Configurations Properties** list page appears.

- c. Select the ACS server to view or modify and then select **View > Properties > Info**.
The **ACS Server Configuration Properties - Info** page appears.
 - d. Click the **Projections & Stores** tab.
The system displays the **ACS Server Configuration Properties - Projections & Stores** page where you can view or modify the connection broker projections, network locations, and local stores information for the ACS server.
2. Select the **Source** from where you want to use projections and stores for the ACS server. Options are:
 - **Associated content server:** Select for the ACS server to use the connection broker projections, network locations, and local stores already configured for the associated Content Server. If selected, the fields are read-only on the ACS Server Configuration Properties - Projections & Stores page.
 - **Settings entered here:** Select for the ACS server to use connection brokers, network locations, and near stores that you manually enter on the ACS Server Configuration Properties - Projections & Stores page.
 3. Add or modify the information in the **Connection Broker Projections** section:
 - a. Click **Add** or select a connection broker and then click **Edit**.
The system displays the **Connection Broker Projection for ACS Server** page.
 - b. Type or modify the name of the host on which the connection broker resides.
 - c. Type or modify the port number on which the connection broker is listening.
 - d. Select **Enabled** to enable projections to the connection broker.
 - e. Click **OK** to save the new or modified projection target or **Cancel** to exit from this page without saving changes.
The system displays the ACS Server Configuration Properties - Projections & Stores page.
 - f. To remove a connection broker, select the connection broker and click **Remove**.
 4. Add or remove network locations from the **Network Location Projections** section.
 - a. To add network locations, click **Add** to access the **Choose Network Locations** page.
 - b. Select the network locations to add.
The network locations you see are in the global registry known to DFC on the Documentum Administrator host.
 - c. Click the **>** button.
The network locations move to the right-hand column.
 - d. To remove a network location, select it and click the **<** button.
The network location moves to the left-hand column.
 - e. Click **OK** to save the change or **Cancel** to exit without saving.
The ACS Server Configuration Properties - Projections & Stores page appears.
 - f. Type in the correct proximity values.
 - g. To enable projection to the network location, select **Enabled**.
 - h. To remove a network location, select the network location and click **Remove**.

5. Add or remove stores from the **Local Stores** section:
 - a. To add local stores, click **Add** to access the **Choose a storage** page.
 - b. Select the local stores to add.
These stores are defined as near to the ACS server.
 - c. Click the **>** button.
The local stores move to the right-hand column.
 - d. To remove a local store, select it and then click the **<** button.
The local store moves to the left-hand column.
 - e. Click **OK** to save the changes or **Cancel** to exit without saving.
The system displays the ACS Server Configuration Properties - Projections & Stores page.
 - f. To delete a local store, select it and then click **Remove**.
6. Exit from the ACS Server Configuration Properties - Projections & Stores page.
 - Click the **Info** tab to view or modify ACS server configuration and connections information for the ACS server.
 - Click **OK** to save projections and stores changes for the ACS server and return to the ACS Servers Configurations list page.
 - Click **Cancel** to exit without saving any changes and return to the ACS Servers Configurations list page.
7. Restart the ACS server.
To enable the changes that you made, restart the ACS server. The ACS server runs in the same servlet container as the Documentum Java method server. You must manually restart the Java method server on the host where it is installed; you cannot restart it from Documentum Administrator.
Refer to the *Content Server Installation Guide* for instructions on stopping and starting the Java method server.

Modifying ACS server communication protocols

On the ACS Server Connection page, modify the communication protocols used by the ACS server.

Access the ACS Server Connection page from the ACS Server Configuration Properties - Info page by selecting the ACS server communication protocol and clicking **Edit** in the ACS Server Connections section. Refer to [Viewing or modifying ACS projections and stores, page 156](#) for instructions.

To modify ACS server communication protocols:

1. Access the **ACS Server Connection** page.
2. In the Protocol field, modify the protocol, which is currently http or https.
3. In the Base URL field, modify the base URL used by the ACS server in the following format:
 $protocol://host:port/ACS/servlet/ACS$
 where *protocol* is http or https; *host* is the name of the computer on which the ACS server is installed; and *port* is the port designated for communications during ACS server installation.

4. Click **OK** or **Cancel** to return to the ACS Server Configuration Properties - Info page.

Designating connection brokers for an ACS server

Use Connection Broker Projection for ACS Server page to provide information about a connection broker to which an ACS server projects. The following instructions apply only to ACS servers that are in acs configuration mode. ACS servers that are in server configuration mode use the connection brokers defined in the associated server configuration object.

To designate a connection broker for an ACS server:

1. Access the Connection Broker Projection for ACS Server page:
 - a. Connect as a Superuser to the repository in which you want to view or modify the connection broker.
 - b. Select **Administration > Configuration > ACS Servers**.
The ACS Servers Configurations list page appears.
 - c. Select the ACS server to view or modify and then select **View > Properties > Info**.
The ACS Server Configuration Properties - Info page appears.
 - d. Click the **Projections & Stores** tab.
The ACS Server Configuration Properties - Projections & Stores page appears.
 - e. Click **Add** in the **Connection Broker Projections** section.
The Connection Broker Projection for ACS Server page appears.
2. Type the name of the host on which the connection broker resides.
3. Type the port number on which the connection broker is listening.
4. To enable projection to the connection broker, select **Enabled**.
5. Click **OK** to save the new projection target or **Cancel** to exit from this page.
The ACS Server Configuration Properties - Projections & Stores page appears.
6. Restart the ACS server.
The ACS server runs in the same servlet container as the Documentum Java method server. You must manually restart the Java method server on the host where it is installed; you cannot restart it from Documentum Administrator.
Refer to the *Content Server Installation Guide* for instructions on stopping and starting the Java method server.

Deleting projections or stores from an ACS server

Use these instructions to delete connection broker projections, network locations projections, or local stores from the acs server configuration object. If the ACS Server is in server configuration mode, the connection broker projections, network location, projections, or stores cannot be deleted on the ACS Server Configuration Properties - Projections & Stores page.

To delete projections and stores:

1. Access the ACS Server Configuration Properties - Projections & Stores page:
 - a. Connect as a Superuser to the repository in which you want to view or modify the ACS projections and stores.
 - b. Select **Administration > Configuration > ACS Servers**.
The ACS Servers Configurations list page appears.
 - c. Select the ACS server to view or modify and then select **View > Properties > Info**.
The ACS Server Configuration Properties - Info page appears.
 - d. Click the **Projections & Stores** tab.
The ACS Server Configuration Properties - Projections & Stores page appears where you can view or modify the connection broker projections, network locations, and local stores information for the ACS server.
2. To remove a connection broker:
 - a. Select a connection broker.
 - b. Click **Remove**.
The connection broker is no longer associated with the ACS server.
3. To remove a network location:
 - a. Select a network location.
 - b. Click **Remove**.
The network location is no longer associated with the ACS server.
4. To remove a local store:
 - a. Select a local store.
 - b. Click **Remove**.
The local store is no longer associated with the ACS server.
5. Click **OK** to save the changes or click **Cancel** to exit without saving any changes.
The ACS Servers Configurations list page appears.
6. Restart the ACS server.
To enable the changes that you made, restart the ACS server. The ACS server runs in the same servlet container as the Documentum Java method server. You must manually restart the Java method server on the host where it is installed; you cannot restart it from Documentum Administrator.
Refer to the *Content Server Installation Guide* for instructions on stopping and starting the Java method server.

Choosing network locations

Use the Choose Network Locations page to designate network locations. The network locations displayed on this page are in the global registry known to DFC on the Documentum Administrator host.

To add or delete network locations:

1. Select the network locations to add.
2. Click the > button.
The network locations move to the right-hand column.
3. To remove a network location, select it and then click the < button.
The network location moves to the left-hand column.
4. Click **OK** to save the change or **Cancel** to exit without saving.

Properties of ACS servers

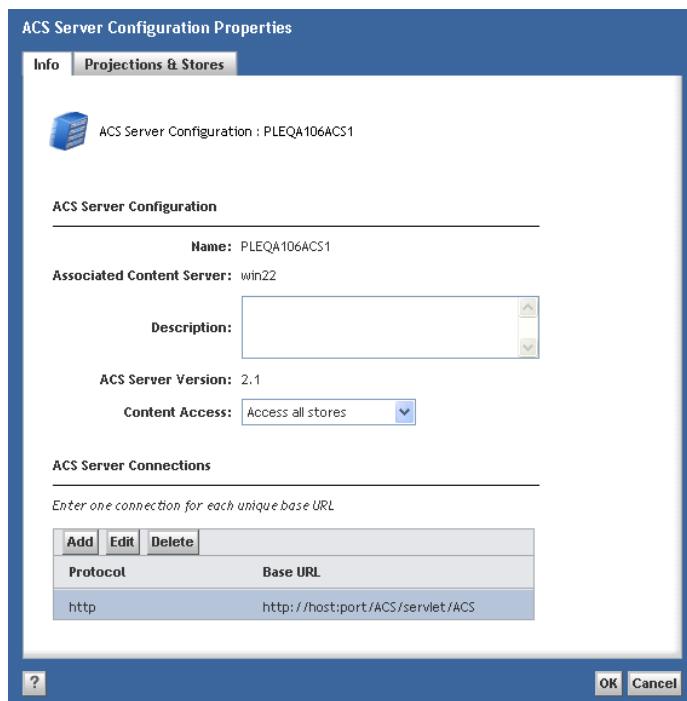
This section describes the ACS server properties configured on these pages:

- ACS Server Configuration Properties - Info and New ACS Server Configuration - Info pages
- ACS Server Configuration Properties - Projections & Stores and New ACS Server Configuration - Projections & Stores pages

You must have Superuser privileges to modify ACS server properties.

ACS Server Configuration Properties - Info page

This section discusses the field properties on the ACS Server Configuration Properties - Info and New ACS Server Configuration - Info pages.

Figure 12. ACS Server Configuration Properties - Info page**Table 20. Field properties on the ACS server configuration Info pages**

Field label	Value
Name	Read only. The value is assigned when the ACS server is installed and the acs configuration object is created, in the format <i>hostACSnumber</i> , where <i>host</i> is the host on which the ACS server is installed and <i>number</i> is an integer incremented by 1 for each acs server configuration object in a repository.
Associated Content Server	Read only. The Content Server associated with this ACS server. The server configuration is displayed regardless of whether the ACS server is in server configuration mode or acs configuration mode.
Description	An optional description of the ACS server.
ACS Server Version	Read only. Displays the major and minor version of the ACS server that the distributed content infrastructure uses to determine what its capabilities are. For example, 2.1 designates that the ACS server is bundled with a Documentum 6.5 repository, while 1.0 designates that the ACS server is bundled with a 5.3 SPx repository.

Field label	Value
Content Access	<p>Select an access type:</p> <ul style="list-style-type: none">• If using a Documentum 6 or later repository, the options are:<ul style="list-style-type: none">— Read and write— Read from local stores only: The ACS server can read content from local file stores, but is unable to use Surrogate Get to request content files it does not find in the local file stores.— Read from all stores— None (disabled): The ACS server is unable to read content from any source.• If using a 5.3 SPx repository, the options are:<ul style="list-style-type: none">— Read from local stores only: The ACS server can read content from local file stores, but is unable to use Surrogate Get to request content files it does not find in the local file stores.— Read from all stores— None (disabled): The ACS server is unable to read content from any source.
ACS Server Connections	<p>This section displays the protocol used by the ACS server (HTTP and HTTPS protocols are supported) and the base URL for the ACS server. The base URL is in the format:</p> <p><i>protocol://host:port/ACS/servlet/ACS</i></p> <ul style="list-style-type: none">• To add a new protocol for an ACS server connection, click Add to access the ACS Server Connection page.• To change the protocol or modify the base URL for the ACS server, select the ACS server connection and then click Edit to access the ACS Server Connection page.• To delete an existing protocol and base URL for the ACS server, select the ACS server connection and then click Delete.

Field label	Value
OK	Click to save any changes and return to the ACS Servers Configurations list page.
Cancel	Click to exit without saving changes and return to the ACS Servers Configurations list page.

ACS Server Configuration Properties - Projections & Stores page

This section discusses the field properties on the ACS Server Configuration Properties - Projections & Stores and New ACS Server Configuration - Projections & Stores pages.

Add, modify, or delete network location projects from this page only if you selected **Settings entered here** under **Source**. If **Associated content server** is selected for **Source**, then the network location projects from the server configuration object used by the ACS server.

Figure 13. ACS Server Configuration Properties - Projections & Stores page

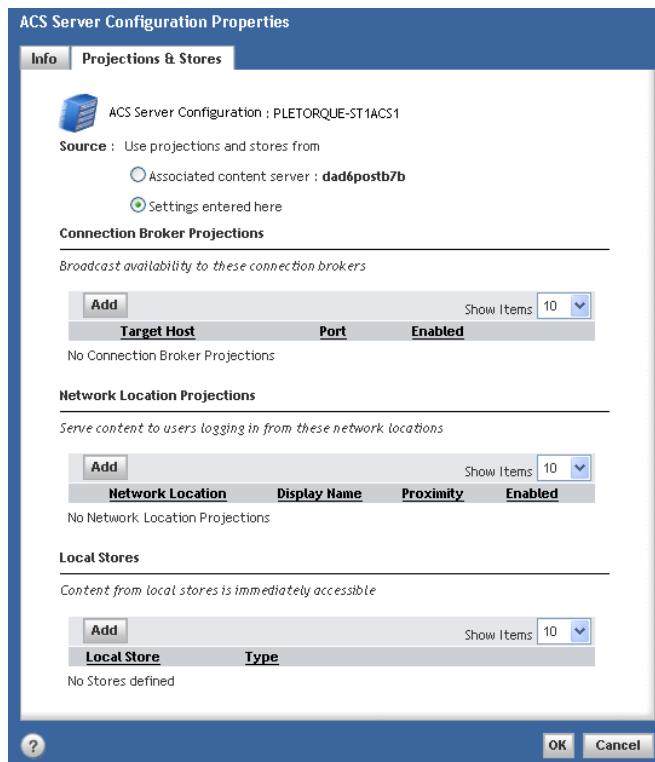


Table 21. Field properties on the ACS server configuration Projections & Stores page

Field label	Value
Source	Select the mode the ACS server uses. Options are: <ul style="list-style-type: none"> • Associated content server: Select for the ACS server to use the connection broker targets, network locations, and local stores already configured for the associated Content Server. These fields are read-only on the ACS Server Configuration Properties - Projections & Stores page. • Settings entered here: Select for the ACS server to use connection brokers, network locations, and near stores that you manually enter on the ACS Server Configuration Properties - Projections & Stores page.
Connection Broker Projections	This section lists the host where there are connection brokers to which the current ACS server projects, the port number used by each connection broker, and if the connection broker is enabled.
Add	Click to access the Connection Broker Projection for ACS Server page to add a connection broker.
Edit	Select a target host and then select Edit to access the Connection Broker Projection for ACS Server page to modify information about a connection broker.
Remove	Select a target host and then click Remove to delete it.
Target Host	Name of the host on which the connection broker resides.
Port	The port number on which the connection broker is listening.
Enabled	Select to enable projection to the connection broker.
Network Location Projections	The Network Location Projections section defines the network locations with which an ACS server is associated and to which it serves content, the proximity value for each network location, and whether projection to that network location is enabled. For more information about network locations, refer to About network locations, page 146 .

Field label	Value
Add	Click to access the Choose Network Locations page to add network locations. The network locations you see on the Choose Network Locations page are in the global registry known to DFC on the Documentum Administrator host.
Remove	Select a network location and then select Remove to remove a network location.
Network Location	Name of the network location.
Display Name	A description of the network location that is easy for end-users to understand. (For example, San Francisco, Paris, Chicago, or Tokyo.) The display name is the name displayed on the login page for Documentum web clients, such as Webtop, when users choose a network location. The display name is not the object name.
Proximity	Type a proximity value.
Enabled	Select to enable projection to the network location.
Local Stores	<p>The information displayed in the Local Stores section on the ACS Server Configuration Properties - Projections & Stores page is determined by whether the ACS server is in acs configuration mode or server configuration mode:</p> <ul style="list-style-type: none"> • If the ACS server is in acs configuration mode, use this section to configure near stores that the ACS server can access.
	<p>You can select from all storage areas for the repository, excluding distributed stores.</p> <ul style="list-style-type: none"> • If the ACS server is in server configuration mode, the stores displayed in this section are the stores that are far from the associated Content Server.
	<p>The ACS server cannot access these storage areas. The ACS Server can access only stores that are <i>not</i> far stores for the associated Content Server.</p>
	<p>For more information about acs configuration mode and server configuration mode, refer to About ACS servers, page 154.</p>
Add	Click to access the Choose a storage page to add local stores.

Field label	Value
Remove	Select a local store and then click Remove to remove a local store.
Local Store	Name of the local store. If in server configuration mode, the stores displayed are read-only. They are stores defined as far from the Content Server.
Type	If in acs configuration mode, the local stores are near to the ACS server and you can add or delete them.
OK	Indicates the type of store.
Cancel	Click to save any changes and return to the ACS Servers Configurations list page.
	Click to exit without saving changes and return to the ACS Servers Configurations list page.

BOCS servers

This section provides conceptual information and instructions for creating, modifying, and deleting BOCS servers.

Use the **Administration > Distributed Content Configuration > BOCS Servers** to access the BOCS Servers Configuration list page. From the BOCS Servers Configuration list page, you can create, view, modify, and delete BOCS servers.

This section contains the following topics:

- [About BOCS servers, page 168](#)
- [Creating BOCS servers, page 169](#)
- [Setting BOCS server security, page 171](#)
- [Setting BOCS server communication protocols, page 173](#)
- [Viewing or modifying BOCS server properties, page 173](#)
- [Deleting BOCS servers, page 174](#)
- [Deleting BOCS server warning, page 174](#)
- [Properties of BOCS servers, page 175](#)

About BOCS servers

Branch Office Caching Services (BOCS) servers are caching servers that cache content locally. Caching content allows users to obtain frequently accessed content very quickly. The amount of content that can be cached and the length of time which the content is held is configurable. You can also cache content prior to users' requests programmatically or through a pre-caching job.

BOCS servers communicate only with ACS servers and DMS servers. They do not communicate directly with Content Servers. A BOCS server can communicate with any ACS server or DMS server.

When creating a new BOCS server for Documentum 6 or later repositories, Documentum Administrator checks the version of the Content Server and creates a dm_bocs_config type. For 5.3 SPx repositories, a dm_acs_config object will be created and is_cache_acs on the dm_acs_config object will be set to TRUE.

All BOCS configuration objects for Documentum 6 or later repositories reside in the global registry in the /System/BocsConfig folder. Use Documentum Administrator to manually create and manage the configuration objects in the global registry repository after the BOCS servers are installed. The installation program for the BOCS server does not create the object at installation time.

A BOCS server may serve content from multiple repositories. For Documentum 6 or later repositories, create one configuration object for each BOCS server for all repositories. For 5.3 SPx repositories, you need to create a BOCS configuration object in each repository.

The network location objects referenced in the configuration object define the network locations served by the BOCS server.

To create, modify, or view BOCS configuration objects, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges. For Documentum 6 or later repositories, administrators logging in to a non-global registry will not see a BOCS Server Configuration list page. If they click the BOCS Server node, the system displays a message informing the administrator that they logged in to a non-global registry repository and BOCS are stored only in the global registry repository. The system will also show a link for the administrator to click to navigate to the login page of the global registry repository.

Creating, modifying, or viewing BOCS servers

Click the links below for topics about creating, modifying, or viewing BOCS servers:

- [Creating BOCS servers, page 169](#)
- [Setting BOCS server security, page 171](#)
- [Viewing or modifying BOCS server properties, page 173](#)
- [Properties of BOCS servers, page 175](#)

Creating BOCS servers

Use the instructions in this section to create the configuration object in the global registry repository for a BOCS server after the BOCS server is installed on its host. To create BOCS configuration objects, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in with Superuser privileges.

To create BOCS servers:

1. Connect to the global registry known to DFC as a user with Superuser privileges.
2. Navigate to **Administration > Distributed Content Configuration > BOCS Servers**.

The **BOCS Server Configurations** list page appears. You will not see any BOCS servers listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the BOCS Server Configurations list page:

BOCS can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create BOCS.

3. Select **File > New > BOCS Server Configuration**.

The **New BOCS Server Configuration - Info** page displays.

4. Enter information in the **BOCS Server Configuration Info** section:

- a. **Name:** Type the name of the new BOCS server.

- b. **Description:** Optionally, type a description of the BOCS server.

- c. **BOCS Server Version:** Select a major version and a minor version level of the BOCS server.

For example, select 2 for the major version and select 1 for the minor version level for a BOCS Documentum 6.5 server. Select 2.0 for a BOCS Documentum 6.0 server. The major and minor version information indicates to the distributed content infrastructure what the capabilities are of the BOCS server. If you select 1.0, the Content Access options are limited to Read Only and None (disabled).

- d. **Content Access:** Select an access type from the drop-down list:

- If using a Documentum 6 or later repository, options are:
 - **Read and synchronous write**

Select this option for the BOCS server to support read and synchronous write.

- **Read, synchronous, and asynchronous write**

Select this option for the BOCS server to support read, synchronous write, and asynchronous write.

- **None (disabled)**

- If using a 5.3 SPx repository, the options are **Read only** and **None (disabled)**.

- e. **Network Locations:** Select the network locations that will be served by the BOCS server.

- Click **Select** to access the **Choose Network Location** page.

- Select network locations and click **Add**.

The selected network locations move to the right side of the page.

- To delete network locations, select network locations on the right side of the page and click **Remove**.

The network locations are removed from the right side of the page.

- Click **OK** to save the changes or **Cancel** to exit without saving.

The New BOCS Server Configuration - Info page appears.

- f. **Repositories:** If using a Documentum 6 or later repository, select from the drop-down list to serve content from:
 - **all repositories**
 - **selected repositories only**
 If selected, the system displays the **Include** list. Click **Edit** to add specific repositories.
 - **all except selected repositories**
 If selected, the system displays the **Exclude** list. Click **Edit** to add specific repositories to exclude.

Note: The Repositories section is not available for 5.3 SPx repositories. You must create a BOCS configuration object in each repository that will be used.

 - g. **Proxy URL:** Optionally, enter the BOCS proxy URL. The BOCS proxy URL is a message URL used only by DMS when BOCS is in push mode. The URL can contain up to 240 characters.
5. In the **BOCS Server Connections** section, set the communication protocols used by the BOCS server.
- The http and https communication protocols may be used by the BOCS server.
- a. Click **Add** to access the **BOCS Server Connection** page.
 - b. In the **Protocol** field, enter the protocol.
 - c. In the **Base URL** field, enter the base URL used by the BOCS server in the following format:
`protocol://host:port/ACS/servlet/ACS`
 where *protocol* is http or https; *host* is the name of the computer on which the BOCS server is installed; and *port* is the port designated for communications during BOCS server installation.
 - d. Click **OK** or **Cancel** to return to the New BOCS Server Configuration - Info page.
6. Exit from the New BOCS Server Configuration - Info page.
- Click the **Security** tab to view or modify BOCS server communications protocols.
 - Click **OK** to save the BOCS server configuration and return to the BOCS Server Configurations list page.
 - Click **Cancel** to exit without saving any changes and return to the BOCS Servers Configurations list page.

Setting BOCS server security

For Documentum 6 repositories, the BOCS server configuration pages have a Security tab. The settings on the New BOCS Server Configuration - Security or BOCS Server Configuration Property - Security pages enable an administrator to designate if the BOCS server is in push or pull mode and to upload a public key from the BOCS server.

When the pull mode is enabled, the BOCS server configuration object in the global registry contains the public key information and generates a digital signature for the BOCS server to use when contacting the DMS server. When the BOCS server connects to the DMS server in pull mode, it sends its digital signature to DMS where DMS matches the digital signature to the public key in the bocs

configuration object. If the DMS server authenticates the BOCS digital signature, the BOCS server can then pull its messages from the DMS server.

Figure 14. New BOCS Server Configuration - Security page



To set BOCS server security:

1. Access the BOCS Server Configuration Property - Security page (or the New BOCS Server Configuration - Security page):
 - a. Connect to the global registry known to DFC as a user with Superuser privileges.
 - b. Navigate to **Administration > Distributed Content Configuration > BOCS Servers**. The **BOCS Server Configurations** list page appears. You will not see any BOCS servers listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the BOCS Server Configurations list page:

BOCS can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create BOCS.

 - c. Locate the correct BOCS server and select **View > Properties > Info**. The **BOCS Server Configuration Properties - Info** page appears.
 - d. Click **Next** or click the **Security** tab. The **BOCS Server Configuration Properties - Security** page appears.
2. Enter, view, or modify the security properties for the BOCS server:
 - a. **Pull Mode Enabled:** Select to designate that the BOCS server will communicate with the DMS server using the pull mode. If selected, you must also upload the public key file for the DMS server to use to authenticate the BOCS server. If not selected, the BOCS server will communicate with the DMS server using the push mode.
 - b. **Public Key Installed:** Displays the last updated status for the public key.
 - c. **Upload Public Key File:** Click **Browse** to locate and install the public key file for the BOCS server.
3. Click **OK** to save changes made to the BOCS server configuration object or **Cancel** to exit without saving the changes. The BOCS Server Configurations list page appears.

Setting BOCS server communication protocols

On the BOCS Server Connection page, set the communication protocols used by the BOCS server.

Access the BOCS Server Connection page from the New BOCS Server Configuration or BOCS Server Configuration Properties page by clicking **Add** or **Edit** in the **BOCS Server Connections** section. Refer to [Creating BOCS servers, page 169](#) or [Viewing or modifying BOCS server properties, page 173](#) for instructions.

To set the BOCS server communication protocols:

1. Access the **BOCS Server Connection** page.
2. In the **Protocol** field, add or modify the protocol, which is currently http or https.
3. In the **Base URL** field, add or modify the base URL used by the BOCS server in the following format:
`protocol://host:port/ACS/servlet/ACS`
 where *protocol* is http or https; *host* is the name of the computer on which the BOCS server is installed; and *port* is the port designated for communications during BOCS server installation.
4. Click **OK** or **Cancel** to return to the **New BOCS Server Configuration - Info** page.

Viewing or modifying BOCS server properties

Use the instructions in this section to view or modify the configuration object in the repository for a BOCS server after the BOCS server is installed on its host.

To modify or view BOCS configuration objects, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges.

To view or modify BOCS servers:

1. Connect to the global registry known to DFC as a user with Superuser privileges.
2. Navigate to **Administration > Distributed Content Configuration > BOCS Servers**.
 The **BOCS Server Configurations** list page appears. You will not see any BOCS servers listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the BOCS Server Configurations list page:

BOCS can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create BOCS.

3. Locate the correct BOCS server and select **View > Properties > Info**.
 The **BOCS Server Configuration Properties - Info** page appears.
4. Modify the properties.

Refer to [Properties of BOCS servers, page 175](#) for information on the properties that can be modified.

5. Click the **Security** tab to view or modify BOCS server communications protocols on the **BOCS Server Configuration Properties - Security** page.
Refer to [Setting BOCS server security, page 171](#) for information on the BOCS server security properties that can be modified.
6. Click **OK** to save changes made to the BOCS server configuration object or **Cancel** to exit without saving the changes.

The BOCS Server Configurations list page appears.

Deleting BOCS servers

Use the instructions in this section to delete BOCS server configuration objects from a global registry repository. Deleting the configuration object does not uninstall the BOCS servers; they must be manually uninstalled from the hosts on which they are running. Without the configuration object, the BOCS server is inoperable.

To delete BOCS servers:

1. Connect to the global registry known to DFC as a user with Superuser privileges.
2. Navigate to **Administration > Distributed Content Configuration > BOCS Servers**.

The **BOCS Server Configurations** list page appears. You will not see any BOCS servers listed if you are not connected to the global registry.

Note: Click **Global Registry Login** and connect to the correct repository if you see the following warning message instead of the BOCS Server Configurations list page:

BOCS can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create BOCS.

3. Select BOCS servers to delete.
4. Select **File > Delete**.
The **BOCS config object Delete** page appears.
5. Click **OK** to delete the selected object or **Cancel** to retain the object.
If deleting multiple BOCS servers, select **Next** or **Finish**.

Deleting BOCS server warning

You have asked to delete a BOCS server configuration object. Without the configuration object, the BOCS Server cannot provide content from this repository.

On the **BOCS config object Delete** page, click **OK** to delete the selected objects or **Cancel** to retain the objects. If deleting more than one BOCS server, select **Next** or **Finish**.

Properties of BOCS servers

This section displays the BOCS Server Configuration Properties - Info page and lists the field properties on the New BOCS Server Configuration - Info and BOCS Server Configuration Properties - Info pages.

To create, view, or modify BOCS configuration objects, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges.

Figure 15. BOCS Server Configuration Properties: Info page

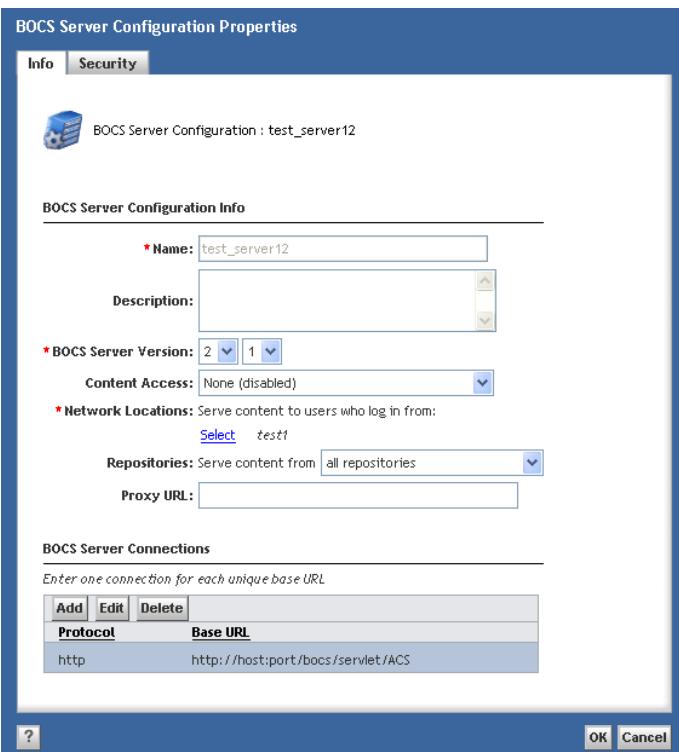


Table 22. Field properties on the BOCS server configuration Info pages

Field label	Value
Name	Object name of the BOCS server.
Description	Description of the BOCS server.

Field label	Value
BOCS Server Version	Select a major version and a minor version level of the BOCS server. For example, select 2 for the major version and select 0 for the minor version level for a BOCS Documentum 6 server. The major and minor version information indicates to the distributed content infrastructure what the capabilities are of the BOCS server.
Content Access	If you select 1, the Content Access options are limited to Read Only and None (disabled). Select an access type: <ul style="list-style-type: none">• If using a Documentum 6 repository, options are:<ul style="list-style-type: none">— Read and synchronous write Select this option for the BOCS server to support read and synchronous write.— Read, synchronous, and asynchronous write Select this option for the BOCS server to support read, synchronous write, and asynchronous write.— None (disabled)• If using a 5.3 SPx repository, the options are Read only and None (disabled).
Network Locations	Network locations served by the BOCS server. Select Click to access the Choose a Network Location page to select network locations.
Repositories	If using a Documentum 6 or later repository, select from the drop-down list to serve content from: <ul style="list-style-type: none">• all repositories.• selected repositories only. If selected, the system displays the Include list. Click the Edit link to add specific repositories.• all except selected repositories.

Field label	Value
	If selected, the system displays the Exclude list. Click the Edit link to add specific repositories to exclude.
	Note: The Repositories section is not available for 5.3 SPx repositories. You must create a BOCS configuration object in each repository that will be used.
Proxy URL	Optionally, enter the BOCS proxy URL. The URL can contain up to 240 characters. The BOCS proxy URL is a message URL that only DMS uses when BOCS is in push mode.
Add	Click to access the BOCS Server Connection page to add a protocol and base URL for the BOCS server.
Edit	Select a communication protocol and then click Edit to access the BOCS Server Connection page to edit a protocol and base URL for the BOCS server.
Delete	To delete a BOCS server protocol and base URL, select a communication protocol and then click Delete .
Protocol and Base URL	The communication protocols used by the BOCS server to provide content to end users. The HTTP and HTTPS protocols are supported. The Base URL must be provided when the BOCS server is created. It is in the form: <i>protocol://host:port/ACS/servlet/ACS</i> where <i>protocol</i> is http or https; <i>host</i> is the name of the computer on which the BOCS server is installed; and <i>port</i> is the port designated for communications during BOCS server installation.
OK	Click to save the new or modified BOCS server configuration object.
Cancel	Click to exit and return to the BOCS Servers Configurations list page without saving any changes.

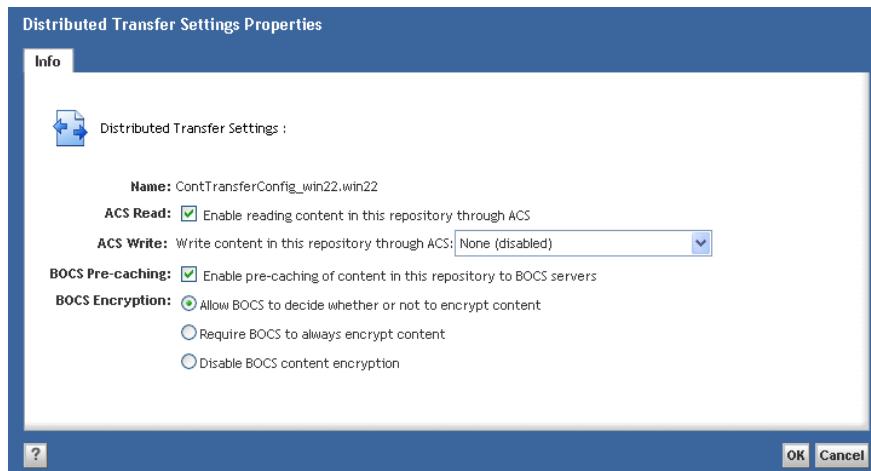
Configuring distributed transfer settings

The distributed transfer object (`dm_cont_transfer_config`) is created when the repository is created. The `dm_cont_transfer_config` configuration object controls whether reading and writing

content through ACS is enabled for the repository and whether BOCS pre-caching is also enabled. Administrators cannot create new distributed transfer objects; however, administrators with Superuser privileges can configure the default object. Use the Administration > Distributed Content Configuration > Distributed Transfer navigation to access the Distributed Transfer Settings list page.

Note: The Distributed Transfer node is available only for Documentum 6 or later repositories. The node is not visible for 5.3x repositories.

Figure 16. Distributed Transfer Settings Properties - Info page



To configure the distributed transfer settings:

1. Connect to the repository as a user with Superuser privileges.
2. Navigate to **Administration > Distributed Content Configuration > Distributed Transfer**. The **Distributed Transfer Settings** list page appears. You will not see the distributed transfer setting listed if you are not connected to the global registry.
3. Locate the distributed transfer setting and select **View > Properties > Info**. The **Distributed Transfer Settings Properties - Info** page appears.
4. Modify the properties:
 - **Name:** Read only. Indicates the name of the content transfer object assigned by the system when the repository is created. There can be only one distributed transfer setting in a repository.
 - **ACS Read:** Select to enable users to read content in this repository through the ACS. If not selected, users requesting documents must go directly to the repository to obtain the requested content.
 - **ACS Write:** Write content in this repository through ACS. Options are:
 - Synchronous write
 - Synchronous and Asynchronous write
 - None (disabled): This is the default.
 - **BOCS Pre-caching:** Select to enable the repository to process pre-caching requests. Clear the checkbox to not pre-cache content in the repository.

5. **BOCS Encryption:** Select to allow, disable, or require content encryption.

If you use a default type-based business object (TBO) and content is in an encrypted store, the Require BOCS to always encrypt option is used, regardless of which option you select on the Distributed Transfer Settings Properties - Info page.

If you write your own TBO, content will be encrypted based on what the doGetContentEncryptionMode method returns, regardless of what option you select on the Distributed Transfer Settings Properties - Info page.

Options are:

- **Use BOCS encryption setting:** Select to encrypt content only if the encryption.mode parameter in BOCS acs.properties file is set to *Required*.
- **Require BOCS to always encrypt content:** Select to encrypt content on BOCS. Content will not be stored on BOCS if BOCS version does not support encryption or if the encryption.mode parameter in BOCS acs.properties file is set to *Disabled*.
- **Disable BOCS content encryption:** Select to not encrypt content on BOCS.

6. Click **OK** to save changes made to the distributed transfer settings properties or **Cancel** to exit without saving the changes.

The Distributed Transfer Settings list page appears.

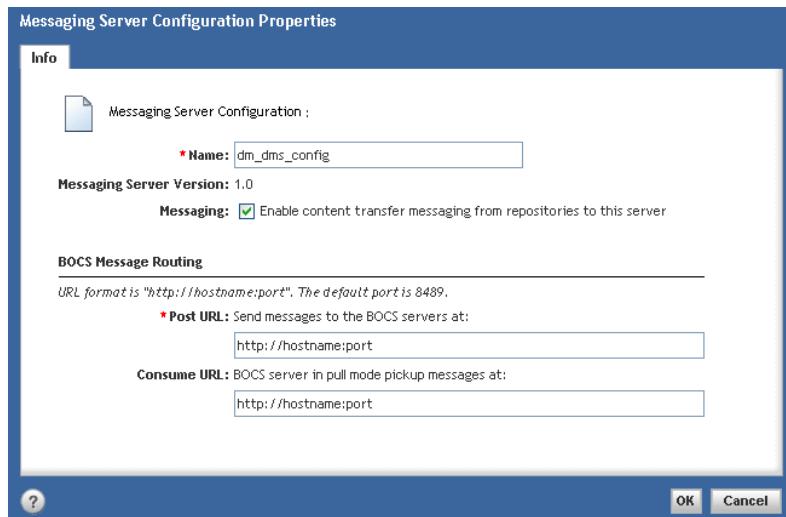
Messaging server configuration

A Documentum Messaging Services (DMS) server is an intermediary server that provides messaging services between an ACS or BOCS server and a web application server. The messaging server configuration object (dm_dms_config) must be created and set up in the global registry using Documentum Administrator. Administrators with Superuser privileges can configure the default messaging server configuration object; however, if a messaging server configuration object already exists, administrators cannot create new objects.

Use the **Administration > Distributed Content Configuration > Messaging Server** navigation to access the Messaging Server Configuration list page.

To modify or view the DMS server configuration object, you must be connected to the repository known to DFC on the Documentum Administrator host as a global registry and you must be logged in as a user with Superuser privileges. Administrators logging in to a Documentum 6 repository that is not the global registry will not see a Messaging Server Configuration list page. If they click the Messaging Server node, the system displays a message informing administrators that they logged in to a non-global registry repository and the messaging server configuration object is stored only in the global registry repository. The system will also show a link for the administrator to click to navigate to the login page of the global registry repository.

Note: The Messaging Server node is available only for Documentum 6 repositories; the node is not visible for 5.3x repositories.

Figure 17. Messaging Server Configuration Properties - Info page**To view or modify the messaging server configuration:**

1. Connect to the global registry known to DFC as a user with Superuser privileges.
2. Navigate to **Administration > Distributed Content Configuration > Messaging Server**.

The **Messaging Server Configuration** list page appears. You will not see the messaging server configuration if you are not connected to the global registry.

Note: Click the **Global Registry Login** link and connect to the correct repository if you see the following warning message instead of the Messaging Server Configuration list page:

Messaging Servers can only be created in repositories that are designated as global registries. The current repository is not a global registry. Click the link below to log in to the global registry repository known to DFC on the Documentum Administrator host. You must have superuser privileges to create Messaging Servers.

3. Select the messaging server configuration and then select **View > Properties > Info**.

The **Messaging Server Configuration Properties - Info** page appears.

4. View the properties or change the messaging flag:

- **Name:** Read-only. The name of the messaging server configuration.
- **Messaging Server Version:** Indicates the version of the messaging server, which is automatically set when creating a new messaging server. The messaging server version must be 1.0 for Documentum 6.
- **Messaging:** Select to enable content transfer messaging to the DMS server. This checkbox must be selected to enable asynchronous content transfer through BOCS and for predictive caching to work.

Clear the checkbox to disable content transfer messages to the DMS server, even if the DMS server is running.

5. Enter information in the **BOCS Message Routing** section:

- a. **Post URL:** Type the hostname and port where to send messages to the DMS server. This is a required field.

- b. **Consume URL:** Type the hostname and port where BOCS servers in pull mode pick up messages from the DMS server. If you do not have BOCS servers using the pull mode, then this field is optional.
6. Click **OK** to save changes made to the messaging server configuration object or **Cancel** to exit without saving the changes.

The Messaging Server Configuration list page appears.

Chapter 6

User Management

This section contains information on managing users, groups, roles, and sessions in the repository. From Documentum Administrator, you can:

- Create, modify, or delete users
- Create, modify, or delete groups
- Add users to groups or delete users from groups
- Create, modify, or delete roles
- Monitor and kill user sessions

Click the links below for information and instruction for:

- [User management and Documentum Collaboration Services, page 183](#)
- [Users, page 184](#)
- [Groups, page 204](#)
- [Roles, page 212](#)
- [Module roles, page 217](#)
- [Sessions, page 221](#)

User management and Documentum Collaboration Services

Some user management features support Documentum Collaboration Services. These are:

- Use authentication with an in-line password

An in-line password is encrypted and stored in the repository. No operating system, domain, or LDAP account is required for the user. An in-line password is set at the time the user is created. Details on in-line passwords can be found in the User Source row of [User attributes, page 191](#).

- Limiting user access to particular folders

Use the Restrict Folder Access To field on the New User or User Properties page to indicate folders or cabinets in a repository that a user can access. If no folders are chosen, the user has

access to all folders and cabinets in the repository, subject to the permissions on those cabinets and folders and subject to folder security.

- Establish user managers to create users

Users with a user manager (dce_user_manager) role can perform a variety of user management tasks without being a system administrator. User managers can browse users and groups, create new users, and modify users.

- Unlist a user

An unlisted username does not appear to regular users in the repository user list. Documentum Collaboration Services creates a group for unlisted users at the root of the repository user list called dce_hidden_users.

Users

This section contains information on creating, modifying, and deleting users in a repository.

To access a repository, a person must be defined as a user in that repository. Adding someone as a user to a non-federated repository does not give that person access to every repository in the enterprise. The person must be explicitly added to each repository.

When you navigate to **Administration > User Management > Users**, you access the users in the current repository. When you first access Users list page, it is in search mode. You can search for users by repository user name, OS user name (name on the operating system), or default group.

Click **Show All Users** to list all users in the repository. The users in the repository are displayed in the order in which they were added to the repository.

You can sort the users by clicking any of the column headings:

- Name, the users name in the repository
- Group, the users default group
- State, which indicates whether the user is active, inactive, locked, or locked and inactive
- E-mail, the users email address

You can also jump to a user by typing the first few letters of the users name in the repository in the **User Name** box or by clicking the letter corresponding to the beginning of the users repository name. The users repository name is not the users login name. For example, a user who connects to the repository as msmith might have the repository name Mary Smith. Search for Mary, not msmith. Similarly, you can search by typing in a part of the **User Login Name**, the users **Default Group**, or the **User Login Domain**.

To search for users in the repository, click **Search**. On the user list page, you can also click **Advanced** to use the advanced search features.

To display more than the default ten users at a time, select a different number from the **Show Items** drop-down list

To view the next page of users, click the > button. To view the previous page of users, click the < button. To jump to the first page of users, click the << button. To jump to the last page, click >>.

This section includes the following topics:

- Locating users, page 185
- Setting the default permissions for the cabinet of a new user, page 186
- Creating users, page 186
- Creating global users, page 190
- User attributes, page 191
- Importing users, page 196
- Import user attributes, page 198
- Deleting users, page 201
- Reassigning objects to another user, page 202
- Changing the home repository of a user, page 202
- Making a user active or inactive, page 202
- Modifying users, page 203
- Viewing groups, workflows, alias sets, permission sets, and documents of a user, page 203
- Viewing or deleting change home repository logs, page 203
- Viewing user reassign logs, page 204
- Reassign reports, page 204

Locating users

Use these instructions to locate users in the repository. You can search by user name, user OS name, or default group.

To locate users:

1. Connect to the repository where you want to locate a particular user.
2. Navigate to **Administration > User Management > Users**.
3. Type the information into a search box. (Depending on your repository version, available search boxes include the following:
 - **User Name**
 - **User Login Name**
 - **Default Group**
 - **User Login Domain**
 - **User OS Name**
 - **User Domain**
4. Click **Search**.

Setting the default permissions for the cabinet of a new user

When you create a new user, you assign the user a default folder. Documentum Administrator allows you to select between assigning an existing folder as the user's default or creating a new folder with the user's name. If you have Documentum Administrator create the folders for new users and you want to control the permissions assigned to new users' folders, use these instructions:

1. Create a new alias set called **UserPropertiesConfiguration**.
2. Assign ownership of the UserPropertiesConfiguration alias set to the repository owner.
This is the user whose account is used for database access (dm_dbo).
3. Create two aliases in UserPropertiesConfiguration.
 - DefaultFolderAcl
Point this alias to the permission set to be applied to the new folder created for new users.
 - DefaultFolderAclDomain
Point this to the user who owns the permission set you use for DefaultFolderAcl.

When the new folder is created during new user creation, Documentum Administrator applies the permission set you designate. If a new user is not present as an accessor in the permission set, the user is granted write permission on the folder. The permission set for the cabinet is then modified to a system-generated permission set, but it otherwise has the permissions from the permission set you created.

You can use Documentum Administrator to create a new default folder for an existing user whose default folder is not the user's name, and permissions on the set are applied as described above if you have created the necessary alias set and aliases.

If the UserPropertiesConfiguration alias set does not exist and a Superuser creates the new user, the new user owns the folder and has delete permission. If a Sysadmin creates the new user, the user is not the owner of the default folder, but the user has change owner permission on the folder as well as write permission.

Creating or modifying users

Click the links for instruction on:

- [Creating users, page 186](#)
- [Modifying users, page 203](#)

Creating users

Use these instructions to create repository users.

Before you create users, determine what type of authentication the server 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 the repository is the governing member of a federation, a new user can be a global user. Global users are managed through the governing repository in a federation, and have the same attribute values in each member repositories within the federation. If you add a global user to the governing repository, that user is added to all the member repositories by a federation job that synchronizes the repositories.

You must have System Administration or Superuser privileges to create users. Superusers and System Administrators cannot modify their own extended privileges.

If a user is authenticated by an LDAP server, only a Superuser can modify the user's LDAP-mapped attributes.

When you create users who will be managed by an LDAP server:

- The `user_name`, and `user_login_name` attributes of the `dm_user` object must have non-null values.
- The `user_name` and `user_login_name` attributes of the `dm_user` object must have unique values.

For information about each attribute, see [User attributes, page 191](#). For more information about users, refer to Users and Groups in the *Content Server Administration Guide*.

To create new users:

1. Connect to the repository where you want to create new users.

2. Navigate to **Administration > User Management > Users**.

3. Select **File > New > User**.

The system displays the **New User - Info** page.

4. Select a **State** for the user:

- **Active:** The user is a currently active repository user. Active users are able to connect to the repository.
- **Inactive:** The user is not currently active in the repository. Inactive users are unable to connect to the repository. A user may be made inactive because of multiple authentication failures or through resetting the state manually. Repositories can be configured so that a user is automatically activated after being inactivated. Refer to the chapter on users in the *Content Server Administration Guide* for information on how to configure this.
- **Locked:** The user is unable to connect to the repository. A System Administrator or Superuser must set a user to this state manually and must manually take a user out of this state.
- **Locked and inactive:** The user is inactive and unable to connect to the repository. A System Administrator or Superuser must set a user to this state.

If the user is a Superuser, only another Superuser can reset the user's state.

5. Type the user's name in the **Name** field.

The username cannot be changed after it is assigned. To change a user's name, you must create a new user with the new name, then assign the existing user's objects to the new user. For instructions on reassigning objects to a different or new user, refer to [Reassigning objects to another user, page 202](#).

6. Type the **User Login Name**. This is the login name used for authenticating a user. If the user is an operating system user, the user login name must match the user's operating system name. If the user is an LDAP user, the user login name must match the LDAP authentication name.
7. If available, type the **User Login Domain**. This field identifies the domain in which the user is authenticated. It is typically a Windows domain or the name of the LDAP server used for authentication.
8. Select a **User Source** from the list for user authentication. Depending on the operating system, some or all of the following choices are available:
 - **None**: Windows repositories only. The user is authenticated in a Windows domain.
 - **LDAP**: The user is authenticated by an LDAP server.
 - **Inline Password**: Select and then type a password to be stored only in the repository.
 - **UNIX only**: Select this for the default UNIX user authentication.
 - **Domain only**: Select this if the repository has Windows domain authentication enabled and the user must be authenticated against a domain.
 - **UNIX first**: Select this if the repository has Windows domain authentication enabled and the user must be authenticated first against UNIX, then against a domain.
 - **Domain first**: Select this if the repository has Windows domain authentication enabled and the user must be authenticated first against a domain, then against UNIX.
9. Type the user's password. The **Password** and **Confirm Password** fields appear if Inline Password is selected as the user source. The password is encrypted and stored in the repository. This must be provided manually for users added using an imported LDIF file.
10. Type a description of the user in the **Description** field.
11. Type the user's email address. This is the address to which notifications are sent for workflow tasks and registered events.
12. Type the user's operating system username in the **User OS Name** field. This is the user's repository username.
13. Type the user's Windows domain in the **Windows Domain** field.
 - If the repository is on a Windows host, type the domain.
 - If the repository is on a UNIX host and you have a domain map set up in order to use Windows domain authentication, browse to the correct domain.
14. Select a home repository for the user, which is where the user receives notifications and tasks.
15. If the user is being created in the governing repository of a federation, select **User is global** if you want the user and the user's attributes to be propagated to all members of the federation.
16. In the **Restrict Folder Access To** option, you can restrict the user's repository access to particular folders or cabinets. If no folders are chosen, the user has access to all folders and cabinets in the repository, subject to the permissions on those cabinets and folders and subject to folder security. If cabinets are mentioned in Restrict Folder Access To option, those cabinets will appear properly under Cabinets section. If folders are specified, folders will not appear under Cabinet section, but they can be accessed by searching through Search or Advanced Search option. This is due to security restriction on complete path of folder. In case, the folder under restricted access is at nth level in some folder hierarchy, the access specified here is only at nth level and user do not have

permission to access folder prior to nth level. So, these won't appear and the nth level folder can be accessed only through Search or Advanced Search option. If user wants to be notified for his accessible folder, then along with search, subscription and web link through email should be used.

To restrict the user's repository access to folders or cabinets:

- a. Click **Select** to access the **Choose a folder** page.
 - b. Locate the folders or cabinets to which the user will have access.
 - c. Select the folders or cabinets.
 - d. Click **OK**.
 - e. Perform the last two substeps on each page where there is a folder or cabinet to which the user will have access.
17. In the **Default Folder** section, select a default storage place for any object the user creates. Normally, this is a cabinet where the user's name is the object name.
- a. To use an existing repository folder as the user's default folder:
 - i. Select **Choose existing folder**.
 - ii. Click **Select** to access the **Choose a folder** page.
 - iii. Select the correct folder.
 - iv. Click **OK**.
 - b. To automatically create a folder with the user's name as the object name, select **Choose > Create folder with user name**.
18. In the **Default Group** section, click **Select** to access the **Choose a group** page to select a default group for the user.
19. In the **Default Permission Set** section, click **Select** to access the **Choose a permission set** page to select a default permission set for the user.
20. To provide a DB name, which is the username in the RDBMS, type the name in the **Db Name** field. The DB name is required only if the user will be a repository owner or a user who registers RDBMS tables.
21. Select the user's privileges from the **Privileges** list. User privileges authorize certain users to perform activities that are required to administer and maintain the system. The privilege levels are:
- None
 - Create Type
 - Create Cabinet
 - Create Cabinet and Type
 - Create Group
 - Create Group and Type
 - Create Group and Cabinet
 - Create Group, Cabinet, and Type

- System Administrator
 - Superuser: 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. If you revoke a user's Superuser privileges, remove the user from the admingroup.
22. Select the user's extended privileges from the **Extended Privileges** list. Extended privileges determine whether the user can configure auditing, view audit trails, and purge audit trails. Superusers and System Administrators cannot modify their own extended privileges. Select one of the following:
- None: The user cannot configure auditing, view audit trails, or purge audit trails.
 - Config audit: The user can configure auditing.
 - Purge audit: The user can purge existing audit trails.
 - Config and Purge Audit: The user can configure auditing and purge existing audit trails.
 - View Audit: The user can view audit trails.
 - Config and View Audit: The user can configure auditing and view existing audit trails.
 - View and Purge Audit: The user can view existing audit trails and purge them.
 - Config, View, and Purge Audit: The user can configure auditing and view and purge existing audit trails.
23. Select the user's client capability from the **Client Capability** list. Select the user type:
- Consumer
 - Contributor
 - Coordinator
 - System Administrator
- Content Server does not recognize or enforce these settings. For information about client capability levels, see the documentation for each client product.
24. In the **Alias Set** section, click **Select** to access the **Choose an alias set** page to select a default alias set for the user.
25. Select **Disable Workflow** to indicate that the user is not available to receive workflow tasks.
26. Select **Disable Authentication Failure Checking** to allow the user more login attempts than the limit set in the repository configuration object.
27. Click **OK**.
- The new user is created.

Creating global users

A *global user* is a repository user who is found in all members of a repository federation and whose attribute values are the same in all of the repositories. Global users are managed through the governing repository. If you add a global user to the governing repository, that user is added to all the member repositories by a federation job that synchronizes the repositories.

To create a global user, connect to the governing repository of a federation and create the user there. On the New User - Info page, select **User is global** to make the user global. Use the instructions in [Creating users, page 186](#) to create the user.

Connect to the governing repository to modify the attributes of a global user.

Global users can also have local attributes, which you can modify in a local repository.

User attributes

The following table describes each field that must be completed to create a new user. For more information on users, see the *Content Server Administration Guide*.

Table 23. Attributes of a user

Field label	Value
State	<p>Indicates the user's state in the repository:</p> <ul style="list-style-type: none"> • Active: The user is a currently active repository user. Active users are able to connect to the repository. • Inactive: The user is not currently active in the repository. Inactive users are unable to connect to the repository. A user may be made inactive because of multiple authentication failures or through resetting the state manually. Repositories can be configured so that a user is automatically activated after being inactivated. Refer to the chapter on users in the <i>Content Server Administration Guide</i> for information on how to configure this. • Locked: The user is unable to connect to the repository. A System Administrator or Superuser must manually set a user to this state and must manually take a user out of this state. • Locked and inactive: The user is inactive and unable to connect to the repository. A System Administrator or Superuser must set a user to this state. <p>If the user is a Superuser, only another Superuser can reset the user's state.</p>

Field label	Value
Name	The user name for the new user. If you are modifying the attributes of a user, you cannot change the user name. Instead, you must reassign the user's objects to another user. Use the instructions in Reassigning objects to another user, page 202 .
User Login Name	The login name used for authenticating a user in repositories. If the user is an operating system user, the user login name must match the user's operating system name. If the user is an LDAP user, the user login name must match the LDAP authentication name.
User Login Domain	Identifies the domain in which the user is authenticated. This is typically a Windows domain or the name of the LDAP server used for authentication.
User Source	Specifies how to authenticate a given repository user's user name and password. Valid values depend on whether the repository runs on UNIX or Windows. On UNIX, the valid values are: <ul style="list-style-type: none"> UNIX only: The user is authenticated using the default UNIX mechanism, <code>dm_check_password</code> or other external password checking program. Domain only: The user is authenticated against a Windows domain. UNIX first: This is used for UNIX repositories where Windows domain authentication is in use. The user is authenticated first by the default UNIX mechanism; if that fails, the user is authenticated against a Windows domain. Domain first: This is used for UNIX repositories where Windows domain authentication is in use. The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default UNIX mechanism. LDAP: The user is authenticated through an LDAP directory server. Inline Password: The user is authenticated based on a password stored in the repository.

Field label	Value
	<p>This option is available only when Documentum Administrator is used to create users. It is not available in other applications in which it is possible to create users.</p>
Password	<p>On Windows, the valid values are:</p> <ul style="list-style-type: none"> • None: The user is authenticated in a Windows domain.
Confirm Password	<ul style="list-style-type: none"> • LDAP: The user is authenticated through an LDAP directory server. • Inline Password: The user is authenticated based on a password stored in the repository. This option is available only when Documentum Administrator is used to create users. It is not available in other applications in which it is possible to create users.
Description	<p>This field is displayed if Inline Password is selected as the User Source. Type the user's password, which is then encrypted and stored in the repository.</p>
E-Mail Address	<p>This must be provided manually for users added using an imported LDIF file.</p>
User OS Name	<p>This field is displayed if Inline Password is selected as the User Source. After typing the encrypted password, type it again in this field for verification.</p>
Windows Domain	<p>A description of the user.</p>
Home Repository	<p>The user's email address for receiving notifications from the repository. This is the address to which notifications are sent for workflow tasks and registered events.</p>
User is global	<p>The new user's operating system username.</p> <ul style="list-style-type: none"> • On Windows, the domain name associated with the new user's Windows account.
	<ul style="list-style-type: none"> • On UNIX, the domain on which the user is authenticated if Windows domain authentication is in use.
	<p>The repository where the user receives notifications and tasks.</p>
	<p>If the user is being created in the governing repository of a federation, select to propagate the user's attributes to all members of the federation.</p>

Field label	Value
Restrict Folder Access To	Indicates folders or cabinets user can access. If no folders are chosen, the user has access to all folders and cabinets in the repository, subject to the permissions on those cabinets and folders and subject to folder security.
Default Folder	The default storage place for any object the user creates. Normally, this is a cabinet where the user's name is the object name. <ul style="list-style-type: none"> • Select Choose existing folder to assign a folder you already created as the user's default folder. • Select Choose/Create folder with the user name to automatically create a folder with the user's name as the object name. <p>The Choose existing folder and Choose/Create folder with the user name radio buttons appear only on the New Users - Info page.</p>
Default Group	When the user creates an object in the repository, it belongs to the group name associated with the user's default permission set.
Default Permission Set	A permission set used to assign the default permissions to objects created by the user.
Db Name	The new user's username in the underlying RDBMS. The DB Name is required only if the user will be a repository owner or a user who registers RDBMS tables.
Privileges	Choose a user privilege from the list. User privileges authorize certain users to perform activities that are required to administer and maintain the system. The privilege levels are: <ul style="list-style-type: none"> • None • Create Type • Create Cabinet • Create Cabinet and Type • Create Group • Create Group and Type • Create Group and Cabinet • Create Group, Cabinet, and Type

Field label	Value
Extended Privileges	<ul style="list-style-type: none"> • System Administrator • Superuser: If you grant Superuser privileges to a user, add that user manually to the group called admingroup. If you revoke a user's Superuser privileges, remove the user from the admingroup. <p>Sets the level of extended privileges for auditing. Superusers and System Administrators cannot modify their own extended privileges.</p> <ul style="list-style-type: none"> • None: The user cannot configure auditing, view audit trails, or purge audit trails. • Config audit: The user can configure auditing. • Purge audit: The user can purge existing audit trails. • Config and Purge Audit: The user can configure auditing and purge existing audit trails. • View Audit: The user can view audit trails. • Config and View Audit: The user can configure auditing and view existing audit trails. • View and Purge Audit: The user can view existing audit trails and purge them. • Config, View, and Purge Audit: The user can configure auditing and view and purge existing audit trails.
Client Capability	<p>Indicates what level of use is expected of the user. Choose the user type from the list. There are four types of users:</p> <ul style="list-style-type: none"> • Consumer • Contributor • Coordinator • System Administrator
Alias Set	<p>Content Server does not recognize or enforce these settings.</p> <p>The default alias set for the user.</p>

Field label	Value
Disable Workflow	Indicates whether a user can receive workflow tasks.
Disable Authentication Failure Checking	If selected, user may exceed the number of failed logins specified in the Maximum Authentication Attempts field of the repository configuration object.

Importing users

You can create repository 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. After the user is created, use the instructions in [Modifying users, page 203](#) to assign the user's password.

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 following default values are assigned when the LDIF file is imported:

Table 24. Default values for new users

Argument	Default
user_login_name	username
privileges	0 (None)
folder	/username
group	docu
client_capability	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 ldif 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 LDIF 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 ACLs 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 ACLs. They cannot represent private ACLs.

Any groups that you identify by user_group_name must exist before you run the file to import the users.

Content Server will create the default folder for each user if it does not already exist.

To import new users:

1. On the file system of the host where your browser is running, create a text file in LDIF format.
2. Save the text file.
3. Connect to the repository where you want to create new users.
4. Navigate to **Administration > User Management > Users**.
5. Select **File > Import Users**.
6. Indicate the **State** for the users you are importing.
 - **Active:** The user is a currently active repository user. Active users are able to connect to the repository.
 - **Inactive:** The user is not currently active in the repository. Inactive users are unable to connect to the repository. A user may be made inactive because of multiple authentication failures or through resetting the state manually. Repositories may be configured so that a user

is automatically activated after being inactivated. Refer to the chapter on users in the *Content Server Administration Guide* for information on how to configure this.

7. Click **Browse** next to **Source** to browse to the location of the LDIF file containing information for creating the new users.
8. Select a **User Source** from the list.
9. In the other fields, specify any attribute values that apply to all the users you are importing. Values specified in the input file override values specified on this page.
10. Indicate whether to overwrite or ignore user information for any users who already exist.
11. Click **Finish**.

Import user attributes

The following table describes the import user attributes.

Table 25. Import user attributes

Field label	Value
State	Indicates the state for the users you are importing. <ul style="list-style-type: none">• Active: The user is a currently active repository user. Active users are able to connect to the repository.• Inactive: The user is not currently active in the repository. Inactive users are unable to connect to the repository. A user may be made inactive because of multiple authentication failures or through resetting the state manually. Repositories may be configured so that a user is automatically activated after being inactivated. Refer to the chapter on users in the <i>Content Server Administration Guide</i> for information on how to configure this. If the user is a Superuser, only another Superuser can reset the user's state.
Source	The name of an input file. Click Browse to browse to the location of the LDIF file containing information for creating the new users.

Field label	Value
User Source	<p>Specifies how to authenticate a given repository user's user name and password. Valid values are:</p> <ul style="list-style-type: none"> • None: Windows only. This means the user is authenticated in a Windows domain. • UNIX only: UNIX Content Servers only. The user is authenticated using the default UNIX mechanism, <code>dm_check_password</code> or other external password checking program. • Domain only: UNIX Content Servers only. The user is authenticated against a Windows domain. • UNIX first: UNIX Content Servers only. This is used for UNIX repositories where Windows domain authentication is in use. The user is authenticated first by the default UNIX mechanism; if that fails, the user is authenticated against a Windows domain. • Domain first: UNIX Content Servers only. This is used for UNIX repositories where Windows domain authentication is in use. The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default UNIX mechanism. • LDAP: The user is authenticated through an LDAP directory server. • Inline Password: The user must provide a password that is stored only in the repository. There is no external authentication. You must manually enter the password for each user authenticated with a password; the passwords cannot be imported in the LDIF file.
Description	A description for the user.
E-Mail Address	The user's email address for receiving notifications from the repository.
Windows Domain	(Windows only.) The domain name associated with the new user's Windows account.
Home Repository	The repository where the user receives tasks and notifications.

Field label	Value
User is global	If the user is being created in the governing repository of a federation, select to propagate the user's attributes to all members of the federation.
Default Folder	The default storage location for any object that the user creates. Depending on how you have set up your site, you may need to create a folder for the user.
Default Group	Choose a group name from the list.
	When the user creates an object in the repository, it belongs to the group name associated with the user's default permission set.
Default ACL	A permission set to use to assign the default permissions to objects created by the new user.
Db Name	The new user's username in the underlying RDBMS. The DB name is required only if the user will be a repository owner or a user who registers RDBMS tables.
Privileges	<p>Choose a user privilege from the list. User privileges authorize certain users to perform activities that are required to administer and maintain the system. The privilege levels are:</p> <ul style="list-style-type: none"> • None • Create Type • Create Cabinet • Create Cabinet and Type • Create Group • Create Group and Type • Create Group and Cabinet • Create Group, Cabinet, and Type • System Administrator • Superuser: If you grant Superuser privileges to a user, add that user manually to the group called admingroup. If you revoke a user's Superuser privileges, remove the user from the admingroup.

Field label	Value
Client Capability	Indicates what level of use is expected of the user. Choose the user type from the list: <ul style="list-style-type: none"> • Default • Consumer • Contributor • Coordinator • System Administrator
Alias Set	Select a default alias set
If user exists, then overwrite user information	If selected and a user exists in the repository, replace existing information with imported information.
If user exists, then ignore information	If selected and a user exists in the repository, retain existing information.

Deleting users

You can remove users from the repository, but Documentum strongly recommends making users inactive or reassigning them rather than deleting them from the repository.

When you delete a user, the server does not remove the user's name from objects in the repository such as groups and ACLs. Consequently, when you delete a user, you must also remove or change all references to that user in objects in the repository. To reassign a user's objects to another user, use the instructions in [Reassigning objects to another user, page 202](#).

You can delete a user and then create a user with the same name. If you add a new user with the same name as a deleted user and have not removed references to the deleted user, 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.

To delete users:

1. Navigate to **Administration > User Management > Users**.
2. Select the users to delete by checking the check boxes next to their names.
3. Select **File > Delete**.
4. Click **Finish**.

Reassigning objects to another user

If deleting a user from the repository or making the user inactive and you want objects owned by the user assigned to another user, use these instructions. In addition, if you want to rename a user, create a new user and then assign the existing user's objects to that user. This is the only way to change a user's name.

To reassign objects to another user:

1. Navigate to **Administration > User Management > Users**.
2. Select the user whose objects are being reassigned and then select **Tools > Reassign User**.
The Reassign User page is displayed.
3. Enter information on the **Reassign Userpage**:
 - a. **Name**: Displays the name of the current repository.
 - b. **Reassign**: Type the name of the user to which to reassign the current user's objects or click **Select User**.
 - c. **Run the Reassign job**: Select when to run the reassign job. Options are **At next job execution** and **Now**.
 - d. **Checked Out Objects**: Indicate whether to unlock check-out objects or ignore them.
 - e. **Report Results**: Indicate whether to save changes and report results or just report results.
4. Click **OK**.

Changing the home repository of a user

The home repository is where users receive tasks and notifications in their inboxes.

To change a home repository:

1. Navigate to **Administration > User Management > Users**.
2. Select the user for whom you want to change the home repository.
3. Select **Tools > Change Home Repository**.
4. From the list, select the user's new home repository.
5. Indicate whether to run the job that changes the home repository when it is next scheduled or to run the job now.
6. Click **OK**.

Making a user active or inactive

Changing a user's state from active to inactive is an alternative to deleting the user from the repository. If the user is a Superuser, only another Superuser can reset the user's state.

To change a user from active to inactive or inactive to active:

1. Navigate to **Administration > User Management > Users**.
2. Select the user and then select **View > Properties > Info** to access the User Properties - Info page..
3. To make an active user inactive, select **Inactive** from the **State** drop-down list.
4. To make an inactive user active, select **Active** from the **State** drop-down list.
5. Click **OK**.

Modifying users

Use these instructions to modify the attributes of an existing user. If a user is authenticated by an LDAP server, only a Superuser can modify the user's LDAP-mapped attributes.

To modify a user:

1. Navigate to **Administration > User Management > Users**.
2. Select the user and then select **View > Properties >Info** to access the User Properties - Info page.
3. Modify the attributes you want to change.
For information about the user attributes, refer to [User attributes, page 191](#)
4. Click **OK**.

Viewing groups, workflows, alias sets, permission sets, and documents of a user

Use these instructions to determine the groups to which a user belongs.

To view the groups, workflows, permission sets, alias sets, or documents of a user:

1. Navigate to **Administration > User Management > Users**.
2. Select the user and then select **View > View Current User Memberships**.
3. From the list, select **Groups, Acl, Alias Sets, Documents, Workflows, or All**.
4. Click the user navigation path at the top of the screen to return to the User list page.

Viewing or deleting change home repository logs

Use these instructions to view or delete the logs generated by changing a user's home repository.

To view or delete change home repository logs:

1. From the User list page, click **View > Change Home Repository Logs**.
2. To view a log, click the job request ID of the job.

3. To delete a log, select the log and the select **File > Delete**.
4. To exit viewing the log, click **OK**.
5. To exit the log list page, click **Users** in the navigation trail at the top of the right pane.

Viewing user reassign logs

Use these instructions to view or delete the logs generated by reassigning a user's objects to another user.

To view the user reassign logs:

1. From the User list page, select **View > Reassign Logs**.
The Reassign Logs list page is displayed. The list page tells you:
 - The job request ID
 - The users old and new names
 - Whether the job generated a report only or proceeded with the reassign operation
 - Whether locked objects were unlocked
 - Whether the request was completedYou can sort on each column.
2. To view a log, click the job request ID for the rename job.
If the job request ID is not a clickable link, a log was not generated for the job.
3. To delete a log, select the log and then click **File > Delete**.
4. To exit viewing the log, click **OK**.
5. To exit the log list page, click **Users** in the navigation path at the top of the right pane.

Reassign reports

This page displays reassign logs, including group and user reassign logs.

Groups

A group represents multiple repository users, and can contain groups, users, or roles. By default, a group is owned by the user who creates the group. Groups can be public or private. By default, groups created by a user with Create Group privileges are private, while groups created by a user with System Administrator or Superuser privileges are public.

A group can be a *dynamic* group. A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. For more information on dynamic groups, refer to [About dynamic groups, page 206](#).

To create or modify groups, you must have privileges as shown in the following table:

Table 26. Privileges for creating or modifying groups

Privilege	Create	Modify	Delete
Create Group	Can create group or assign ownership to a group to which the user belongs	Can add or delete members and assign ownership to a group to which the user belongs	Can delete groups the user owns, including groups where a group is owner and the user is a member of the group
Sysadmin	Can create group or assign ownership to a group to which the user belongs	Can update group administrator, owner, or members of a group	Can delete groups the user owns, including groups where a group is owner and the user is a member of the group
Superuser	Can create a group and assign ownership to a different user or group	Can update group administrator, owner, or members of a group	Can delete any group

A group can own sysobjects and permission sets.

The name assigned to a group must consist of characters that are compatible with Content Server's server **OS code page**.

If you create a role as a domain, it is listed on the groups list, not the roles list.

To jump to a particular group, type the first few letters of its object name in the **Starts with** box and click **Search**. To view a list of all groups beginning with a particular letter, click that letter. To view a different number of groups than the number currently displayed, select a different number in the **Show Items** list.

To view the members of a group, click the group's name.

From this page, you can find instructions for:

- [About dynamic groups, page 206](#)
- [Locating groups, page 206](#)
- [Viewing where a group is used, page 206](#)
- [Creating groups, page 207](#)
- [Modifying or viewing groups, page 208](#)
- [Adding users, groups, or roles to a group, page 208](#)
- [Removing users from a group, page 209](#)
- [Deleting groups, page 209](#)
- [Reassigning the objects owned by a group, page 210](#)
- [Viewing group reassign logs, page 210](#)
- [Group attributes, page 210](#)

About dynamic groups

A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. A dynamic group is created and populated with members like any other group. Whether or not a group is dynamic is part of the groups definition. It is recorded in the `is_dynamic` attribute and may be changed after the group is created. (In this application, `is_dynamic` is the field labeled **Dynamic Group**.)

When a session is started, whether Content Server treats a user in a dynamic group as an actual member is dependent on two factors:

- The default membership setting in the group object
- Whether the application from which the user is accessing the repository requests that the user be added or removed from the group

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 Content 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. For more information on dynamic groups, refer to the *Content Server Administration Guide*.

Locating groups

Use these instructions to locate groups in a repository.

To locate groups:

1. Connect to a repository.
2. Navigate to **Administration > User Management > Groups** to access the Groups list page.
The first ten groups in the repository are displayed.
3. To jump to a particular group or to groups starting with a particular string, type the string in the **Starts with** field and click **Search**.
4. To see more groups, click the **Forward** or **Back** buttons or click a letter corresponding to the first letter of a group.
5. To change the number of groups displayed, select a different number from the **Show Items** list.

Viewing where a group is used

Use these instructions to see where a group is used.

To view where a group is used:

1. Select the correct group.
2. Select **View > View Current Group Memberships**.

Creating or modifying groups

Click the links below for instructions on:

- [Creating groups, page 207](#)
- [Modifying or viewing groups, page 208](#)

Creating groups

Use these instructions to create new groups.

To create groups:

1. Navigate to **Administration > User Management > Groups** to access the Groups list page.
2. Select **File > New > Group** to access the New Group - Info page.
3. Enter information on the **New Group - Info** page:
 - a. **Name:** Type the name of the new group.
 - b. **Group Native Room:** Select the group's native room. This field appears only if the rooms feature of Collaborative Services is enabled.
 - c. **E-Mail Address:** Type an email address for the group. This is typically the email address of the group's owner.
 - d. **Owner:** Click **Select** to access the Choose a user/group page to select an owner of the group.
 - e. **Administrator:** Click **Select** to access the Choose a user/group page to select an administrator of the group.
 - f. **Alias Set:** Click **Select** to access the Choose an alias set page to select an alias set for the group.
 - g. **Group is Global:** Select if connected to the governing repository of a federation and the group must be a global group.
 - h. **Description:** Optionally, type a description of the group.
 - i. **Private:** Select to make the group a private group. A group with Private enabled can be updated only by a user who is the owner of the group or is listed as the group administrator of the group. A group with Private not enabled can be updated by a user with System Administrator privileges as well as by the group owner or administrator. A Superuser can update any group, regardless if Private is enabled or not.
 - j. **Dynamic:** Select to make the group a dynamic group. A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The

members of a dynamic group comprise of the set of users who are allowed to use the group; but a session started by one of those users will behave as though it is not part of the group until it is specifically requested by the application.

For more information about dynamic groups, refer to [About dynamic groups, page 206](#).

- k. **Protected:** Select to prevent adding or deleting members. Use of a protected dynamic group is limited to applications running with a DFC installation that has been configured as privileged through the Documentum Administrator client rights administration.

The Protected Group checkbox is enabled only if Dynamic Group is selected.

4. Click **OK**.

Modifying or viewing groups

To modify a group, you must be the group's owner, a Superuser, a member of the group that owns the group to be modified, or identified in the group's group_admin attribute, either as an individual or as a member of a group specified in the attribute. Use these instructions to modify groups.

To modify or view a group:

1. Navigate to **Administration > User Management > Groups** to access the **Groups** list page.
2. Select the correct group and then select **View > Properties > Info** to access the **Groups Properties - Info** page.
3. Modify the group's attributes if you have sufficient permissions.
Refer to [Group attributes, page 210](#) for information about the group attributes.
4. Click **OK**.

Adding users, groups, or roles to a group

A group can contain users, other groups, or roles. Use these instructions to add users, groups, or roles to a group.

To add users to a group:

1. Navigate to **Administration > User Management > Groups** to access the **Groups** list page.
2. To filter the list, select **Only Groups**, **Only Users**, or **Only Roles** from the list.
3. Select the name of the group to which you want to add users and then select **File > Add Members**.
4. To jump to a particular user, group, or role, type the name in the text box and click **Go**.
5. To filter the page, select one of the following:
 - **Show Users, Groups, And Roles**
 - **Show Users**
 - **Show Groups**

- **Show Roles**
 - **Show Private Groups and Roles**
6. Select the names of the users, groups, or roles you are adding to the group.
 7. Click the right arrow.
The members are moved to the right-hand side of the page.
 8. Click **OK**.

Removing users from a group

Use these instructions when users must be removed from a group.

To delete users from a group:

1. Navigate to **Administration > User Management > Groups** to access the **Groups** list page.
2. To filter the list, select **Only Groups**, **Only Users**, or **Only Roles** from the list.
3. Click the group from which you want to delete users.
4. Select the names of the users you are deleting from the group.
5. Select **File > Remove Member(s)**.

Deleting groups

You can delete a group if you are the group's owner, a Superuser, a member of the group that owns the group to be deleted, or identified in the group's group_admin attribute, either as an individual or as a member of a group specified in the attribute. However, to preserve repository consistency, do not remove groups from the repository. Instead, remove all members of the group and leave the group in the repository, or reassign all objects owned by the group to another group or user and then delete the group.

To delete a group:

1. Navigate to **Administration > User Management > Groups** to access the **Groups** list page.
2. Select the name of the group you are deleting and then select **File > Delete**.
3. Click **OK** to confirm that you want to delete the group.

Reassigning the objects owned by a group

Use these instructions to reassign the objects owned by a group to another group.

To reassign a group:

1. Navigate to **Administration > User Management > Groups** to access the **Groups** list page.
2. Select the group you are reassigning and then select **Tools > Reassign**.
3. Type the name of the group to which this group's users and objects are being reassigned or click **Select** to select a group.
4. Indicate whether to run the reassign job at the next time the job is scheduled or now.
5. Indicate whether to unlock or ignore checked-out objects.
6. Indicate whether to save changes and report results or just report results.
7. Click **OK**.

Viewing group reassign logs

Use these instructions to view or delete the logs generated by reassigning the members of a group to another group.

1. From the groups list page, select **View > Reassign Logs**.
2. To view a log, click the job request ID.
If the job request ID is not a clickable link, no log was generated for the job.
3. To delete a log, select the log and then select **File > Delete**.
4. To exit viewing the log, click **OK**.

Group attributes

The following table lists the fields completed when you create or modify a group:

Table 27. Attributes of a group

Field label	Value
Name	The name of the new repository group.
Group Native Room	The group's native room. This field appears only if the rooms feature of Collaborative Services is enabled.

Field label	Value
E-Mail Address	The email address for the new group. If no value is entered in this field, the group email address defaults to the group name.
Owner	The name of a repository user who has the Create Group privilege and who owns this group. 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	Specifies a user or group, in addition to a Superuser or the group owner, who can modify the group. If this is null, only a Superuser and the group owner can modify the group.
Alias Set	The default alias set for the group.
Group is Global	Displayed only in the governing repository of a federation and the group must be a global group.
Description	A description of the group.
Private	Defines whether the group is private. If not selected, the group is created as a public group. A group with Private enabled can be updated only by a user who is the owner of the group or is listed as the group administrator of the group. A group with Private not enabled can be updated by a user with System Administrator privileges as well as by the group owner or administrator. A Superuser can update any group, regardless if Private is enabled or not.
Dynamic	Indicates if the group is a dynamic group. A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic group comprise of the set of users who are allowed to use the group; but a session started by one of those users will behave as though it is not part of the group until it is specifically requested by the application.

Field label	Value
Protected	<p>For more information about dynamic groups, refer to About dynamic groups, page 206.</p> <p>Indicates if the group is protected against adding or deleting members. Use of a protected dynamic group is limited to applications running with a DFC installation that has been configured as privileged through the Documentum Administrator client rights administration.</p> <p>The Protected checkbox does not appear in 5.3x repositories and is enabled only when Dynamic Group is selected.</p>

Roles

A role is a type of group that contains a set of users or other groups that are assigned a particular role within a client application domain. For information on roles and domains, refer to the section on security services in *Content Server Fundamentals*.

If you create a role as a domain, it is listed in the groups list, not the roles list.

To jump to a particular role, type the first few letters of its object name in the **Starts with** box and click **Search**. To view a list of all roles beginning with a particular letter, click that letter. To view a different number of roles than the number currently displayed, select a different number in the **Show Items** list.

This section describes the following:

- [Creating roles, page 213](#)
- [Adding users, groups, or roles to a role, page 214](#)
- [Modifying roles, page 214](#)
- [Reassigning roles, page 215](#)
- [Deleting roles, page 215](#)
- [Role attributes, page 215](#)

Creating or modifying roles

Click the links below for instructions on:

- [Creating roles, page 213](#)
- [Modifying roles, page 214](#)

Creating roles

Use the instructions in this section to create new roles.

To create roles:

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Select **File > New > Role** to access the **New Role - Info** page.
3. Enter information on the **New Role - Info** page:
 - a. **Name:** Type the name of the new repository role.
 - b. **Group Native Room:** Select a native room for the role. This field appears only if the rooms feature of Collaborative Services is enabled.
 - c. **E-Mail Address:** Type an email address for the role. This is typically the email address of the role's owner.
If no value is entered in this field, the role email address defaults to the role name.
 - d. **Owner:** Click **Select** to access the Choose a user/group page to select an owner of the role.
This is the name of a repository user who has the Create Group privilege and who owns this group.
 - e. **Administrator:** Click **Select** to access the Choose a user/group page to select a user or group as the administrator of the role.
If this is null, only a Superuser and the role owner can modify the role.
 - f. **Alias Set:** Click **Select** to access the Choose an alias set page to select an alias set for the role.
 - g. **Role is Global:** If the role is being created in the governing repository of a federation, select to propagate the role's attributes to all members of the federation.
 - h. **Description:** Optionally, provide a description of the role.
 - i. **Private:** Select to create the role as a private role. A role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A role with Private not enabled can be updated by a user with System Administrator privileges as well as by the role owner or administrator. A Superuser can update any role, regardless if Private is enabled or not.
 - j. **Create role as domain:** Select to create the role as a domain.
If you create the role as a domain, it is listed on the groups list, not the roles list.
 - k. **Dynamic:** Select to make the role a dynamic role. A dynamic role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic role comprise of the set of users who are allowed to use the role; but a session started by one of those users will behave as though it is not part of the role until it is specifically requested by the application.
 - l. **Protected:** Select to prevent adding or deleting members to the role. Use of a protected dynamic role is limited to applications running with a DFC installation that has been configured as privileged through the Documentum Administrator client rights administration.

4. To save the role and return to the **Roles** list page, click **OK**.

Adding users, groups, or roles to a role

Use these instructions to add users, groups, or roles to a role.

To add users, groups, or roles to a role:

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Click the role to which you want to add users.
The list page with members of the role is displayed.
3. To filter the list, select **Only Groups**, **Only Users**, or **Only Roles** from the list.
4. Click **File > Add Member(s)** to access the **Choose a user/group** page.
5. To jump to a particular user, group, or role, type the name in the text box and click **Go**.
6. To filter the page, select one of the following:
 - **Show Users, Groups, And Roles**
 - **Show Users**
 - **Show Groups**
 - **Show Roles**
 - **Show Private Groups and Roles**
7. Select the names of the users, groups, or roles you are adding to the role.
8. Click the right arrow.
The members are moved to the right-hand side of the page.
9. Click **OK**.

Modifying roles

Use these instructions to modify the attributes of an existing role.

Web Publisher users only: You can modify Web Publisher roles using XML files to change the functionality available to Web Publisher roles and to replace or add roles to your Web Publisher application. For further details on configuring Web Publisher roles, refer to the *Web Development Kit Applications Configuration Guide*.

To modify a role:

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Select the correct role and then select **View > Properties > Info**.
3. Modify the role's attributes.
[Role attributes, page 215](#) provides information on role attributes.

-
4. Click **OK**.

Reassigning roles

If you plan to delete a role, consider reassigning the users and other objects belonging to the role. Use these instructions to reassign the users and other objects.

To reassign a role:

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Select the name of the role you are reassigning and then select **Tools > Reassign**.
3. Type the name of the role or group to which this role's users and objects are being reassigned, or click **Select** to select a group.
4. Indicate whether to run the reassign job at the next time the job is scheduled or now.
5. Indicate whether to unlock or ignore checked-out objects.
6. Indicate whether to save changes and report results or just report results.
7. Click **OK**.

Deleting roles

Roles are a type of group. It is therefore recommended that you do not delete a role. Instead, remove all members of the role and leave the role in the repository. You can also reassign the members of the role to another role.

To delete a role:

1. Navigate to **Administration > User Management > Roles** to access the **Roles** list page.
2. Select the name of the role to delete.
3. Select **File > Delete**.
4. Click **OK**.

Role attributes

The following table lists the fields you complete to create or modify a role:

Table 28. Attributes of a role

Field label	Value
Name	The name of the repository role.

Field label	Value
Group Native Room	The native room for the role. The field appears only if the rooms feature of Collaborative Services is enabled.
E-Mail Address	The email address for the new role. This is typically the email address of the role's owner.
	If no value is entered in this field, the role email address defaults to the role name.
Owner	The name of a repository user who has the Create Group privilege and who owns this role.
Administrator	Specifies 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.
Alias Set	The default alias set for the role.
Description	A description of the role.
Private	Defines whether the role is private. If not selected, the role is created as a public role.
	A role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A role with Private not enabled can be updated by a user with System Administrator privileges as well as by the role owner or administrator. A Superuser can update any role, regardless if Private is enabled or not.
	By default, roles created by users with System Administration or Superuser privileges are public, and roles created by users with a lower user privilege level are private.
Create role as domain	Select to create a dm_group object with group_class as domain.
	This field only appears on the New Role - Info page.

Field label	Value
Dynamic	Indicates if the role a dynamic role. A dynamic role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic role comprise of the set of users who are allowed to use the role; but a session started by one of those users will behave as though it is not part of the role until it is specifically requested by the application.
Protected	Indicates if the role is protected against adding or deleting members. Use of a protected dynamic role is limited to applications running with a DFC installation that has been configured as privileged through the Documentum Administrator client rights administration. The Protected checkbox does not appear in 5.3x repositories and is enabled only when Dynamic Role is selected.

Module roles

Module roles are required by applications that run privileged escalations and they behave the same as roles with respect to memberships. Module roles are dm_group objects with group_class set to module role. Any user, group, or dynamic group can be a member of a module role.

By default, module roles are dynamic. A dynamic module role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic module role comprise of the set of users who are allowed to use the module role; but a session started by one of those users will behave as though it is not part of the module role until it is specifically requested by the application. Administrators should not modify module roles unless they are configuring a client that requires privileged escalations.

To jump to a particular module role, type the first few letters of its object name in the **Starts with** box and click **Search**. To view a list of all module roles beginning with a particular letter, click that letter. To view a different number of module roles than the number currently displayed, select a different number in the **Show Items** list.

This section describes the following:

- [Creating module roles, page 218](#)
- [Reassigning module roles, page 219](#)
- [Modifying module roles, page 219](#)

- [Deleting module roles, page 219](#)
- [Module role attributes, page 220](#)

Creating module roles

Use these instructions to create new module roles.

To create roles:

1. Navigate to **Administration > User Management > Module Roles** to access the **Modules Roles** list page.
2. Select **File > New > Module Role** to access the **New Module Role - Info** page.
3. Enter information on the **New Module Role - Info** page:
 - a. **Name:** Type the name of the new module role.
 - b. **E-Mail Address:** Type an email address for the module role. This is typically the email address of the module role's owner.
If no value is entered in this field, the module role email address defaults to the module role name.
 - c. **Group Native Room:** Select a native room for the module role. This field appears only if the rooms feature of Collaborative Services is enabled.
 - d. **Owner:** Click **Select** to access the Choose a user/group page to select the owner of the module role.
This is the name of a repository user who has the Create Group privilege and who owns this module role.
 - e. **Administrator:** Click **Select** to access the Choose a user/group page to select a user or group as the administrator of the module role.
If this is null, only a Superuser and the module role owner can modify the module role.
 - f. **Alias Set:** Click **Select** to access the Choose an alias set page to select an alias set for the module role.
 - g. **Module Role is Global:** If the module role is being created in the governing repository of a federation, select to propagate the module role's attributes to all members of the federation.
 - h. **Description:** Optionally, provide a description of the module role.
 - i. **Private:** Select to create the module role as a private module role. A role with Private enabled can be updated only by a user who is the owner of the role or is listed as the role administrator. A role with Private not enabled can be updated by a user with System Administrator privileges as well as by the role owner or administrator. A Superuser can update any role, regardless if Private is enabled or not.
 - j. **Protected:** Select to restrict the module role to be used only by applications running on a privileged client.
4. To save the module role and return to the **Module Roles** list page, click **OK**.

Reassigning module roles

If you plan to delete a module role, consider reassigning the users and other objects belonging to the module role. Use these instructions to reassign the users and other objects.

To reassign a module role:

1. Navigate to **Administration > User Management > Module Roles** to access the **Module Roles** list page.
2. Select the name of the module role you are reassigning and then select **Tools > Reassign**.
3. Type the name of the module role to which this module role's users and objects are being reassigned, or click **Select** to select a group.
4. Indicate whether to run the reassign job at the next time the job is scheduled or now.
5. Indicate whether to unlock or ignore checked-out objects.
6. Indicate whether to save changes and report results or just report results.
7. Click **OK**.

Modifying module roles

Use these instructions to modify the attributes of an existing module role.

To modify a module role:

1. Navigate to **Administration > User Management > Module Roles** to access the **Module Roles** list page.
2. Select the correct module role and then select **View > Properties > Info**.
3. Modify the module role's attributes.
4. Click **OK**.

Deleting module roles

Module Roles are a type of group. It is therefore recommended that you do not delete a module role. Instead, remove all members of the module role and leave the module role in the repository. You can also reassign the members of the module role to another module role.

To delete a module role:

1. Navigate to **Administration > User Management > Module Roles** to access the **Module Roles** list page.
2. Select the name of the module role to delete.
3. Select **File > Delete**.

4. Click **OK**.

Module role attributes

The following table lists the fields you complete to create or modify a module role:

Table 29. Attributes of a role

Field label	Value
Name	The name of the repository module role.
Group Native Room	The native room for the module role. The field appears only if the rooms feature of Collaborative Services is enabled.
E-Mail Address	The email address for the module role.
	If no value is entered in this field, the module role email address defaults to the module role name.
Owner	The name of a repository user who has the Create Group privilege and who owns this module role.
Administrator	Specifies a user or group, in addition to a Superuser or the module role owner, who can modify the module role. If this is null, only a Superuser and the module role owner can modify the module role.
Alias Set	The default alias set for the module role.
Module Role is Global	If the module role is being created in the governing repository of a federation, select to propagate the module role's attributes to all members of the federation.
Description	A description of the module role.
Private	Defines whether the module role is private. If not selected, the module role is created as a public module role.
	A module role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A module role with Private not enabled can be updated by a user with System Administrator privileges as well as by the role owner or administrator. A Superuser can update any

Field label	Value
	module role, regardless if Private is enabled or not.
Protected	Select to restrict the module role to be used only by applications running on a privileged client.

Sessions

A repository session is opened when an end user or application establishes a connection to a server. Each repository session has a unique ID.

During any single API session, an external application can have multiple repository sessions, each with a different repository or server or both.

A repository session is terminated when the end user explicitly disconnects from the repository or the application terminates.

You can use Documentum Administrator to monitor repository sessions only. It cannot monitor any other sessions (for example, eConnector for JDBC sessions).

The Sessions page lists sessions in the current repository. For each session, the name, Documentum Session ID, Database Session ID, Client Host, Start Time, time Last Used, and State are displayed. To view all sessions or user sessions, make a selection from the drop-down list. To view a different number of sessions, select a new number from the **Show Items** drop-down list. To view the next page of sessions, click the > button. To view the previous page of sessions, click the < button. To jump to the first page of sessions, click the << button. To jump to the last page, click >>.

For more information about sessions, see *Content Server Administration Guide*, and *Content Server Fundamentals*.

Use these procedures to view sessions and session logs or kill sessions:

- [Viewing user sessions, page 221](#)
- [Viewing user session information, page 222](#)
- [Viewing user session logs, page 223](#)
- [Killing user sessions, page 223](#)

Viewing user sessions

Use these instructions to view user sessions and details of user sessions. User session information that can be viewed includes the root process start time, root process ID, session ID, client library version, and how the user is authenticated.

To view user sessions:

1. Connect to the repository where you are viewing users sessions.
If you are viewing user sessions in a federation, connect to the governing repository.

2. Navigate to **Administration > Sessions**.
3. A list of current user sessions is displayed.
 - To view all sessions, select **All** from the drop-down list.
 - To view user sessions, select **User Sessions** from the drop-down list.

Viewing user session information

Use these instructions for viewing information about user sessions.

To view user session info:

1. On the Sessions list page, click the Session ID corresponding to the session for which you want to view session details.

The following session information is displayed:

Table 30. Session information

Field	Description
Root Process Start Date	The last start date for the server to which the session is connected
Root Process ID	The process ID of the server on its host
User Name	The session user
Client Host	The host from which the session is connected
Session ID	The ID of the current repository session
Database Session ID	The ID of the current database session
Session Process ID	The operating system ID of the current session process
Start Time	The time the session was opened
Last Used	The time of the last activity for the session
Session Status	The status of the current session
Client Library Version	The DMCL version in use
User Authentication	The authentication type
Shutdown Flag	An internal flag
Client Locale	The preferred locale for repository sessions started during an API session

2. Click **OK** or **Cancel** to return to the Sessions page.

Viewing user session logs

Use these instructions to view user session logs. Session logs provide information about the actions performed in a session.

To view user session logs:

1. From the Sessions list page, select the session whose sessions logs you want to view.
2. Select **View > Session Log**.
The session log is displayed.
3. Click **OK** or **Cancel** to return to the Session list page.

Killing user sessions

Use these instructions to kill user sessions.

To kill user sessions:

1. From the Sessions page, select the session you want to kill.
2. Select **Tools > Kill Session**.
The Kill Session page is displayed.
3. Indicate when to kill the session:
 - When the sessions has no open transactions
 - After the current request is completed
 - Immediately
4. Type a message to be sent to the session owner.
5. Click **OK**.

Security

A permission set (also known as access control lists, or ACLs) defines the object-level permissions applied to objects to which the permission sets are assigned.

The security chapter in the *Content Server Administration Guide* contains more information on how permission sets behave in the Documentum system.

Click the links below for information and instructions on:

- [Permissions overview, page 226](#)
 - [Object permissions, page 226](#)
 - [Folder security, page 228](#)
 - [Additional access control entries, page 229](#)
 - [Default alias sets, page 230](#)
- [How Content Server evaluates access to an object, page 230](#)
- [Locating a permission set, page 231](#)
- [Viewing where a permission set is used, page 232](#)
- [Creating a permission set, page 233](#)
 - [Copying a permission set, page 236](#)
- [Setting a user's basic and extended object permissions, page 236](#)
- [Viewing or modifying permission sets, page 237](#)
 - [Viewing or modifying a permission set, page 238](#)
 - [Adding users to permission sets, page 239](#)
 - [Deleting users from permission sets, page 241](#)
 - [Changing the permissions assigned to a user, page 241](#)
- [Permission set properties, page 242](#)
- [Deleting a permission set, page 246](#)

Permissions overview

This section describes the following:

- Object permissions, page 226
- Folder security, page 228
- Additional access control entries, page 229
- Default alias sets, page 230

Object permissions

Access to folders and documents in a repository is subject to an organization's security restrictions. All content in the repository is associated with object permissions, which determines the access users have to each object in the repository such as a file, folder, or cabinet and governs their ability to perform specific actions. There are two categories of object permissions:

- Basic: Required for each object in the repository
- Extended: Optional

Basic permissions grant the ability to access and manipulate an object's content. The seven basic permission levels are hierarchical and each higher access level includes the capabilities of the preceding access levels. For example, a user with Relate permission also has Read and Browse.

Table 31. Basic permissions

Basic permission	What it allows
None	No access to the object is permitted.
Browse	Users can view the object's properties but not the object's content.
Read	Users can view both the properties and content of the object.
Relate	Users can do the above and add annotations to the object.
Version	Users can do the above and modify the object's content and check in a new version of the item (with a new version number). Users cannot overwrite an existing version or edit the item's properties.
Write	Users can do the above and edit object properties and check in the object as the same version.
Delete	Users can do all the above and delete objects.

Extended permissions are optional, grant the ability to perform specific actions against an object, and are assigned in addition to basic permissions. The six levels of extended permissions are not hierarchical, so each must be assigned explicitly. Only System Administrators and Superusers can grant or modify extended permissions.

Table 32. Extended permissions

Extended permission	What it allows
Execute Procedure	Superusers can change the owner of an item and use Execute Procedure to run external procedures on certain object types. A procedure is a Docbasic program stored in the repository as a dm_procedure object.
Change Location	Users can move an object from one folder to another in the repository. A user also must have Write permission to move the object. To link an object, a user also must have Browse permission.
Change State	Users can change the state of an item with a lifecycle applied to it.
Change Permission	Users can modify the basic permissions of an object.
Change Ownership	Users can change the owner of the object. If the user is not the object owner or a Superuser, they also must have Write permission.
Extended Delete	Users can only delete the object. For example, you may want a user to delete documents but not read them. This is useful for Records Management applications where discrete permissions are common.

When a user tries to access an object, the Content Server first determines if the user has the necessary level of basic permissions. If not, extended permissions are ignored.

Permission sets (also known as access control lists, or ACLs) are configurations of basic and extended permissions assigned to objects in the repository that lists users and user groups and the actions they can perform. Each repository object has a permission set that defines the object-level permissions applied to it, including who can access the object. Depending on the permissions, users can create new objects; perform file-management actions such as importing, copying, or linking files; and start processes, such as sending files to workflows.

Each user is assigned a default permission set. When a user creates an object, the repository assigns the user's default permission set to that object. For example, if the default permission set gives all members of a department Write access and all other users Read access, then those are the access levels assigned to the object.

Users can change an object's access levels by changing the object's permission set. To do this, the user must be the object's owner (typically the owner is the user who created the object) or they must have Superuser privileges in the object's repository.

When a user modifies a permission set, it is saved as a permission set assigned to them. They can then apply the permission set to other objects in the repository.

The ability to modify permission sets depends on the user privileges in the repository:

- Users with Superuser privileges can modify any permission set in the repository. They can designate any user as the owner of a permission set, and change the owner of a permission set. This permission is usually assigned to the repository administrator.
- Users with System Administrator privileges can modify any permission set owned by them or by the repository owner. They can designate themselves or the repository owner as the owner

of a permission set they created and can change whether they or the repository owner owns the permission set. This permission is usually assigned to the repository administrator.

- Users with any privileges less than the Superuser or System Administrator privileges are the owner only of the permission sets they create. They can modify any permission set they own, but cannot change the owner of the permission set.

If you designate the repository owner as the owner of a permission set, that permission set is a System (or Public) permission set. Only a Superuser, System Administrator, or the repository owner can edit the permission set. If a different user is the owner of the permission set, it is a Regular (or Private) permission set. It can be edited by the owner, a Superuser, System Administrator, or the repository owner.

A user with Write or Delete permission can change which permission set is assigned to an object.

Security protects the information in each repository using object permissions to control access to cabinets, folders, documents, and other objects. Object permissions determine what actions users can perform on objects. Permissions can be added, removed, modified, or replaced, and set differently for different users.

The section on security in the *Content Server Administration Guide* contains additional information on permission sets.

If you use Documentum's Web Publisher and if the user does not assign the default permission set, the Content Server assigns a default permission set according to the setting in the `default_acl` property in the server config object.

Folder security

Folder security is an additional level of security that supplements the existing repository security. Implementing this security option further restricts allowable operations in a repository. Folder security prevents unauthorized users from adding documents to, removing documents from, or changing contents of secured folders. 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 move or delete an object from a folder.

Folder security only pertains to changing the contents in a folder. For example, a user with Browse permission on a folder can still check out and check in objects within the folder. The *Content Server Administration Guide* contains information about assigning folder security to a repository.

If you use Documentum's Web Publisher, and if folder security is used in a repository, any content files in the WIP state must have the same permission as the folder. To use the same folder permission, the administrator must ensure the lifecycle in WIP state does not apply any set ACL action. For example:

```
WIP - folder acl  
Staging - WP "Default Staging ACL"  
Approved - WP "Default Approved ACL"
```

The following table lists the actions affected by folder security.

Table 33. Permissions required under folder security

Action	Requires at least Write permission for:
Create an object	Cabinet or folder in which you create the new object
Import file(s) or folder	Cabinet or folder to which you import the file(s) or folder
Move an object	Both the cabinet or folder from which you remove the object and the destination folder or cabinet
Copy an object	Destination cabinet or folder
Link an object	Destination cabinet or folder
Unlink an object	Cabinet or folder from which you unlink the object
Delete one version of a document	The document's primary folder
Delete all versions of a document	The document's primary folder
Delete unused versions of a document	The document's primary folder
Consult the repository administrator to determine if folder security is enabled in the repository.	

Additional access control entries

When Trusted Content Services is enabled in a repository, additional access control entries are available. Set up the additional access control entries on the Permissions page under the Security node. The access control entries described in the following table are independent of each other, not hierarchical, and must be explicitly assigned.

Table 34. Additional access control entries

Access control entry	Effect of the entry
Access Restriction	An access restriction entry denies a user the right to the base object-level permission level specified in the entry. For example, if a user would otherwise have Delete permission as a member of a particular group, an access restriction might limit the user to, at most, Version permission. The user would therefore lose Write and Delete permissions.

Access control entry	Effect of the entry
Extended Restriction	An extended restriction entry denies a user or the members of a specified group the specified extended object-level permission. For example, if a user would otherwise have Change Permission rights as a member of a particular group, an extended restriction would remove that right.
Required Groups	A required group entry requires a user requesting access to an object governed by the permission set to be a member of the group identified in the entry. If there are entries for multiple groups, the user must be a member of all the groups before Content Server allows access to the object.
Required Group Set	A required group set entry requires a user requesting access to an object governed by the permission set to be a member of at least one group in the set of groups.

Default alias sets

The Content Server adds two default aliases to a permission set:

- **dm_owner** Represents the owner of the permission set.
- **dm_world** Represents all repository users.

Note: You cannot delete dm_owner or dm_world from a permission set.

How Content Server evaluates access to an object

When a user who is not an object's owner or a Superuser requests access to a SysObject, Content Server evaluates the entries in the object's permission set in the following manner:

1. Checks for a basic access permission or extended permission entry that gives the user the requested access level (Browse, Read, Write, and so forth)

Note: Users are always granted Read access if the user owns the document, regardless of whether there is an explicit entry granting Read access or not.

2. Checks for no access restriction or extended restriction entries that deny the user access at the requested level.

A restricting entry, if present, can restrict the user specifically or can restrict access for a group to which the user belongs.

3. If there are required group entries, the server checks that the user is a member of each specified group.
4. If there are required group set entries, the server checks that the user is a member of at least one of the groups specified in the set.

If the user has the required permission, with no access restrictions, and is a member of any required groups or groups sets, the user is granted access at the requested level.

When a user is an object's owner, Content Server evaluates the entries in the object's permission set in the following manner:

1. Checks if the owner belongs to any required groups or a required group set.
If the owner does not belong to the required groups or group set, then the owner is allowed only Read permission as their default base permission, but is not granted any extended permissions.
2. Determines what base and extended permissions are granted to the owner through entries for dm_owner, the owner specifically (by name), or through group membership.
3. Applies any restricting entries for dm_owner, the owner specifically (by name), or any groups to which the owner belongs.
4. The result constitutes the owner's base and extended permissions.
 - If there are no restrictions on the base permissions of the owner and the dm_owner entry does not specify a lower level, the owner has Delete permission by default.
 - If there are restrictions on the base permission of the owner, the owner has the permission level allowed by the restrictions. However, an owner will always have at least Browse permission; they cannot be restricted to None permission.
 - If there are no restrictions on the owner's extended permissions, they have, at minimum, all extended permissions except delete_object by default. The owner may also have delete_object if that permission was granted to dm_owner, the user specifically (by name), or through a group to which the owner belongs.
 - If there are restrictions on the owner's extended permissions, then the owner's extended permissions are those remaining after applying the restrictions.

When Content Server evaluates a Superuser's access to an object, the server does not apply AccessRestriction, ExtendedRestriction, RequiredGroup, or RequiredGroupSet entries to the Superuser. A Superuser's base permission is determined by evaluating the AccessPermit entries for the user, for dm_owner, and for any groups to which the user belongs. The Superuser is granted the least restrictive permission among those entries. If that permission is less than Read, it is ignored and the Superuser has Read permission by default.

A Superuser's extended permissions are all extended permits other than delete_object plus any granted to dm_owner, the Superuser by name, or to any groups to which the Superuser belongs. This means that the Superuser's extended permissions may include delete_object if that permit is explicitly granted to dm_owner, the Superuser by name, or to groups to which the Superuser belongs.

Locating a permission set

Use the instructions in this section to locate permission sets.

To locate a permission set:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. To view a specific permission set type:
 - Select **Current User's Permission Sets** to view only your permission sets.
 - Select **System Permission Sets** to view only system permission sets.
 - Select **Manually Created** to view only manually-created permission sets.
 - Select **Auto Generated** to view only automatically-created permission sets.

Viewing where a permission set is used

Use the instructions in this section to locate the objects that use a particular permission set.

To view where a permission set is used:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Locate and select a permission set.
3. Select **View > Associations**.
The **Permission Set Associations** page appears that displays a list of documents that use the permission set.
4. To view sysobjects or users who use the permission set, select that object type from the list.

Creating or modifying permission sets

Use the Info and Permissions pages under the Security node to create, view, or modify permission sets. Click the links for instructions on:

- [Creating a permission set, page 233](#)
 - [Copying a permission set, page 236](#)
- [Setting a user's basic and extended object permissions, page 236](#)
- [Viewing or modifying permission sets, page 237](#)
 - [Viewing or modifying a permission set, page 238](#)
 - [Adding users to permission sets, page 239](#)

-
- [Deleting users from permission sets, page 241](#)
 - [Changing the permissions assigned to a user, page 241](#)

Creating a permission set

Use the instructions in this section to create new permission sets.

Before a permission set is saved, it is validated as follows:

1. New accessors (users or groups) for permissions are evaluated to confirm they belong to all the required groups and at least one of the groups listed in the required group set.
2. New accessors for restrictions are evaluated to confirm that they belong to all the required groups and at least one of the groups listed in the required group set.
3. When new groups are added to a required group list, all accessors listed for both permissions and restrictions are evaluated and any accessors who do not belong to the newly added groups are flagged.
4. When new groups are added to a required group set list, all accessors listed for both permissions and restrictions are evaluated and any accessors who do not belong to the newly added groups are flagged.
5. When a user accesses the permissions tab in this application:
 - Accessors currently listed for both permissions and restrictions are evaluated.
 - Accessors who do not belong to all the groups in the required groups list and to at least one of the groups in the required group set are flagged.

If Trusted Content Services is not enabled, only steps 1 and 2 are performed. If Trusted Content Services is enabled, all five steps are performed.

To create a new permission set:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Select **File > New > Permission Set**.
The **New Permission Set - Info** page appears.
3. Enter general information on the **New Permission Set - Info** page:
 - a. **Name:** Type the name of the permission set.
 - b. **Description:** Type a description of the permission set.
 - c. **Owner:** Click **Select** to access the **Choose a user/group** page to select an owner of the permission set.
If you are connected as a Superuser or the repository owner, you can change who owns the permission set. If you are connected with user privileges other than Superuser or the repository owner, you are the owner.

- d. **Class:** Select a class for the permission set:
 - **Regular:** Select for the permission set to 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:** Select for the permission set to 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, and deleted only by the permission set owner (the user or group that creates it), 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.

4. Click **Next**.

The **New Permission Set - Permissions** page appears. The default access control entries are displayed:

- dm_owner: The owner of the permission set.
- dm_world: All repository users.

5. To add **Required Groups** in a repository where Trusted Content Services is enabled:
 - a. Click **Add** in the Required Groups section to access the **Choose a group** page.
 - b. Select all groups of which a user must be a member.
 - c. Click the right arrow.
 - d. Click **OK**.
6. To remove **Required Groups** in a repository where Trusted Content Services is enabled:
 - a. In the Required Groups section, select the groups.
 - b. Click **Remove**.
7. To add **Required Group Sets** in a repository where Trusted Content Services is enabled:
 - a. Click **Add** in the Required Group Sets section to access the **Choose a group** page.
 - b. Select the groups.
 - c. Click the right arrow.
 - d. Click **OK**.
8. To remove **Required Group Sets** in a repository where Trusted Content Services is enabled:
 - a. In the **Required Group Sets** section, select the groups.
 - b. Click **Remove**.
9. To add accessors (users or groups) to the permission set:
 - a. Click the **Add** link.
 - b. To select from all users or groups, click the **All** tab. To select from recently used users and groups, click the **Recently Used** tab.
 - c. Select the checkboxes adjacent to the users or groups to add, and then click **Add**.
To remove an item from the list of selected items, select the item's checkbox and click **Remove**.
 - d. Click **OK**.

- The Set Access Permission page appears. The section [Setting a user's basic and extended object permissions, page 236](#) contains more information about the Set Access Permission page.
- e. In the **Basic Permissions** area, select the access level.
 - f. In the **Extended Permissions** area, select the checkboxes of any extended permissions you want to add.
 - g. If you added multiple users, click **Next** to apply different permissions to each user. Otherwise click **OK**.
10. To edit a user or group's permissions levels:
- a. Select the checkboxes for the users or groups you want to edit permissions.
 - b. Click the **Edit** link.
- The Set Access Permission page appears. The section [Setting a user's basic and extended object permissions, page 236](#) contains more information about the Set Access Permission page.
- c. In the **Basic Permissions** area, select the access level.
 - d. In the **Extended Permissions** area, select the checkboxes of any extended permissions you want to add.
 - e. Click **OK**.
11. To remove users or groups, select the checkboxes for the users or groups. Click the **Remove** link.
12. To add **Access Restrictions** in a repository with Trusted Content Services enabled:
- a. Click **Add**.
 - b. Select users and groups whose rights must be restricted.
 - c. Click the right arrow.
 - d. Click **OK**.
- If there are validation conflicts, they are displayed along with reasons for the conflicts. Refer to the introductory section of this topic for information on how accessors are evaluated for conflicts.
- To continue despite the conflicts, click **OK**.
 - To resolve the conflicts, click **Cancel** and select new users or groups.
- e. Select the permission level to deny the accessor.
 - f. Select the extended permission level to deny the accessor.
 - g. Click **Next** to go on to the next accessor or **Finish** to apply the same restrictions to all accessors.
13. To delete or edit Access Restrictions, select the accessors and click **Remove** or **Edit**.
14. Click **OK**.

Copying a permission set

Use the instructions in this section to copy a permission set. You can copy a permission set ONLY if you are connected as a Superuser (**File > Save As...** option is visible ONLY to Superusers).

To copy a permission set:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Select a permission set that you want to copy.
3. Select the **File > Save As...** option.
The **Permission Set Properties** page appears.
4. Edit general information on the **Permission Set Properties - Info** page.
5. Click the **Permissions** tab to edit/assign permission sets for users/groups.
6. Click **OK**.

Setting a user's basic and extended object permissions

On the Set Access Permissions page, set the basic and extended permissions for a user.

To set a user's basic and extended permissions:

1. To set the user's basic permissions, select the correct level from the **Basic Permissions** drop-down list.

The permission levels are cumulative; that is, a user with Read permission on an object can read an associate content file and also view the object's properties. The permission levels are:

- **None**

No access is permitted to the item.

- **Browse**

Users can view the item's properties but not the item's content.

- **Read**

Users can view both the properties and content of the item.

- **Relate**

Users can do the above plus they can add annotations to the item.

- **Version**

Users can do the above plus they can modify the item's content and they can check in a new version of the item (with a new version number). Users cannot overwrite an existing version or edit the item's properties.

- **Write**

Users can do the above plus they can edit item properties and check in the item as the same version.

- **Delete**

Users can do all the above and delete items.

2. To set the user's extended permissions, select the appropriate checkboxes.

The extended user permissions are not cumulative. The extended permission levels are:

- **Execute Procedure**

Superusers can change the owner of an item and can use Execute Procedure to run external procedures on certain item types. A procedure is a Docbasic program stored in the repository as a dm_procedure object.

- **Change Location**

Users with Change Location permissions can move an item in the repository. A user must also have Write permission to move the object. To link an object, a user must also have Browse permission.

- **Change State**

Users with Change State permissions can change the state of an item with a lifecycle applied to it.

- **Change Permission**

Users with Change Permissions can modify the basic permissions of an item.

- **Change Ownership**

Users with Change Ownership permissions can change the owner of the item. If the user is not the object owner or a Superuser, the user must also have Write permission.

- **Extended Delete**

Users with the Delete Object extended permission have the right only to delete the object. For example, you may want a user to delete documents but not read them. This is useful for Records Management applications where discrete permissions are common.

3. Click **Next** to assign the permissions of the next accessor, **Finish** to assign the same permissions to all accessors whose permissions you are changing, or **Cancel** to exit the operation without saving any changes.

Viewing or modifying permission sets

This section discusses how to:

- Viewing or modifying a permission set, page 238
- Adding users to permission sets, page 239
- Deleting users from permission sets, page 241
- Changing the permissions assigned to a user, page 241

Viewing or modifying a permission set

To view or modify a permission set:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Select the permission set you want to view or modify and then select **View > Properties > Info**.
The **Permission Set Properties - Info** page appears.
3. Edit properties on the **Permission Set Properties - Info** page.
The section [Permission set properties, page 242](#) contains more information about the page properties.
4. Click the **Permissions** tab to access the **Permission Set Properties - Permission** page.
Documentum Administrator displays the list of users and groups given permissions by the permission set. For each user or group, Documentum Administrator displays the permissions and extended permissions given.
The section [Permission set properties, page 242](#) contains more information about the Permissions page properties.
5. To add **Required Groups** in a repository where Trusted Content Services is enabled:
 - a. Click **Add** in the Required Groups section.
 - b. Select all groups in which a user must be a member.
 - c. Click the right arrow.
 - d. Click **OK**.
6. To remove **Required Groups** in a repository where Trusted Content Services is enabled:
 - a. In the **Required Groups** section, select the groups.
 - b. Click **Remove**.
7. To add **Required Group Sets** in a repository where Trusted Content Services is enabled:
 - a. Click **Add** in the Required Group Sets section.
 - b. Select the groups.
 - c. Click the right arrow.
 - d. Click **OK**.
8. To remove **Required Group Sets** in a repository where Trusted Content Services is enabled:
 - a. In the **Required Group Sets** section, select the groups.
 - b. Click **Remove**.
9. To add users or groups (accessors) to the selected permission set, do the following. You must have adequate permission levels to add users or groups to the permission set:
 - a. To add users or groups, click **Add**.
 - b. To select from all users or groups, click **All**. To select from recently used users and groups, click **Recently Used**.

- c. Select the users or groups to add and click **Add**. To remove an item from the list of selected items, select them and then click **Remove**.
 - d. Click **OK**.

The Set Access Permission page appears. The section [Setting a user's basic and extended object permissions, page 236](#) contains more information about the Set Access Permission page.
 - e. In the **Basic Permissions** area, select the access level.
 - f. In the **Extended Permissions** area, select the checkboxes of any extended permissions to add.
 - g. If you added multiple users or groups, click **Next** to apply different permissions to each. When you are done, click **OK**.
10. To edit a user or group's permissions:
 - a. Select the users or groups you want to edit permissions.
 - b. Click the **Edit** link.

The Set Access Permission page appears. The section [Setting a user's basic and extended object permissions, page 236](#) contains more information about the Set Access Permission page.
 - c. In the **Permission** area, select the access level.
 - d. In the **Extended Permissions** area, select the checkboxes of any extended permissions you want to add.
 - e. Click **OK**.
 11. To add **Access Restrictions** in a repository with Trusted Content Services enabled:
 - a. Click **Add**.
 - b. Select users and groups whose rights must be restricted.
 - c. Click the right arrow.
 - d. Click **OK**.

If there are validation conflicts, they are displayed along with reasons for the conflicts.

 - To continue despite the conflicts, click **OK**.
 - To resolve the conflicts, click **Cancel** and select new users or groups.
 - e. Select the permission level to deny the accessor.
 - f. Select the extended permission level to deny the accessor.
 - g. Click **Next** to go on to the next accessor or **Finish** to apply the same restrictions to all accessors.
 12. To delete or edit Access Restrictions, select the accessors and click **Remove** or **Edit**.
 13. To remove users or groups, select the users or groups and then click Remove..
 14. Click **OK**.

Adding users to permission sets

Use the instructions in this section to add users to a permission set.

To add users to an existing permission set:

1. Navigate to **Administration > Security**.

The **Permission Sets** list page appears.

2. Select the permission set to modify and then select **View > Properties > Info**.

The Info page appears where you can edit the description or change the class of the permission set.

3. Click the **Permissions** tab.

The Permissions page appears.

4. In the **Grant access to** section, click **Add**.

The first set of users, groups, and roles in the repository is displayed on the **Choose a user/group** page.

To view more users, groups, and roles, click the navigation arrows.

To display only users, groups, or roles, select **Show Users**, **Show Groups**, or **Show Roles**.

5. Select the users, groups, or roles to add to the permission set.

- a. Select the checkbox next to the names of any users, groups, or roles to add to the permission set.

- b. Click the **Add** arrow.

- c. Click **OK** or **Cancel**.

- Click **OK** to add the users, groups, and roles to the permission set.

The system displays the **Set Access Permission** page.

- Click **Cancel** to cancel the operation and return to the Permissions page.

6. On the Set Access Permission page, select the basic and extended permissions for each user, group, or role being added. The section [Setting a user's basic and extended object permissions, page 236](#) contains more information about the Set Access Permission page.

7. Click **Next, Finish, or Cancel**.

- Click **Next** to assign permissions to each individual user, group, or role.

- Click **Finish** to apply the changes to all the remaining users, groups, and roles.

The system displays the Confirm page with the message that proceeding will apply the changes to all the remaining selections. To apply individual changes to different selections, click **Cancel** and walk through the selections using the **Next** and **Previous** buttons.

- Click **Cancel** to cancel the operation and return to the Permissions page without adding any users, groups, or roles to the permission set.

Deleting users from permission sets

Use the instructions in this section to delete a user from a permission set.

To delete users from a permission set:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Select the permission set to modify and then select **View > Properties > Info**.
The Info page appears where you can edit the description or change the class of the permission set.
3. Click the **Permissions** tab.
The Permissions page appears.
4. In the **Grant access to** section, select the checkbox next to the users to delete.
5. Click **Remove**.
6. Click **OK** or **Cancel**.
 - Click **OK** to delete the users from the permission set.
 - Click **Cancel** to cancel the operation and return to the Permission Sets list page without deleting users from the permission set.

Changing the permissions assigned to a user

Use the instructions in this section to change a user's permissions in a permission set.

To change the permissions of a user:

1. Navigate to **Administration > Security**.
The **Permission Sets** list page appears.
2. Select the permission set to modify and then click **View > Properties > Info**.
The Info page appears.
3. Click the **Permissions** tab.
The Permissions page appears.
4. In the **Grant access to** section, select the users to modify.
5. Click **Edit**.
The **Set Access Permission** page appears
6. Change the user permissions.
7. Click **OK**, **Previous**, **Next**, **Finish**, or **Cancel**.
 - Click **OK** to apply the changes to the permission set and return to the Permissions page.
 - Click **Next** or **Previous** to assign different permissions to the next or previous user.
 - Click **Finish** to apply the changes to all remaining users.

The system displays the Confirm page with the message that proceeding will apply the changes to all the remaining selections. To apply individual changes to different selections, click **Cancel** and walk through the selections using the **Next** and **Previous** buttons.

- Click **Cancel** to cancel the operation and return to the Permissions page without changing the permission set.

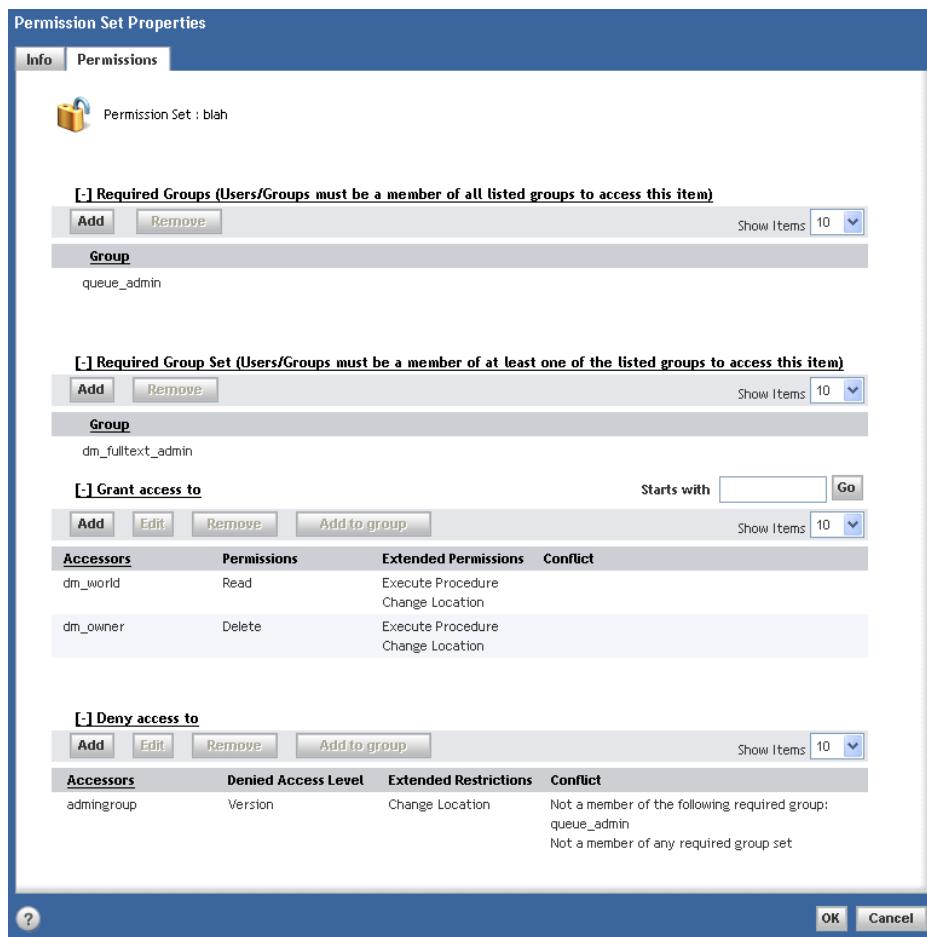
Note: The **OK** and **Cancel** buttons appear when only one checkbox is selected in the **Grant access to** section on the Permissions page. If more than one checkbox is selected, the **Previous**, **Next**, **Finish**, and **Cancel** buttons appear.

8. Click **OK** or **Cancel** on the Permissions page.
 - Click **OK** to save the changes made to the permission set.
 - Click **Cancel** to cancel the operation and return to the Permission Sets list page without deleting users from the permission set.

Permission set properties

This section describes the field values for:

- New Permission Set - Info page
- Permission Set Properties - Info page
- New Permission Set - Permissions page
- Permission Set Properties - Permissions page

Figure 18. Permission Set Properties - Permissions page**Table 35. New Permission Set - Info and Permission Set Properties - Info page properties**

Field label	Value
Name	(Required) The name of the permission set.
Description	A description of the permission set.
Owner	Indicates who owns the permission set. <ul style="list-style-type: none"> • If connected as a Superuser or the repository owner, you can change who owns the permission set. • If creating a permission set and connected with user privileges other than Superuser or the repository owner, you are the owner.

Field label	Value
Class	From the list, select a class for the permission set. <ul style="list-style-type: none"> • Regular: A permission set 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: A permission set 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 and deleted only by the permission set owner (the user or group that creates it), 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.
Next	Click to continue to the Permissions page.
Cancel	Click to cancel creating or modifying a permission set and return to the Permission Sets list page without saving any changes.

Table 36. New Permission Set - Permissions and Permission Set Properties - Permissions page properties

Field label	Value
Required Groups	A required group entry requires a user requesting access to an object governed by the permission set to be a member of the group identified in the entry. If there are entries for multiple groups, the user must be a member of all of the groups before Content Server allows access to the object. Click Add to access the Choose a group page to add groups to the permission set, of which a user must be a member for repositories where Trusted Content Services is enabled. Select a group and click Remove to remove a required group.
Group	Displays groups of which a user must be a member for repositories where Trusted Content Services is enabled. If no groups are defined, the system displays the message No Required Groups exist for the permission set.
Required Group Set	A required group set entry requires a user requesting access to an object governed by the permission set to be a member of at least one group in the set of groups. Click Add to access the Choose a group page to add groups to the permission set, of which a user must be a member of at least one for repositories where Trusted Content Services is enabled. Select a group and click Remove to remove a group set.

Field label	Value
Group	Displays groups of which a user must be a member of at least one for repositories where Trusted Content Services is enabled. If no groups are defined, the system displays the message No Required Groups exist for the permission set.
Grant access to	<p>The Content Server automatically adds dm_owner and dm_world to a permission set. The default alias dm_owner represents the owner of the permission set and dm_world represents all repository users. You cannot delete dm_owner or dm_world from a permission set.</p> <ul style="list-style-type: none"> • Click Add to add users or groups and their permissions for the permission set.
	<ul style="list-style-type: none"> • Select a user and click Edit to modify basic or extended permissions. • Select a user and click Remove to delete a user or group from the permission set. • Select a user and click Add to group to add them to access the Add to Group page.
Accessors	Displays users and groups who are included in the permission set.
Permissions	Displays the basic permission level access for the user or group. To change the basic permission level access, select a user and click Edit .
Extended Permissions	Displays the extended permissions for the user or group. To change the extended permissions, select a user and click Edit .
Conflict	<p>If there are validation conflicts, the system displays reasons for the conflicts. For example:</p> <ul style="list-style-type: none"> • Not a member of the following required group: Indicates which required groups that a user currently does not have any membership to. • Not a member of any required group set: Indicates that the user currently is not a member of any group in the required group set.

Field label	Value
Deny access to	<p>An access restriction entry denies a user the right to the base object-level permission level specified in the entry. For example, if a user would otherwise have Delete permission as a member of a particular group, an access restriction might limit the user to, at most, Version permission. The user would therefore lose Write and Delete permissions.</p> <ul style="list-style-type: none"> Click Add to add users or groups to restrict their permissions for the permission set. Select a user and click Edit to modify basic or extended permission restrictions. Select a user and click Remove to delete an access restriction entry. Select a user and click Add to group to access the Add to Group page to add the user to a group or group set.
Accessors	Displays users and groups who have restricted permissions in the permission set.
Denied Access Level	Displays the restricted access level for the user or group. For example, if the user would otherwise have Delete permission as a member of a particular group and you set it to Version, the user loses Write and Delete permissions. To change the restricted basic permission level access, select a user and click Edit .
Extended Restrictions	Displays the extended restrictions for the user or group. To change the extended restrictions, select a user and click Edit .
Conflict	If there are validation conflicts, the system displays reasons for the conflicts.
Previous	Click to return to the Info page.
Finish	Click to save changes and return to the Permission Sets list page.
Cancel	Click to cancel creating or modifying a permission set and return to the Permission Sets list page without saving any changes.

Deleting a permission set

Use these instructions to delete permission sets. You cannot delete permission set templates using this application. To delete a permission set template, use Application Builder. The Application Builder documentation provides instructions on how to delete permission set templates.

To delete a permission set:

1. Navigate to **Administration > Security**.
2. Select the permission sets to delete.

3. Select **File > Delete**.
4. Click **OK**.

Audit Management

Auditing is a security feature that enables you to monitor events that occur in a repository or application. Auditing records information about events in an audit trail.

An *event* is something that happens to an object in the repository or an operation defined as an event by a user-written application. Events that happen to a repository object that are recognized by the server are called *system events*. Events defined and recognized only by user applications are called *user-defined events*.

An *audit trail* is a recorded history of the occurrence of repository events that have been marked for auditing. Each occurrence is recorded in one *audit trail entry*. Audit trail entries are stored in the repository as dm_audittrail objects. Auditing an event stores pertinent data, such as when the event occurred and what object was involved, in the audit trail object.

Content servers auditing support enables users to initiate automatic auditing for any system event. When an audited system event occurs, Content Server automatically generates the audit trail entry. Documentum provides a large set of system events. These events are associated with API methods, lifecycles (business policies), workflows, and jobs.

Audit trail entries are generated automatically after auditing is set up and can take up considerable space in the repository. Periodically, you should remove audit trail entries from the repository. If you have Purge Audit privileges, use the instructions below to remove the entries or run the PURGE_AUDIT administration method from the command line. The *Content Server DQL Reference Manual* contains more information on PURGE_AUDIT.

Extended privileges govern whether and how a repository user can use audit management:

- Config Audit

A user with Config Audit extended privileges can register events for auditing.

- View Audit

A user with View Audit extended privileges can search and view existing audit trail entries.

- Purge Audit

A user with Purge Audit extended privileges can delete audit trail entries from the repository.

A user can have no extended audit privileges or can have any combination of the above three privilege levels; for example, a user might have View Audit and Config Audit privileges. That user would be able to register events for auditing and view audit trail entries, but could not remove them from the repository.

If any of the links to auditing functions are not enabled, you do not have the correct extended privileges for those functions.

Audit trail entries can be signed by Content Server. Signing an entry increases security by making it possible to detect whether the entry was changed after it was saved to the repository. An audit trail entry that has been signed can be verified when the entry is viewed.

The *Content Server Administration Guide* for your server version contains additional information on auditing.

A user can have no extended audit privileges or can have any combination of the three privilege levels; for example, a user might have View Audit and Config Audit privileges. These privileges are set when a user is created or modified. The section [Users, page 184](#) contains additional information on creating or modifying users.

On a new installation of Documentum 6, Content Server audits a set of events on dm_document and its subtypes. This set of events is represented by the event named dm_default_set. Refer to the *Content Server Administration Guide* for more information.

Users can access register audit screen from **Administration > Audit Management > Manage Object by Object Type**. Click **Add** to add an event in register audit screen.

Click the links below for instructions on:

- [Managing auditing by object type, page 250](#)
- [Managing auditing by object instance, page 252](#)
- [Managing auditing by events selected for all objects in the repository, page 254](#)
- [Modifying or removing audits for an object type, page 254](#)
- [Modifying or removing audits for object instances, page 255](#)
- [Modifying or removing audits for events, page 256](#)
- [Searching for and viewing audit trails, page 257](#)
- [Verifying audit trails, page 258](#)
- [Deleting audit trails, page 258](#)
- [Choosing a type, page 259](#)
- [Selecting criteria for an audit, page 259](#)
- [Criteria and event page, page 260](#)
- [Audit trails, page 260](#)
- [Audit policies, page 260](#)

Managing auditing by object type

Auditing by object type creates audit trails for events for all objects of a particular type. Use these instructions to select the types, restrict the set of objects on which audit trails are created, and select the events.

You can set audits only for one object type at a time. Complete these instructions for each object type you audit.

You must have Config Audit privileges to use this function.

To manage auditing by object type:

1. Connect to the repository and navigate to **Administration > Audit Management**.

The **Audit Management** list page is displayed.

2. Click **Manage Auditing by Object Type**.

The **Choose a type** page is displayed. With the 6.5 SP3 release, the objects locator displays the aspect types along with the existing standard types. Until the 6.5 SP2 release, only the standard types were displayed. In order to audit the object instances with aspect attributes, related aspect type needs to be registered for auditing.

3. Select a type to audit and then click **OK**.

The **Register Audit** page with the selected object type is displayed.

If you click the **Select** link at the top of the page, the selected type is replaced by the type you select now.

4. Click **Add Audit**.

Another **Register Audit** page is displayed. On this page, specify criteria for which objects are audited and specify the events to audit for the object.

- a. To audit only those objects with a particular application code, type that application code in the **Application Code** field.

The application code is a property set by the client application that creates the object. For example, an application might set the application code to the value Internal. To audit objects of the type you selected with application code Internal, you would type **Internal** in the Application Code field.

You cannot enter a value in the field if the object type you selected is dm_user, dm_acl, or dm_group.

- b. To audit only those objects attached to a lifecycle:

- i. Click **Select Lifecycle** to access the **Choose a lifecycle** page.

- ii. Select the correct lifecycle and then click **OK**.

The Register Audit page is displayed.

- iii. To audit only those objects attached to the lifecycle and in a particular state, select one from the **State** drop-down list.

- c. To record the values of particular properties of the object in the audit trail:

- i. Click **Select Attributes** to access the **Choose an attribute** page.

- ii. Select the properties whose values you want to record, click **>**, and then click **Add**.

- iii. To remove any properties, select them on the right-hand side of the page and click **<**.

- iv. Click **OK**.

The Register Audit page is displayed.

- d. Select **Has signature manifested** to sign the audit trail.

- e. Select **Include all subtypes** to include all subtypes of the type you selected in the objects audited.

- f. Select **Authentication Required** to require authentication for custom (user-defined) events that are audited.

5. Select events to register.

Each event selected is recorded for each object designated by the criteria selection already completed.

- a. Click **Add** to access the **Choose an event** page.
- b. Select the events to audit and then click **>**.
- c. To remove any events, select them on the right-hand side of the page and click **<**.
- d. Click **OK**.
- e. To filter the events, select **All Events**, **System Events**, or **Custom Events** from the drop-down list.
- f. To unregister any events, select them and click **Remove**.
- g. Click **OK**.

The Register Audit page displays the events and criteria selected for the object type.



Caution: If you click the **Select** link at the top of the page, the type selected is replaced by the type you select now and the events and criteria already selected are lost.

6. Click **OK**.

The system displays the Audit Management list page.

Managing auditing by object instance

Auditing by object instance creates audit trails for events for a particular object in the repository. Use these instructions to select objects and events.

You must have Config Audit privileges to use this function.

To manage auditing by object instance:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The **Audit Management** list page is displayed.
2. Click **Manage Auditing by Object Instance**.
The **Choose Objects** page is displayed.
3. Select objects to audit and then click **>**.
By default, the Choose Objects page displays the cabinets in the repository. Click cabinet names and folder names within cabinets to browse to the correct documents.
4. When the correct objects are selected, click **OK**.
The **Register Audit** page is displayed with the selected objects listed. If you click the **Select** link at the top of the page, the objects you already selected are replaced by the objects you select now.
5. Select an object and click **Edit**.
Another **Register Audit** page is displayed. On this page, specify properties to record in the audit trail and the events to audit for the object.

The following fields are disabled on the Register Audit page:

- **Application Code**
- **Lifecycle**
- **State**
- **Has signature manifested**
- **Include all subtypes**
- **Authentication Required**

6. To record the values of the object properties in the audit trail:

- a. Click **Select Attributes** to access the **Choose an attribute** page.
- b. Select the properties whose values you want to record, click **>**, and then click **Add**. With the 6.5 SP3 release, the attributes locator displays the aspect attributes, if any, that are attached to the selected object instance along with the existing standard attributes. Until the 6.5 SP2 release, only the standard attributes were displayed.
- c. To remove any properties, select them on the right-hand side of the page and click **<**.
- d. Click **OK**.

The Register Audit page is displayed.

7. Select events to register.

Each event selected is recorded for each object designated by the criteria selection already completed.

- a. Click **Add** to access the **Choose an event** page.
- b. Select the events to audit and then click **>**.
- c. To remove any events, select them on the right-hand side of the page and click **<**.
- d. Click **OK**.

The Register Audit page displays the events and criteria selected for the object type.

8. To unregister any events, select them, and then click **Remove**.

9. Click **OK** to return to the original Register Audit page.

10. Repeat steps 5 through 9 for each object on the list.

11. To stop auditing an object, select it and click **Unaudit**.



Caution: If you click the **Select** link at the top of the page, the objects already selected are replaced by the objects you select now and all events and criteria are lost.

12. Click **OK** to return to the Audit Management list page.

In order to audit the object instances for aspect attributes, related aspect type needs to be registered for auditing, otherwise the auditing will not happen for aspect attributes.

Managing auditing by events selected for all objects in the repository

Use these instructions to add or remove auditing events for all objects in the repository.

You must have Config Audit privileges to use this function.

To manage auditing by events:

1. Connect to the repository and navigate to **Administration > Audit Management**.

The Audit Management list page is displayed.

2. Click **Manage Auditing by events selected for all objects in the repository**.

The Register Audit page is displayed.

Any events already selected for repository-wide auditing are listed. The following fields are disabled:

- Application Code
- Lifecycle
- State
- Attributes
- Has signature manifested
- Include all subtypes
- Authentication Required

These fields are enabled only for auditing by object type.

3. Select events to register.

- a. Click **Add** to access the **Choose an event** page.

- b. Select the events to audit and then click **>**.

- c. To deselect any events, select them on the right-hand side of the page and click **<**.

- d. Click **OK**.

All events selected are displayed on the Register audit page.

4. To remove events, select them and click **Remove**.

5. Click **OK**.

The changes are saved and the Audit Management list page is displayed.

Modifying or removing audits for an object type

Use these instructions to remove or modify existing audits for a type.

You must have Config Audit privileges to use this function.

To remove or modify audits for a type:

1. Connect to the repository and Navigate to **Administration > Audit Management**.
The system displays **Audit Management** list page.
2. Click **Manage Auditing by Object Type**.
The system displays the **Choose a type** page.
3. Select a type and click **OK**.
Existing audits for the type are listed.
4. Select an object name and do one of the following:
 - a. To unregister auditing, click **Unaudit**.
 - b. To change the criteria or events audited for the type, click **Edit** to access the Register Audit page.
 - i. Remove or add events or change the criteria.
 - ii. Click **OK** to return to the original Register Audit page.The audits for the type are displayed with the changes you just made.
5. Click **OK**.
The Audit Management list page is displayed.

Modifying or removing audits for object instances

Use these instructions to modify or remove audits for objects in the repository.

You must have Config Audit privileges to use this function.

To unregister or modify audits for particular objects:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The Audit Management list page is displayed.
2. Click **Manage Auditing by Object Instance**.
The Choose Objects page is displayed.
3. Select the correct objects and click **>**.
4. Click **OK**.
The Register Audit page is displayed and the selected objects are listed.
5. Select the object to change.
6. To unregister all auditing for the object, click **Unaudit**.
All audits are deleted.
7. To change the audits, click **Edit** to access the second Register Audit page.
8. Change the audit criteria or add or remove events.

9. Click **OK** to return to the original Register Audit page.
10. Click **OK** to return to the Audit Management list page.

Modifying or removing audits for events

Use these instructions to modify or remove audits for events.

You must have Config Audit privileges to use this function.

To modify or remove auditing an event:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The Audit Management list page is displayed.
2. On the Audit Management page, click **Manage Auditing by events selected for all objects in the repository**.
The Register Audit page is displayed.
Any events already selected for repository-wide auditing are listed. The following fields are disabled:
 - **Application Code**
 - **Lifecycle**
 - **State**
 - **Has signature manifested**
 - **Include all subtypes**
 - **Authentication Required**
 - **Attributes**These fields are only enabled for auditing by object type.
3. Select the events and click **Remove**.
The events are removed from the list.
4. Click **OK**.
The changes are saved and the Audit Management list page is displayed.

Searching for and viewing audit trails

You must first search for audit trails before you can view them. You must have View Audit extended privileges to search for and view existing audit trails. Complete a DQL query or any combination of fields on the Search Criteria page.

To view audit trails:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The Audit Management list page is displayed.
2. Click **Search Audit**.
The Search Criteria page is displayed.
3. Select audit trails using a DQL query.
 - a. Select **DQL**.
 - b. Type the Where clause of a DQL query.
 - c. Click **OK**.
The results are displayed.
4. To select events:
 - a. Click **Select Events**.
 - b. Select the correct events.
 - c. Click **Add**.
 - d. Click **OK**.
5. To restrict the search by object names, select **Begins With**, **Contains**, or **Ends With** and type in a string.
6. To restrict the search by version, type in a version.
7. To restrict the search to a particular folder, click **Select Folder** and select the folder.
8. To restrict the search by time:
 - a. Click **Local Time** or **UTC**.
 - b. In the **From** field, type or select a beginning date for the search.
 - c. In the **Through** field, type or select an ending date for the search.
9. To restrict the search to a particular type, click **Select Type** and select the type; to include subtypes of the type, click **Include Subtype**.
10. To restrict the search to objects attached to a lifecycle, click **Select Lifecycle**.
11. To restrict the search to objects with an application code, type the application code.
12. To restrict the search to those audit trails that are signed, select **Has Signature**.
13. Click **OK**.
The audit trails matching the DQL query or selection criteria are displayed.

You can sort the audit trails by clicking the Object Name, Event Name, User Name, or Date Created column.

14. To view the properties of an audit trail, click the Information icon.
15. To return to the Audit Management list page, click **Audit Management** in the breadcrumb at the top of the page.

Verifying audit trails

To verify that an audit trail has not changed since it was stored in the repository, first search for and view the audit trails. Use the instructions in [Searching for and viewing audit trails, page 257](#) to locate the audit trails first.

To verify audit trails:

1. Connect to the repository and navigate to **Administration > Audit Management**.
2. Use the instructions in [Searching for and viewing audit trails, page 257](#) to locate the correct audit trails.
3. Select an audit trail to verify.
Only audit trails marked for a signature when auditing was configured can be verified.
4. Select **Tools > Verify Audit Record**.
The results are displayed in the message line.
5. To return to the audit management page, click **Audit Management** in the breadcrumb at the top of the page.

Deleting audit trails

Use these instructions to delete audit trail entries from a repository.

To delete audit trails:

1. Connect to the repository and navigate to **Administration > Audit Management**.
2. Use the instructions in [Searching for and viewing audit trails, page 257](#) to locate the correct audit trails.
3. To delete one or more audit trails, select them and then select **Tools > Purge Audit Records**
4. To delete all audit trails returned by the search, click **Purge All Audit Records** in the upper right-hand corner of the page.
The results are displayed in the message line.
5. To return to the Audit Management list page, click **Audit Management** in the breadcrumb at the top of the page.

Choosing a type

On this page, select a type and then click **OK** to accept the type or **Cancel** to cancel the action.

Selecting criteria for an audit

Use this page to define which objects are audited and the events to audit.

To select the criteria for an audit:

1. To audit only those objects with an application code, type the code in the **Application Code** field.
The application code is a property set by the client application that creates the object. For example, an application might set the application code to the value Internal. To audit objects of the selected type with application code Internal, type **Internal** in the Application Code field. You cannot enter a value in the field if the object type selected is dm_user, dm_acl, or dm_group.
2. To audit only those objects attached to a particular lifecycle:
 - a. Click **Select Lifecycle**.
 - b. Select the correct lifecycle and then click **OK**.
 - c. To audit only those objects attached to the lifecycle and in a particular state, select the state from the drop-down list.
3. To record the values of particular properties of the object in the audit trail:
 - a. Click **Attributes**.
 - b. Select the properties whose values you want to record.
 - c. Click **Add**.
 - d. To see more pages of properties, use the forward and back arrows or select a different number from the drop-down list.
 - e. Repeat steps b through d until you see all of the properties.
 - f. To remove any properties, select them on the right-hand side of the page and click **Remove**.
 - g. Click **OK**.
4. To sign the audit trail, select **Has signature manifested**.
5. To include all subtypes of the type you selected in the objects audited, select **Include all subtypes**.
6. To require authentication for custom (user-defined) events that are audited, select **Authentication Required**.
7. Select events to register.
Each event selected is recorded for each object designated by the criteria selection you have already completed.
 - a. Click **Add**.
 - b. Select the events to audit.

- c. To see more pages of events, use the forward and back arrows or select a different number from the drop-down list.
- d. Repeat steps b through d until you see all of the events.
- e. To remove any events, select them on the right-hand side of the page and click **Remove**.
- f. Click **OK**.

Criteria and event page

This page lists either object instances or an object type that you selected for auditing, as well as the selected criteria and events. Use the page to add, edit, or remove audits.

- To add an audit, select it, click **Add Audit**, and select the criteria.
When the page appears again, click **OK**.
- To modify an audit, select it, click **Edit**, and change the criteria.
When the page appears again, click **OK**.
- To remove an audit, select it, click **Remove**, then click **OK**.

Audit trails

This page displays audit trails found by a search you executed. From this page, you can:

- Verify audit trails
Use the instructions in [Verifying audit trails, page 258](#).
- Delete audit trails, if you have Purge Audit privileges.
Use the instructions in [Deleting audit trails, page 258](#).
- Click the properties icon to view the properties of an audit trail.

To navigate back to the Audit Management list page, click **Audit Management** in the breadcrumb at the top of the page.

Audit policies

In 6.5 SP3, Content Server introduces auditing improvements to achieve DOD 5015 compliance. The following improvements are available in this release of Documentum Administrator:

- Audit for aspect attributes, which audits the aspect attribute changes attached to the object along with the object type attributes.
- Restriction in purge audit, which adds a purge policy for users and groups, so the user whose purge policy satisfies the audit record can purge that audit record. Purge policy is a condition of audit trail attributes, which ensures that only authorized users can delete the audit record.

You must be an Install Owner to access and manage audit policies. Other users can only view the listing of audit policies. Use these instructions to create, edit, save as, and delete audit policies. The **Audit Policies** page displays the following attributes:

- Name: This is the name of audit policy based on the attribute *Name*. It is a required field.
- Accessor Name: This contains the user, group, or role name to which this condition belongs to based on the attribute *accessor_name*.
- Is Group: This displays Yes or No depending on the attribute *is group*. This informs the user if the accessor name is group or not.

The **Audit Policies** page displays the list of audit policies. From this page, you can:

- [Creating an audit policy, page 261](#)
- [Editing an audit policy, page 262](#)
- [Saving a copy of an audit policy, page 262](#)
- [Deleting an audit policy, page 263](#)

Creating an audit policy

You must be an Install Owner to create an audit policy. Use these instructions to create an audit policy.

To create an audit policy:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The **Audit Management** list page is displayed.
2. Click **Audit Policies**.
The **Audit Policies** page is displayed.
3. Click **File > New > Audit Policy**.
The **New Audit Policy - Info** page is displayed.
4. Enter information on the **New Audit Policy - Info** page:
 - a. **Name:** Type the name of an audit policy.
 - b. **Accessor Name:**
Click **Select** to access the **Choose a user/group** page.
 - c. Select a user, group, or a role and then click **OK**.
The **New Audit Policy - Info** page is displayed.
5. Click **Add**.
The **Create/Edit Rule** page is displayed.
6. Enter information on the **Create/Edit Rule** page:
 - a. **Attribute Name:** Select the name of the attribute from the dropdown box.
 - b. **Attribute Value:** Type the attribute value.
If the attribute value is of type date then the value should be provided in yyyy-mm-dd hh:mm:ss format.

Note: There should be at least one rule or condition to create an audit policy.

- c. Click **OK**.
7. Click **OK**.
The **Audit Policies** page is displayed. This page lists the new audit policy.

Editing an audit policy

You must be an Install Owner to edit an audit policy. Use these instructions to edit an audit policy.

To edit an audit policy:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The **Audit Management** list page is displayed.
2. Click **Audit Policies**.
The **Audit Policies** page is displayed.
3. Click **View > Properties > Info**.
The **Audit Policy Properties** page is displayed.
4. Edit the information on the **Audit Policy Properties - Info** page.

Note: There should be at least one rule or condition for saving an edited audit policy.

Saving a copy of an audit policy

Users can save a copy of an audit policy as equivalent to duplicating an audit policy for any minor changes. Use these instructions to save a copy of an audit policy.

To save a copy of an audit policy:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The **Audit Management** list page is displayed.
2. Click **Audit Policies**.
The **Audit Policies** page is displayed.
3. Select an audit policy for saving it as a copy.
4. Click **File > Save As**.
The **Audit Policy Properties - Info** page is displayed.
5. Edit the information on the **Audit Policy Properties - Info** page, if required.
6. Click **OK**.
The **Audit Policies** page is displayed. This page lists the copy of an audit policy you saved.

Deleting an audit policy

You must be an Install Owner to delete an audit policy. Use these instructions to delete an audit policy.

To delete an audit policy:

1. Connect to the repository and navigate to **Administration > Audit Management**.
The **Audit Management** list page is displayed.
2. Click **Audit Policies**.
The **Audit Policies** page is displayed.
3. Select an audit policy for deletion.
4. Click **File > Delete**.
The confirmation page for deletion is displayed.
5. Click **OK** to confirm the deletion.
The audit policy is deleted and the **Audit Policies** page is displayed.

Job Management

This section discusses jobs, methods, and administration methods.

- Jobs are objects that automate method execution.
- Methods are executable scripts or programs that are represented by method objects in the repository.
- Administration methods are methods that perform a variety of administration and monitoring tasks.

Click the links for information and instructions on:

- [Jobs, page 265](#)
- [Methods, page 321](#)
- [Administration methods, page 328](#)

Jobs

Jobs are repository objects that automate method object execution. Methods associated with jobs are executed automatically on a user-defined schedule. The properties of a job define the execution schedule and turn execution on or off. Jobs are invoked by the agent exec process, a process installed with Content Server. At regular intervals, the agent exec process examines the job objects in the repository and runs those jobs that are ready for execution. Any user can create jobs.

When a repository is created, it contains jobs for:

- CA Store (EMC Centera and NetApp SnapLock stores)
- Content
- Data Dictionary
- Distributed Content
- Docbase
- Federation
- Fulltext
- Other

- Replication
- Workflow

You can create additional jobs to automate the execution of any method and you can modify the schedule for executing existing jobs.

For more information:

- On content, data dictionary, repository, and full-text management jobs, refer to the chapter entitled Tools and Tracing in the *Content Server Administration Guide*.
- On records migration jobs, refer to the chapter entitled Content Management in the *Content Server Administration Guide*.
- On federation and replication jobs, refer to the *Distributed Configuration Guide*.

On the Jobs list page, you can sort the jobs in the repository by clicking the headings for:

- Name (object name)
- Description
- Job Type
- Last Run (date and time)
- State (Active or Inactive)
- Job Status (running or no status)

You can also sort the jobs by selecting a job type from the drop-down list. The drop-down list is generated from the job type property. Job types you define when you create jobs are included in the list. The types available by default are:

- CA Store (EMC Centera and NetApp SnapLock stores)
- Content
- Data Dictionary
- Distributed Content
- Docbase
- Federation
- Fulltext
- Other
- Replication
- Workflow

Records migration, job sequence, and retention expired objects will also appear in the drop-down list after you create jobs for them.

Jump to jobs whose names start with a particular string by typing the string into the **Starts with** box and then clicking **Go**, or click a letter and jump to jobs starting with that letter.

To display more or fewer jobs at a time, select a different number from the **Show Items** drop-down list.

To view the next page of jobs, click the > button. To view the previous page of jobs, click the < button.

To jump to the first page of jobs, click the << button. To jump to the last page, click >>.

These selection criteria can be combined. For example, if you select repository jobs from the drop-down list and click a letter, you will see only repository jobs beginning with that letter.

This section contains instructions for:

- [Creating jobs, page 268](#)
- [Creating basic information for a job, page 270](#)
- [Changing the schedule of a job, page 271](#)
- [Setting the qualifier rules for the remove retention-expired objects job, page 272](#)
- [Assigning a method to a job, page 273](#)
- [Locating a method for a job, page 275](#)
- [Creating, viewing, or modifying sysobject properties, page 275](#)
- [Creating replication jobs, page 276](#)
 - [Selecting the source repository for a replication job, page 280](#)
 - [Selecting the target repository for a replication job, page 281](#)
 - [Setting replication job options, page 282](#)
 - [Choosing a replication folder, page 283](#)
 - [Choosing a replication job user, page 284](#)
 - [Choosing a permission set for replica objects, page 284](#)
 - [Choosing a storage area, page 284](#)
 - [Choosing replication and security modes, page 285](#)
- [Creating records migration jobs, page 286](#)
 - [Setting the rules of a records migration job, page 289](#)
 - [Defining selection criteria for a records migration job, page 290](#)
 - [Defining version criteria for records migration job, page 291](#)
- [Creating BOCS caching jobs, page 292](#)
- [Creating job sequences, page 296](#)
 - [Providing repository connection and job information for a job sequence, page 300](#)
 - [Selecting repositories for a job sequence, page 301](#)
 - [Selecting jobs for a job sequence, page 301](#)
 - [Setting dependencies for a job sequence, page 302](#)
- [Running jobs, page 302](#)
- [Viewing the status of a running job, page 303](#)
- [Viewing job reports, page 303](#)
- [Setting the trace level for a job, page 303](#)
- [Viewing job trace logs, page 304](#)
- [Modifying jobs, page 304](#)

- [Deleting jobs, page 304](#)
- [Deactivating jobs on failure, page 305](#)
- [Job descriptions, page 305](#)

Creating jobs

Jobs automate method execution. For example, define jobs that transfer existing content files from one storage area to another.

Before you create a job, determine which method the job will run or create a Docbasic script, Java method, or other program to perform the task. If you create your own script, method, or program, you must then create a method object referencing the program. Refer to [Methods, page 321](#), for information on creating method objects.

To create a new job using Documentum Administrator, you must provide general information on the New Job - Info page, set the job's schedule on the New Job - Schedule page, define the method executed by the job on the New Job - Method page, and provide sysobject properties on the New Job - SysObject Info page.

If creating a replication job, records migration job, BOCS caching job, or job sequence, click the links below for information on creating those job types:

- [Creating replication jobs, page 276](#)
- [Creating records migration jobs, page 286](#)
- [Creating BOCS caching jobs, page 292](#)
- [Creating job sequences, page 296](#)

To create a job:

1. Navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select **File > New > Job**.
The system displays the New Job - Info page.
3. Enter information on the **New Job - Info** page:
 - a. **Name:** Type the name of the job.
 - b. **Job Type:** Optionally, type the job type. This may be any value. The job type is displayed on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level:** Select a trace level. Trace levels range from 0 (no tracing) to 10 (a debugging level of tracing).
 - d. **Designated Server:** Select a server to run the job. The drop-down list displays all servers running against the repository of which Documentum Administrator is aware.
 - e. **State:** Select **Active** or **Inactive** to create the job in an active or inactive state.
 - f. **Deactivate on Failure:** Select to deactivate the job after a run that fails to execute correctly.
 - g. **Run After Update:** Select to run the job immediately after you save it.

- h. **Save if Invalid:** Select to save the job, even if it is invalid.
 - i. Click **Next** to access the New Job - Schedule page.
4. Enter information on the **New Job - Schedule** page:
 - a. **Start Date And Time:** Designate a start date and time for the job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat:** Select a unit of time.
 - **Frequency:** Type how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
 - c. **End Date And Time:** Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive. The default end date is 10 years from the current date and time.
 - d. Click **Next** to access the New Job - Method page.
 5. Enter information on the **New Job - Method** page:
 - a. **Select Method:** Click to access the **Choose a method** page.
 - i. Select a method you want the job to run.

Refer to [Locating a method for a job, page 275](#) for instructions to locate a method.
 - ii. Click **OK** to return to the New Job - Method page.
 - b. Click **Edit** to access the **Method Arguments** page to modify the arguments passed to the method by this job:
 - Type a new argument in the **Enter new value** box and then click **Add**.
 - To remove an argument, select the argument and click **Remove**.
 - To change the order in which arguments are passed, click the argument and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.

The system displays the New Job - Method page.
 - c. **Pass standard arguments:** Select to pass the standard arguments for the method.

The standard arguments are:

 - Repository owner
 - Repository name
 - Job ID
 - Trace level
 - d. Click **Next** to access the New Job - SysObject Info page.
 6. Enter information on the **New Job - SysObject Info** page:
 - a. **Title:** Type the title.
 - b. **Subject:** Type the subject.

- c. **Keywords:** Click **Edit** to access the **Keywords** page:
 - Type a new keyword in the **Enter new value** box and click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to nullify the changes.The system displays the New Job - SysObject Info page.
 - d. **Authors:** Click **Edit** to access the **Authors** page:
 - Type a new author in the **Enter new value** box and click **Add**.
 - To remove an author, select the name and click **Remove**.
 - To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The system displays the New Job - SysObject Info page.
 - e. **Owner Name:** Click **Edit** to access the **Choose a user** page:
 - Select an owner.
 - Click **OK**.The system displays the New Job - SysObject Info page.
 - f. To view more sysobject properties of the job, click **See More**.
7. Click **Finish**.
- The system saves the job and displays the Jobs list page.

Creating basic information for a job

The New Job - Info and Job Properties - Info pages are identical for standard jobs, replication jobs, records migration jobs, BOCS caching jobs, and job sequences. The table below lists the fields on the page with information about how to complete them. For complete instructions on creating each type of job, refer to:

- [Creating jobs, page 268](#)
- [Creating replication jobs, page 276](#)
- [Creating records migration jobs, page 286](#)
- [Creating BOCS caching jobs, page 292](#)
- [Creating job sequences, page 296](#)

Table 37. New Job - Info and Job Properties - Info page properties

Field label	Description
Name	The job's object name.

Field label	Description
Job Type	A label identifying the job type. Used to populate the drop-down list on the Jobs list page.
Trace Level	Controls how much information is recorded in trace logs. May be set from 0 to 10. For instructions on viewing trace logs, refer to Viewing job trace logs, page 304 .
Designated Server	When more than one server runs against a repository, use to designate a server to run the job. The default is <i>Any Running Server</i> .
State	<p>Determines how the job runs:</p> <ul style="list-style-type: none"> • If set to Active, the job runs as scheduled. • If set to Inactive, the job does not run automatically, but can be executed manually.
Next Scheduled Date	Displays the next date and time on which the job is scheduled to run. Read only.
Deactivate on Failure	Determines whether to make the job inactive if it does not run successfully.
Run After Update	Determines whether to run the job immediately after any changes to the job are saved.
Save If Invalid	Determines whether to save the job object if Documentum Administrator is unable to validate the job.
Last Run	Displays the last date and time the job ran and was completed. Read only.
Last Status	Displays the last time the job completed and the length of time the job took to run. Read only.
Last Return Code	Displays the last value returned by the job. Read only.
Runs Completed	Displays the number of times the job has run to completion. Read only.

Changing the schedule of a job

Use these instructions to modify a job's schedule, whether the job is a standard job, replication job, BOCS caching job, records migration job, or job sequence. Schedule each job to run with a frequency that meets your business needs. If a job is installed in the inactive state, change its status on the Job Properties - Info page.

Set up the schedules for replication jobs so that jobs for the same target repository do not run at the same time. Running replication jobs simultaneously to the same target repositories causes repository corruption.

To change a job schedule:

1. Connect to the repository and navigate to **Job Management > Jobs**.
The system displays the Jobs list page.
2. Locate the job whose schedule you want to change.
3. Select the job and then select **View > Properties > Info**.
The system displays the Job Properties - Info page.
4. Click the **Schedule** tab.
The system displays the Job Properties - Schedule page.
5. Designate a start date and time for the job.
The default is the current date and time.
6. Designate how often and at what interval the job runs.
 - The **Repeat** drop-down list specifies a unit of time.
 - The **Frequency** box specifies how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.

7. Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive.
The default end date is 10 years from the current date and time.
8. Click **OK**.

The system displays the Jobs list page.

Setting the qualifier rules for the remove retention-expired objects job

Qualifier rules determine which objects to remove from a content-addressable store when the remove expired retention objects (dm_RemoveExpiredRetn_Objects) job runs. Use the instructions in this section to select the type to be queried and to create the rules.

Create standard rules or custom rules on the New Job - Qualifier Rules or Job Properties - Qualifier Rules page for content-addressable stores. There are no restrictions on the number of conditions in a custom rule, but the length is limited to 255 characters.

Standard rules are limited to five selection criteria defined by choosing properties from drop-down lists. The available properties are:

- Name
- Title
- Subject

- Authors
- Keywords
- Created
- Modified
- Accessed

After selecting a property, select an operand and type or select the correct value. For example, two rules might be **Name contains UNIX** and **Created before January 1, 2004**. When the job runs, the criteria are connected with AND, so that all criteria must apply to a particular object for it to be deleted. If you require an OR for example, **Name contains UNIX OR Created before January 1, 2004** use a custom rule.

A custom rule is entered into a text box as a DQL WHERE clause. There are no restrictions on the number of conditions in a custom rule, but the length is limited to 255 characters. Custom rules can be based on the values of any standard SysObject properties, provided those values are present before an object is saved. For example, a custom rule might be **object_name="Test" or object_name="Delete"**. Custom rules are not validated by Documentum Administrator.

To set qualifier rules for the remove expired retention objects job:

1. Access the New Job - Qualifier Rules or Job Properties - Qualifier Rules page.
2. Click **Select** next to **Object Type**.
The **Choose a type** page appears.
3. Select a type and click **OK**.
The **New Job - Qualifier Rules or Job Properties - Qualifier Rules** page appears.
4. To create a standard rule, select **Standard**.
 - a. Select a property from the first drop-down list.
 - b. Select an operand from the second drop-down list.
 - c. If you selected Name, Title, Subject, Authors, or Keywords, type a value.
 - d. If you selected Created, Modified, or Accessed, select a date.
 - e. To add additional criteria, click **Add Criteria** and repeat steps a through d.
 - f. To delete a criterion, click **Remove**.
5. To create a custom rule, select **Custom** and then type the WHERE clause of a DQL query.
6. Click **OK**.

Assigning a method to a job

Each job executes a method to perform particular tasks. Methods are executable scripts or programs represented by method objects in the repository. The script or program can be a Docbasic script, a Java method, or a program written in another programming language such as C++. The associated method object has properties that identify the executable and define command line arguments and the execution parameters. For example, the dm_DMclean job executes the dm_DMclean method.

Some Documentum jobs execute a specific method that cannot be changed. For example, you cannot change the method executed by the dm_RemoveExpiredRetnObjects job, which removes expired content from a content-addressable store. When you create a job, you must designate on the New Job - Method or Job Properties - Method page a method to be executed.

Many jobs take the queueperson and window_interval arguments.

- The queueperson argument defines which repository user receives the inbox and email notifications generated by the jobs. If you do not designate a repository user for a specific job, the notifications are sent to the user identified by the operator_name property of the server's server config object. This property is set to the repository owner's name by default.
- The window_interval argument defines a window on either side of the job's scheduled run time in which the job can run. This ensures that if a server must be restarted, the startup is not delayed by jobs that must be run.

If you assign a user-defined method to a job, that method must contain the code to generate a job report. If you turn on tracing, only a DMCL trace is generated.

To assign a method to a job:

1. Access the New Job - Method or Job Properties - Method page.
2. Click **Select Method** to access the **Choose a method** page.
Refer to [Locating a method for a job, page 275](#) for instructions to locate a method.
3. Select a method name and click **OK**.
The **New Job - Method or Job Properties - Method** page appears.
4. Click **Edit** to access the **Method Arguments** page to enter new arguments, remove unnecessary arguments, or change the values to the method by the job:
 - a. Type a new argument in the **Enter new value** box.
 - b. Click **Add**.
 - c. To remove an argument, select the argument and click **Remove**.
 - d. To change the order in which arguments are passed, select the argument and click **Move Up** or **Move Down**.
 - e. Click **OK** to save the changes or **Cancel** to abandon the changes.The **New Job - Method or Job Properties - Method** page appears.
5. Select **Pass standard arguments** to pass the standard arguments for the method.
The standard arguments are:
 - Repository owner
 - Repository name
 - Job ID
 - Trace level
6. Click **OK** to save the changes or **Cancel** to abandon the changes.
The **Jobs** list page appears.

Locating a method for a job

On the **Choose a method** page, select the method to be executed by a job.

To locate a method for a job:

1. To locate the method by name, type the first few letters into the **Starts with** box and click **Go**.
2. To view additional pages of methods, click the forward or back buttons.
3. To view a different number of methods, select a different number from the **Show Items** drop-down list.
4. To sort the items, select **Show All** or **Show System Methods** from the drop-down list.
5. When you locate the correct method, select it and click **OK**.

Creating, viewing, or modifying sysobject properties

The SysObject Info page displays read-only information about an object. You can modify the **Title** or **Subject**, or change the **Authors** or **Keywords**. To see more or less information, click the **show more** or **hide more** links. To change the authors or keywords, click the correct link. To enter values, type them in the **Enter new value** box and click **Add**. You can move a value up or down in the resulting list by selecting it and clicking **Move Up** or **Move Down**. You can remove a value by selecting it and clicking **Remove**. When you are done entering values, click **OK**.

To create, view, or modify sysobject properties:

1. Access the SysObject Info page.
2. Type or modify the title.
3. Type or modify the subject.
4. In the **Keywords** section, click **Edit** to access the **Keywords** page.
 - a. To add a keyword, type a new keyword in the **Enter new value** box and click **Add**.
 - b. To remove a keyword, select the keyword and click **Remove**.
 - c. To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - d. Click **OK** to save the changes or **Cancel** to abandon the changes.
The **New Job - SysObject Info** or **Job Properties - SysObject Info** page appears.
5. In the **Authors** section, click **Edit** to access the **Authors** page.
 - a. Type a new author in the **Enter new value** box and click **Add**.
 - b. To remove an author, select the name and click **Remove**.
 - c. To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - d. Click **OK** to save the changes or click **Cancel** to abandon the changes.
The **New Job - SysObject Info** or **Job Properties - SysObject Info** page appears.

6. In the **Owner Name** section, click **Edit** to access the Choose a user page.
 - a. Select an owner.
 - b. Click **OK**.The New Job - SysObject Info or Job Properties - SysObject Info page appears.

Creating replication jobs

A replication job automates replication between the component storage areas of a distributed storage area. You can use replication jobs to replicate objects (property data and content) between repositories. By using parameters that you define, the replication job dumps a set of objects from one repository, called the *source* repository, and loads them into another repository, called the *target* repository. After the replication job is saved and the job runs successfully for the first time, you cannot change the source or target repository. If you need to change the source or target repository, set the job to inactive or delete the job, then create a new replication job with the correct source or target repository.

If you are replicating objects from multiple source repositories into the same target repository, or if you are replicating replica object, use a job sequence to designate the order in which the jobs run so that they do not conflict with each other. For information on creating job sequences, refer to [Creating job sequences, page 296](#).

The instructions and information in this section apply only to object replication, not to content replication. You cannot configure content replication with Documentum Administrator.

When you create a replication job, you must choose a replication mode and a security mode. Each security mode behaves differently depending on which replication mode you choose. In addition, replica objects in the target repository are placed in different storage areas depending on which security mode you choose. For complete information on choosing replication and security modes, refer to [Choosing replication and security modes, page 285](#).

For more information about replication jobs, refer to Chapter 1, "Building Blocks and Models," in the *Distributed Configuration Guide*.

To create a replication job:

1. Navigate to **Administration > Job Management > Jobs**.
The **Jobs** list page appears.
2. Select **File > New > Replication Job**.
The New Replication Job - Info page appears.
3. Enter information on the **New Replication Job - Info** page:
 - a. **Name:** Type the name of the replication job.
 - b. **Job Type:** The system automatically prepopulates this field with *Replication*. You may, optionally, change the job type to be any value. The job type is displayed on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level:** Select a trace level. Trace levels range from 0 (no tracing) to 10 (a debugging level of tracing).

- d. **Designated Server:** Select a server to run the job. The drop-down list displays all servers running against the repository of which Documentum Administrator is aware.
 - e. **State:** Select **Active** or **Inactive** to create the job in an active or inactive state.
 - f. **Deactivate on Failure:** Select to deactivate the job after a run that fails to execute correctly.
 - g. **Run After Update:** Select to run the job immediately after you save it.
 - h. **Save if Invalid:** Select to save the job, even if it is invalid.
 - i. Click **Next** to access the New Replication Job - Schedule page.
4. Enter information on the **New Replication Job - Schedule** page:
- a. **Start Date And Time:** Designate a start date and time for the job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat:** Select a unit of time.
 - **Frequency:** Type how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
 - c. **End Date And Time:** Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive. The default end date is 10 years from the current date and time.
 - d. Click **Next** to access the New Replication Job - From Source page.
5. Enter information on the **New Replication Job - From Source** page:
- a. **Login Name:** Type the name of a Superuser in the source repository.
 - b. **Password:** Type the password for the Superuser.
 - c. **Domain:** On Windows, type the name of the domain where the source repository resides.
 - d. **Repository and Connection broker:** Select the source repository and connection broker from the drop-down lists.

The repository list displays those repositories that project to the currently-selected connection broker. If the source repository you want does not appear in the repository list, choose a connection broker to which that repository projects.

After the job runs successfully for the first time, you cannot change the source repository.
 - e. **From Source:** Indicates the path to the source.
 - Click **Select Path** to access the **Choose a folder** page.
 - Select the source cabinet or navigate to the correct folder in a cabinet.
 - Click **OK** to return to the New Replication Job - From Source page.
 - f. Click **Next** to access the New Replication Job - To Target page.
6. Enter information on the **New Replication Job - To Target** page:
- a. **Name:** Type the name of a Superuser in the target repository.
 - b. **Password:** Type the password for the Superuser.

- c. **Domain:** On Windows, type the name of the domain where the target repository resides.
 - d. **Repository and Connection broker:** Select the target repository and connection broker from the drop-down lists.
If the correct source repository does not project to a particular connection broker, choose a different connection broker.
After the job runs successfully for the first time, you cannot change the target repository.
 - e. **To Target:** Indicates the path to the target folder.
 - Click **Select Path** to access the **Choose a folder** page.
 - Select the target cabinet or navigate to the correct folder in a cabinet.
 - Click **OK** to return to the New Replication Job - To Target page.
 - f. **Owner:** Indicates the owner of the target repository.
 1. Click **Select Owner** to access the **Choose a user** page.
 2. Select an owner for the target repository.
 3. Click **OK** to return to the New Replication Job - To Target page.
 - g. **Permission Set:** Indicates the permission set assigned to the replica objects.
 - Click **Select Permission Set** to access the **Choose a permission set** page.
 - Select a permission set assigned to the replica objects.
 - Click **OK** to return to the New Replication Job - To Target page.

If you leave the Permission Set field blank, the server creates a default permission set that gives RELATE permission to the world and group levels and DELETE permission to the replica owner.
 - h. **Storage Area:** Indicates the storage area for the content associated with the replica.
 - Click **Select Storage** to access the **Choose a storage** page.
 - Select a storage area for the content associated with the replica.
 - Click **OK** to return to the New Replication Job - To Target page.

By default, the content is stored in a storage area named replica-filestore_01. However, this area is located on the same device as the default file store (filestore_01) for local documents. It is recommended that you create a new file store on a different device to store replica content.
- i. Click **Next** to access the New Replication Job - Replication Options page.
7. Enter information on the **New Replication Job - Replication Options** page.
 - a. **Code Page:** Optionally, select the correct code page for the replication job.
Leave the value at the default, UTF-8, unless you must change it.
 - b. **Full Refresh:** Select to replicate every object in the source cabinet or folder.
By default, the replication job is incremental and only replicates objects that have changed since the last execution of the job. However, even if the job is set to incremental, the first time the job runs, it is by default a full refresh.
 - c. **Fast Replication:** Select to use fast replication.



Caution: Fast replication does not replicate all relationships and therefore may not be appropriate for all users. For more information, refer to the *Distributed Configuration Guide*.

- d. **Full Text Indexing:** Select a full-text indexing mode. Options are:
 - **Same as source** means that the same documents are indexed in the source and target.
 - **All possible** means that all replicas in a format that can be indexed are marked for indexing.
 - **None** means none of the replicas are marked for indexing.
- e. **Replication Mode:** Select a replication mode.
 - Select **Federated** mode whether or not the source and target repositories are in a federation.
 - Select **Non-Federated**, which is named external replication mode in the *Distributed Configuration Guide*

For more information on selecting a replication mode, refer to [Choosing replication and security modes, page 285](#).

- f. **Security Option:** Select how to handle security if there is no matching permission set in the target repository.
 - Select **Preserve** to replicate the source permission set in the target repository.
 - Select **Remap** to reset the replica's acl_domain to the permission set specified on the target if the source permission set is an external permission set.

For more information on choosing a security mode, refer to [Choosing replication and security modes, page 285](#).

- g. **Maximum objects per transfer:** In 5.3 and later repositories, optionally specify the maximum number of objects dumped and transferred in each operation.
When set, the replication job dumps and transfers the total number of objects to be replicated in batches of the size specified. For example, if 100,000 objects must be replicated and the maximum is set to 10,000, the objects are replicated in 10 batches.
- h. **Manual Transfer:** Select if you intend to manually move the dump file from the source to the target. If selected, click **Select User** and select the user in the target repository to notify that a replication job is ready for manual transfer.
The system sends an email notification to the selected user.



Caution: The replication job creates a dump file and a delete synchronization file. Both files must be transferred to the target. Always transfer the dump file first.

- i. Click **Next** to access the New Replication Job - SysObject Info page.
8. Enter information on the **New Replication Job - SysObject Info** page:
 - a. **Title:** Type the title.
 - b. **Subject:** Type the subject.

- c. **Keywords:** Click **Edit** to access the **Keywords** page:
 - To add a keyword, type a new keyword in the **Enter new value** box and click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The system displays the New Replication Job - SysObject Info page.
- d. **Authors:** Click **Edit** to access the **Authors** page:
 - Type a new author in the **Enter new value** box and click **Add**.
 - To remove an author, select the name and click **Remove**.
 - To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The system displays the New Replication Job - SysObject Info page.
- e. **Owner Name:** Click **Edit** to access the **Choose a user** page:
 - Select an owner.
 - Click **OK**.The New Replication Job - SysObject Info page appears.
- f. To view more sysobject properties of the job, click **See More**.
- g. Click **Finish**.
The job is saved and the Jobs list page appears.

Selecting the source repository for a replication job

The New Replication Job - From Source and Job Properties - From Source pages are used to select the source repository for a replication job. The source repository is the repository from which objects are replicated.

For instructions on how to access the New Replication Job - Source page and create new replication jobs, refer to [Creating replication jobs, page 276](#).

To select the source repository:

1. Access the Job Properties - From Source page:
 - a. Navigate to **Administration > Job Management > Jobs** to access the Jobs list page.
 - b. Select an existing replication job and then select **View > Properties > Info** to access the Job Properties - Info page.
 - c. Select the **From Source** tab.
The **Job Properties - From Source** page appears.

2. Type the login name of a Superuser in the source repository.
3. Type the password for the Superuser you chose in step 2.
4. On Windows, type the name of the domain where the source repository resides.
5. Select the source repository and connection broker from the drop-down lists.

If the correct source repository does not project to a particular connection broker, choose a different connection broker.

After the replication job runs successfully for the first time, you cannot change the source repository.
6. Click **Select Path** to access the **Choose a folder** page.
 - a. Select the source cabinet or navigate to the correct folder in a cabinet.
 - b. Click **OK**.

The Job Properties - From Source page appears.
7. Click a tab to move to another Job Properties page, or click **OK** or **Cancel** to return to the Jobs list page.

Selecting the target repository for a replication job

The New Replication Job - To Target and Job Properties - To Target pages are used to select the target repository for a replication job. The target repository is the repository to which objects are replicated.

For instructions on how to access the New Replication Job - To Target page and create new replication jobs, refer to [Creating replication jobs, page 276](#).

To select the target repository:

1. Access the Job Properties - To Target page:
 - a. Navigate to **Administration > Job Management > Jobs** to access the Jobs list page.
 - b. Select an existing replication job and then select **View > Properties > Info** to access the Job Properties - Info page.
 - c. Select the **To Target** tab.

The system displays the Job Properties - To Target page.
2. Type the name and password of a Superuser in the target repository.
3. On Windows, type the name of the domain where the target repository resides.
4. Select the target repository and connection broker from the drop-down lists.

If the correct source repository does not project to a particular connection broker, choose a different connection broker.

After the replication job runs successfully for the first time, you cannot change the target repository.
5. Click **Select Path** to access the **Choose a folder** page.
 - a. Select the target cabinet or navigate to the correct folder in a cabinet.

- b. Click **OK** to return to the Job Properties - To Target page.
6. Optionally, click **Select Owner** to access the **Choose a user** page.
 - a. Select the user who is the owner of the target repository.
 - b. Click **OK** to return to the Job Properties - To Target page.This updates objects to the owner you choose. Most replication jobs do not require this.
7. Click **Select Permission Set** to access the **Choose a permission set** page.
 - a. Select a permission assigned to the replica objects.
 - b. Click **OK** to return to the Job Properties - To Target page.If you leave the **Permission Set** field blank, the server creates a default permission set that gives RELATE permission to the world and group levels and DELETE permission to the replica owner.
8. Click **Select Storage** to access the **Choose a storage** page.
 - a. Select a storage area for the content associated with the replica.
 - b. Click **OK** to return to the Job Properties - To Target page.By default, the content is stored in a storage area named replica_filestore_01. However, this area is located on the same device as the default file store (filestore_01) for local documents. It is recommended that you create a new file store on a different device to store replica content.
9. Click a tab to move to another Job Properties page, or click **OK** or **Cancel** to return to the Jobs list page.

Setting replication job options

The New Replication Job - Replication Options and Job Properties - Replication Options pages are used to set replication job options.

For instructions on how to create new replication jobs, refer to [Creating replication jobs, page 276](#).

To set options:

1. Access the Job Properties - Replication Options page:
 - a. Navigate to **Administration > Job Management > Jobs** to access the Jobs list page.
 - b. Select an existing replication job and then select **View > Properties > Info** to access the Job Properties - Info page.
 - c. Select the **Replication Options** tab.The **Job Properties - Replication Options** page appears.
2. Select the correct code page for the replication job.
Keep the value at the default, UTF-8, unless it must be changed.
3. To replicate every object in the source cabinet or folder, select **Full Refresh**.
By default, the replication job is incremental and only replicates objects that have changed since the last execution of the job.
4. To use fast replication, select **Fast Replication**.



Caution: Fast replication does not replicate all relationships. For more information, refer to the *Distributed Configuration Guide*.

5. Select the full-text indexing mode. Options are:

- **Same as source** means that the same documents are indexed in the source and target.
- **All possible** means that all replicas in a format that can be indexed are marked for indexing.
- **None** means none of the replicas are marked for indexing.

6. Select a replication mode.

You may select federated mode whether or not the source and target repositories are in a federation. For more information on selecting a replication mode, refer to [Choosing replication and security modes, page 285](#).

Nonfederated replication mode is called external replication mode in the *Distributed Configuration Guide*.

7. Select how to handle security if there is no matching permission set in the target repository.

- Select **Preserve** to replicate the source permission set in the target repository.
- Select **Remap** to reset the replica's acl_domain to the permission set specified on the target if the source permission set is an external permission set.

For more information on choosing a security mode, refer to [Choosing replication and security modes, page 285](#).

8. Optionally, specify the maximum number of objects dumped and transferred in each operation.

When set, the replication job dumps and transfers the total number of objects to be replicated in batches of the size specified. For example, if 100,000 objects must be replicated and the maximum is set to 10,000, the objects are replicated in 10 batches.

9. Select **Manual Transfer** if you intend to manually move the dump file from the source to the target. If selected, click **Select User** and select the user in the target repository to notify that a replication job is ready for manual transfer.

The system sends an email notification to the selected user.



Caution: The replication job creates a dump file and a delete synchronization file. Both files must be transferred to the target. Always transfer the dump file first.

10. Click a tab to move to another Job Properties page, or click **OK** or **Cancel** to return to the Jobs list page.

Choosing a replication folder

Use these instructions to choose a replication source or target folder on the Choose a folder page.

To choose a folder:

1. To choose a cabinet, select it and then click **OK**.
2. To choose a folder, do the following:

- a. Double-click the correct cabinet to view its folders.
- b. Select the correct folder.
- c. Click **OK**.

Choosing a replication job user

Use these instructions to select a user.

To choose a user:

1. To locate the user by name, type the first few letters into the **Starts with** box and click **Go**.
2. To view additional pages of users, click the forward or back buttons.
3. To view a different number of users, select a different number from the **Items per page** drop-down list.
4. To sort the items, select **Show Users, Groups, and Roles**; **Show Users**; **Show Groups**; or **Show Roles** from the drop-down list.
5. To view the members of a group or role, double-click the role or group's name.
6. When you locate the correct user, select it and then click **OK**.

Choosing a permission set for replica objects

Use these instructions to choose a permission set.

To choose a user:

1. To locate the permission set by name, type the first few letters into the **Starts with** box and click **Go**.
2. To view additional pages of permission sets, click the forward or back buttons.
3. To view a different number of permission sets, select a different number from the **Items per page** drop-down list.
4. To sort the items, select **Show All**, **Show System Owned**, or **Show User Owned** from the drop-down list.
5. When you locate the correct permission set, select it and then click **OK**.

Choosing a storage area

On the Choose a storage page, select a storage area and then click **OK**.

Choosing replication and security modes

On the New Replication Job - Replication Options and Job Properties - Replication Options pages, you select a replication mode and a security mode.

The replication modes are:

- Federated mode, which may be used whether or not the source and target repositories are in a federation.
- Non-federated mode, which is named external replication mode in the *Distributed Configuration Guide*. This mode may be used whether or not the source and target repositories are in a federation.

The security modes determine how a permission set is assigned to replica objects in the target repository. The security modes are:

- Preserve
- Remap

Depending on whether you selected federated or non-federated (external) mode, the two security modes behave differently and replica objects are stored differently.

- When Federated and Preserve are selected:
 - If a replicated object's permission set exists in the target repository, the replica is assigned that permission set.
 - If a replicated object's permission set does not exist in the target repository, the object's permission set in the source repository is replicated to the target repository and the replica is assigned that permission set.
 - Replica objects in the target repository are stored in the same storage area as in the source repository.

If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.

- When Non-Federated and Preserve are selected:
 - If a replicated object's permission set exists in the target repository, the replica is assigned that permission set.
 - If a replicated object's permission set does not exist in the target repository, the replica is assigned the default replica permission set designated in the replication job.

This is the permission set selected on the New Replication Job - Target or Job Properties - Target page. If no permission set is chosen, the server creates a default permission set that gives RELATE permission to the world and group levels and DELETE permission to the replica owner.

- Replica objects in the target repository are stored in the same storage area as in the source repository.

If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.

- When Federated and Remap are selected:
 - If a replicated object's permission set exists in the target repository, the replica is assigned that permission set.
 - If a replicated object's permission set does not exist in the target repository, the replica is assigned the default replica permission set designated in the replication job.

This is the permission set selected on the New Replication Job - Target or Job Properties - Target page. If no permission set is selected, the server creates a default permission set that gives RELATE permission to the world and group levels and DELETE permission to the replica owner.

- Replica objects in the target repository are stored in the same storage area as in the source repository.

If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.

- When Non-Federated and Remap are selected:
 - The replica is assigned the default replica permission set designated in the replication job.
- This is the permission set chosen on the New Replication Job - Target or Job Properties - Target page. If no permission set is selected, the server creates a default permission set that gives RELATE permission to the world and group levels and DELETE permission to the replica owner.
- Replica objects are stored in the replica storage area designated in the replication job.

For more information on how the two replication modes operate, refer to the sections External Replication Mode and Federated Replication Mode in chapter 1, Building Blocks and Models, in the *Distributed Configuration Guide*.

Creating records migration jobs

To move content files from one storage area to another, use a records migration job. The target storage area can be another file store storage area or a secondary storage medium, such as an optical jukebox or a tape. If the target storage area is secondary storage, the storage must be defined in the repository as a storage area. That is, it must be represented in the repository by some type of storage object. When you define the records migration job, you can define parameters for selecting the files that are moved. For example, you might want to move all documents that carry a particular version label or all documents created before a particular date. All the parameters you define are connected with an AND to build the query that selects the content files to move.

When a records migration job runs, it generates a report that lists the criteria selected for the job, the query built from the criteria, and the files selected for moving. You can execute the job in report-only mode, so that the report is created but the files are not actually moved.

You must have Superuser privileges to create a records migration job.

To create a records migration job:

1. Navigate to **Administration > Job Management > Jobs**.
The **Jobs** list page appears.
2. Select **File > New > Records Migration Job**.
The New Records Migration Job - Info page appears.
3. Enter information on the **New Records Migration Job - Info** page:
 - a. **Name**: Type the name of the job.
 - b. **Job Type**: The system automatically prepopulates this field with Records Migration. You may, optionally, change the job type to be any value. The job type is displayed on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level**: Select a trace level. Trace levels range from 0 (no tracing) to 10 (a debugging level of tracing).
 - d. **Designated Server**: Select a server to run the job. The drop-down list displays all servers running against the repository of which Documentum Administrator is aware.
 - e. **State**: Select **Active** or **Inactive** to create the job in an active or inactive state.
 - f. **Deactivate on Failure**: Select to deactivate the job after a run that fails to execute correctly.
 - g. **Run After Update**: Select to run the job immediately after you save it.
 - h. **Save if Invalid**: Select to save the job, even if it is invalid.
 - i. Click **Next** to access the New Records Migration Job - Schedule page.
4. Enter information on the **New Records Migration Job - Schedule** page:
 - a. **Start Date And Time**: Designate a start date and time for the job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat**: Select a unit of time.
 - **Frequency**: Type how often the job is invoked.For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
 - c. **End Date And Time**: Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive. The default end date is 10 years from the current date and time.
 - d. Click **Next** to access the New Records Migration Job - Rules page.
5. Enter information on the **New Records Migration Job - Rules** page:
 - a. **Move Objects**: Designate the object type to migrate.
 - i. Click **Select type** to access the **Choose a type** page.
 - ii. Select the object type to migrate.
 - iii. Click **OK** to return to the New Records Migration Job - Rules page.
 - b. **To storage**: From the drop-down list, choose a target file store.

This is the file store to which the records are being migrated.

- c. **Select objects:** Select the objects for migration by setting criteria:
 - To select objects by setting criteria, select **By criteria** and then click **Define selection criteria** to access the Selection Criteria page.
For instructions about entering information on the Selection Criteria page, refer to [Defining selection criteria for a records migration job, page 290](#).
 - To select objects by query, select **By query**.
 - d. **Exclude objects if already migrated to secondary:** Select to exclude objects that are already migrated.
 - e. **Sub-components of virtual documents:** Select to include subcomponents of virtual documents. If selected, optionally designate an assembly version label by selecting **With assembly version label** and typing a version label.
 - f. **Formats:**
 - Clear **Primary format** to omit migrating the primary format of the documents. Primary format is selected by default.
 - Select **Annotations or Renditions** to include annotations or renditions in the migration job.
 - g. **Define version criteria:** Select to define version criteria for the migration job.
Use the instructions in [Defining version criteria for records migration job, page 291](#).
 - h. To designate the job as a test only, select **Test only**.
After you run the job, review the job report to ensure that the report migrates the correct documents. Clear the **Test only** checkbox when confident that the job runs as desired.
 - i. Click **Next** to access the New Records Migration Job - SysObject Info page.
6. Enter information on the **New Records Migration Job - SysObject Info** page:
- a. **Title:** Type the title.
 - b. **Subject:** Type the subject.
 - c. **Keywords:** Click **Edit** to access the **Keywords** page:
 - Type a new keyword in the **Enter new value** box and then click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.
The New Records Migration Job - SysObject Info page appears.
 - d. **Authors:** Click **Edit** to access the **Authors** page:
 - Type a new author in the **Enter new value** box and then click **Add**.
 - To remove an author, select the name and click **Remove**.

- To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.
- The New Records Migration Job - SysObject Info page appears.
- e. **Owner Name:** Click **Edit** to access the **Choose a user** page:
 - i. Select an owner.
 - ii. Click **OK**.

The system displays the New Records Migration Job - SysObject Info page.
 - f. To view more sysobject properties of the job, click **See More**.
7. Click **Finish**.
- The system saves the job and displays the Jobs list page.

Setting the rules of a records migration job

Use the New Records Migration Job - Rules or Job Properties - Rules page to define which documents are migrated by a records migration job.

To set the rules of a records migration job:

1. Access the Job Properties - Rules page:
 - a. Navigate to **Administration > Job Management > Jobs** to access the Jobs list page.
 - b. Select an existing records migration job and then select **View > Properties > Info** to access the Job Properties - Info page.
 - c. Select the **Rules** tab.

The **Job Properties - Rules** page appears.
2. **Move Objects:** Designate the object type to migrate.
 - a. Click **Select Type** to access the **Choose a type** page.
 - b. Select the object type to migrate.
 - c. Click **OK** to return to the New Records Migration Job - Rules page.
3. **To storage:** From the drop-down list, choose a target file store.
This is the file store to which the records are being migrated.
4. **Select objects:** Select the objects for migration by setting criteria:
 - To select objects by setting criteria, select **By criteria** and then click **Define selection criteria** to access the Selection Criteria page.
For instructions about entering information on the Selection Criteria page, refer to [Defining selection criteria for a records migration job, page 290](#).
 - To select objects by query, select **By query**.

5. **Exclude objects if already migrated to secondary:** Select to exclude objects that are already migrated.
6. **Sub-components of virtual documents:** Select to include subcomponents of virtual documents. If selected, optionally designate an assembly version label by selecting **With assembly version label** and typing a version label.
7. **Formats:**
 - Clear **Primary format** to omit migrating the primary format of the documents. Primary format is selected by default.
 - Select **Annotations** or **Renditions** to include annotations or renditions in the migration job.
8. **Define version criteria:** Select to define version criteria for the migration job.
Use the instructions in [Defining version criteria for records migration job, page 291](#).
9. To designate the job as a test only, select **Test only**.
After you run the job, review the job report to ensure that the report migrates the correct documents. Clear the **Test only** checkbox when confident that the job runs as desired.

Defining selection criteria for a records migration job

Use the Selection Criteria page to define selection criteria for a records migration job. At least one criterion must be selected. The four primary choices are not mutually exclusive; you can select any combination of the following:

- **Select documents by location**
- **Select documents by age**
- **Select documents by attributes**
- **Select documents by version**
- **Search all versions**

To define selection criteria:

1. To select documents by location:
 - a. Select the **Select documents by location** checkbox.
 - b. Select the **Use descend flag** checkbox to include all subfolders of the folder location.
 - c. Click the **Select location** link, select a cabinet or folder, and then click **OK**.
2. To select documents by age:
 - a. Select the **Select documents by age** checkbox.
 - b. Select a unit of time from the drop-down list and type a number in the field before the drop-down list.
For example, type 30 and select **Days**, or type 12 and select **Weeks**.
 - c. From the **Use age criteria** drop-down list, select the correct date property from which to measure the units of time: creation date, modify date, or access date.
3. To select documents by properties:

- a. Select the **Select documents by attributes** checkbox.
 - b. Select the **Select attribute** link to access the **Choose an attribute** page, locate the correct property, select the checkbox next to its name, and click **OK**.
 - c. From the drop-down list, select a **Comparison operator**, such as **is** or **begins with**.
This is the operator to use to compare the current value of the property you selected with the value entered in the **Attribute Value** field.
 - d. Type a value in the **Attribute value** field.
This is the value to compare with the current value of the property on which migration is based.
For example, if you want to migrate all records with a Project Name property of Proton, type *Proton* here.
4. To select documents by version, select the **Select documents by version** checkbox and type a version label.
For example, type *CURRENT*.
 5. To search all versions matching the selection criteria, select the **Search all versions** checkbox.
 6. Click **OK**.

Defining version criteria for records migration job

Set the version criteria for a records migration job on the Define Version page. At least one version criterion must be selected.

To set the version criteria for a records migration job:

1. To migrate the current version, select **Affect the current version**.
2. To migrate previous versions, select **Affect the previous versions** and select one of the following:
 - Affect all previous versions
This is the default choice.
 - Affect previous versions
Optionally type a number of most recent previous versions to ignore.
 - Affect only this specified version
Type the version you want affected, for example, 1.0.
 - Affect all versions prior to and including this version
For example, if you type 1.14, versions 1.0 through 1.14 are affected.
 - Affect all versions prior to this specific version
For example, if you type 1.14, versions 1.0 through 1.13 are affected. To exclude a number of older versions, type that number. If the specific version is 1.14 and the number of versions to ignore is 3, only versions 1.0 through 1.10 are affected.
3. Click **OK**.

Creating BOCS caching jobs

A BOCS content caching job will do the following:

- Create and schedule a job to collect a set of documents based on a query.
- Create caching requests for the documents with the BOCS destination information where the documents need to be.
- Send caching requests to DMS on a predetermined schedule.

Any user type can create a BOCS caching job; however, users must be logged in to a Documentum 6 repository.

Create criteria or a DQL query on the New BOCS Caching Job - Caching Rules or Job Properties - Caching Rules page for BOCS caching jobs.

Build criteria are limited to five lines of selection criteria defined by choosing properties from drop-down lists. The total length of the criteria cannot exceed 255 characters. The available properties are:

- Name
- Title
- Subject
- Authors
- Keywords
- Created
- Modified
- Accessed

After selecting a property, select an operand and type or select the correct value. For example, two rules might be **Name contains Chicago** and **Created before January 1, 2007**. When the BOCS caching job runs, the criteria are connected with AND, so that all criteria must apply to a particular object for it to be cached. If you require an OR, for example, **Name contains Chicago** or **Created before January 1, 2007** use a DQL query.

Use a DQL query to select objects from any selected object type using a DQL WHERE clause. There are no restrictions on the number of conditions in a DQL query, but the length is limited to 255 characters. BOCS caching job DQL queries can be based on the values of any standard SysObject properties, provided those values are present before an object is saved. For example, a BOCS caching DQL rule might be **object_name=Chicago or object_name=San Francisco**. DQL queries for BOCS caching jobs are not validated by Documentum Administrator.

To create a BOCS caching job:

1. Navigate to **Administration > Job Management > Jobs**.
The **Jobs** list page appears.
2. Select **File > New > BOCS Caching Job**.
The New BOCS Caching Job - Info page appears.
3. Enter basic information on the **New BOCS Caching Job - Info** page:

- a. **Name:** Type the name of the job.
 - b. **Job Type:** The system automatically prepopulates this field with *Distributed Content*. You may, optionally, change the job type to be any value. The job type is displayed on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level:** Select a trace level. Trace levels range from 0 (no tracing) to 10 (a debugging level of tracing).
 - d. **Designated Server:** Select a server to run the job. The drop-down list displays all servers running against the repository of which Documentum Administrator is aware.
 - e. **State:** Select **Inactive** or **Active** to create the job in an inactive or active state.
 - f. **Deactivate on Failure:** Select to deactivate the job after a run that fails to execute correctly.
 - g. **Run After Update:** Select to run the job immediately after you save it.
 - h. **Save if Invalid:** Select to save the job, even if it is invalid.
 - i. Click **Next** to access the New BOCS Caching Job - Schedule page.
4. Enter information on the **New BOCS Caching Job - Schedule** page:
 - a. **Start Date And Time:** Designate a start date and time for the BOCS caching job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat:** Select a unit of time.
 - **Frequency:** Type how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
 - c. **End Date And Time:** Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive. The default end date is 10 years from the current date and time.
 - d. Click **Next** to access the New BOCS Caching Job - Caching Rules page.
 5. Enter caching criteria on the **New BOCS Caching Job - Caching Rules** page:
 - a. **Object Type:** The type of objects needed to create caching messages. By default, dm_sysobject is selected.

Click the **Select** link to access the **Choose a type** page to select an object type.
 - b. **Selection Criteria:** Users can write their own DQL query or use the query builder to build the query for selecting the documents they want to create caching requests for.
 - Select **Build criteria (Maximum of 5 lines)** to create up to five lines using query builder. The first query section will have the property name; the second query section will have the condition (operator); the third query section will hold the value (operand). The length of the criteria is limited to 255 characters.
 - Select **DQL query** to create more complex queries.

There are no restrictions on the number of conditions in a DQL query, but the length is limited to 255 characters.
 - c. **Network Location:** The destination list of the cached content.

Click the **Select** link to access the **Choose Network Locations** page to select from which network locations the content should be cached.

- d. **Cutoff Date:** Select a cutoff date preference.
The caching method compares the cutoff date to the last updated date of the document to determine if a caching request needs to be generated for the document.
 - Select **Cache all selected content** to cache all documents without considering the last modified date of the document.
 - Select **Cache only selected content added/modified after** and then select a date, hour, minute, and second to cache documents based on the selected date and time criteria.
 - e. **Expiration:** Enter an expiration date at which the caching request will expire if it is not fulfilled by that date.
 - f. Click **Next** to access the New BOCS Caching Job - SysObject Info page.
6. Enter information on the **New BOCS Caching Job - SysObject Info** page:
- a. **Title:** Type the title.
 - b. **Subject:** Type the subject.
 - c. **Keywords:** Click **Edit** to access the **Keywords** page:
 - Type a new keyword in the **Enter new value** box.
 - Click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The New BOCS Caching Job - SysObject Info page appears.
 - d. **Authors:** Click **Edit** to access the **Authors** page:
 - Type a new author in the **Enter new value** box.
 - Click **Add**.
 - To remove an author, select the name and click **Remove**.
 - To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The New BOCS Caching Job - SysObject Info page appears.
 - e. **Owner Name:** Click **Edit** to access the **Choose a user** page:
 - Select an owner.
 - Click **OK**.The New BOCS Caching Job - SysObject Info page appears.
 - f. **Version Label:** The system displays the version information.
 - g. To view more sysobject properties of the job, click **See More**.

7. Click **Finish**.

The system saves the BOCS caching job and displays the Jobs list page.

Setting BOCS caching rules

Specify the caching options and the content to be selected for caching to the BOCS servers on the New BOCS Caching Job - Caching Rules or Job Properties - Caching Rules page.

Refer to [Creating BOCS caching jobs, page 292](#) for complete instructions on how to create a BOCS caching job.

The table below lists the fields on the New BOCS Caching Job - Caching Rules and Job Properties - Caching Rules pages with information about how to complete them.

Table 38. New BOCS Caching Job - Caching Rules and Job Properties - Caching Rules page properties

Field label	Description
Object Type	The type of objects needed to create caching messages. By default, dm_sysobject is selected. Click Select to access the Choose a type page to select an object type.
Selection Criteria	Users can write their own DQL query or use the query builder to build the query for selecting the documents they want to create caching requests for. <ul style="list-style-type: none"> • Select Build criteria (Maximum of 5 lines) to create up to five lines using query builder (maximum of 255 characters). The first query section will have the property name; the second query section will have the condition (operator); the third query section will hold the value (operand). • Select DQL query to create more complex queries. There are no restrictions on the number of conditions in a DQL query, but the length is limited to 255 characters.
Network Location	The destination list of the cached content. Click Select to access the Choose Network Locations page to select from which network locations the content should be cached.

Field label	Description
Cutoff Date	Select a cutoff date preference. The caching method compares the cutoff date to the last updated date of the document to determine if a caching request needs to be generated for the document. <ul style="list-style-type: none"> • Select Cache all selected content to cache all documents without considering the last modified date of the document. • Select Cache only selected content added/modified after and then select a date, hour, minute, and second to cache documents based on the selected date and time criteria.
Expiration	Enter an expiration date at which the caching request will expire if it is not fulfilled by that date.
Previous	Click to move to the previous page.
Next	Click to move to the next page.
OK or Finish	Click to save the changes and return to the Jobs list page.
Cancel	Click to return to the Jobs list page without saving any changes.

Creating job sequences

A job sequence is a job that runs a series of other jobs. The jobs in a sequence may be in any number of designated 5.3 and later repositories. For each job in the sequence, one or more predecessor jobs may be designated. Each job is run in sequence after any predecessors run. Jobs that do not have predecessors run in parallel. Each job sequence must contain at least one job that does not have any predecessors.

Use a job sequence when jobs must run in a particular order or the periods of time in which jobs run must not overlap. For example, if replication jobs replicate objects from multiple source repositories to a single target repository or if replication jobs replicate replica objects, use a job sequence to control the order in which the jobs execute.

You must be a Superuser to create a job sequence.

Job sequences can be created only in 5.3 and later repositories. All jobs in the sequence must be in 5.3 and later repositories.

All jobs in a job sequence must be inactive or the job sequence fails. This means you cannot use jobs that are active and scheduled to run independently of the job sequence. However, you are not prevented from selecting a job that is in the active state. If you select a job that is in the active state, change its state to inactive.

All jobs in a job sequence must execute a method where there is a method success code or method success status in the method object, and only such jobs are displayed in the user interface when a job sequence is created. Before you create a job sequence, examine the jobs you plan to include and the methods executed by those jobs to ensure that a method success code or method success status is present.

Each job sequence must include at least one job that has no predecessors. This job is the first job to run. There can be more than one job in the sequence with no predecessors.

The jobs in the sequence run in parallel except when a job has a predecessor. Documentum Administrator ensures that the job dependencies do not create a situation where job A must run after job B, job B must run after job C, and job C must run after job A. (This is called a cyclic dependency.)

Before you create a job sequence, obtain the username and password for a Superuser in each repository where the sequence runs a job.

Job sequences are on the Jobs list page with other types of jobs, and are deleted and edited as any other job.

To create a job sequence:

1. Navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select **File > New > Job**.
The New Job Sequence - Info page appears.
3. Enter information on the **New Job Sequence - Info** page:
 - a. **Name:** Type the name of the job.
 - b. **Job Type:** The system automatically populates this field with *Job Sequence*. You can, optionally, change the job type to be any value. The job type is displayed on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level:** Select a trace level. Trace levels range from 0 (no tracing) to 10 (debugging level of tracing).
 - d. **Designated Server:** Select a server to run the job. The drop-down list displays all servers running against the repository of which Documentum Administrator is aware.
 - e. **State:** Select **Active** or **Inactive** to create the job in an active or inactive state.
 - f. **Deactivate on Failure:** Select to deactivate the job after a run that fails to execute correctly.
 - g. **Run After Update:** Select to run the job immediately after you save it.
 - h. **Save if Invalid:** Select to save the job, even if it is invalid.
 - i. Click **Next** to access the New Job Sequence - Schedule page.
4. Enter information on the **New Job Sequence - Schedule** page:
 - a. **Start Date And Time:** Designate a start date and time for the job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat:** Select a unit of time.
 - **Frequency:** Type how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.

- c. **End Date And Time:** Designate an end date and time for the job or indicate a number of invocations after which the job becomes inactive. The default end date is 10 years from the current date and time.
 - d. Click **Next** to access the New Job Sequence - Connection Info page.
5. Enter information on the **New Job Sequence - Connection Info** page.

In the **Job Repositories** section, provide the name of each repository in which the sequence runs jobs and information for connecting to each repository.

By default, the current repository is listed with the currently-connected Superuser, but you are not required to run any jobs in the current repository.

In the **Job Sequence Information** section, select jobs to be placed in the sequence and enter job dependencies.

- a. **Add:** Click **Add** in the Job Repositories section to access the **Choose Repositories** page.
The system displays a list of repositories in which Documentum Administrator is aware. If a repository where you want to run a job is not listed, add a connection broker to which that repository projects to the list of connection brokers of which Documentum Administrator is aware. To add connection brokers, use the instructions in [Setting the connection broker list, page 36](#)
Select the repositories in which you want to run jobs, click **Add**, then click **OK** to return to the New Job Sequence - Connection Info page.
 - b. **Remove:** To remove a repository from the list, select it and then click Remove in the Job Repositories section.
If jobs in the repository are part of the sequence, you must remove the jobs first.
 - c. **User Name and Password:** Type the username and password for a Superuser in each repository.
The system validates the credentials when you provide the job sequence information in step f.
 - d. **Domain:** Type the domain for any repository running in domain-required mode.
 - e. **Add:** Click Add in the Job Sequence Information section.
The connection information entered in the Job Repositories section are validated when you click Add. If the connection information for any repository is not valid, provide correct credentials.
When all connection information is valid, the system displays the Choose Jobs page for one of the repositories. It lists jobs in that repository that can be included in the job sequence. Select the jobs to run in the sequence, click **Add**, then **OK** to return to the New Job Sequence - Connection Info page.
- Note:** The selected jobs must be inactive or the job sequence fails when it runs. If you select any active jobs, set them to inactive before the job sequence runs for the first time.
- f. **Remove:** To remove a job from the list, select it and then click Remove in the Job Sequence section.
You cannot remove a job if other jobs are dependent on it.

- g. **Edit:** To designate the job dependencies for each job that must run after another job completes, click **Edit** to access the **Choose jobs dependency** page. Select the listed job(s) that must run before the current job runs, then click **OK** to return to the New Job Sequence - Connection Info page.
- To remove a dependency, click **Edit** in the Job Sequence section to access the **Choose jobs dependency** page, clear the checkbox for any selected job, then click **OK**.
- Note:** Each job sequence must include one job that has no predecessors. This job is the first job to run. The jobs in the sequence run in parallel except when a job has a predecessor.
- h. Click **Next** to access the New Job Sequence - SysObject Info page.
- The system validates the job dependencies. If the job sequence cannot be validated, correct the errors before moving on to the next page.
6. Enter information on the **New Job Sequence - SysObject Info** page:
- Title:** Type the title.
 - Subject:** Type the subject.
 - Keywords:** Click **Edit** to access the **Keywords** page:
 - Type a new keyword in the **Enter new value** box.
 - Click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.
 The New Job Sequence - SysObject Info page appears.
 - Authors:** Click **Edit** to access the **Authors** page:
 - Type a new author in the **Enter new value** box.
 - Click **Add**.
 - To remove an author, select the name and click **Remove**.
 - To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.
 The New Job Sequence - SysObject Info page appears.
 - Owner Name:** Click **Edit** to access the **Choose a user** page:
 - Select an owner.
 - Click **OK**.
 The New Job Sequence - SysObject Info page appears.
 - To view more sysobject properties of the job, click **See More**.
7. Click **Finish**.
- The job is saved and the Jobs list page appears.

Providing repository connection and job information for a job sequence

Use the New Job Sequence - Connection Info or Job Properties - Connection Info page to select repositories and provide connection information, and to designate the jobs to run in a job sequence.

To provide connection and job information for a job sequence:

1. In the **Job Repositories** section, provide the name of each repository in which the sequence runs jobs and information for connecting to each repository.

By default, the current repository is listed with the currently-connected Superuser, but you are not required to run any jobs in the current repository.

- a. **Add:** To add a repository, click Add to access the Choose Repositories page.

The system displays the Choose Repositories page. A list is displayed of 5.3 and later repositories of which Documentum Administrator is aware. If a repository where you want to run a job is not listed, add a connection broker to which that repository projects to the list of connection brokers of which Documentum Administrator is aware. To add connection brokers, use the instructions in [Setting the connection broker list, page 36](#).

Select the repositories in which you want to run jobs, click **Add**, then click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

- b. **Remove:** To remove a repository from the list, select it and then click Remove in the Job Repositories section.

If jobs in the repository are part of the sequence, you must remove the jobs first.

- c. **User Name and Password:** Type the usernames and passwords for a Superuser in each repository.

The credentials are validated when you provide job sequence information in step 2.

- d. **Domain:** Type the domain for any repository running in domain-required mode.

2. In the **Job Sequence Information** section, enter job sequence information.

- a. **Add:** Click to add job sequence information for one of the repositories.

The connection information entered in the Job Repositories section are validated when you click Add. If the connection information for any repository is not valid, provide correct credentials.

When all connection information is valid, the system displays the Choose Jobs page for one of the repositories. It lists jobs in that repository that can be included in the job sequence. Select the jobs to run in the sequence, click **Add**, then click **OK** to return to the New Job Sequence - Connection or Job Properties - Connection Info page.

Note: The selected jobs must be inactive or the job sequence fails when it runs. If you select any active jobs, set them to inactive before the job sequence runs for the first time.

- b. **Remove:** To remove a job from the list, select it and then click Remove in the Job Sequence Information section.

You cannot remove a job if other jobs are dependent on it.

- c. **Edit:** To designate the job dependencies for each job that must run after another job completes, click Edit to access the Choose jobs dependency page. Select the listed job(s) that

must run before the current job runs, then click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

To remove a dependency, click **Edit** in the Job Sequence Information to access the Choose jobs dependency page, clear the checkbox for any selected job, then click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

Note: Each job sequence must include one job that has no predecessors. This job is the first job to run. The jobs in the sequence run in parallel except when a job has a predecessor.

Selecting repositories for a job sequence

Use the instructions in this section to select repositories on the Choose Repositories page for a job sequence.

To access the Choose Repositories page, click **Add** in the Job Repositories section on the New Job Sequence - Connection Info or Job Properties - Connection Info page.

The Choose Repositories page displays 5.3 and later repositories of which Documentum Administrator is aware. If a repository where you want to run a job is not listed, add a connection broker to which that repository projects to the list of connection brokers of which Documentum Administrator is aware. To add connection brokers, use the instructions in [Setting the connection broker list, page 36](#).

To select repositories:

1. On the Choose Repositories page, select the repositories in which you want to run jobs and click **Add**.
The repositories are moved to the right side of the selector.
2. To remove a repository from the right-hand list, select the repository and click **Remove**.
3. Click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

Selecting jobs for a job sequence

Use the instructions in this section to select jobs on the Choose jobs page that the job sequence runs.

To access the Choose jobs page, click **Add** in the Job Sequence Information section on the New Job Sequence - Connection Info or Job Properties - Connection Info page.

To select jobs for a job sequence:

1. On the Choose jobs page, select a repository from the **Select from repository** drop-down list.
2. Select the jobs to run in the sequence and click **Add**.
The jobs move to the right-hand side of the page. The jobs must be inactive or the job sequence fails when it runs. If you select any active jobs, set them to inactive before the job sequence runs for the first time.
3. To remove jobs from the sequence, select the jobs and click **Remove**.

4. Click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

Setting dependencies for a job sequence

Use the instructions in this section to designate job dependencies in a job sequence. A dependency defines which job(s) must run before the current job is run.

Access the Choose jobs dependency page by clicking **Edit** in the Job Sequence Information section on the New Job Sequence - Connection Info or Job Properties - Connection Info page.

Note: Each job sequence must include one job that has no predecessors. This job is the first to run. The jobs in the sequence run in parallel except when a job has a predecessor.

To set job dependencies:

1. On the Choose jobs dependency page, select the listed job(s) that must run before the current job runs.
2. To remove a dependency, clear the checkbox for any selected job.
3. Click **OK** to return to the New Job Sequence - Connection Info or Job Properties - Connection Info page.

Running jobs

Jobs typically run at predetermined intervals. The jobs that exist in all repositories have default schedules when they are created. Refer to [Changing the schedule of a job, page 271](#), for instructions on modifying a job's schedule.

Most jobs pass standard arguments to the method executed by the job. The arguments are set on the Method tab for each job, and can be modified in most cases.

Use these instructions to run a job manually (at a time other than the scheduled run time). Note that a job invoked in this fashion runs when the agent exec process starts the job, not when you click **Run**. The agent exec process polls the repository every five minutes, so the start of the job is delayed up to five minutes, depending on when you clicked **Run** and when the agent exec process last polled the repository.

To run a job:

1. Select the job to run.
2. Click **Tools > Run**.
When the agent exec process next polls the repository, the job runs.
3. To view the status of a running job after you start it, click **View > Refresh**.
The list page refreshes and the Status column for the job is updated. You may need to click **View > Refresh** several times because the job does not run immediately after you click **Tools > Run**.
4. To view the job report, select the job and click **View > Report**.

5. To view the trace log for the job, select the job and click **View > Trace**.

The tracing level for the job must be set high enough to generate a trace log, or no trace log is found.

Viewing the status of a running job

To view the status of a running job after you start it, click **View > Refresh**.

The list page refreshes and the Status column for the job is updated. You may need to click **View > Refresh** several times because the job does not run immediately after you click **Tools > Run**.

Viewing job reports

When a job runs, it generates a report. The report summarizes the results of the job. You can view the reports for one or more jobs.

To view jobs reports:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the jobs whose reports you want to view.
3. Select **View > Report** (or right-click and select **View Job Report**).
The system displays the job report.
4. If you selected multiple jobs, click **Next** to view the next report.
5. After the last report is viewed, click **OK** or **Cancel** to return to the Jobs list page.

Setting the trace level for a job

Trace logs contain status information logged by a job. The trace level set for a particular job determines the amount of information logged. The default trace level for a job is 1 (minimal trace information), with a maximum level of 10 (debug-level tracing). A trace level of 4 through 6 provides a medium level of debugging.

To set the trace level for a job:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the job and then select **View > Properties > Info**.
The system displays the Job Properties - Info page.
3. Select a trace level from the **Trace Level** drop-down list.
4. Click **OK**.

The system displays the Jobs list page.

Viewing job trace logs

Trace logs contain status information logged by a job. The trace level set for a particular job determines the amount of information logged. The default trace level for a job is 1 (minimal trace information), with a maximum level of 10 (debug-level tracing). For information on setting a different trace level, refer to [Setting the trace level for a job, page 303](#).

Use these instructions to view the trace log for a job.

To view job trace logs:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the jobs whose trace logs you want to view.
3. Select **View > Trace** (or right-click and select **View Trace File**).
The Job Trace File page displays the log file, if available.
4. If you selected more than one job, click **Next** to view the next trace log.
5. After viewing the last trace log, click **OK** or **Cancel** to return to the Jobs list page.

Modifying jobs

The pages for modifying a job are identical to those used for creating a job. Click the Help button on each page for assistance in completing that page.

To modify a job:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the job to modify and then select **View > Properties > Info**.
The system displays the Job Properties - Info page.
3. Modify fields on the Job Properties - Info page.
4. Click the tabs to access other pages where you want to change information.
5. Click **OK** or **Cancel** to return to the Jobs list page.

Deleting jobs

Use the instructions in this section to delete a job.

To delete a job:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the job to delete.
3. Select **File > Delete**.
The job is deleted.

Deactivating jobs on failure

Use the instructions in this section to configure a job so that it becomes inactive if it fails.

To deactivate jobs on failure:

1. Connect to the repository and navigate to **Administration > Job Management > Jobs**.
The system displays the Jobs list page.
2. Select the job and then select **View > Properties > Info**.
The system displays the Job Properties - Info page.
3. Select the **Deactivate on failure** checkbox.
4. Click **OK**.
The system displays the Jobs list page.

Job descriptions

These jobs are created at repository creation. The descriptions discuss arguments that can be modified for each job.

- [ACL replication \(dm_ACLReplication\), page 306](#)
- [ACL replication \(dm_ACLRepl_repository\), page 306](#)
- [Archive \(dm_DMArchive\), page 307](#)
- [Audit management \(dm_AuditMgt\), page 307](#)
- [Consistency checker \(dm_ConstistencyChecker\), page 308](#)
- [Content replication \(dm_ContentReplication\), page 308](#)
- [Content warning \(dm_ContentWarning\), page 309](#)
- [Create full-text events \(dm_FTCreateEvents\), page 309](#)
- [Index agent startup \(dm_FTIndexAgentBoot\), page 311](#)
- [Data dictionary publisher \(dm_DataDictionaryPublisher\), page 312](#)
- [Database space warning \(dm_DBWarning\), page 312](#)
- [Distributed operations \(dm_DistOperations\), page 312](#)

- Dmclean (dm_DMClean), page 313
- Dmfilescan (dm_DMfilescan), page 313
- Federation copy (dm_FederationCopy), page 313
- Federation export (dm_FederationExport), page 313
- Federation import (dm_FederationImport), page 314
- Federation status (dm_FederationStatus), page 314
- Federation update (dm_FederationUpdate), page 314
- File report (dm_FileReport), page 314
- Group rename (dm_GroupRename), page 315
- LDAP synchronization (dm_LDAPSynchronization), page 315
- Log purge (dm_LogPurge), page 316
- Queue management (dm_QueueMgt), page 316
- Remove expired retention objects (dm_RemoveExpiredRetnObjects), page 317
- Rendition manager (dm_RenditionMgt), page 318
- SCS log purge (dm_SCSLogPurgeJob), page 318
- State of repository report (dm_StateOfDocbase), page 318
- Swap info (dm_SwapInfo), page 319
- Update statistics (dm_UpdateStats), page 319
- User change home repository (dm_UserChgHomeDb), page 319
- User rename (dm_UserRename), page 320
- Version management (dm_VersionMgt), page 320
- WfmsTimer (dm_WfmsTimer), page 320

ACL replication (dm_ACLReplication)

The ACL Replication job first sets external ACLs for replication within a repository federation and then launches ACL (permission set) replication. It is installed in an inactive state. For complete information on replication and replication jobs, refer to the *Distributed Configuration Guide*.

ACL replication (dm_ACLRepl_repository)

The dm_ACLRepl_job replicates ACLs to repositories in a federation. There is one job for each member repository, and *repository* is the first 19 bytes of the repository's name. It is an internal template job that is installed in an inactive state. Do not edit or remove this job. For complete information on replication and replication jobs, refer to the *Distributed Configuration Guide*.

Asynchronous Write (dm_AsyncronousWrite)

When users import documents in asynchronous mode, there may be instances where some or all content may not be immediately replicated from BOCS to ACS. This might happen if the Documentum Messaging Services (DMS) server was not available or there were network issues between BOCS, DMS, and/or ACS.

The Asynchronous Write job polls for content still in a parked state and generates new messages for the DMS server to pass to BOCS to request the upload of the parked content. After execution, the job lists all content objects that had yet to be moved from the parked state and for which messages were sent to the DMS server. If a BOCS server receives a request to migrate content that is has already processed, it will ignore the request.

This job is inactive by default, but should be enabled whenever asynchronous mode is allowed. The job is scheduled to run daily at 2:00 a.m. by default.

Archive (dm_DMArchive)

The Archive tool automates archive and restore between content areas. Archive older or infrequently accessed documents to free up disk space for newer or more frequently used documents. Restore archived documents to make the archived documents available when users request them. For complete information on how to configure archiving, refer to Archiving and restoring documents in the *Content Server Administration Guide*.

The Archive tool is active by default and runs once daily. Refer to the *Content Server Administration Guide* for full details on the arguments.

Audit management (dm_AuditMgt)

The Audit Management tool deletes audit trail entries. When an audited event occurs, an audit trail entry is created for that event. If the audit trail entries are not removed periodically, the tables for the dm_audittrail object type can grow quite large and performance degrades when audited events occur. The Audit Management tool automates the task of removing unnecessary audit trail objects.

Which audit trail objects to remove is determined by the cutoff_days and custom_predicate arguments. The cutoff_days argument specifies the age of the objects to delete. The custom_predicate argument is then applied to those items meeting the age requirement.

By default, the cutoff_days argument is set to 90 and the custom_predicate argument is set to remove only audit trail objects generated by system-defined events. (The tool does not delete audit trail objects generated by user-defined events by default.)

To change the age cutoff, reset the cutoff_days argument.

To choose the objects to remove from the subset selected by cutoff_days, change the custom_predicate argument. By default, the custom predicate includes three conditions:

- delete_flag=TRUE
- dequeued_date=value (value is computed using the cutoff_days argument)
- r_gen_source=1

You cannot change the first two conditions. The third condition, r_gen_source=1, directs the server to delete only audit trail objects generated by system-defined events. If you want to remove only audit trail objects generated by user-defined events, reset this to r_gen_source=0. If you want to remove audit trail objects generated by both system- and user-defined events, remove the r_gen_source expression from the custom predicate.

You may also add other conditions (for example, event=approved) to the default custom predicate.

The Audit Management tool generates a status report that lists the deleted dm_audittrail entries. The report is saved in the repository in /System/Sysadmin/Reports.

If an error occurs while the tool is executing, the server sends email and inbox notification to the user specified by the -auditperson argument.

The Audit Management tool is installed in the inactive state. The first time you execute the tool, it may take a long time to complete.

Consistency checker (dm_ConsistencyChecker)

The Consistency Checker tool scans the repository and reports any inconsistencies such as type or object corruption, objects that reference a user, group, or other object that is nonexistent in the repository, and so forth. This tool does not attempt to fix any of the inconsistencies. Contact Documentum Technical Support for assistance in correcting errors in your repository found by the consistency checker.

It is recommended that you run this tool on a repository before upgrading the repository to a new version of the Documentum Server.

The Consistency Checker job is active by default and is set to run once a day.

For information on each check run by the job, refer to Appendix A, Consistency Checks, in the *Content Server Administration Guide*.

Content replication (dm_ContentReplication)

The Content Replication tool automates content replication between the component storage areas of a distributed storage area. A content replication job looks for all content not locally present, gets the files while connected to other sites, and performs an IMPORT_REPLICA for each content file in need of replication. The job generates a report that lists each object replicated. The report is saved to the repository in /System/Sysadmin/Reports/ContentReplication.

If the report runs against the content at a remote distributed site, the report name will have the sites server configuration name appended. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/ContentReplicationLondon.

In a distributed environment, the jobs argument values for the remote sites are based on those of the Content Replication job for the primary site, but the job name and target server will be unique for each site. The job name has the format:

```
dm_ContentReplicationserverconfig.object_name
```

The jobs target_server property identifies the local server performing the replication using the format repository.serverconfig@hostname. The Content Replication job is inactive by default.

The Content Replication tool requires enough temporary disk space to transfer the largest content file to be replicated.

Content warning (dm_ContentWarning)

The Content Warning tool notifies you when disks that you use for content and index file storage approach a user-defined capacity. The notification is sent to the repository inbox of the queueperson and as an email message. The tool also generates a report that is stored in the Reports folder under the Sysadmin folder in the System cabinet.

The tool determines where the repository is storing its content and index files and then uses operating system commands to determine whether these disks are reaching the specified threshold. When the disk space used meets or exceeds the value in the tools percent_full argument, a notification is sent to the specified queueperson and a report is generated and saved to the repository in /System/Sysadmin/Reports/ContentWarning.

If the tool was run against the content at a remote distributed site, the report name will have the sites server config name appended. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/ContentWarningLondon.

The Content Warning tool is installed in the active state by default.

Create full-text events (dm_FTCreateEvents)

The dm_FTCreateEvents job may be used in two ways:

- To complete an upgrade by causing any objects missed by the pre-upgrade indexing operations to be indexed

The job generates events for each indexable object added to a repository between the time a new 5.3 or later full-text index is created for a 5.2.5 repository and when the repository is upgraded to 5.3

For example, a copy of a 5.2.5 repository can be used to create a new 5.3 index. Depending on when the production repository is upgraded, new indexable objects may be created in the production repository after the new 5.3 index is created. When the production repository is upgraded to 5.3 and begins to use the new index, the repository contains objects that are not yet indexed. Running dm_FTCreateEvents generates events for the new objects. An index agent running in normal mode uses the events to submit the objects for indexing.

This is the default behavior of the job.

- To generate the events required to reindex an entire 5.3 SP1 or later repository

The `-full_reindex` argument must be set to TRUE to generate the required events. Reindexing the repository does not require deleting the existing index.

The job itself does not update the index. The job can optionally generate a list of object IDs of objects that must be indexed, rather than generating events for those objects. The list is used to submit objects to the index agent in file mode for indexing. The *Content Server Full-Text Indexing System Installation and Administration Guide* contains instructions for using the index agent's file mode.

By default, the job is installed in the active state to run daily at 11 p.m. The job processes new objects in batches of 50,000. If all objects are not processed in one run, the job continues executing each day at 11 p.m. When it finds no more objects to process, it sets itself to inactive. When the `-full_reindex` argument is set to TRUE, the events are created in reverse chronological order by `r_modify_date` and therefore the most recently-modified or created objects are indexed first.

The first time the job runs in its default mode, the job determines the last object indexed by an index agent running in migration mode and the date on which that object was indexed. The job searches for objects modified after that date and before the job runs for the first time and generates events for those objects. On its subsequent iterations, the job searches for objects modified after the end of the last iteration and before the beginning of the current iteration.

Before the job is run in a 5.3 SP1 or later repository with `full_reindex` set to TRUE, you must manually create a high-water-mark queue item (`dmi_queue_item`) and specify the `r_object_id` of the queue item as the `-high_water_mark_id` argument of the `dm_FTCreateEvents` job.

There are nine arguments to `dm_FTCreateEvents` that you can optionally modify:

- `-max_events_per_run`

This is the maximum number of events generated each time the job runs. The default value is 50,000. If `max_events_per_run` is not set or is set to zero, the job creates events for all objects changed or created between `min_date` and `max_date`.

- `-high_water_mark_id`

This is the object ID of the queue item to use for obtaining the last date for which queue items were created. If it is not specified, the job queries for the most recently created `dmi_queue_item` in which the value of `item_name` is Full-text re-index high water mark and the value of `task_state` is done.

In full reindex mode, you must provide the `r_object_id` of the manually-created high-water-mark queue item.

- `-min_date`

The earliest date on which objects were modified for which the job creates events. The default value is the value of the `date_sent` property of the migration-mode queue item for indexing.

- `-max_date`

The most recent date on which objects were modified for which the job creates events. The default value is the date on which the job runs for the first time.

- `-file`

When submitted with a filename, the object IDs of objects that require events are written to a file. The syntax is:

```
-file full_path_of_file
```

The file may then be used with the index agent in file mode for submitting objects for indexing. The *Content Server Full-Text Indexing System Installation and Administration Guide* contains information on how to use a file of object IDs to submit objects for indexing.

- **-full_reindex**

This argument is available only in 5.3 SP1 and later Content Servers. The default value is FALSE. When set to false, the job generates events for each indexable object added to a repository between the time a new 5.3 full-text index is created for a 5.2.5 repository and when the repository is upgraded. This is the behavior of the job when it is installed.

When set to TRUE, events are generated for all indexable objects in reverse chronological order by the value of the r_modify_date.

- **-current_only**

This argument is available only in 5.3 SP1 and later Content Servers. Use when -full_reindex is set to TRUE. The default value is FALSE. When set to TRUE, new events are generated only for the CURRENT version of each indexable object.

- **-queueperson**

User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server config object.

- **-window_interval**

Execution window for the tool, expressed in minutes. The *Content Server Full-Text Indexing System Installation and Administration Guide* contains complete information on the -window_interval argument.

Use these instructions to create the high-water mark queue item.

To create the high-water mark queue item:

1. On any Documentum Administrator list page, click **API**.
2. In the **Command** box, type **create,c,dmi_queue_item** .
Use the r_object_id displayed by this command when you use this job to reindex the repository.
3. Click **Execute**.
4. Type **save,c,1**.
5. Click **Execute**.
6. Click **OK**.

Index agent startup (dm_FTIndexAgentBoot)

The dm_FTIndexAgentBoot job starts index agents associated with a Content Server when that Content Server starts up. Do not modify the dm_FTIndexAgentBoot job. Modifying the job is not supported.

Data dictionary publisher (dm_DataDictionaryPublisher)

The Data Dictionary Publisher tool publishes the data dictionary information. The data dictionary is information about object types and properties stored in internal objects by Content Server and made available to client applications through the publishing operation. For more information on the data dictionary, refer to Chapter 4, The Data Model, in *Content Server Fundamentals* and Appendix E, Populating and Publishing the Data Dictionary, in the *Content Server Administration Guide*.

Database space warning (dm_DBWarning)

The Database Space Warning tool scans the RDBMS to determine how full the tablespace (Oracle or DB2) or device (Sybase) is, whether any tables are fragmented beyond a user-specified limit, and whether the expected number of Documentum indexes are present. The tool is not installed in repositories running with SQL Server.

You can modify these arguments to the method:

- percent_full is the percent-full threshold at which a message is sent.
- queueperson is the name of the user who receives email and inbox notifications from the tool. The default is the username specified in the Operator Name property of the server config object.
- max_extents is the number of extents that an RDBMS table can have before it is reported as fragmented.

If space or extents reach the specified limit, an inbox notification is sent to the queueperson. The job also checks that the repository has the expected number of indexes and automatically rebuilds missing indexes.

The Database Space Warning tool is installed in the active state. On Sybase, you must set the ddl in tran database option to TRUE to run this job.

Distributed operations (dm_DistOperations)

The dm_DistOperations job performs inter-repository distributed operations. These tasks include:

- Propagating distributed events (dmi_queue_items) across repositories
- Creating checkout references for remote checkout operations
- Refreshing reference links

The dm_DistOperations job is configured to run every five minutes by default. Do not change the schedule.

It is installed in the repository in an inactive state.

Dmclean (dm_DMClean)

The Dmclean tool automates the dmclean utility. The utility scans the repository for orphaned content objects, ACLs, and annotations (dm_note objects). The utility also scans for the workflow templates created by the SendToDistributionList command (a DTC command that routes a document to multiple users concurrently) and left in the repository after the workflow completed. The utility generates an API script to remove these orphans. The Dmclean tool performs dmcleans operations and (optionally) runs the generated script. For more information on the dmclean utility, refer to Chapter 7, Content Management, in the *Content Server Administration Guide*.

When the agent exec program invokes the script, the tool generates a report showing what content objects, content files, ACLs, notes, and workflow templates would be removed upon execution of the generated script. The status report is saved in /System/Sysadmin/Reports/DMClean.

Whether the generated script runs is controlled by the tools clean_now argument. This argument is set to TRUE by default. If you set it to FALSE, the script is not run; it must be run manually to remove the orphan objects. (The script is stored in %DOCUMENTUM\dba\log\hexrepositoryid\sysadmin.)

The Dmclean tool is installed in the inactive state.

Dmfilescan (dm_DMfilescan)

The Dmfilescan tool automates the dmfilescan utility. This utility scans a specific storage area or all storage areas for any content files that do not have associated content objects and generates an IDQL script to remove any that it finds. The tool generates and (optionally) executes the IDQL script.

Dmfilescan also generates a status report that lists the files it has removed. The report is saved in the repository in /System/Sysadmin/Reports/DMFilescan.

Dmfilescan is installed in the inactive state.

Federation copy (dm_FederationCopy)

The Federation Copy tool transfers LDIF files, which contain user and group information, to member repositories from the governing repository. The job is installed in an inactive state. For complete information on repository federations and the federation jobs, refer to the *Distributed Configuration Guide*.

Federation export (dm_FederationExport)

The Federation Export tool exports user and group information from the governing repository to an LDIF file. The job is installed in an inactive state. For complete information on repository federations and the federation jobs, refer to the *Distributed Configuration Guide*.

Federation import (dm_FederationImport)

The Federation Import tool imports an LDIF file that contains user and group information into a member repository. The job is installed in an inactive state. When you create a federation, the job is activated in the member repositories. For complete information on repository federations and the federation jobs, refer to the *Distributed Configuration Guide*.

Federation status (dm_FederationStatus)

The Federation Status tool polls the members of a federation to determine the current status of any Federation Import jobs running on the member repository. The job is installed in an inactive state. When you create a federation, the job is activated in the governing repository. For complete information on repository federations and the federation jobs, refer to the *Distributed Configuration Guide*.

Federation update (dm_FederationUpdate)

The Federation Update tool executes on the governing repository of a federation to run all other methods in sequence, pushing user, group, and ACL changes to the member repositories. The job is installed in an inactive state. When you create a federation, the job is activated in the governing repository. For complete information on repository federations and the federation jobs, refer to the *Distributed Configuration Guide*.

File report (dm_FileReport)

The File Report tool generates a report listing all documents in the repository and their corresponding content files. The tool assists you in restoring deleted repository documents.

When a document must be re-created, this report can identify which files to restore from backup to rebuild the document. This tool is useful for restoring a single document (or a small set of documents), which cannot be done from database backup files.

The File Report tool, as installed, runs a full report once a week against all file storage areas in the repository. You can also run incremental reports and reports that examine only a subset of the storage areas for the repository.

File Report only provides a mechanism for restoring document content. Document metadata must be restored based upon the metadata in the report.

The File Report tool is installed in an inactive state. When you make the job active, set it up to run on the same schedule as file system backups. We recommend scheduling nightly incremental reports and less-frequent full repository reports. Set the `incremental_report` argument to TRUE to run an incremental job.

If your repository is so large that creating full reports is not practical or generates cumbersome files, set up multiple jobs, each corresponding to a different storage area. Set the `storage_area` argument to the storage area on which you are running the report.

Refer to the *Content Server Administration Guide* for more information on the arguments for the File Report tool.

Group rename (dm_GroupRename)

The Group Rename tool renames repository groups and works in conjunction with Documentum Administrator's Groups pages. To rename a group, use the Groups pages to identify the group and its new name. You then have two options for executing the rename operation:

- Run the Group Rename tool immediately after you identify the new name.
- queue the operation until the next scheduled execution of the Group Rename tool.

The Group Rename tool generates a report that lists the changes made to the repository objects for the group rename. The report is saved in the repository in /System/Sysadmin/Reports/GroupRename.

The tool is installed in the inactive state.

LDAP synchronization (dm_LDAPSynchronization)

The LDAP Synchronization tool finds the changes in the user and group information in an LDAP-compliant directory server that have occurred since the last execution of the tool and propagates those changes to the repository. If necessary, the tool creates default folders and groups for new users. If there are mapped user properties, those are also set.

Which operations the tool can perform depends on what kind of directory server is in use. If using Netscape iPlanet Directory Server, Oracle Intranet Directory Server, or MS Active Directory on a Microsoft Windows platform, the tool can:

- Import new users and groups in the directory server into the repository.
- Rename users in the repository if their names changed in the directory server.
- Rename groups in the repository if their names changed in the directory server.
- Inactivate users in the repository that if they were deleted from the directory server.

If you use iPlanet, you must enable the changelog feature to use the renaming and inactivation operations. Instructions for enabling the changelog feature are found in the vendors iPlanet Administration Guide.

The renaming and inactivation operations are not supported on MS Active Directory on UNIX platforms.

The tool is installed in the inactive state. After it is activated, it is executed once a day at 4 a.m. by default. Before you set it to the active state, you must define the ldap_config object for the repository. For information on creating the ldap_config object for the repository, refer to the *Content Server Administration Guide* and to [LDAP Servers, page 110](#).

The behavior of the tool is determined by the property settings of the ldap_config object. The tool has four arguments that you can use to override the property settings controlling which operations the tool performs. The arguments override the properties of the same names in the ldap_config object. They are deactivate_user_option, import_mode, rename_group_option, and rename_user_option.

In repositories 5.3 and later, use the method argument source_directory to designate the LDAP servers that are being synchronized. All LDAP servers associated with a particular server config object can be synchronized or only particular LDAP servers. If the argument is not used to designate particular LDAP servers, the job synchronizes all LDAP servers associated with the server config object.

Log purge (dm_LogPurge)

The Log Purge tool deletes old logs. The logs and the locations from which they are deleted are:

Table 39. Logs deleted by log purge job

Log type	Delete from
Server log files	Documentum Server installation log location
Connection broker log files	Documentum Server installation log location
Agent Exec log files	Documentum Server installation log location
Session log files	Documentum Server installation log location
Result log files	Temp cabinet
Job log files	Temp cabinet
Job reports	/System/Sysadmim/Reports folder
Lifecycle log files	Documentum Server installation log location

Files are considered old and are deleted if they were modified prior to a user-defined cutoff date. By default, the cutoff date is 30 days prior to the current date. For instance, if you run Log Purge on July 27, all log files that were modified before June 28 are deleted. You can change the cutoff interval by setting the -cutoff_days argument for the tool.

Log Purge generates a report that lists all directories searched and the files that were deleted. The report is saved in the repository in /System/Sysadmin/Reports/LogPurge.

The Log Purge tool is installed in the inactive state.

Site Caching Services logs are deleted by the SCS Log Purge job. Refer to [SCS log purge \(dm_SCSLogPurgeJob\), page 318](#) for information on that job.

Queue management (dm_QueueMgt)

The QueueMgt tool deletes dequeued inbox items. Whenever an item is queued to a user's inbox, an object of type dmi_queue_item is created for the queued item. When a user forwards or otherwise removes the item from the inbox, the corresponding dmi_queue_item object is marked dequeued, but it is not removed from the repository. This tool automates the task of removing these unnecessary dmi_queue_item objects.

Which dmi_queue_items to remove is determined by the cutoff_days and custom_predicate arguments. The cutoff_days argument specifies the age of the objects to delete. The custom_predicate argument is applied to those items meeting the age requirement, allowing you to delete all or only

some of them. For example, the tool could delete all dequeued dmi_queue_items that are older than 30 days and were queued to a specific user.

QueueMgt generates a status report that provides a list of the deleted dmi_queue_items.

The QueueMgt tool is installed in the inactive state.

Remove expired retention objects (dm_RemoveExpiredRetnObjects)

The RemoveExpiredRetnObjects tool removes objects with expired retention dates from content-addressed storage areas. It is available only in repositories version 5.2.5 SP1 and later, and can be used only in content-addressable storage areas.

The tool invokes the CHECK_RETENTION_EXPIRED administration method to determine which objects to remove. By default, the tool operates only on objects stored in content-addressable storage areas that require a retention date. You can also direct the tool to operate on content-addressable storage areas that allow but do not require a retention date by setting the INCLUDE_ZERO_RETENTION_OBJECTS argument. The tool never includes objects stored in content-addressable storage areas that do not allow retention periods. For more information on retention type storage areas, refer to [Storage, page 379](#) and the *Content Server Administration Guide*.

The tool generates a status report that provides a list of the deleted objects. The report is saved in the repository in /System/Sysadmin/Reports/ RemoveExpiredRetnObjects. For each deleted object, the report lists the following properties:

- r_object_id
- object_name
- a_storage_type
- r_creation_date
- retention_date

The retention_date property is a computed property.

The tool is installed in the inactive state.

In addition to the -queueperson and -window_interval arguments, the tool takes two arguments:

- -query *qualification*, a string argument which identifies the objects that are selected for possible removal.

This is a DQL where clause qualification.

- -include_zero_retention_objects, a Boolean argument that is set to FALSE by default.

Setting this to T (TRUE) directs the job to consider objects stored in a content-addressable storage area that allows but does not require a retention period.

After you find and remove the repository objects that have expired content, use Dmclean with the -include_ca_store argument to remove the resulting orphaned content files and content objects. For more information on Dmclean, refer to [Dmclean \(dm_DMclean\), page 313](#).

Refer to CHECK_RETENTION_EXPIRED in the Administration method operations section of the *Content Server DQL Reference Manual* for information about the method underlying RemoveExpiredRetnObjects.

Rendition manager (dm_RenditionMgt)

The Rendition Manager tool removes unwanted renditions of versioned documents. A rendition is a copy of a document's content in a format different than the original. Renditions, like the original content files, are stored in storage areas. Over time, unnecessary renditions from previous versions of documents can take up noticeable amounts of disk space.

The tools arguments define which renditions are removed. The tool can delete renditions based on their age, format, or source (client- or server-generated). The tool removes the content objects associated with unwanted renditions. The next execution of the Dmclean tool automatically removes the renditions orphaned content files (assuming that Dmcleans clean_content argument is set to TRUE). The report generated by the tool lists the renditions targeted for removal.

The Rendition Manager tool is installed in the inactive state.

SCS log purge (dm_SCSLogPurgeJob)

Only repositories where you have installed Site Caching Services 5.2 or above contain this job and its associated method. It is similar to the Log Purge job.

Files are considered old and are deleted if they were modified prior to a user-defined cutoff date. By default, the cutoff date is 30 days prior to the current date. For instance, if you run SCS Log Purge on July 27, all log files that were modified before June 28 are deleted. You can change the cutoff interval by setting the -cutoff_days argument for the tool.

SCS Log Purge generates a report that lists all directories searched and the files that were deleted. The report is saved in the repository in /System/Sysadmin/Reports/SCSLogPurge.

The SCS Log Purge tool is installed in the inactive state.

State of repository report (dm_StateOfDocbase)

The StateofDocbase tool generates a report to help troubleshoot repository problems. A partial list of the information included in the report is:

- The property values in the docbase config object
- Server initialization information from the server.ini file
- The directory paths defined by the location objects in the server config object
- Version numbers of your server, RDBMS, and operating system

The State of the Repository Report is installed in the active state.

Swap info (dm_SwapInfo)

The Swap Info tool uses operating system commands to retrieve information about swap space usage and availability. The tool generates a report but does not issue warnings because there is no realistic way to determine if the swap space is too low as this determination has too many variables.

The Swap Info tool is installed in the active state.

The Swap Info tool is not installed if Content Server is running on an HP-UX machine.

Update statistics (dm_UpdateStats)

The Update Statistics tool generates current statistics for the RDBMS tables.

Generating statistics is always useful, particularly after performing load operations or if table key values in the underlying RDMBS tables are not normally distributed.

When you run the tool against an Oracle or Sybase database, the tool uses a file that contains commands to tweak the database query optimizer. For Oracle, the file is named `custom_oracle_stat.sql`. For Sybase, it is named `custom_sybase_stat.sql`. The file is stored in `%DOCUMENTUM%\dba\config\repository_name` (`$DOCUMENTUM/dba/config/repository_name`). You can add commands to this file; however, do so with caution. Adding to this file affects query performance. If you do add a command, you can use multiple lines, but each command must end with a semi-colon (`;`). You cannot insert comments into this file.

For Sybase, you must set the `ddl in tran` database option to TRUE to run this job. The sql syntax is:

```
sp_dboption dbname, "ddl in tran", true
```

where `dbname` is the name of the database for the repository.

For SQL Server, Sybase, and DB2, you can use the `-dbreindex` argument to control whether the tool only reports on fragmented tables or reports on fragmented tables and fixes them.

The `-dbreindex` argument has no effect on a Oracle database.

The tool generates a report that is saved in the repository in System/Sysadmin/Reports/ UpdateStats. The exact format of the report varies for each database.

The Update Statistics tool is installed in the active state, running once a week. Because this tool can be CPU and disk-intensive, it is recommended that you run the tool during off hours for database use. Consult with your RDBMS DBA to determine an optimal schedule for this tool.

User change home repository (dm_UserChgHomeDb)

The User Change Home Repository tool changes a user's home repository. This job works in conjunction with Documentum Administrator's User pages. To change a users home repository, refer to the instructions in [Changing the home repository of a user, page 202](#).

You have two options for performing the change:

- Execute the `UserChgHomeDb` tool immediately after you save the change.
- Queue the change, to be performed at the next scheduled execution of `UserChgHomeDb`.

The User Change Home Repository tool is installed in the inactive state.

User rename (dm_UserRename)

The User Rename tool changes a users repository name. To change a user's name, use the Reassign User pages in Documentum Administrator. For instructions, refer to [Reassigning objects to another user, page 202](#).

You have two options for performing the change:

- Execute the User Rename tool immediately after you save the change.
- Queue the change, to be performed at the next scheduled execution of User Rename.

The User Rename tool is installed in the inactive state.

Version management (dm_VersionMgt)

The Version Management tool removes unwanted versions of documents from the repository. This tool automates the Destroy and Prune methods.

Refer to *Content Server Fundamentals* for a discussion of how Documentum versioning works. The *Content Server API Reference Manual* describes the Destroy and Prune methods.

The Version Management tool removes only the repository object. It does not remove content files associated with the object. To remove the content files, use the DmClean tool, which is described in [Dmclean \(dm_DMclean\), page 313](#).

The arguments you define for the tool determine which versions are deleted.

To generate a report on unwanted versions without deleting them, run the Version Management tool with the report_only argument set to TRUE.

Before running the Version Management tool, review the Guidelines section of the tool's documentation in the *Content Server Administration Guide*.

WfmsTimer (dm_WfmsTimer)

The WfmsTimer tool checks running workflows for expired activity timers. Workflow designers can set timers that send a message to the workflows supervisor when an activity fails to start or complete within a given time frame. The tool also sends an email message to the activity's performer. The WfmsTimer tool is installed in the inactive state. When activated, the tool runs every 30 minutes by default.

Methods

Methods are executable programs that are represented by method objects in the repository. The program can be a Docbasic script, a Java method, or a program written in another programming language such as C++. The associated method object has properties that identify the executable and define command line arguments, and the execution parameters.

Methods are executed by issuing a DO_METHOD administration method from the command line or using a job. Using a DO_METHOD allows you to execute the method on demand. Using a job allows you to schedule the method for regular, automatic execution. For information on creating jobs, refer to [Jobs, page 265](#).

A newly-created repository contains methods used by Content Server. For additional information on creating methods and using DO_METHOD, refer to the *Content Server Administration Guide*.

Do not modify the default methods without reviewing the documentation for Content Server. At install time, all methods whose object names begin with dm_ are default methods.

To sort the Methods list page alphabetically, click the **Name** or **Method Type** link. To filter the page, select **All**, **System Methods** (which are the default methods), or **User Methods** (which are custom methods) from the drop-down list.

This section contains instructions for:

- [Creating or modifying methods, page 321](#)
- [Importing method content, page 324](#)
- [Running methods, page 324](#)
- [Viewing the results of a method, page 326](#)
- [Exporting method content, page 326](#)
- [Editing method content, page 326](#)
- [Checking in method content, page 327](#)
- [Deleting methods, page 328](#)

Creating or modifying methods

Use these instructions to create or modify a method. Before you create a method, review Chapter 4, Methods and Jobs, in the *Content Server Administrator's Guide*.

Methods are executable programs that are represented by method objects in the repository. The program can be a Docbasic script, a Java method, or a program written in another programming language such as C++. The associated method object has properties that identify the executable and define command line arguments, and the execution parameters.

The executable invoked by the method can be stored in an external file or as content of the method object.

If the program is a Java method and you want to execute it using the Java method server, install it on the application server host's file system. (Java methods may be executed only by the application

server instance installed during Content Server installation.) Do not store the program in the repository as the content of the method object.

Store other programs on the Content Server's file system or in the repository as the content of the method object.

- To store the program as the content of the method object, you must import the content after the method is created.

For information on importing the content, refer to [Importing method content, page 324](#).

- To store the program on the file system, include the file system path in the **Verb** field.

For information on determining which execution agent to use, refer to the sections entitled The Execution Agents and Choosing an Execution Agent in Chapter 4, Methods and Jobs, in the *Content Server Administration Guide*.

To create or modify a method:

1. Connect to the repository where you want to create the method and navigate to **Administration > Job Management > Methods**.

The system displays the Methods list page.

2. To create a new method, select **File > New > Method**.

The system displays the New Method - Method Info page.

3. To modify a method, select the method and then select **View > Properties > Info**.

The system displays the Method Properties - Method Info page.

To edit the method content, refer to [Editing method content, page 326](#).

4. Type the method name.

Do not use the format `dm_methodname` to name the method. This naming convention is reserved for default Documentum objects.

5. Type in the method verb, including arguments.

The method verb is the command-line name of the procedure or the name of the interpretive language that will execute the program file.

You can specify a full path, a relative path, or no path for the `method_verb`. If you do not specify a path, the server searches the directories in the user's search path.

If you specify `./program_name` (`.\program_name` on Windows), the server looks for the executable in the directory in which the server itself resides (by default, `$DM_HOME/bin` or `%DM_HOME\bin`). If the method object represents a Docbasic script, specify the `method_verb` as `dmbasic -entrypoint`, where `entrypoint` is the name of the subroutine to run first.

6. Select one of the following method types:

- `dmbasic`, if the method verb you entered in the previous step is `dmbasic`, select `dmbasic`.
- `dmawk`, if the method verb you entered in the previous step is `dmawk`, select `dmawk`.
- `java`, if the Java method server is executing the method, select `java`.
- `program`

If executing the method using Content Server or the `dmbasic` method server and the executable is stored as content for the method, then setting this to `dmawk` or `dmbasic`, directs the server to add

- f in front of the filename and to pass all arguments specified on the DO_METHOD command line to the program.
7. To add arguments, click **Edit**.
 8. To change the time-out minimum, type a new number.

This is the minimum timeout that you can specify on the command line for this procedure. The default is 30 seconds and cannot be greater than the default timeout (timeout_default).
 9. To change the time-out default, type a new number.

Use if no other time-out is specified on the command line. The default is 60 seconds and cannot be greater than the maximum timeout (timeout_max).
 10. To change the time-out maximum, type a new number.

This is the maximum timeout specified on the command line for this procedure. The default is 300 seconds.
 11. To launch the method directly, select **Launch Direct**.

This controls whether the program is executed by the operating systems system or exec API call. If selected, the server uses the exec call to execute the procedure. In such cases, the method_verb must be a fully qualified path name. If the checkbox is cleared, the server uses the system call to execute the procedure.
 12. To launch the method asynchronously, select **Launch Async**.

The method's return status is reported differently, depending on whether it is launched asynchronously or not. If this is selected and the method is launched on the Java method server, setting SAVE_RESPONSE to TRUE on the command line is ignored. This setting is ignored if the method is launched on the Dmbasic method server or Content Server and SAVE_RESULTS is set to TRUE on the command line. The method is always launched synchronously.
 13. To run the method as the installation owner, select **Run as Owner**.

If selected, it indicates that you want the method to run as the installation owner account, with the installation owner's privileges. Otherwise, the method runs as the user creating the method, with that user's privileges. The default is cleared.

Run as Owner must be selected to execute a method on the method server or application server.
 14. To save internal trace messages generated by the method to the session log, select **Trace Launch**.
 15. To use the dmbasic method server or Java method server to execute a dmbasic or Java method, select **Use Method Server**.
 16. Click **Next** to access the New Method - SysObject Info or Method Properties - SysObject page.
 17. Type the title.
 18. To add an author, click the **Edit** link in the **Authors** line.
 - a. Type a new author in the **Enter new value** box.
 - b. Click **Add**.
 - c. To remove an author, click the author name and click **Remove**.
 - d. To change the order in which authors are listed, click the author and click **Move Up** or **Move Down**.
 - e. Click **OK** to save the changes or **Cancel** to abandon the changes.

19. To add keywords, click the **Edit** link in the **Keywords** line.
 - a. Type a new keyword in the **Enter new value** box.
 - b. Click **Add**.
 - c. To remove a keyword, click the keyword and click **Remove**.
 - d. To change the order in which keywords are listed, click the keyword and click **Move Up** or **Move Down**.
 - e. Click **OK** to save the changes or **Cancel** to abandon the changes.
20. Type a subject.
21. Type the owner of the job.
22. To view more sysobject properties of the method, click **See More**.
23. To store the executable program as the content of the method, refer to [Importing method content, page 324](#).

Importing method content

If the program that a method is running is a script that requires an interpretive language to run it, store the program as the content of the associated method object. Use the instructions in this section to import the content into the method object after you create the method itself. Use the instructions in [Creating or modifying methods, page 321](#) to create the method.

To import method content:

1. Navigate to **Administration > Job Management > Methods**.
The system displays the Methods list page.
2. Select the method for which you are importing content and then select **File > Import Method Content**.
3. Type the full path of the script or click **Browse**, locate the script, and click **Open** in the dialog box.
The path of the script appears in the **Content File Name** field.
4. Click **OK**.
The content is imported.

Running methods

Use the instructions in this section to manually run a method.

To run the method periodically, create a job to execute the method on a schedule by using the instructions in [Creating jobs, page 268](#).

If you run a default Documentum method from the Run Method page, select **Run as server** unless you are logged in as the installation owner.

To run a method:

1. Navigate to **Administration > Job Management > Methods**.

The system displays the Methods list page.

2. Locate the method and then select **Tools > Run Method**.

The system displays the Run Method page.

3. Enter information on the Run Method page:

- a. **Arguments:** Type any arguments required by the method.

- b. **Timeout:** Type a time-out interval.

- c. **Save Results:** Select to save the results.

- d. **Launch Direct:** Select to launch the method directly.

This controls whether the program is executed by the operating systems system or exec API call. If checked, the server uses the exec call to execute the procedure. In such cases, the method_verb must be a fully qualified pathname. If unchecked, the server uses the system call to execute the procedure.

- e. **Launch Async:** Select to launch the method asynchronously.

- f. **Run as Server:** Select to run the method as the application owner.

If selected, it indicates that you want the method to run as the installation owner account. If you run a default Documentum method from this page, select the checkbox unless you are logged in as the installation owner. The checkbox is cleared by default.

Run as Server must be selected to execute a method on the method server or application server.

- g. **Trace Launch:** Select to save method execution messages to the server log.

4. Click **OK**.

If you did not select Launch Asynchronously, the following method results appear:

- The result returned, if any
- Any document IDs that result
- The process ID
- Whether the method launched successfully
- The return value, if any
- Whether there were errors on the operating system from running the method
- Whether the method timed out
- The method time-out length

5. Click **OK**.

The system displays the Methods list page.

Viewing the results of a method

The results of a method are displayed only after you run a method from Documentum Administrator.

After you run the method, the following method results appear:

- The result returned, if any
- Any document IDs that result
- The process ID
- Whether the method launched successfully
- The return value, if any
- Whether there were errors on the operating system from running the method
- Whether the method timed out
- The method timeout length

Click **OK** to exit the results page and return to the Methods list page.

Exporting method content

Use the instructions in this section to view a script imported into a method object.

To export method content:

1. Locate the correct method.
The method must have a script stored in the method object. The method's name is a clickable link.
2. Click the method name.
The content is exported and displayed in a text editor.

Editing method content

Use these instructions to edit the content of a method.

To edit method content:

1. Navigate to **Administration > Job Management > Methods**.
The system displays the Methods list page.
2. Select the appropriate method and then select **File > Edit**.
The method must have a script stored in the method object. For such methods, the method name is a clickable link. The script is checked out and displayed in a text editor.
3. Edit the script, save, and close it.
4. Select **File > Check In**.

5. Optionally modify the properties:

- Version Label

This is a symbolic label for the version.

- Description

- Format

- Whether to full-text index the script

The method content must be checked in as the same version.

6. To display other editable properties, click **More Options** and make appropriate changes.

- To keep the file checked out, select **Retain Lock**.

- To keep a local copy on the file system after check in, select **Keep a local copy after check in**.

- To subscribe to the file, select **Subscribe to this file**.

- To substitute a different file for the one being checked in, select **Check in from file**, browse the file system, and select a different file.

The version checked in is always the CURRENT version. You cannot clear the **Make this the current version** checkbox.

7. Click **OK**.

The file is checked in.

Checking in method content

You see this page only when you check in a checked-out script that is method content.

To check in method content:

1. Optionally modify the properties:

- To check in the file as the same version, click **Save as (same version)**.

- Version Label

This is a symbolic label for the version.

- Description

- Format

- Whether to full-text index the script

2. To display other editable properties, click **More Options** and make any desired changes.

- Select **Retain Lock** to keep the file checked out

- Clear the **Make this the current version** checkbox if you do not want the checked-in document to be current.

- To keep a local copy on the file system after check in, select **Keep a local copy after check in**.

- To subscribe to the file, select **Subscribe to this file**.
 - To substitute a different file for the one being checked in, select **Check in from file**, browse the file system, and select a different file.
3. Click **OK**.
The file is checked in.

Deleting methods

Use these instructions to delete a method.

1. Navigate to **Administration > Job Management > Methods**.
The system displays the Methods list page.
2. Locate the appropriate method.
3. Select the method name and then select **File > Delete**.
The most recent version of the method is deleted.
4. To delete the method completely, repeat step 3 until the method disappears from the list page.

Administration methods

Administration methods are methods that perform a variety of administrative and monitoring tasks, in categories such as process management, content storage management, full-text indexing, and database methods. Use Documentum Administrator to execute the administration methods interactively.

Click the links below for information and instructions on:

- [Viewing administration methods, page 328](#)
- [Running administration methods, page 329](#)

There are links to instructions for running all administration methods in [Running administration methods, page 329](#). The Help topic for each method lists the permissions you must have to run the method, the results returns, and any arguments you must supply to run the method.

Viewing administration methods

To view a list of administration methods, Navigate to **Administration > Job Management > Administration Methods**. The system displays the Administration Methods list page.

Running administration methods

The following instructions provide a general procedure for running administration methods. The instructions are followed by a list of all administration methods. Click the method name for more information about the method, including the permissions you must have to run it, the arguments it takes, and the results it returns.

To run an administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click the method you want to run.
3. Provide any parameters required by the method.
4. Click **Run**.

For information on each administration method, click the method name.

The following sections provide more information about content methods:

- [CAN_FETCH, page 330](#)
- [CLEAN_LINKS, page 331](#)
- [DELETE_REPLICA, page 331](#)
- [DESTROY_CONTENT, page 332](#)
- [GET_PATH, page 333](#)
- [IMPORT_REPLICA, page 334](#)
- [MIGRATE_CONTENT, page 334](#)
- [PURGE_CONTENT, page 339](#)
- [REPLICATE, page 340](#)
- [RESTORE_CONTENT, page 340](#)
- [SET_STORAGE_STATE, page 341](#)

The following sections provide more information about database methods:

- [DB_STATS, page 342](#)
- [EXEC_SQL, page 343](#)
- [MAKE_INDEX, page 343](#)
- [DROP_INDEX, page 344](#)
- [MOVE_INDEX, page 345](#)
- [FINISH_INDEX_MOVES, page 345](#)
- [GENERATE_PARTITION_SCHEME_SQL, page 346](#)

The following are full-text indexing methods.

- [ESTIMATE_SEARCH](#), page 348
- [MARK_FOR_RETRY](#), page 348
- [MODIFY_TRACE](#), page 349

The following administration methods are trace methods:

- [GET_LAST_SQL](#), page 350
- [LIST_RESOURCES](#), page 350
- [LIST_TARGETS](#), page 351
- [MODIFY_TRACE](#), page 349
- [SET_OPTIONS](#), page 352

CAN_FETCH

Any user can run the CAN_FETCH administration method to determine whether the server can fetch a specified content file.

CAN_FETCH returns TRUE if the fetch is possible or FALSE if it is not.

To run the CAN_FETCH administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **CAN_FETCH**.
The system displays the Parameters page.
3. Type a comma-delimited list of the content object IDs of the content files to be fetched.
4. If you do not know the content object ID of the content file to be fetched, click **Select Object(s)**.
The system displays the Select Object(s) page.
 - a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions**.
 - d. Click **Go**.
 - e. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.
 - f. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - g. Click **OK** to return to the Parameters page.
The content object IDs are displayed in the **Content Id** field.
5. Click **Run**.
The results are displayed.
5. Click **Close**.

The system displays the Administration Methods list page.

CLEAN_LINKS

The CLEAN_LINKS administration method removes linked_store links not associated with sessions, unnecessary dmi_linkrecord objects, and auxiliary directories.

CLEAN_LINKS returns TRUE if the operation succeeds or FALSE if it fails.

You must have Superuser privileges to run CLEAN_LINKS.

To run the CLEAN_LINKS administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **CLEAN_LINKS**.
3. To clean both active and inactive sessions, select the **Clean All (active and inactive) Sessions** checkbox.
The default is to clean only inactive sessions.
4. Click **Run**.
The results are displayed.
5. Click **Close**.
The Administration Methods page is displayed.

DELETE_REPLICA

The DELETE_REPLICA administration method removes a content file from a component area of a distributed storage area.

DELETE_REPLICA returns TRUE if the operation succeeds or FALSE if it fails.

You must have Superuser privileges to run DELETE_REPLICA.

To run the DELETE_REPLICA administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **DELETE_REPLICA**.
The system displays the Parameters page.
3. Type a comma-delimited list of the content object IDs of the content files whose replicas are to be deleted.
4. If you do not know the content object ID of the content file whose replicas are to be deleted, click **Select Object(s)**.
The system displays the Select Object(s) page.

- a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions**.
 - d. Click **Go**.
 - e. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.
 - f. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - g. Click **OK** to return to the Parameters page.
The content object IDs are displayed in the **Content ID** field.
5. Select a file store from the **Store Name** drop-down list.
 6. Click **Run**.
The results are displayed.
 7. Click **Close**.
The system displays the Administration Methods list page.

DESTROY_CONTENT

The DESTROY_CONTENT method removes content objects from the repository and their associated content files from storage areas.

DESTROY_CONTENT returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to run DESTROY_CONTENT.

To run the DESTROY_CONTENT administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **DESTROY_CONTENT**.
The system displays the Parameters page.
3. Type in a comma-delimited list of the content object IDs of the content files to be destroyed.
4. If you do not know the content object ID of the content file to be destroyed, click **Select Object(s)**.
The system displays the Select Object(s) page.
 - a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions**.
 - d. Click **Go**.
 - e. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.
 - f. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - g. Click **OK** to return to the Parameters page.

The content object IDs are displayed in the **Content ID** field.

5. Click **Run**.

The results are displayed.

6. Click **Close**.

The system displays the Administration Methods page.

GET_PATH

The GET_PATH administration method returns the directory location of a content file stored in a distributed storage area.

Any user can run GET_PATH.

To run the GET_PATH administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **GET_PATH**.

The system displays the Parameters page.

3. Type in a comma-delimited list of the content object IDs of the content files whose paths you want.

4. If you do not know the content object IDs, click **Select Object(s)**.

The system displays the Select Object(s) page.

a. Select an object type from the **Select From** drop-down list.

b. To further restrict the search, provide a Where clause.

c. To display all versions, select **Use all versions**.

d. Click **Go**.

e. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.

f. To remove an object from the list, select the checkbox next to its name and click **Remove**.

g. Click **OK** to return to the Parameters page.

The content object IDs are displayed in the **Content ID** field.

5. Optionally, select a store name from the drop-down list.

If you do not select a store name, the method looks in the local component of the distributed storage area. If the file is not found in the local component, the method tries to create a replica of the file in the local area and returns the path of the local replica.

6. Click **Run**.

The results are displayed.

7. Click **Close**.

The system displays the Administration Methods page.

IMPORT_REPLICA

The IMPORT_REPLICA administration method imports files from one distributed storage area into another distributed storage area.

The IMPORT_REPLICA method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to use the IMPORT_REPLICA method.

To run the IMPORT_REPLICA administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **IMPORT_REPLICA**.
The system displays the Parameters page.
3. Type a comma-delimited list of the content object IDs of the content files whose replicas you are importing.
4. If you do not know the content object IDs, click **Select Object(s)**.
The system displays the Select Object(s) page.
 - a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions**.
 - d. Click **Go**.
 - e. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.
 - f. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - g. Click **OK** to return to the Parameters page.
The content object IDs are displayed in the **Content ID** field.
5. Select a store name from the drop-down list.
6. Click **Select File**.
The system displays the Choose a file on the server filesystem page.
7. Select a server-side file for import and click **OK** to return to the Parameters page.
8. Click **Run**.
The results are displayed.
9. Click **Close**.
The system displays the Administration Methods page.

MIGRATE_CONTENT

The MIGRATE_CONTENT administration method migrates content files from one storage area to another. You must have Superuser privileges to use the MIGRATE_CONTENT method.

The MIGRATE_CONTENT method enables administrators to migrate:

- a single content object.
- a single sysobject.
- a set of content objects qualified by a DQL predicate against dmr_content.
- a set of content objects qualified by a DQL predicate against dm_sysobject or its subtypes.
- all content in a file store.

Use the MIGRATE_CONTENT administration method to move content from file stores, retention type stores, blob stores, and distributed stores to file stores, retention type stores, and distributed stores. Documentum Administrator 6.5 SP2 and later supports migration from external stores. You cannot move files to a blob store. The storage areas can be online, offline, or read-only.

For Documentum 6.5 repositories, Administrators can optionally enter a Content Migration Threads value to enable the MIGRATE_CONTENT method to perform content migration in parallel for better performance. To use parallel migration, you must have a Content Storage Services license and the license must be enabled on the Content Server. The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config). The *Content Server Administration Guide* contains additional information about parallel content migration.

Before running MIGRATE_CONTENT:

- Ensure that all objects to be migrated are checked in to the repository. If you migrate any checked-out objects, check-in fails because of mismatched versions.
- Ensure that the file store to which you migrate objects has sufficient disk space for the migration.

The MIGRATE_CONTENT method returns an integer indicating the number of objects migrated successfully.

Regardless of the mode in which MIGRATE_CONTENT is run, the original content file can be removed or left in the source file store. If you do not have the file removed, you must specify the path to a log file that logs the path of the source content file. Those files can be removed at another time using Dmfilescan.

Separate instructions are provided for each mode in which you can run MIGRATE_CONTENT:

- **Migrating Single Object**

Use the instructions in this section to migrate the content of single object. The object selector enables you to select single object.

To migrate single object:

1. Access the **Parameters** page for the MIGRATE_CONTENT administration method:
 - a. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the **Administration Methods** list page.
 - b. Click **MIGRATE_CONTENT**.
The system displays the **Parameters** page.
2. Select **A single object** from the **Migrate** drop-down list.
3. Click **Select Object** to access the **Select Object(s)** page.

- a. Select an object type from the **Select From** drop-down list.
 - b. Optionally, type a limiting Where clause.
If the Where box is blank, you can browse and select from all objects in the repository.
 - c. To display all versions, select the **Use all versions** checkbox and then click **Go**.
 - d. Select the objects to migrate and click **Add**.
The objects are moved to the right side of the selector.
 - e. Click **OK** to return to the Parameters page.
4. Select **Remove the original source** to remove the original content file.
- Note:** The **Remove the original source** checkbox will not be editable if the selected object belongs to an external store.
5. Click **Select Path** to access the **Choose a file on the server filesystem** page.
 - a. Select a location on the server file system for the log file path
 - b. Click **OK** to return to the Parameters page.
 6. Select a target file store from the **Target** drop-down list.
- Optional controls:**
- **Source Direct Access:** Indicates whether the content files in the source store can be directly accessed through full file paths or not.
 - **Migrate With:** Indicates whether the source contents will be copied or moved to the target store during migration. Note that Direct Move is applicable to file store only.
 - **Update Only:** It is used only in conjunction with either Direct Copy or Direct Move. When specified 'move' or 'copy' commands will be written to the log file, which was specified by Command File Name.
 - **Command File Name:** This will be available only when **Update Only** checkbox is checked. This is a string parameter to indicate a file path.
- Note:** These controls are visible if the source is an external store and target is either file store or ca store.
7. Click **Run**.
The content files are migrated.

- **Migrating File Stores**

Before you migrate a file store, use the SET_STORAGE_STATE administration method to mark it READ-ONLY. If the source file store has associated full-text indexes, the target file store must also have full-text indexes. Documentum Administrator does not allow you to select a target file store without full-text indexes.

To migrate the content files in a file store:

1. Access the **Parameters** page for the MIGRATE_CONTENT administration method:
 - a. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the **Administration Methods** list page.
 - b. Click **MIGRATE_CONTENT**.

The system displays the **Parameters** page.

2. Select **All content in a file store** from the **Migrate** drop-down list to migrate all objects.
3. Select a source file store from the **Source** drop-down list.
4. Select **Remove the original source** to remove the original content file.

Note: The **Remove the original source** checkbox will not be editable if the original source is an external store.

5. Click **Select Path** to access the **Choose a file on the server filesystem** page.
 - a. Select a location on the server file system for the log file path.
 - b. Click **OK** to return to the Parameters page.
6. Select a target file store from the **Target** drop-down list.
7. Type the maximum number of objects to migrate.
The default is to migrate all objects.
8. Type the number of objects to be migrated in a single transaction.
The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.
9. Optionally, enter a value in the **Content Migration Threads** field to indicate the number of internal sessions to use to execute the method. The default value is 0, indicating that migration will execute sequentially.

Note:

- This field displays only if you have a Content Storage Services license and the license is enabled on the Content Server.
- The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config).

Optional controls:

- **Source Direct Access:** Indicates whether the content files in the source store can be directly accessed through full file paths or not.
- **Migrate With:** Indicates whether the source contents will be copied or moved to the target store during migration. Note that Direct Move is applicable to file store only.
- **Update Only:** It is used only in conjunction with either Direct Copy or Direct Move. When specified 'move' or 'copy' commands will be written to the log file, which was specified by Command File Name.
- **Command File Name:** This will be available only when **Update Only** checkbox is checked. This is a string parameter to indicate a file path.

Note: These controls are visible if the source is an external store and target is either file store or ca store.

10. Click **Run**.

The content files are migrated.

- **Migrating Objects Selected by a DQL Query**

Use the instructions in this section to designate objects to migrate by using a DQL query.

To migrate objects selected by a query:

1. Access the **Parameters** page for the MIGRATE_CONTENT administration method:
 - a. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the **Administration Methods** list page.
 - b. Click **MIGRATE_CONTENT**.
The system displays the **Parameters** page.
2. Select **All content satisfying a query** from the **Migrate** drop-down list to migrate objects returned by a query.
3. Select an object type to migrate: **dmr_content** or **dm_sysobject or it's subtype**.
If you selected **dm_sysobject or it's subtype**, click **Select** to access the **Choose a type** page to select a subtype of **dm_sysobject**.
4. Type a DQL query.
5. Select **Remove the original source** to remove the original content file.
6. Click **Select Path** to access the **Choose a file on the server filesystem** page.
 - a. Select a location on the server file system for the log file path.
 - b. Click **OK** to return to the Parameters page.
7. Select a target file store from the **Target** drop-down list.
8. Type the maximum number of objects to migrate.
The default is to migrate all objects.
9. Type the number of objects to be migrated in a single transaction.
The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.
10. Optionally, enter a value in the **Content Migration Threads** field to indicate the number of internal sessions to use to execute the method. The default value is 0, indicating that migration will execute sequentially.

Note:

- This field displays only if you have a Content Storage Services license and the license is enabled on the Content Server.
- The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (**dm_server_config**).

Optional controls:

- **Source Direct Access:** Indicates whether the content files in the source store can be directly accessed through full file paths or not.
- **Migrate With:** Indicates whether the source contents will be copied or moved to the target store during migration. Note that Direct Move is applicable to file store only.

- **Update Only:** It is used only in conjunction with either Direct Copy or Direct Move. When specified ‘move’ or ‘copy’ commands will be written to the log file, which was specified by Command File Name.
- **Command File Name:** This will be available only when **Update Only** checkbox is checked. This is a string parameter to indicate a file path.

11. Click **Run**.

The content files are migrated.

PURGE_CONTENT

The PURGE_CONTENT administration method marks a content file as offline and deletes the file from its storage area. The method does not back up the file before deleting it; ensure that you have archived the file before running PURGE_CONTENT on it.

The PURGE_CONTENT method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to use the PURGE_CONTENT method.

To run the PURGE_CONTENT administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **PURGE_CONTENT**.
3. Type a comma-delimited list of the content object IDs of the content files you want to purge.
4. If you do not know the content object IDs, click **Select Object(s)**.
The system displays the Select Object(s) page.
 - a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions** and click **Go**.
 - d. Select the checkboxes next to the objects whose content object IDs you want and click **Add**.
 - e. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - f. Click **OK** to return to the Parameters page.
The content object IDs are displayed in the **Content ID** field.
5. Click **Run**.
The results are displayed.
6. Click **Close**.
The Administration Methods list page is displayed.

REPLICATE

The REPLICATE administration method copies content files from one component of a distributed storage area to another. This task is normally performed by the Content Replication tool or by the Surrogate Get feature. Use the REPLICATE administration method as a manual backup to Content Replication and Surrogate Get. (Refer to the *Content Server Administration Guide* for more information on Content Replication and to the *Distributed Configuration Guide* for more information on Surrogate Get.)

The REPLICATE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to use the REPLICATE method.

To run the REPLICATE administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **REPLICATE**.
The system displays the Parameters page.
3. Select a file store that is a component of a distributed store.
This is the store to which the copies are replicated.
4. Optionally, select the type of the documents you want replicated from the **Type Name** drop-down list.
5. Type an expression that would be a valid DQL WHERE clause in the **DQL Query Predicate** field.
6. Click **Run**.
7. Click **Close**.
The system displays the Administration Methods list page.

RESTORE_CONTENT

The RESTORE_CONTENT administration method restores an offline content file to its original storage area. It operates on one file at a time. If you need to restore more than one file at a time, use the API Restore method.

You can use RESTORE_CONTENT only when one server handles both data and content requests. If your configuration uses separate servers for data requests and content file requests, you must issue a Connect method that bypasses the Content Server to use RESTORE_CONTENT in the session.

The RESTORE_CONTENT method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to use the RESTORE_CONTENT method.

To run the RESTORE_CONTENT administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **RESTORE_CONTENT**.

- The system displays the Parameters page.
3. Type the content object ID of the content file you want to restore.
 4. If you do not know the content object ID, click **Select Object(s)**.
The system displays the Select Object(s) page.
 - a. Select an object type from the **Select From** drop-down list.
 - b. To further restrict the search, provide a Where clause.
 - c. To display all versions, select **Use all versions** and then click **Go**.
 - d. Select the checkbox next to the object whose content object IDs you want and click **Add**.
 - e. To remove an object from the list, select the checkbox next to its name and click **Remove**.
 - f. Click **OK** to return to the Parameters page.
The content object ID is displayed in the **Content ID** field.
 5. Click **Select Path** to access the Choose a file on the server filesystem page.
 - a. Navigate to the correct location on the file system.
 - b. Select the checkbox next to the correct location.
 - c. Click **OK** to return to the Parameters page.
The selected path appears in the **Server-Side File for Restore** field.
 6. Click **Run**.
The results are displayed.
 7. Click **Close**.
The system displays the Administration Methods list page.

SET_STORAGE_STATE

The SET_STORAGE_STATE administration method changes the state of a storage area. A storage area is in one of three states:

- On line
An on-line storage area can be read and written to.
- Off line
An off-line storage area cannot be read or written to.
- Read only
A read-only storage area can be read, but not written to.

You can use SET_STORAGE_STATE only when one server handles both data and content requests. If your configuration uses separate servers for data requests and content file requests, you must issue a Connect method that bypasses the content file server to use SET_STORAGE_STATE in the session.

The SET_STORAGE_STATE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to use the SET_STORAGE_STATE method.

To run the SET_STORAGE_STATE administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **SET_STORAGE_STATE**.
The system displays the Parameters page.
3. Select a storage area from the **Store** drop-down list.
The current state of the storage area and the states to which it can be moved are displayed.
4. To change the storage area's state, click the radio button for the correct state.
Which radio buttons appear depends on whether the storage area is online, offline, or read-only.
5. Click **Run**.
The method runs and the results are displayed.
6. Click **Close**.
The system displays the Administration Methods page.

DB_STATS

The DB_STATS administration method displays statistics about database operations for the current session. The statistics are counts of the numbers of:

- Inserts, updates, deletes, and selects executed
- Data definition statements executed
- RPC calls to the database
- Maximum number of cursors opened concurrently during the session

Any user can run the DB_STATS method.

To run the DB_STATS method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **DB_STATS**.
The system displays the Parameters page.
3. To clear the statistical counters, select **Clear the counters**.
4. Click **Run**.
The method runs and the results are displayed.
5. Click **Close**.
The system displays the Administration Methods list page.

EXEC_SQL

The EXEC_SQL administration method executes SQL statements, with the exception of SQL Select statements.

The EXEC_SQL method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Superuser privileges to run the EXEC_SQL method.

Note the following restrictions on how the method works:

- If you use the Apply method to execute the method and the query contains commas, you must enclose the entire query in single quotes.
- In an EXECUTE statement, character-string literals must always be single-quoted.

To run the EXEC_SQL administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **EXEC_SQL**.

The system displays the Parameters page.

3. Type a SQL statement.

The statement must not include a Select clause.

4. Click **Run**.

The method runs and the results are displayed.

5. Click **Close**.

The system displays the Administration Methods list page.

MAKE_INDEX

The MAKE_INDEX administration method creates an index for any persistent object type. You can specify one or more properties on which to build the index. If you specify multiple properties, you must specify all single-valued properties or all repeating properties. Also, if you specify multiple properties, the sort order within the index corresponds to the order in which the properties are specified in the statement. You can also set an option to create a global index.

If the MAKE_INDEX method succeeds, it returns the object ID of the dmi_index object for the new index. If the method fails, MAKE_INDEX returns F. If the specified index already exists, the method returns 0000000000000000.

You must have Superuser privileges to run the MAKE_INDEX administration method. To run an index space query, you must have sufficient privileges in the database.

To run the MAKE_INDEX administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **MAKE_INDEX**.

The system displays the Parameters page.

3. Enter information on the **Parameters** page:
 - a. **Type Name:** Select a name type from the drop-down list box.
 - b. **Attribute Name:** Select a property name from the drop-down list box.
 - c. **Unique:** Select if the values in the index must be unique.
 - d. **Index Space:** Select a specific tablespace or segment in which to place the new index.
 - e. **Global Index:** Select to create a global index.
The Global Index option:
 - Is available only on version 6.5 repositories.
 - Is available only for partitioned types.
 - Is not available for DB2 or Sybase repositories.If selected, the global index is applied to all partitions.
4. To identify a specific tablespace or segment in which to place the new index, select the tablespace or segment from the **Index Space** drop-down list.
You must have sufficient privileges in the database to do this.
5. Global Index:
6. Click **Run**.
The method runs and the results are displayed.
7. Click **Close**.
The system displays the Administration Methods list page.

DROP_INDEX

The DROP_INDEX administration method destroys a user-defined index on an object type.

The DROP_INDEX method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Superuser privileges to run the DROP_INDEX administration method.

To run the **DROP_INDEX administration method:**

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **DROP_INDEX**.
The system displays the Parameters page.
3. Select an index from the **Index** drop-down list.
4. Click **Run**.
The method runs and the results are displayed.
5. Click **Close**.
The system displays the Administration Methods list page.

MOVE_INDEX

The MOVE_INDEX administration method moves an existing object type index from one tablespace or segment to another. The method is not supported for servers running against DB2.

The MOVE_INDEX method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to run the MOVE_INDEX administration method.

To run the MOVE_INDEX administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **MOVE_INDEX**.
The system displays the Parameters page.
3. Select an index from the **Index Name** drop-down list.
4. Select the index space to which you want to move the index.
5. Click **Run**.
The method runs and the results are displayed.
6. Click **Close**.
The system displays the Administration Methods list page.

FINISH_INDEX_MOVES

The FINISH_INDEX_MOVES administration method completes unfinished object type index moves.

The FINISH_INDEX_MOVES method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Superuser privileges to run the FINISH_INDEX_MOVES administration method.

To run the FINISH_INDEX_MOVES administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **FINISH_INDEX_MOVES**.
The system displays the Parameters page.
3. Click **Run**.
The method runs and the results are displayed.
4. Click **Close**.
The system displays the Administration Methods list page.

GENERATE_PARTITION_SCHEME_SQL

The GENERATE_PARTITION_SCHEME_SQL administration method is available to administrators and Superusers. These additional restrictions apply:

- The method is available only on version 6.5 repositories.
- The method is not available for DB2 or Sybase repositories.

Running the method generates a script, which can then be run to partition the repository. The GENERATE_PARTITION_SCHEME_SQL administration method has three options:

- **DB_PARTITION** (Database Partition)

Generate a script to upgrade or convert a non-partitioned repository to a Documentum 6.5 partitioned repository.

- **ADD_PARTITION** (Add Partition)

Add a partition to a partitioned type.

- **EXCHANGE_PARTITION** (Exchange Partition)

Generate a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table.

To run the GENERATE_PARTITION_SCHEME_SQL administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the **Administration Methods** list page.

2. Click **GENERATE_PARTITION_SCHEME_SQL**.

The system displays the **Parameters** page.

3. Enter parameters for the method:

- a. **Operation:** Select an operation from the dropdown list box to define the subcommand.

The options are:

- i. **DB_PARTITION:** Generates a script to upgrade or convert a repository to a 6.5 partitioned repository. If selected:

- Select Partition Type or Table Name.
- If Table Name is defined, optionally define the Owner Name.
- Include object type is optional. Select to apply the partition operation to the dmi_object_type table.
- Last Partition and Last Tablespace are optional.
- In the Partitions section, Partition Name, Range, and Tablespace are required.

ADD_PARTITION: Generates a script to add a partition to a partitioned type. If selected:

- Select Partition Type or Table Name.
- If Table Name is defined, optionally define the Owner Name.
- Include object type is optional. Select to apply the partition operation to the dmi_object_type table.
- In the Partitions section, Partition Name, Range, and Tablespace are required.

EXCHANGE_PARTITION: Generates a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table. If selected:

- Partition Type and Table Name are mutually exclusive.
 - If Table Name is defined, optionally define the Owner Name.
 - Include object type is optional. Select to apply the partition operation to the dmi_object_type table.
 - Partition Name, Range, and Tablespace are required.
 - Temp Table Suffix is optional.
- b. **Partition Type:** Select and then select a partition type from the dropdown list box, which displays a list of the partition types available for the repository. *All* is the default for DB_PARTITION and ADD_PARTITION, but is not available for EXCHANGE_PARTITION. If you select Partition Type, then you cannot select Table Name.
 - c. **Table Name:** Select and then type a table name. If you select Table Name, then you cannot select Partition Type.
 - d. **Include object type:** Optionally, select to apply the partition operation to the dmi_object_type table.
 - e. **Owner Name:** Type an owner name. This field is enabled only if Table Name is selected.
 - f. **Last Partition:** Optionally, type a name for the last partition. This field appears only when DB_PARTITION is selected as the operation.
 - g. **Last Tablespace:** Optionally, type a tablespace name for the last partition. This field appears only when DB_PARTITION is selected as the operation.
 - h. **Partition Name:** Type a name for the partition. For DB_PARTITION and ADD_PARTITION operations, you must first click **Add** in the **Partitions** section to add information for each partition.
 - i. **Range:** Type the upper limit for the partition key range. For DB_PARTITION and ADD_PARTITION operations, you must first click **Add** in the **Partitions** section to add information for each partition.
 - j. **Tablespace:** Type the partition tablespace name. If not specified, the default tablespace is used. For DB_PARTITION and ADD_PARTITION operations, you must first click **Add** in the **Partitions** section to add information for each partition.
 - k. **Temp Table Suffix:** Type a temporary table suffix. This field is enabled and optional only if EXCHANGE_PARTITION is selected as the operation.
4. Click **Run** to execute the method.
The GENERATE_PARTITION_SCHEME_SQL method creates a script object in the /Temp folder in the repository when the method successfully completes. The partition script is not automatically executed; you must execute it separately.
 5. Click **Close** to return to the Administration Methods list page.

ESTIMATE_SEARCH

The ESTIMATE_SEARCH administration method returns the number of results matching a particular full-text search condition.

ESTIMATE_SEARCH returns one of the following:

- The exact number of matches that satisfy the SEARCH condition, if the user running the method is a Superuser or there are more than 25 matches.
- The number 25 if there are 0-25 matches and the user running the method is not a Superuser.
- The number -1 if there is an error during execution of the method.

Errors are logged in the session log file.

Any user can execute this method. However, the user's permission level affects the return value.

To run the ESTIMATE_SEARCH administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **ESTIMATE_SEARCH**.

The system displays the Parameters page.

3. Select an index from the **Index Name** drop-down list.

4. Select a name type from the **Type Name** drop-down list.

5. Type in the string for which you want to search.

6. Click **Run**.

The method runs and the results are displayed.

7. Click **Close**.

The system displays the Administration Methods list page.

MARK_FOR_RETRY

The MARK_FOR_RETRY administration method finds content that has a particular negative update_count property value and marks such content as awaiting indexing. Use MARK_FOR_RETRY at any time to mark content that failed indexing for retry. Note that MARK_FOR_RETRY does not take the update_count argument.

When the UPDATE_FTINDEX method fails, it changes the update_count property for the content object associated with the bad content to the negative complement of the update_count value in the fulltext index object. For example, if the update_count of the full-text index object is 5, the update_count property of the bad content object is set to -5 (negative 5). For more information, refer to the section in the *DQL Reference Manual* on MARK_FOR_RETRY. For information on recovering from failed full-text indexing operations, refer to Troubleshooting in the *Content Server Administration Guide*.

The MARK_FOR_RETRY method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to run the MARK_FOR_RETRY administration method.

To run the MARK_FOR_RETRY administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **MARK_FOR_RETRY**.
The system displays the Parameters page.
3. Select an index from the **Index Name** drop-down list.
4. Type a value in the **Update Count Value** field.
This can be any negative number.
5. Click **Run**.
The method runs and the results are displayed.
6. Click **Close**.
The system displays the Administration Methods list page.

MODIFY_TRACE

The MODIFY_TRACE administration method turns tracing on and off for full-text indexing operations.

The MODIFY_TRACE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to run the MODIFY_TRACE administration method.

To run the MODIFY_TRACE administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **MODIFY_TRACE**.
The system displays the Parameters page.
3. Select a tracing level from the drop-down list.
Options are:
 - **None**: Select to turn tracing off.
 - **All**: Select to log both Content Server and Verity messages.
4. Click **Run**.
The method runs and the results are displayed.
5. Click **Close**.
The system displays the Administration Methods list page.

GET_LAST_SQL

The GET_LAST_SQL administration method retrieves the SQL translation of the last DQL statement issued.

Any user can run GET_LAST_SQL.

To run the GET_LAST_SQL administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **GET_LAST_SQL**.

The system displays the Parameters page.

3. Click **Run**.

The method runs and the last SQL statement is displayed.

4. Click **Close**.

The system displays the Administration Methods list page.

LIST_RESOURCES

The LIST_RESOURCES administration method lists information about the server and the server's operating system environment.

You must have Sysadmin or Superuser privileges to run the LIST_RESOURCES administration method.

To run the LIST_RESOURCES administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.

The system displays the Administration Methods list page.

2. Click **LIST_RESOURCES**.

The system displays the Parameters page.

3. Select **Reset** to reinitialize the file handle and heap size counters.

4. Click **Run**.

The method runs and the results are displayed:

file_handles_in_use

The number of file handles in use by the current child process.

file_handles_max

The configured limit at the operating-system level on the number of file handles the process can open.

file_handles_new	A counter that indicates how many file handles have been created or destroyed since the last LIST_RESOURCES with RESET = T. If the number is negative, it means that there are fewer handles open than there were at the last LIST_RESOURCES call. (Issuing LIST_RESOURCES with RESET=T reinitializes file_handles_new to zero.)
session_heap_size_max	How much, in bytes, of the currently allocated heap (virtual memory) is in use by the session.
current_heap_size_max	Maximum size of the threads session heap. This reflects the value that was in session_heap_size_max when the session was started, and is the size of the heap available to the session.
session_heap_size_in_use	The size, in bytes, of the session heap.
session_heap_size_new	A count of the bytes that the heap has grown or shrunk since the last LIST_RESOURCES call.
root_heap_size_in_use	Issuing LIST_RESOURCES with RESET=T reinitializes heap_size_new to zero.
root_heap_size_new	How much, in bytes, of the main server threads heap is in use.
max_processes	A count of the bytes that the heap has grown or shrunk since the last LIST_RESOURCES call.
server_init_file	The maximum number of processes that can be created by the account under which the server is running.
initial_working_directory	The full path to the servers server.ini file.

5. Click **Close**.

The system displays the Administration Methods list page.

LIST_TARGETS

The LIST_TARGETS administration method lists the connection brokers to which the server is currently projecting. Additionally, it displays the projection port, proximity value, and connection broker status for each connection broker, as well as whether the connection broker is set (in server.ini or the server config object).

Any user can run LIST_TARGETS.

To run the LIST_TARGETS administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **LIST_TARGETS**.
The system displays the Parameters page.
3. Click **Run**.
The method runs and the projection targets and other information are displayed.
4. Click **Close**.
The system displays the Administration Methods list page.

SET_OPTIONS

The SET_OPTIONS administration method turns tracing options on or off. You can set the following options:

Option	Action
clean	Removes the files from the server common area.
debug	Traces session shutdown, change check, launch and fork information.
docbroker_trace	Traces connection broker information.
i18n_trace	Traces client session locale and codepage. An entry is logged identifying the session locale and client code page whenever a session is started. An entry is also logged if the locale or code page is changed during the session.
last_sql_trace	Traces the SQL translation of the last DQL statement issued before access violation and exception errors. If an error occurs, the last_sql_trace option causes the server to log the last SQL statement that was issued prior to the error. This tracing option is enabled by default.
lock_trace	It is strongly recommended that you do not turn off this option. It provides valuable information to Technical Support if it ever necessary to contact them.
net_ip_addr	Traces Windows locking information. Traces the IP addresses of client and server for authentication.

Option	Action
nettrace	Turns on RPC tracing. Traces Netwise calls, connection ID, client host address, and client hostname.
sql_trace	Turns on RPC tracing. Traces Netwise calls, connection ID, client host address, and client hostname.
trace_authentication	Traces detailed authentication information.
trace_complete_launch	Traces Unix process launch information.
trace_method_server	Traces the operations of the method server.

The SET_OPTIONS method returns TRUE if the operation succeeds or FALSE if it fails.

You must have Sysadmin or Superuser privileges to run the SET_OPTIONS administration method.

To run the SET_OPTIONS administration method:

1. Navigate to **Administration > Job Management > Administration Methods**.
The system displays the Administration Methods list page.
2. Click **SET_OPTIONS**.
The system displays the Parameters page.
3. Type the name of an option.
4. To turn the option on, select **On**; to turn the option off, clear the checkbox.
5. Click **Run**.
The method runs and the results are displayed.
6. Click **Close**.
The system displays the Administration Methods list page.

Administration Methods Results Page

This page displays the results of running an administration method. For information on the results, click the method name. The following are content methods:

- [CAN_FETCH, page 330](#)
- [CLEAN_LINKS, page 331](#)
- [DELETE_REPLICA, page 331](#)
- [DESTROY_CONTENT, page 332](#)
- [GET_PATH, page 333](#)
- [IMPORT_REPLICA, page 334](#)
- [PURGE_CONTENT, page 339](#)
- [REPLICATE, page 340](#)

- RESTORE_CONTENT, page 340
- SET_STORAGE_STATE, page 341

The following are database methods:

- DB_STATS, page 342
- EXEC_SQL, page 343
- MAKE_INDEX, page 343
- DROP_INDEX, page 344
- MOVE_INDEX, page 345
- FINISH_INDEX_MOVES, page 345

The following are full-text indexing methods:

- ESTIMATE_SEARCH, page 348
- MARK_FOR_RETRY, page 348
- MODIFY_TRACE, page 349

The following administration methods are trace methods:

- GET_LAST_SQL, page 350
- LIST_RESOURCES, page 350
- LIST_TARGETS, page 351
- MODIFY_TRACE, page 349
- SET_OPTIONS, page 352

Choosing a file on the server file system

Click the links below for information and instructions about the **Choose a file on the server filesystem** page for the different administration methods:

- IMPORT_REPLICA, page 334
- RESTORE_CONTENT, page 340

Chapter 10

Alias Sets

An *alias set* is an object that defines one or more aliases and their corresponding values.

An *alias* is a placeholder for usernames, group names, or folder paths. You can use aliases in:

- SysObjects or SysObject subtypes, in the owner_name, acl_name, and acl_domain properties
- ACL template objects, in the r_accessor_name property
- Workflow activity definitions (dm_activity objects), in the performer_name property
- A Link or Unlink method, in the folder path argument

Any user can create an alias set. If you use Documentum Administrator, you must be the alias set's owner or a Superuser to change or delete the alias set. If you use the server API, the constraints are different:

- To change the owner of an alias set, you must be either the owner of the alias set or a Superuser.
- To change other properties or to delete an alias set, you must be the owner of the alias set or a user with Sysadmin or Superuser privileges.

Using aliases enables you to write applications or procedures to use and reuse in many situations because important information such as the document owner, a workflow activity performer, or the user permissions in a documents ACL is not hard-coded into the application. Instead, aliases are placeholders for these values. When the application executes, the aliases are resolved to real usernames or group names or folder paths.

For example, you create an alias set called Administrators that contains five aliases: Admin1, Admin2, Admin3, Admin4, and Admin5. Each alias has a value that corresponds to a user, group, or folder path, and you can change that value at will. To illustrate, the Admin1 alias is assigned to a user in your repository who creates site publishing configurations. You can create workflows in which Admin1 is the performer. As different individuals fill that position, you change the value of Admin1, but you do not need to change the performer in the workflows.

For more information on alias sets and aliases, refer to Aliases in *Content Server Fundamentals*.

Click the links below for instructions and information on:

- Locating alias sets, page 356
- Creating alias sets, page 356
- Viewing or modifying alias sets, page 357
- Viewing alias set aliases, page 357

- Adding, modifying, and deleting alias set aliases , page 358
- Deleting alias sets, page 360

Locating alias sets

Use these instructions to locate an alias set in the repository.

To locate alias sets:

1. Connect to the correct repository.
2. Navigate to **Administration > Alias Sets** to access the Alias Sets list page.
3. Locate the correct alias set.
 - To sort the alias sets by object name or by description, click the link in the column headers.
 - To list a different number of items, select a new number from the **Show Items** list box.
 - To jump to a particular part of the alphabet, click the letter.
 - Click the arrows to advance to the next page or a previous page that lists alias sets.

Creating or modifying alias sets

Click the links for help on the following topics:

- Creating alias sets, page 356
- Viewing or modifying alias sets, page 357

Creating alias sets

Use these instructions to create new alias sets. Any user may create an alias set.

To create an alias set:

1. Navigate to **Administration > Alias Set** to access the Alias Sets list page.
2. Select **File > New > Alias Set** to access the New Alias Set - Info page.
3. Enter information on the **New Alias Set - Info** page:
 - a. **Name:** Type the name of the new alias set.
 - b. **Description:** Type a description of the alias set.
 - c. **Owner:** To assign an owner other than you, click **Select** to access the Choose a user/group page.
 - i. Select a new owner's name.
 - ii. Click **OK** to accept the new owner or **Cancel** to cancel.

- The system displays the New Alias Set - Info page.
- d. Click **Next** to continue to the New Alias Set - Aliases page.
 4. Enter information on the **New Alias Set - Aliases** page.
Refer to [Adding, modifying, and deleting alias set aliases , page 358](#) for instructions to add an alias to an alias set, modify an existing alias, or delete an alias from an alias set.
 5. After adding aliases to the alias set, click **Finish**.
The alias set is created.

Viewing or modifying alias sets

This section discusses how to view or modify alias sets.

You must be the alias set's owner or a Superuser to use the Alias Set Properties - Info page in Documentum Administrator to change or delete an alias set. (The constraints are different if you are using the API. Refer to the *Content Server Administration Guide* for more information.)

To view or modify an alias set:

1. Connect to the correct repository.
2. Navigate to **Administrator > Alias Sets** to access the Alias Sets list page.
3. Select the alias set to modify or view and then select **View > Properties > Info** to access the Alias Set Properties - Info page.
4. View or modify the information on the **Alias Set Properties - Info** page:
 - a. **Name:** The name of the alias set. Display only.
 - b. **Description:** Type or modify the description for the alias.
 - c. **Owner:** To assign an owner other than you, click **Select** to access the Choose a user/group page.
 - i. Select a new owner's name.
 - ii. Click **OK** to accept the new owner or **Cancel** to cancel.

The system displays the Alias Set Properties - Info page.
5. Click the **Aliases** tab to access the Alias Set Properties - Aliases page to add, modify, or delete aliases.
Refer to [Adding, modifying, and deleting alias set aliases , page 358](#) for instructions to add an alias to an alias set, modify an existing alias, or delete an alias from an alias set.
6. Click **OK** to save the modifications or click **Cancel** to exit without saving any modifications.
The system displays the Alias Sets list page.

Viewing alias set aliases

Use these instructions to view aliases for an alias set.

To view alias set aliases:

1. Access the Alias Set Properties - Alias page:
 - a. Navigate to **Administrator > Alias Sets** to access the Alias Sets list page.
 - b. Select the alias set to modify or view and then select **View > Properties > Info** to access the Alias Set Properties - Info page.
 - c. Click the **Aliases** tab to access the Alias Set Properties - Aliases page.
2. View the information on the Alias Set Properties - Aliases page:
 - a. **Name:** The name of the alias.
 - b. **Category:** The category the alias belongs to.
 - c. **Value:** The value assigned to the alias.
 - d. **Description:** The description of the alias.
 - e. Click **OK** to save the new alias or click **Cancel**.
The system displays the Alias Set Properties - Aliases page.
3. Add a new alias, edit an existing alias, or delete an alias from the alias set:
 - a. Click **Add** to access the Alias: New Alias page to add a new alias.
 - b. Select an alias and then click **Edit** to modify information about an existing alias.
 - c. Select an alias and then click **Remove** to remove an existing alias from the alias set.
Refer to [Adding, modifying, and deleting alias set aliases , page 358](#) for instructions to add an alias to an alias set, modify an existing alias, or delete an alias from an alias set.
4. Click **OK** to save the modifications, if any, or click **Cancel** to exit without saving any modifications.
The system displays the Alias Sets list page.

Adding, modifying, and deleting alias set aliases

Use these instructions to add an alias to an alias set, modify an existing alias, or delete an alias from an alias set.

You must be the alias set's owner or a Superuser to use the Alias Set Properties - Aliases page in Documentum Administrator to add, modify, or delete aliases.

To add, modify, or delete alias set aliases:

1. Access the Alias Set Properties - Aliases page:
 - a. Navigate to **Administrator > Alias Sets** to access the Alias Sets list page.
 - b. Select the alias set to modify or view and then select **View > Properties > Info** to access the Alias Set Properties - Info page.
 - c. Click the **Aliases** tab to access the Alias Set Properties - Aliases page.
2. To add a new alias, click **Add** to access the Alias: New Alias page.

Enter information on the Alias: New Alias page:

- a. **Name:** Type the name of the new alias.
- b. **Category:** Select a category from the list box.
- c. **Value:** If the category is user, group, permission set, cabinet path, or folder path, click **Get Value**. Select the correct value and then click **OK** to return to the Alias: New Alias page.
Which screen appears after clicking Get Value depends on your category choice:
 - If you selected *Permission Set*, the system displays the Choose a permission set page.
 - If you selected *Cabinet Path*, the system displays the Choose a cabinet page.
 - If you selected *Folder Path*, the system displays the Choose a folder page.
 - If you selected *Group*, the system displays the Choose a group page.
 - If you selected *User*, the system displays the Choose a user page.
 - If you selected *User or Group*, the system displays the Choose a user/group page.
 - The Get Value link does not appear if the category is *Unknown*. If you selected Unknown, you must type in a value.
- d. **User Category:** Type a user category.
- e. **During DocApp Installation:** Select **Prompt Alias value** to indicate to prompt for the alias value during DocApp installation.
If the category is folder path or cabinet path, select between prompting for the value during DocApp installation or creating the folder or cabinet if it does not exist.
- f. **Description:** Type a description for the new alias.
- g. Click **OK** to save the new alias or click **Cancel**.

The system displays the Alias Set Properties - Aliases page.

3. To modify an existing alias, select an alias and then click **Edit** to access the **Alias** page.

Enter information on the Alias page:

- a. **Name:** The name of the alias. Read only.
- b. **Category:** The category for the alias. Read only.
- c. **Value:** If the category is user, group, permission set, cabinet path, or folder path, click **Get Value**. Select the correct value and then click **OK** to return to the Alias: New Alias page.
Which screen appears after clicking Get Value depends on the category:
 - If the category is *Permission Set*, the system displays the Choose a permission set page.
 - If the category is *Cabinet Path*, the system displays the Choose a cabinet page.
 - If the category is *Folder Path*, the system displays the Choose a folder page.
 - If the category is *Group*, the system displays the Choose a group page.
 - If the category is *User*, the system displays the Choose a user page.
 - If the category is *User or Group*, the system displays the Choose a user/group page.
 - The Get Value link does not appear if the category is *Unknown*. If you selected Unknown, you must type in a value.

- d. **User Category:** Modify the user category.
 - e. **During DocApp Installation:** Select **Prompt Alias value** to indicate to prompt for the alias value during DocApp installation.
If the category is folder path or cabinet path, select between prompting for the value during DocApp installation or creating the folder or cabinet if it does not exist.
 - f. **Description:** Modify the description for the alias.
 - g. Click **OK** to save the modifications or click **Cancel**.
The system displays the Alias Set Properties - Aliases page.
4. To delete an alias, select an alias and then click **Remove**.
The alias is removed from the alias set.
 5. Click **OK** to save alias additions, modifications, or deletions and return to the Alias Sets list page.

Deleting alias sets

Use these instructions to delete an alias set. To use Documentum Administrator to change or delete an alias set, you must be the alias set's owner or a Superuser. (The constraints are different if you are using the API. Refer to the *Content Server Administration Guide* for more information.)

To delete an alias set:

1. Navigate to **Administration > Alias Set** to access the Alias Sets list page.
2. Select the alias set to delete and then select **File > Delete**.
The system displays the Delete Object(s) page.
3. Click **OK** to delete the alias set or **Cancel** to not delete the alias set.
The system displays the Alias Sets list page.

Formats

Format objects define file formats. Content Server only recognizes formats for which there is a format object in the repository. When a user creates a document, the format of the document must be a format recognized by the server. If the format is not recognized by the server, the user cannot save the document into the repository.

The Content Server installation process creates a basic set of format objects in the repository. You can add more format objects, delete objects, or change the properties of any format object.

For more information about formats and format objects, refer to Content Repositories in the *Content Server Administration Guide*.

Click the links for instructions on:

- [Locating formats, page 361](#)
- [Creating new formats, page 361](#)
- [Viewing or modifying a format, page 362](#)
- [Deleting formats, page 362](#)
- [Format properties, page 362](#)

Locating formats

Use these instructions to locate an existing format to view, modify, or delete.

To locate formats:

1. Navigate to **Administration > Formats** to access the Formats list page.
2. To view an alphabetic group of formats, click **Format Name** or **Description**.
3. To jump to a particular format, type the format name in the **Starts With** box and click **Go**.

Creating new formats

Use the instructions in this section to create new formats.

To create a new format:

1. Navigate to **Administration > Formats** to access the Formats list page.
2. Select **File > New > Format** to access the New Format - Info page.
3. Complete the properties for the new format.
For information on each property, refer to [Format properties, page 362](#).
4. Click **OK** to save the new format or **Cancel** to exit without saving the changes.
The system displays the Formats list page.

Viewing or modifying a format

Use the instructions in this section to view or modify an existing format.

To view or modify a format:

1. Navigate to **Administration > Formats** to access the Formats list page.
2. Locate the format to view or modify and then select **View > Properties > Info** to access the Format Properties - Info page.
3. Edit the format if you have sufficient privileges.
For information on each field, refer to [Format properties, page 362](#).
4. Click **OK** to save the changes or **Cancel** to exit without saving the changes.
The system displays the Formats list page.

Deleting formats

Use the instructions in this section to delete formats. You cannot delete a format if the repository contains content files in that format.

To delete a format:

1. Navigate to **Administration > Formats** to access the Formats list page.
2. Locate the format to delete and then select **File > Delete**.
 - If there are content objects associated with the format, the format is not deleted.
 - If there are no content objects associated with the format, the format is deletedThe Format list page is displayed.

Format properties

The table in this section lists the fields on the New Format - Info and Format Properties - Info pages.

Click the links for information on:

- [Creating new formats, page 361](#)
- [Viewing or modifying a format, page 362](#)

Table 40. Format properties

Field label	Value
Name	The name of the format (for example: doc, tiff, or lotmanu).
Default File Extension	The DOS file extension to use when copying a file in the format into the common area, client local area, or storage.
Description	A description of the format.
Com Class ID	The class ID (CLSID) recognized by the Microsoft Windows registry for a content type.
Mime Type	The Multimedia Internet Mail Extension (MIME) for the content type.
Windows Application	The name of the Windows application to launch when users select a document in the format represented by the format object.
Macintosh Creator	Information used internally for managing Macintosh resource files.
Macintosh Type	Information used internally for managing Macintosh resource files.
Class	<p>Identifies the classes or classes of formats to which a particular format belongs.</p> <p>To assign a class to a format, click Edit to access the Format Class page. Type a value in the Enter new value box and click Add.</p> <p>Two values are used by the full-text indexing system to determine which renditions of a document are indexed:</p> <ul style="list-style-type: none"> • ftalways <p>All renditions in formats whose <code>format_class</code> property is set to <code>ftalways</code> are indexed. For example, if a document has renditions in Microsoft Word and PDF formats and the <code>format_class</code> property for both formats is set to <code>ftalways</code>, both renditions are indexed.</p> <ul style="list-style-type: none"> • ftpREFERRED <p>If a document has multiple renditions in indexable formats and one is in a format</p>

Field label	Value
	whose format_class property is set to ftpreferred, the rendition in that format is indexed rather than any renditions in other formats, with the exception that any formats whose format_class property is set to ftalways are also indexed. If a document has more than one rendition whose format_class property is set to ftpreferred, the first rendition processed for indexing is indexed and the other renditions are not. It is recommended that for any document, only one rendition is in a format whose format_class property is set to ftpreferred.
	If a document has renditions in four different formats, of which the format_class of one is set to ftpreferred and the format_class of the other three is set to ftalways, all four renditions are indexed.
Asset Class	Used by applications. Identifies the kind of asset (video, audio, and so on) represented by this format.
Filename Modifier	The modifier to append to a filename to create a unique file name.
Default Storage	Identifies the default storage area for content files in this format. Click Select to access the Choose a Storage page.
Re-Initialize Server	Select to reinitialize the server so changes occur immediately.
Rich Media	Indicates whether thumbnails, proxies, and metadata are generated for content in this format. You must have Documentum Media Transformation Services installed to generate the thumbnails, proxies, and metadata.
Hide	Determine whether the format object should appear in the WorkSpace list of formats. Select to hide the object.

Chapter 12

Types

Documentum is an object-oriented system. An object type represents a class of objects. All items manipulated by users are objects. Every document is an object, as are the cabinets and folders in which documents are stored in Documentum. Even users are handled as objects. Each of the objects belongs to an *object type*.

Object types are similar to templates. When you create an object, identify the type of object to create. Content Server then uses the type definition as a template to create the object.

The definition of an object type is a set of properties, fields whose values describe individual objects of the type. When an object is created, its properties are set to values that describe that particular instance of the object type. For example, two properties of the document object type are title and subject. When creating a document, you provide values for the title and subject properties that are specific to that document. Properties are also referred to as attributes.

To create a type, you must have Superuser, Sysadmin, or Create Type user privileges. If you have Superuser privileges, you can create a subtype with no supertype. Only a Superuser or the owner of a type can update the type. Base types and custom types can be modified using Documentum Administrator. On the Types Properties - Info page, a Superuser connected to a 5.3 SP5 or later repository can select to register a type and its subtypes for full-text indexing.

On the Types list page, you can filter types by selecting **All**, **DCTM Types**, or **Custom Types** from the list box. Types whose names are displayed as clickable links have subtypes; if you click the name, the subtypes are displayed. To navigate back to a previous list page, click a link in the breadcrumb at the top of the page. The Category and Parent Type columns only appear on the Types list page if the High-Volume Server license is enabled and the Content Server version is 6 or later.

A heavyweight object type can be converted to a shareable object type or lightweight object type and split to a shareable and lightweight object type.

A lightweight sysobject type is an object type whose implementation is optimized to reduce the storage space needed in the database for instances of the type. All lightweight sysobject types are subtypes of the dm_sysobject object type and are a subtype of a shareable type. When a lightweight sysobject is created, it references a shareable supertype object. As additional lightweight sysobjects are created, they can reference the same shareable object. The shareable object is called the lightweight sysobject's parent. Each lightweight sysobject shares the information in its shareable parent object. Instead of containing multiple identical rows in the system object tables to support all instances of the lightweight type, a single instance of the parent object is created for multiple lightweight

sysobjects. The *Documentum High-Volume Server Development Guide* provides additional information on lightweight system objects. Administrators can use Documentum Administrator to:

- Create, modify, and delete shareable object types.
- Create, modify, and delete lightweight sysobject types.
- Convert heavyweight object types to a shareable object type.
- Convert heavyweight object types to a lightweight sysobject type.
- Convert heavyweight object types to a shareable type and lightweight sysobject type.

Assignment policies determine the correct storage area for content files. A new type inherits a default assignment policy from the nearest supertype in the type hierarchy that has an active assignment policy associated with it. After the type is created, you can associate a different assignment policy with the type using the instructions in *Associating an assignment policy with an object type*.

Click the links for information and instructions on:

- [Creating types, page 366](#)
- [Modifying types, page 368](#)
- [Type Properties, page 370](#)
- [Selecting supertypes, page 374](#)
- [Selecting default groups, page 374](#)
- [Adding properties to types, page 375](#)
- [Deleting types, page 375](#)
- [Viewing assignment policies, page 376](#)
- [Converting types to shareable object types, page 376](#)
- [Converting types to lightweight object types, page 377](#)
- [Converting types to shareable and lightweight object types, page 378](#)

For more information on types, refer to The Data Model chapter in *Content Server Fundamentals*. For complete information on the system-defined object types, including the properties of each type, refer to the *Object Reference Manual*.

Creating types

Use the instructions in this section to create new object types.

To create an object type:

1. Navigate to **Administration > Types** to access the **Types** list page.
2. Select **File > New > Type** to access to **New Type - Info** page.
3. Enter information on the **New Type - Info** page:
 - a. **Type Name:** Type the name of the new object type.

- b. **Model Type:** Select a model type. This option is available only on version 6 and later repositories where the High-Volume Server license is enabled.
- Options are:
- **Standard:** The type is heavy. This is the default setting.
 - **Shareable:** Defines a shareable SysObject model type for SysObject supertypes and their subtypes.
 - **Lightweight:** The system checks for the existence of shareable types in the current repository. If there are no shareable types in the current repository, this option will not be available.
- If selected, the Parent Type, Materialize, and Full Text fields become available and the Super Type Name field is not displayed.
- c. **Super Type Name:** The default supertype is dm_document.
- If you want a supertype other than dm_document:
- i. Click **Select Super Type** to access the **Choose a type** page.
 - ii. Select the object type that you want to be the supertype.
 - iii. Click **OK** to return to the **New Type - Info** page.
- d. **Default Storage:** Select a default file store for the new object type.
- e. **Default Group:** Assign a default group for the type.
- i. Click **Select Default Group** to access the **Choose a group** page.
 - ii. Select the group to which you want the type to belong.
 - iii. Click **OK** to return to the **New Type - Info** page.
- f. **Default Permission Set:** Assign a default permission set to the type.
- i. Click **Select Default Permission Set** to access the **Choose a permission set** page.
 - ii. Select the permission set that you want to be the default.
 - iii. Click **OK** to return to the **New Type - Info** page.
- g. **Parent Type:** Select a parent type for the lightweight sysobject. This option is available only when Model Type is Lightweight.
- h. **Materialize:** This option is available only when Model Type is Lightweight.
- Select one of the following options:
- **Auto materialize:** The lightweight object will be automatically materialized to a full object when the object is saved with changes to some attributes of the parent object.
 - **Materialize on request:** The lightweight object can only be materialized by explicitly calling the materialize API. Any changes to the parent object by the lightweight object before materialization will result in an error.
 - **Do not materialize:** The lightweight object is not allowed to be materialized. Calling the materialize API will result in an error. Any changes to the parent object by the lightweight object will result in an error.
- i. **Full Text:** This option is available only when Model Type is Lightweight.

Select one of the following options:

- **No fulltext**: This is the default.
- **Light fulltext**: No attributes inherited from the shared parent will be full-text indexed.
- **Full fulltext**

4. Click **Next** to access the **New Type - Attribute** page.

A list of the properties inherited from the supertype is displayed. You cannot delete the inherited properties.

5. To add a property to the type, click **Add** to access the **Attribute Info: New Attribute** page.

- a. Type the new attribute's name.
- b. Select the property type from the list box.
- c. If the property is the String type, type its size.
- d. To make the property a repeating property, select the **Repeating** checkbox.
- e. Click **OK**.

6. To remove a user-defined property (not a property inherited from the supertype), select the property and then click **Remove**.

7. Click **Finish**.

The type is saved.

Modifying types

Use the instructions in this section to modify a type.

For any user- or system-defined type you can change the default group, ACL (permission set), and storage area.

In repositories where Content Storage Services is enabled, the **Default Assignment Policy** displays the name of the assignment policy assigned to the type, if there is one.

You can only modify the definition of a user-defined type if you are the owner of the type or have Superuser user privileges. An owner or user with Superuser user privileges can add or delete read/write properties or lengthen string properties. Users with Superuser user privileges also can add read-only properties to the type.

Properties are stored as columns in a table representing the type in the underlying RDBMS. However, not all RDBMSs allow you to drop columns from a table. Consequently, if you delete a property, the corresponding column in the table representing the type may not actually be removed. In such cases, if you later try to add a property to the type with the same name as the deleted property, you will receive an error message.

Any changes made to a type apply to all objects of that type, to its subtypes, and to all objects of any of its subtypes.

To modify a type:

1. Navigate to the Type Properties - Info page:
 - a. Navigate to **Administration > Types** to access the **Types** list page.
A list of existing object types is displayed.
 - b. Select the type to modify and then select **View > Properties > Info** to access the **Type Properties - Info** page.
2. View or modify information on the **Type Properties - Info** page:
 - a. **Type Name:** The name of the object type. Display only.
 - b. **Model Type:** Name of the model type. Display only. This option is available only on version 6 and later repositories where the High-Volume Server license is enabled.
 - c. **Super Type Name:** The name of the supertype. Display only. This field will not be displayed if Model Type is Lightweight.
 - d. **Default Storage:** The default file store for the object type.
If the type is a Documentum type, you cannot change the default storage. If the type is a custom type, you can change the default storage.
 - e. **Default Group:** The default group for the type.
 - i. Click **Select Default Group** to access the **Choose a group** page.
 - ii. Select the group to which you want the type to belong.
 - iii. Click **OK** to return to the **Type Properties - Info** page.
 - f. **Default Permission Set:** The default permission set for the type.
 - i. Click **Select Default Permission Set** to access the **Choose a permission set** page.
 - ii. Select the permission set that you want to be the default.
 - iii. Click **OK** to return to the **Type Properties - Info** page.
 - g. **Default Assignment Policy:** The default assignment policy for the type, if there is one.
Click the link to access the assignment policy. Use the information in [Assignment policies, page 419](#) to modify the assignment policy or to remove the type from the assignment policy. Use the instructions in the Assignment Policy section to associate a different policy with a particular type.
 - h. **Enable Indexing:** Select to register the type for full-text indexing.
If registering a particular type for indexing, the system automatically selects all of its subtypes for indexing. When registering a type for indexing, the system checks for any of its subtypes that are registered. If a subtype is registered, the system unregisters it before registering the type.
The system displays the Enable Indexing checkbox based on the following criteria:
 - If the type is dm_sysobject or its subtypes and you are connected as a Superuser to a 5.3 SP5 or later repository, the system displays the checkbox. If neither of these conditions is met, the system does not display the checkbox.
 - If a type and none of its supertypes are registered, the system displays the checkbox cleared and enabled. You can select the checkbox to register the type for full-text indexing.

- If a type is registered and none of its supertypes are registered, the system displays the Enable Indexing checkbox selected and enabled.
- If a type's supertype is registered for indexing, the system displays the Enable Indexing checkbox selected but disabled. You cannot clear the checkbox.

Note: The system does not display the Enable Indexing checkbox on the New Types - Info page when you create a new type. You must first create the type and then save it.

- i. **Partitioned:** Displays whether a type that can be partitioned is or is not partitioned. This field:
 - is available only for Documentum version 6.5 repositories.
 - does not appear if the type cannot be partitioned.
 - displays *False* if the type can be partitioned but is not.
 - displays *True* if the type is partitioned.
 - j. **Parent Type:** Displays only when Model Type is Lightweight.
 - k. **Materialize:** Displays only when Model Type is Lightweight.
 - l. **Full Text:** Displays only when Model Type is Lightweight.
 3. Click **OK** to save the changes or click the **Attributes** tab to access the **Type Properties - Attributes** page to change the type's properties.
A list of the properties inherited from the supertype is displayed. You cannot delete the inherited properties.
 4. To add a new property to the type, click **Add** to access the **Attribute Info: New Attribute** page.
 - a. Type the name of the new property.
 - b. Select the property type from the list box.
 - c. If the property is the String type, type its size.
 - d. To make the property a repeating property, select the **Repeating** checkbox.
 - e. Click **OK**.
 5. To remove a user-defined property, select the checkbox next to that property and click **Remove**. You cannot remove a property inherited from the supertype.
 6. Click **OK**.
- The changes to the type are saved.

Type Properties

This section defines the type properties that appear on the following pages:

- New Type - Info
- Type Property - Info
- New Type - Attribute
- Type Property - Attribute

Click the links for information on:

- [Creating types, page 366](#)
- [Modifying types, page 368](#)

Table 41. Type properties

Field label	Value
Type Name	The name of the object type. This field is display-only in modify mode.
Model Type	This field is display-only in modify mode. Options are: <ul style="list-style-type: none"> • Standard: This is the default and is for heavy types. • Shareable: Defines a shareable SysObject model type for SysObject supertypes and their subtypes. • Lightweight: The system checks for the existence of shareable types in the current repository. If there are no shareable types in the current repository, this option will not be available. If selected, the Parent Type, Materialize, and FullText fields become available and the Super Type Name field is not displayed.
Super Type Name	The name of the supertype. The default supertype is dm_document. This field is: <ul style="list-style-type: none"> • Not available if Model Type is Lightweight. • Display-only in modify mode. Unless you are a Superuser, you must identify the new type's supertype. If you are a Superuser and want to create the type without a Supertype, select NULL as the supertype.
Default Storage	A default file store for the object type.
Default Group	A default group for the type. Click Select Default Group to access the Choose a group page to add or change the default group.
Default Permission Set	A default permission set for the type. Select Default Permission set to access the Choose a permission set page to add or change the default permission set.

Field label	Value
Default Assignment Policy	<p>The system displays the default assignment policy for the type, if there is one. This field appears only when modifying a type and if Content Storage Services is enabled for the repository.</p>
Enable Indexing	<p>Click the link to access the assignment policy. Use the information in Assignment policies, page 419 to modify the assignment policy or to remove the type from the assignment policy. Use the instructions in the Assignment Policy section to associate a different policy with a particular type.</p>
	<p>The system displays the Enable Indexing checkbox based on the following criteria:</p> <ul style="list-style-type: none"> • If the type is dm_sysobject or its subtype and you are connected as a Superuser to a 5.3 SP5 or later repository, the system displays the checkbox. If neither of these conditions is met, the system does not display the checkbox. • If a type and none of its supertypes are registered, the system displays the checkbox cleared and enabled. You can select the checkbox to register the type for full-text indexing. • If a type is registered and none of its supertypes are registered, the system displays the Enable Indexing checkbox selected and enabled. • If a type's supertype is registered for indexing, the system displays the Enable Indexing checkbox selected but disabled. You cannot clear the checkbox.
	<p>The system does not display the Enable Indexing checkbox on the New Types - Info page when you create a type. You must first create the type and then save it.</p>
	<p>If registering a particular type for indexing, the system automatically selects all of its subtypes for indexing. When registering a type for indexing, the system check for any of its subtypes that are registered. If a subtype is registered, the system unregisters it before registering the type.</p>

Field label	Value
Partitioned	<p>Displays whether a type that can be partitioned is or is not partitioned. This field:</p> <ul style="list-style-type: none"> • does not appear if the type cannot be partitioned. • displays <i>False</i> if the type can be partitioned but is not. • displays <i>True</i> if the type is partitioned.
Parent Type	<p>This option is available only when creating a type and Model Type is Lightweight. This field is display-only in modify mode. This field appears only if the High-Volume Server license is enabled and the Content Server version is 6 or later.</p>
Materialize	<p>This option is available only when creating a type and Model Type is Lightweight. this field is display-only in modify mode.</p>
	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Auto materialize: The lightweight object will be automatically materialized to a full object when the object is saved with changes to some attributes of the parent object. • Materialize on request: The lightweight object can only be materialized by explicitly calling the materialize API. Any changes to the parent object by the lightweight object before materialization will result in an error. • Do not materialize: The lightweight object is not allowed to be materialized. Call the materialize API will result in an error. Any changes to the parent object by the lightweight object will result in an error.
Full Text	<p>This option is available only when creating a type and Model Type is Lightweight. This field is display-only in modify mode.</p>
	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • No fulltext: This is the default. • Light fulltext: No attributes inherited from the shared parent will be full-text indexed. • Full fulltext

Field label	Value
Name or Attribute Name	The name of the attribute. This field is display-only in modify mode.
Type	The property type.
Size	The size of the property, if the property is the String type.
Inherited	<i>Yes</i> indicates that a property is inherited from a supertype. <i>No</i> indicates that the property is user-defined. You cannot remove a property inherited from the supertype.
Repeating	If selected, the property is a repeating property.

Selecting supertypes

Use the instructions in this section to select supertypes for a type.

To select a supertype:

1. Access the Choose a type page:
 - a. Navigate to **Administration > Types** to access the **Types** list page.
 - b. Select **File > New > Type** to access the **New Type - Info** page.
 - c. Click **Select Super Type** to access the **Choose a type** page.
2. Select the object type to be the supertype.
3. Click **OK** to return to the **New Type - Info** page.

Selecting default groups

Use the instructions in this section to select default groups for a type.

To select a default group:

1. Access the Choose a group page:
 - a. Navigate to **Administration > Types** to access the **Types** list page.
 - b. Select **File > New > Type** to access the **New Type - Info** page.
 - c. Click **Select Default Group** to access the **Choose a group** page.
2. Select the group to which you want the type to belong.
3. Click **OK** to return to the **New Type - Info** page.

Adding properties to types

Use the instructions in this section to add properties to a type.

To add properties to a type:

1. Access the Attribute Info: New Attribute page.
 - a. Navigate to **Administration > Types** to access the **Types** list page.
 - b. Select **File > New > Type** to access the **New Type - Info** page.
Enter required information.
 - c. Click **Next** to access the **New Type - Attributes** page.
 - d. Click **Add** to access the **Attribute Info: New Attribute** page.
2. Enter information on the **Attribute Info: New Attribute** page:
 - **Attribute Name:** Type the new attribute's name.
 - **Type:** Select the property type from the list box.
 - **Size:** If the property is the String type, type its size.
 - **Repeating:** Select to make the property a repeating property.
3. Click **OK** to return to the **New Type - Attribute** page.

Deleting types

Use the instructions in this section to delete types.

You can only remove a user-defined type from the repository if:

- You are the owner of the type or have Superuser privileges.
- The type has no subtypes.
- There are no existing objects of that type in the repository.

You cannot remove system-defined types from the repository. If you delete an object type with an associated assignment policy, the assignment policy is not removed. You can delete it manually.

You cannot delete a shareable type that is shared by a lightweight sysobject. Delete the dependent lightweight objects first.

To delete a type:

1. Navigate to **Administration > Types** to access the **Types** list page.
A list of existing object types is displayed.
2. Select the type to delete.
3. Select **File > Delete**.
The type is deleted.

Viewing assignment policies

The Assignment Policy Inheritance page displays a type, its supertypes, and the assignment policy for each type and supertype with an active assignment policy associated with it.

Use the Assignment Policy Inheritance page to view the assignment policies defined for a type or to understand policy inheritance and gauge the impact of changes to any policies. For example, before making changes to an assignment policy, you may need to know how many and which types will be affected. Knowing the inheritance hierarchy may also help with troubleshooting if content files are not saved in the correct storage area for that type.

The page displays a type that you select and its supertypes in descending order, with the type highest in the type hierarchy at the top of the list. The assignment policy associated with each type is displayed, if the assignment policy is active. If the selected type does not have an active assignment policy associated with it, the assignment policy associated with its immediate supertype is applied. If its immediate supertype does not have an active assignment policy, the policy associated with the next supertype in the hierarchy is applied until the SysObject supertype is reached.

An assignment policy is associated with a type in one of two ways:

- Direct association, when the type is specified in the policy
- Inheritance from a supertype

To view assignment policies associated with a type:

1. On the **Types** list page, select the type for which you want to view the associated assignment policies.
2. Select **View > Assignment Policy Inheritance**.
The **Assignment Policy Inheritance** page is displayed.
3. To view or modify the assignment policy associated with a type, click the policy name link.
The Info page for the selected assignment policy displays the properties. Use the instructions in [Viewing or modifying the properties of an assignment policy, page 424](#) to make changes.
4. Click **OK** or **Cancel** to return to the Types list page.

Converting types to shareable object types

If a type is a sysobject or subtype of sysobject, you can convert the type to a shareable type, even if its supertype is shareable. However, you cannot convert a type to shareable if any of its children are shareable types. This option is available only on 6.5 repositories where the High-Volume Server license is enabled.

To convert a type to a shareable object type:

1. Navigate to **Administration > Types** to access the **Types** list page.
A list of existing object types is displayed.
2. Select the type to share and then select **Tools > Convert to sharable object type**.
The **Convert Object** page is displayed.

-
3. Click **OK** to convert the object to a shareable object type or click **Cancel**.

Converting types to lightweight object types

You can convert dm_sysobject types and their subtypes to shareable object types for 6.5 repositories. This option is available only on 6.5 repositories where the High-Volume Server license is enabled.

To convert a type to a lightweight sysobject type:

1. Navigate to **Administration > Types** to access the **Types** list page.
A list of existing object types is displayed
2. Select the type and then select **Tools > Convert to lightweight object type**.
The **Convert Object** page is displayed.
3. Enter information on the **Convert Object** page:
 - a. **Shared Parent Type:** Select a shareable parent type.
If Recovery Mode is selected, the shared parent type does not need to be an existing type. If it is an existing type, it must be a shareable type.
If Recover Mode is not selected, the shared parent type cannot be an existing type.
 - b. **Execution Mode:** Select one of these options:
 - **Generate a Script Only:** Select to only generate the script file. This is the default setting.
 - **Run and Finalize:** Select to generate the script file and then run the conversion process.
 - **Run without Finalize:** Select to generate the script file and then run the conversion process without changing the original types.
 - **Finalize:** Select to replace the original types with the internal types.
 - c. **Recovery Mode:** Select to run the conversion in recovery mode. This field appears when Execution Mode is *Run without Finalize*.
 - d. **Default Parent Id:** Specify the parent ID to assign for lightweight sysobjects that are not qualified with any predicates. This field appears when Execution Mode is *Run and Finalize* or *Finalize*.
 - e. **Parent SQL Predicate:** Specify a SQL predicate to qualify a set of objects and the parent ID to assign. This field appears when Execution Mode is *Run and Finalize* or *Finalize*.
 - f. **SQL Predicate Parent Id:** Specify a SQL predicate to qualify a set of objects and the parent ID to assign. This field appears when Execution Mode is *Run and Finalize* or *Finalize*.

Converting types to shareable and lightweight object types

A heavy type object type can be converted to both a shareable object type and lightweight sysobject type. This option is available only on 6.5 repositories where the High-Volume Server license is enabled.

To convert a type to a shareable object type and lightweight sysobject type:

1. Navigate to **Administration > Types** to access the **Types** list page.
A list of existing object types is displayed.
2. Select the type and then **Select Tools > Convert to Sharable and lightweight object type**.
The **Convert Object** page is displayed.
3. Enter information on the **Convert Object** page:
 - a. **Shared Parent Type:** Type the new shared parent type name.
If Recovery Mode is selected, the shared parent type does not need to be an existing type. If it is an existing type, it must be a shareable type.
If Recover Mode is not selected, the shared parent type cannot be an existing type.
 - b. **Execution Mode:** Select one of these options:
 - **Split and Finalize:** Select to generate the script file and then run the conversion process.
 - **Split without Finalize:** Select to generate the script file and then run the conversion process without changing the original types. This is the default setting.
 - **Finalize:** Select to replace the original types with the internal types.
 - c. **Recovery Mode:** Select to run the conversion in recovery mode. This field appears when Execution Mode is *Split and Finalize* or *Split without Finalize*.
 - d. **Parent Attributes:** To select a type for the shareable parent types, click **Select Attributes** to access the **Choose an attribute** page.

Storage Management

The Storage Management chapter is divided into three sections:

- [Storage, page 379](#)

Access the Storage pages to create file stores, retention stores (EMC Centera and NetApp SnapLock), blob stores, turbo stores, mount point objects, location objects, and storage plug-ins.

- [Assignment policies, page 419](#)

Access the Assignment Policy pages to create assignment policies. These pages only appear when connected to a repository in which the Content Storage Services feature is enabled.

- [Migration policies, page 429](#)

Access the Migration Policies pages to create jobs to move content files among storage areas based on user-defined rules and schedules. These pages only appear when connected to a repository in which the Content Storage Services feature is enabled.

Storage

Use the pages in the Storage node to create, modify, or view storage areas, mount point objects, locations, and plug-ins:

- Storage areas are where content files are located.
 - Storage options for content files are directories on the file system (including file stores and retention stores).
 - Blob storage, in which content files are stored in a database table.
 - Turbo storage, in which content is stored in a property of the content's content object.
 - External storage, which provides access to legacy content and other sources stored outside the Documentum system.
- Mount point objects represent directories that are or will be mounted by a client.
- Location objects represent directories or files that are accessed by Content Server.
- Plug-ins are required for access to external stores.

When you view the Storage list page, the first ten storage areas in the repository are displayed in the order in which they were created.

- To sort the storage areas by **Name**, **storage Type**, **Size**, or **Status**, click the corresponding column head.
- To display only a type of storage, select the type from the drop-down list.
- To display a different number of items, select the number from the **Show Items** drop-down list.
- To jump to storage areas whose object names start with a particular letter, click that letter.
- To view more pages of storage areas, click the > or >> link.
- To jump to a storage area, type its object name in the **Starts With** box and click **Go**.

Click the links for information on the following topics:

- [Storage area types, page 382](#)
- [Viewing the properties of storage areas, page 383](#)
- [Deleting storage areas, locations, mount points, and plug-ins, page 383](#)

- File stores, page 383
 - Creating file stores, page 384
 - Modifying file stores, page 386
 - Properties of a file store, page 387
- Linked stores, page 389
 - Creating linked stores, page 389
 - Modifying linked stores, page 390
 - Properties of a linked store, page 390
- Blob stores, page 391
 - Creating blob stores, page 391
 - Viewing or modifying blob store properties, page 392
 - Properties of a blob store, page 392
- Distributed stores, page 393
 - Creating distributed stores, page 393
 - Modifying distributed stores, page 394
 - Properties of a distributed store, page 395
- External stores, page 396
 - Creating external stores, page 397
 - Modifying an external store, page 399
 - Editing a server root location, page 400
- EMC Centera stores, page 402
 - Creating EMC Centera stores, page 403
 - Modifying an EMC Centera store, page 405
 - Defining the storage parameters for an EMC Centera store, page 405

- Defining the content attributes saved in an EMC Centera store, page 407
- Properties of an EMC Centera store, page 408
- NetApp SnapLock stores, page 410
 - Creating NetApp SnapLock stores, page 411
 - Modifying a NetApp SnapLock store, page 412
 - Properties of a NetApp SnapLock store, page 412
- Mount points, page 414
 - Creating or modifying mount points, page 414
- Locations, page 416
 - Creating or modifying locations, page 416
- Plug-ins, page 417
 - Creating or modifying plug-ins, page 418

For more information about storing content files, refer to "Content Management" in the *Content Server Administration Guide*.

Storage area types

Storage areas are where Content Server stores content. Documentum offers various storage options:

- File stores hold content as files.
- Thumbnail stores and streaming stores are file stores whose media type is set to thumbnail content or streaming content.
- Linked stores do not contain content, but point to the actual storage area, which is a file store.

Linked stores are not available if connected to a Documentum 6 or later repository; however, linked stores are available if connected to a 5.3x repository. On Windows hosts, the actual storage area is implemented as a shared directory. On UNIX and Linux hosts, the linked store contains a logical link to the actual storage area.

- Distributed stores do not contain content; instead, they point to component storage areas that store the content.

The component storage areas in a distributed store can be any mixture of the file store and linked store storage types, provided that all have the same value in the media_type property.



Caution: When a repository is configured to use distributed storage, it cannot be converted back to nondistributed storage.

- Blob stores store files directly in the repository in a special table.
- Turbo stores store content in a property of the content's content object.
- External stores do not store any content. Instead, they point to the actual storage area, which can be a CD-ROM, a file system, a URL, or be user-defined.

- XML file store is an external free store used specifically to optimize performance with XML content files.
- Retention storage areas store content that you want to retain for a specified time. They are often used for storing massive amounts of unchanging data, such as email archives or check images. The two types of retention stores are EMC Centera store and NetApp SnapLock store. EMC Centera store storage areas also enable the storage of metadata values with each piece of content.

Viewing the properties of storage areas

Use the instructions in this section to view the properties of a storage area.

To view the properties of a storage area:

1. Connect to a repository.
2. Navigate to **Administration > Storage Management > Storage**.
The system displays the **Storage** list page.
3. Select the storage area to view and then select **View > Properties > Info**.
The system displays the Info page for the storage area.
4. Click **OK** or **Cancel** to return to the Storage list page.

Deleting storage areas, locations, mount points, and plug-ins

You must have System Administrator or Superuser privileges to delete a storage area.

To delete a storage area:

1. Connect to the repository.
2. Navigate to **Administration > Storage Management > Storage**.
The **Storage** list page appears.
3. Select the correct object (storage area, location, mount point, or plug-in) to delete and then select **File > Delete**.
4. Click **OK** to delete the storage area.
The object is deleted and the Storage list page appears.
If you deleted a file store, the associated location object is not automatically deleted; if you want to remove it from the repository, you must delete it separately.

File stores

A file store is a directory that contains content files. It is the basic storage type of a repository.

Use the instructions in this section to create a new file store. Each file store must have a corresponding location object. You can create a location object pointing to the file system directory that corresponds to the file store before creating the file store, using the instructions in [Creating or modifying locations, page 416](#), or you can select the location while creating the file store and Documentum Administrator will create the location object for you.

File store storage areas may enable three special content-handling features:

- Digital shredding

Digital shredding is a security feature that removes deleted content files and their associated content objects. Next, it overwrites the file's addressable locations with a character, then its complement, and finally a random character. Enable digital shredding when a file store is created or at a later time. Digital shredding requires a Trusted Content Services license.

- Content compression

Content compression is a feature that automatically compresses files to a smaller size when the file is created. Content compression requires a Content Storage Services license. You cannot enable content compression after the file store is created.

- Content duplication checking

This feature minimizes the amount of content file duplication in the file store. Content duplication checking requires a Content Storage Services license.

If you enable content duplication checking, you must then indicate whether to check for duplicate content and generate the hash values used to determine the existence of duplicates, or just generate the hash values. You cannot enable content duplication checking after the file store is created.

Note: After you create a file store, you can change its status or the SurrogateGet method it uses by viewing the file store's properties.

Click the links for information on the following topics:

- [Creating file stores, page 384](#)
- [Modifying file stores, page 386](#)
- [Properties of a file store, page 387](#)

Creating file stores

Use the instructions in this section to create file stores.

To create new file stores:

1. Connect to the repository where you want to create a new file store.

2. Navigate to **Administration > Storage Management > Storage**.

The system displays the **Storage** list page.

3. Select **File > New > File Store**.

The system displays the **New File Store - Info** page.

4. Enter information on the **New File Store - Info** page:

a. **Name:** Type the name of the new file store. The name must be unique within the repository.

- b. **Description:** Type a description of the new file store. The description may be up to 128 bytes long.
- c. **Location or Server Path:** Select the location object that represents the file store, or select the server path and browse to the location on the server host where the new file store will reside.
- d. **Media Type:** Select a media type to store in the storage area. Options are:
 - Regular Content
 - Thumbnail Content
 - Streaming Content
 For more information about thumbnails and streaming media, refer to the documentation for Documentum Media Services and to the *Documentum Content Server Administration Guide*.
- e. **Base URL:** Type the base URL used to retrieve content directly from a storage area.
- f. **Encrypted:** Select **Yes** to create an encrypted file store. This option is only available in repositories with Trusted Content Services enabled.
- g. **Make Public:** Select to make the file store publicly accessible with no restrictions.
- h. **Add Extension:** Select to require that the server append an extention to the file when writing it into the storage area.
- i. **Require Ticket:** Select to require the server to generate a ticket when returning the URL to a content file.
- j. **Digital Shredding:** Select to enable digital shredding. 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. This option is only available in 5.3 SP1 and later repositories with Trusted Content Services enabled.



Caution: The Documentum Administrator interface for version 6 and later displays the **Digital Shredding** checkbox for all file stores. If the file store is a component of a distributed store, files are not digitally shredded even when it appears that digital shredding is enabled for the file store.

- k. **Content Compression:** Select to compress all content in the file store. This option is only available in 5.3 SP1 and later repositories with Content Storage Services enabled.
 - l. **Content Duplication:** Select to enable content duplication checking. This option is only available in repositories with Trusted Content Services enabled.
 - When **Generate content hash values only** is selected, for each piece of content checked in to the repository, Content Server calculates the value needed to determine whether or not it is duplicate content.
 - When **Generate content hash values and check for duplicate content** is selected, for each piece of content checked in to the repository, Content Server calculates the value needed to determine whether or not it is duplicate content and then checks for duplicate content.
5. After adding information for the new file store, click **OK**.

The system displays the Storage list page.

Modifying file stores

When viewing the properties of a file store, a number of fields can no longer be changed and additional fields are available for modification.

To modify a file store:

1. Connect to the repository where you want to modify the file store.
2. Navigate to **Administration > Storage Management > Storage**.
The system displays the **Storage** list page.
3. Select the file store to modify and then select **View > Properties > Info**.
The system displays the File Store Properties - Info page.
4. Modify information on the **File Store Properties - Info** page.

Note: This section only discusses editable fields. The [Properties of a file store, page 387](#) section discusses other fields displayed on the File Store Properties - Info page.

- a. **Description:** Add or change a description, which can be up to 128 bytes long.
- b. **Make Public:** Select to make the file store publicly accessible with no restrictions.
- c. **Require Ticket:** Select to require the server to generate a ticket when returning the URL to a content file.
- d. **SurrogateGet Method:** If the repository is used in replication and you want to designate a custom SurrogateGet method, click **Select** and browse to the custom SurrogateGet.
- e. **Offline Get Method:** Select to use an offline Get method.
- f. **Status:** Select a radio button to change the status of the file store to on line, offline or read-only.
- g. **Digital Shredding:** Select to remove deleted content files and their associated content objects, then overwrite the file's addressable locations with a character, then its complement, and finally a random character. This option is only available in 5.3 SP1 and later repositories with Trusted Content Services enabled.



Caution: The Documentum Administrator interface for version 6 and later displays the **Digital Shredding** checkbox for all file stores. If the file store is a component of a distributed store, files are not digitally shredded even when it appears that digital shredding is enabled for the file store.

5. Click the **Space Info** tab to access the **File Store Properties - Space Info** page to view **Active Space/Files** and **Orphaned Space/Files**.
6. Click **OK** to save any changes and return to the Storage list page or **Cancel** to exit without saving changes.

Properties of a file store

Some of the fields discussed in this table are only available or visible when modifying an existing file store. Others are only available or editable when a new file store is created.

Table 42. Properties of a file store

Field label	Value
Name	The name of the new storage object. The name must be unique within the repository.
Description	A description of the file store. The description can be up to 128 bytes in length if in English, German, Italian, Spanish, or French. The description can be up to approximately 64 bytes in Japanese.
Location or Path	The location object associated with this file store.
Select Server Path	Storage path on the server machine.
Media Type	Identifies the type of media stored in a content area. Options are Regular Content, Thumbnail Content, or Streaming Content. Media type cannot be changed once set.
Base URL	The basic URL used to retrieve content directly from a storage area.
Encrypted	Indicates if the file store is encrypted. To encrypt a file store, Trusted Content Services must be enabled for the server installation.
Make Public	Indicates if the area is accessible to the public with no restrictions.
Add Extension	Indicates if the server should append an extension to a file when writing it into the storage area.
Require Ticket	Boolean. Select to require the server to generate a ticket when returning the URL to a content file.
SurrogateGet Method	To install a custom SurrogateGet, click Select Method and browse to the method on the server host file system. This field and link only appear when modifying a file store.
Offline Get Method	Select to use an offline Get method. This link only appears when modifying a file store.
Status	Select a radio button to change the status of the file store to on line, off line, or read-only.

Field label	Value
Digital Shredding	<p>Select to enable digital shredding, which 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. This option is available only for repositories where Trusted Content Services is enabled.</p>
Content Compression	<p>The Documentum Administrator interface for version 6 and later displays the Digital Shredding checkbox for all file stores. If the file store is a component of a distributed store, files are not digitally shredded even when it appears that digital shredding is enabled for the file store.</p>
Content Duplication	<p>Select during file store creation to enable content compression.</p> <p>In an existing file store, an information-only field indicates if the file store has content compression enabled or not.</p> <p>Content compression can be enabled only during file store creation and only with a Content Storage Services license.</p> <p>In 5.3 SP1 and later repositories, select during file store creation to examine content files to eliminate content duplication in the repository.</p> <ul style="list-style-type: none"> • When Generate content hash values only is selected, for each piece of content checked in to the repository, Content Server calculates the value needed to determine if it is duplicate content. • When Generate content hash values and check for duplicate content is selected, for each piece of content checked in to the repository, Content Server calculates the value needed to determine whether or not it is duplicate content and then checks for duplicate content. <p>In an existing file store, an information-only field indicates whether content hash values will or will not be generated and whether the check for duplicate content is or is not enabled.</p>

Field label	Value
Active Space/Files	Content duplication checking can be enabled only during file store creation and only with a Content Storage Services license.
Orphaned Space/Files	The space used by the file store and the number of files (information only on the File Store Properties - Space Info page).
	The amount of orphaned space in the file store and the number of orphaned files (information only on the File Store Properties - Space Info page).

Linked stores

A linked store is a storage area that does not contain content files. Instead, it contains a logical link to the actual storage area, which is a file store.

Note: Linked stores are not available for Documentum 6 or later repositories; however, linked stores are available if connected to a 5.3x repository.

Click the links for information on the following topics:

- [Creating linked stores, page 389](#)
- [Modifying linked stores, page 390](#)
- [Properties of a linked store, page 390](#)

Creating linked stores

Use these instructions to create a linked store.

To create a linked store:

1. Connect to a 5.3x repository to create a new linked store.
2. Select **Administration > File Management > Storage**.
The **Storage** list page appears.
3. Click **File > New > Linked Store**.
The Info page for a linked store appears.
4. Type the name of the new linked store.
The name must be unique in the repository.
5. Select the location object that represents the link store or click **Server Path** and select the directory on the server host where the new link store will reside.
6. Select the store to which the links are made from the **Linked Store** drop-down list.

7. Select **Use symbolic links** to use symbolic links.

8. Click **OK**.

The linked store is created. If you selected a directory on the host, a location object is also created.

The Storage list page appears.

Modifying linked stores

When you view the properties of a linked store, a number of fields can no longer be changed and some additional fields are available for modification.

To modify a linked store:

1. Connect to a 5.3x repository to modify or view an existing linked store.
2. Select **Administration > File Management > Storage**.
The **Storage** list page appears.
3. Locate the correct linked store and then select **View > Properties > Info**.
The Info page appears.
4. If the repository is used in replication and you want to designate a custom SurrogateGet method, click **Select Method** and browse to the custom SurrogateGet.
5. To use an offline Get method, select **Offline Get Method**.
6. To place the linked store on line or offline or to make it read-only, select a radio button.
7. Click **OK** to make the changes and return to the Storage list page or **Cancel** to exit without changes.

Properties of a linked store

Some fields discussed in this table are only available or visible when you modify an existing linked store. Others are only available when a linked store is created.

Table 43. Properties of a linked store

Field label	Value
Name	The name of the storage object. This name must be unique within the repository.
Location	The name of the directory containing the logical link.
Linked Store	The name of the storage area to which the link is pointing.
Use symbolic links	If selected, symbolic links are used.

Field label	Value
Get Method	To install a custom SurrogateGet, click Select Method and browse to the method on the server host file system.
Offline Get Method	Select to use an offline Get method.
Status	Select a radio button to change the status of the file store to on line, off line, or read only.

Blob stores

The content in a blob store is stored directly in the repository rather than on the server host's file system, as in a file store. The content in a blob store is stored in rows in an RDBMS table. The content stored in a blob store must be less than or equal to 64 KB.

Content stored in a blob store is ASCII or arbitrary sequences of 8-bit characters. This is designated when creating the blob store. To allow arbitrary sequences of 8-bit characters, you can store ASCII in the store, but if you decide on ASCII, you cannot store 8-bit characters.

You cannot define a blob storage area as the underlying area for a linked store or as a component of a distributed storage area. That is, blob storage cannot be accessed through a linked store storage area or through a distributed storage area.

Note that if a repository uses the DB2 database and two or more blob stores are created for the repository, the first 16 characters in the name of each blob store must be unique.

Click the links for information on the following topics:

- [Creating blob stores, page 391](#)
- [Viewing or modifying blob store properties, page 392](#)
- [Properties of a blob store, page 392](#)

Creating blob stores

Use the instructions in this section to create a blob store.

To create a blob store:

1. Connect to a repository to create a blob store.
2. Navigate to **Administration > File Management > Storage**.
The **Storage** list page appears.
3. Select **File > New > Blob Store** to access the **New Blob Store - Info** page.
4. Type the name of the new blob store.
If the repository uses the DB2 database and two or more blob stores are created for the repository, the first 16 characters in the name of each blob store must be unique.
5. Select **ASCII or 8-bit Characters**.

6. Click **OK**.

The blob store is created and the Storage list page is displayed.

Viewing or modifying blob store properties

Use the instructions in this section to view or modify properties of a blob store.

To view or modify blob store properties:

1. Access the Blob Store Properties - Info page.
 - a. Connect to a repository and navigate to **Administration > File Management > Storage** to access the **Storage** list page.
 - b. Select an existing blob store and then select **View > Properties > Info** to access the Blob Store Properties - Info page.
2. View or modify information on the **Blob Store Properties - Info** page.
 - a. **Name:** Name of the blob store. Read only.
 - b. **Content Type:** Select **ASCII** or **8-bit Characters**.
 - c. **Get Method:** To install a custom SurrogateGet, click **Select Method** and browse to the method on the server host file system.
 - d. **Offline Get Method:** Select to use an offline Get method.
 - e. **Status:** Select a radio button to change the status of the blob store. Options are
 - On Line
 - Off Line
 - Read Only
3. Click **OK** to save changes or **Cancel** to exit without saving changes.

The system displays the Storage list page.

Properties of a blob store

The table below lists the properties of a blob store.

Table 44. Properties of a blob store

Field label	Value
Name	The name of the storage object. This name must be unique within the repository and must conform to the rules governing type names. If the repository uses DB2 database and two or more blob stores are created for the repository,

Field label	Value
	the first 16 characters in the name of each blob store must be unique.
Content Type	Valid values are: <ul style="list-style-type: none">• ASCII• 8-bit Characters
Get Method	To install a custom SurrogateGet, click Select Method and browse to the method on the server host file system.
Offline Get Method	Select to use an offline Get method.
Status	Select a radio button to change the status of the file store to on line, off line, or read only.

Distributed stores

A distributed store storage area does not contain content. Instead, it points to component storage areas containing the content. The component storage areas in a distributed store can be any mixture of the file store and linked store storage types, but all must have the same value in their `media_type` property. That is, all the components must store the same kind of content.

Distributed storage areas are useful when repository users are located in widely separated locations. For example, a company might have offices in New York, San Francisco, Tokyo, and London, with users in each office using the same repository. You can define a distributed storage area with a component in each geographic location and set up the appropriate content replication jobs to ensure that content is current at each location. This provides users in each office with fast access to local copies of the documents.

The *Distributed Configuration Guide* describes how to implement and administer a distributed storage area. The *Object Reference Manual* lists the properties defined for the distributed store object type.

Note: When a repository is configured to use distributed storage, it cannot be converted back to nondistributed storage.

Click the links for information on the following topics:

- [Creating distributed stores, page 393](#)
- [Modifying distributed stores, page 394](#)
- [Properties of a distributed store, page 395](#)

Creating distributed stores

Use the instructions in this section to create a distributed store.

Note: When a repository is configured to use distributed storage, it cannot be converted back to nondistributed storage.

To create a distributed store:

1. Access the New Distributed Store - Info page to create a distributed store:
 - a. Connect to a repository to create a distributed store.
 - b. Navigate to **Administration > File Management > Storage** to access the **Storage** list page.
 - c. Select **File > New > Distributed Store**.
The system displays the New Distributed Store - Info page.
2. Enter information about the distributed store on the **New Distributed Store - Info** page.
 - a. **Name:** Type the name of the distributed store. This name must be unique within the repository and must conform to the rules governing type names.
 - b. **Fetch Content Locally Only:** Select to require the server to fetch all content from the local component of the store.
The default is not selected.
 - c. Click **Next** to access the New Distributed Store - Components page.
3. Define the components of the distributed store on the **New Distributed Store - Components** page.
 - a. Click **Add** to access the **Choose a storage** page.
 - b. Select storage areas to add to the distributed store and then click **>** to add.
 - c. Click **OK** to return to the New Distributed Store - Components page.
4. Click **Finish**.
The system displays the Storage page.

Modifying distributed stores

Use the instructions in this section to modify a distributed store. To designate a different surrogate get method from the default after you create the store, go to the Info page for the store and browse to a user-defined surrogate get.

To modify a distributed store:

1. Access the Distributed Store Properties - Info page for a distributed store to modify:
 - a. Connect to a repository to modify a distributed store.
 - b. Navigate to **Administration > File Management > Storage**.
The system displays the **Storage** list page.
 - c. Select a distributed store and then select **View > Properties > Info**.
The system displays the Distributed Store Properties - Info page for the distributed store.
2. Modify information on the **Distributed Store Properties - Info** page:
 - a. **Name:** The name of the storage object. Read only.
 - b. **Fetch Content Locally Only:** Select to require the server to fetch all content from the local component of the store.

- The default is not selected.
- c. **Get Method:** To install a custom SurrogateGet, click **Select Method** and browse to the method on the server host file system.
The *Distributed Configuration Guide* and *Properties of a distributed store, page 395* contain additional information on surrogate get.
 - d. **Offline Get Method:** Controls whether the server regards retrieved content as immediately available or awaiting restoration.
 - e. **Status:** Designates whether the storage area is on line, off line, or read only.
 - f. Click **OK** to return to the Storage list page or click the **Components** tab to access the Distributed Store Properties - Components page.
3. Define or remove components of the distributed store on the **Distributed Store Properties - Components** page.
 - a. To add components to the distributed store:
 - i. Click **Add** to access the **Choose a storage** page
 - ii. Select storage areas to add to the distributed store and click **>**.
 - iii. Click **OK** to return to the Distributed Store Properties - Components page.
 - b. To remove components of the distributed store:
 - i. Select the component.
 - ii. Click **Remove**.
 4. Click **OK** to save changes or click **Cancel** to exit without saving changes.
The system displays the Storage list page.

Properties of a distributed store

Some of the fields discussed in this table are only available or visible when you modify an existing distributed store. Others are only available when creating a distributed store.

Table 45. Properties of a distributed store

Field label	Value
Name	The name of the storage object. This name must be unique within the repository and must conform to the rules governing type names. This field is read only in modify mode.
Fetch Content Locally Only	Controls whether an attempt will be made to fetch content from far stores that are not available locally.

Field label	Value
Get Method	To install a custom SurrogateGet, click Select Method to access the Choose a method page to select a method on the server host file system. Generally, when users attempt to fetch a document that is stored in an inaccessible far storage area, the server returns an error message. In such cases, the system administrator has to replicate the content into a storage area that is accessible. To automate this administrative task, Documentum provides the surrogate get feature, which allows the server to automatically replicate content when a fetch fails.
Offline Get Method	Implement this feature using the surrogate get method provided by default with the Content Server system administration tool suite (named dm_SurrogateGet), or write your own surrogate get program. If you write your own, fill in the method name here.
Status	Controls whether the server regards retrieved content as immediately available or awaiting restoration. This field is only meaningful when the Get Method field contains a value. Designates whether the storage area is on line, off line, or read only.

External stores

External storage areas do not store content. Instead, external stores point to the actual storage area, which can be a CD-ROM, a file system, a URL, or a user-defined store.

Data in an external store is not physically managed by Content Server. There are significant limitations on content in an external store. For example, you cannot index content or the properties of content in an external store.

External stores require a plug-in that you must create. The plug-in can run on the server side or client side, although a client-side plug-in may provide better performance. To assist you, Documentum provides code for sample plug-ins in the DM_HOME/unsupported/plugins directory. The *Content Server API Reference Manual* contains information on plug-ins.

There are three types of external stores:

- External file store

Use external file stores for legacy files in external file systems, optical disks, and CD-ROM files.

- External free store

External free store storage areas allow users to specify a token that is not a file path or a URL. An external free store enables you to define your own token standard and means of retrieving the content associated with the token. Write your own content retrieval mechanism through a DLL plug-in, which is described by a plug-in object.

You can also use the external free store pages to manually create XML stores. Use XML stores to store and query large volumes of XML content. An XML store is a native XML database that is fully optimized for XML content. When you select *XML* for the storage class on the New External Free Store - Info page, the system will display these additional fields for an XML store:

- Writable
 - Application Server URL
 - Store Location
- External URL store

External URL stores provide support for token-mode operation where the token is a URL. The tokens specified in the Setpath operation must follow the URL standard. The client and the server do not validate the format of the URL.

Click the links for information on the following topics:

- [Creating external stores, page 397](#)
- [Modifying an external store, page 399](#)
- [Editing a server root location, page 400](#)

The Content Management section in the *Content Server Administration Guide* provides more information about external stores.

The *Documentum XML Store Installation and Administration Guide* provides more information about external XML file stores.

Creating external stores

Create the appropriate plug-ins before configuring the external store. The *Content Server Administration Guide* contains information on how to create plug-ins. Use the instructions in this section to create an external file store, external free store, or external URL store. To create an XML store, follow the basic instructions for an external free store.

To create an external store:

1. Connect to a repository to create an external store.
2. Navigate to **Administration > File Management > Storage**.

The system displays the **Storage** list page.

3. Select one of the following:
 - **File > New > External File Store** to access the **New External File Store - Info page**.
 - **File > New > External Free Store** to access the **New External Free Store - Info page**.
 - **File > New > External URL Store** to access the **New External URL Store - Info page**.
4. Enter information on the Info page for the external store:
 - a. **Name:** Type the name of the new external store.
 - b. **Execute Plug-In:** Select whether the plug-in is executed on the server or client.
 - c. Select a plug-in for each applicable platform:
 - **Windows**
 - **Solaris**
 - **Aix**
 - **HP-UX**
 - **Macintosh**
 - **Linux**
 - **HP-UX-Itanium**
 - d. **Client Root:** Click **Browse** and select a client root.
This is the name of the location object that represents the default root of the content for client side plug-in execution when mount is not executed. The default is NULL. This option is available only on the New External File Store - Info page.
 - e. **Storage Class:** Select a storage class identifier.
The storage class indicates the purpose of the store and is available only for external free stores. Options are *None* and *XML*.
Select *XML* to create an XML store. When you select *XML* for the storage class, the system displays the following fields:
 - **Writable**
 - **Application Server URL**
 - **Store Location**You cannot change the storage class identifier after you create the external free store.
 - f. **Writable:** Select to indicate if content is pushed to an XML store that Documentum manages. This option is available only for external free stores where Storage Class is *XML*.
 - g. **Application Server URL:** Type the path to the application server that hosts an Xhive database. This option is available only for external free stores where Storage Class is *XML*.
 - h. **Store Location:** Type the location of the external XML file store. This option is available only for external free stores where Storage Class is *XML*.
 - i. Click **Next** to access the New External File Store - Server page. This page is available only for external file stores.
5. Complete information on the **New External File Store - Server** page for the external file store:
 - a. Click **Add** or select the server and click **Edit** to access the **Choose a server config** page.

- b. On the Choose a server config page, select a server config object and then click **OK** to access the Select Root Location for Server page.
 - c. On the **Select Root Location for Server** page, click **Select Location** to access the **Choose a location** page.
 - d. Select a root location for the server, and then click **OK** to return to the Select Root Location for Server page.
The server root location is the default root of the content for the server side plug-in execution.
 - e. Click **OK** to return to the New External File Store - Server page for the external file store.
6. Click **Finish** (external file store) or **OK** (external free store or external URL store).

Modifying an external store

Use the instructions in this section to modify an external file store, external free store, or external URL store. To modify an XML store, follow the basic instructions for an external free store.

To modify an external store:

1. Access the Info page for the external store:
 - a. Connect to a repository to modify an external store.
 - b. Select **Administration > File Management > Storage**.
The Storage list page is displayed.
 - c. Locate the external store and select **View > Properties > Info**.
The Info page for the external store is displayed.
2. View or modify information on the Info page for the external store:
 - a. **Name:** The name of the new external store. This field is display-only.
 - b. **Execute Plug-In:** Indicates whether the plug-in is executed on the server or client. This field is editable.
 - c. Indicates a plug-in for each applicable platform. These fields are editable for the following platforms:
 - **Windows**
 - **Solaris**
 - **Aix**
 - **HP-UX**
 - **Macintosh**
 - d. **Client Root:** The name of the location object that represents the default root of the content for client side plug-in execution when mount is not executed. The default is NULL.
This option is available only on the External File Store Properties - Info page.
Click **Browse** to select a client root.

- e. **Storage Class:** Indicates the purpose of the store. Storage class is available only for external free stores and is not editable after the store is created. When the storage class is XML, the system displays the following fields:
 - Writable
 - Application Server URL
 - Store Location
 - f. **Writable:** Indicates if content is pushed to an XML store that Documentum manages. This option is available only for external free stores where Storage Class is XML.
 - g. **Application Server URL:** The path to the application server that hosts an Xhive database. This option is available only for external free stores where Storage Class is XML.
 - h. **Store Location:** The location of the external XML file store. This option is available only for external free stores where Storage Class is XML.
 - i. Click the **Server** tab to access the External File Store Properties - Server page. This page is available only for external file stores and is not available for external free stores or external URL stores.
3. Modify information on the **External File Store Properties - Server** page for an external file store:
- a. Click **Add** or select the server and click **Edit** to access the Choose a server config page.
 - b. On the **Choose a server config** page, select a server config object and then click **OK** to access the Select Root Location for Server page.
 - c. On the **Select Root Location for Server** page, click **Select Location** to access the **Choose a location** page.
 - d. Select a root location for the server, and then click **OK** to return to the Select Root Location for Server page.
The server root location is the default root of the content for the server side plug-in execution.
 - e. Click **OK** to return to the Server page for the external store.
4. Click **Finish** (external file store) or **OK** (external free store or external URL store).

Editing a server root location

The Select Root Location for Server page displays the server, location, and path that is the default root of the content for server side plug-in execution.

Use the instructions in this section to select a server root location.

To select a server root location:

1. On the **Select Root Location for Server** page, click **Select Location**.
The **Choose a location** page appears.
2. Locate the correct location.
Use the forward and back buttons or the **Items per page** drop-down list to view more locations.
3. Select the location.

-
4. Click **OK**.

Properties of an external store

Some of the fields discussed in this table are only available or visible when you modify an existing external store. Others are only available when creating an external store.

Table 46. Properties of external stores

Field label	Value
Name	The name of the external store. This field is display-only in modify mode.
Execute Plug-in	Indicates whether the plug-in is executed on the server or client.
Windows	The name of the plug-in if using a Windows platform.
Solaris	The name of the plug-in if using a Solaris platform.
Aix	The name of the plug-in if using an AIX platform.
HP-UX	The name of the plug-in if using a HP-UX platform.
Macintosh	The name of the plug-in if using a Macintosh platform.
Current Client Root	The name of the current location object that represents the default root of the content for client side plug-in execution when mount is not executed. This field is not editable and appears only when creating or modifying an external file store.
Client Root	The name of the location object that represents the default root of the content for client side plug-in execution when mount is not executed. The default is NULL. This field is available only for external file stores. Click Browse to select a client root.

Field label	Value
Storage Class	Indicates the purpose of the store. Storage class is available only for external free stores and is not editable after the store is created. When the storage class is XML, the system displays the following fields: <ul style="list-style-type: none"> • Writable • Application Server URL • Store Location
Writable	Indicates if content is pushed to an XML store that Documentum manages. This option is available only for external free stores where Storage Class is XML.
Application Server URL	The path to the application server that hosts an Xhive database. This option is available only for external free stores where Storage Class is XML.
Store Location	The location of the XML store. This option is available only for external free stores where Storage Class is XML.

EMC Centera stores

An EMC Centera store is a retention store for large amounts of unchanging data such as email archives or check images. To use Centera storage, you must purchase a license for Content Services for EMC Centera (CSEC), and you must enter the CSEC license key when you install the Content Server software. Storage systems made by vendors other than EMC are not supported.

In an EMC Centera store, you can:

- Store metadata values with a piece of content.
- Define a retention date or, with Content Server 5.3 SP3 or later, a retention period for the content.
- Index content.
- Enable content compression in 5.3 SP1 and later repositories, if you have a CSEC license.

Files created on a Macintosh computer cannot be stored in an EMC Centera store.

Click these links for more information on:

- [Creating EMC Centera stores, page 403](#)
- [Modifying an EMC Centera store, page 405](#)
- [Defining the storage parameters for an EMC Centera store, page 405](#)
- [Defining the content attributes saved in an EMC Centera store, page 407](#)
- [Properties of an EMC Centera store, page 408](#)

The Content Management chapter in the *Content Server Administration Guide* contains additional information about EMC Centera stores.

Creating EMC Centera stores

To create an EMC Centera store, you must:

- Have a license for Content Services for EMC Centera (CSEC).
- Enable the feature with the license key in the Content Server software installation containing the repository for which you are creating the Centera store.
- Know the connection string of the Centera storage system.

A repository can have multiple Centera stores. For ease of administration, maintenance, and management, it is recommended that you use the same plug-in for all the Centera stores.

Set the C-clip buffer size or configure use of embedded blob storage by using optional storage parameters. Setting the C-clip buffer size is available only in 5.3 SP3 and later repositories.

Support is provided for distributed Centera clusters in 5.3 SP3 and later repositories. The Centera store plug-in must be stored depending on where the Content Servers in such a configuration are running:

- If all Content Servers are running on the same computer, the Centera store plug-in must be in a file store.
- If the Content Servers are running on different hosts, then the Centera store plug-in must be stored in a file store that is shared by all Content Server instances or in a distributed store in which each Content Server has at least one component defined as a near store.

Refer to the Content Management chapter in the *Content Server Administration Guide* information on configuring support for distributed Centera clusters.

A default retention period is optionally available with Content Server 5.3 SP3 and later. When you create an EMC Centera store in a 5.3 SP3 or later repository for the first time, the system asks if you want to upgrade. The upgrade runs a method that adds a new property, `default_retention_days`, to the store object type definition. After the method runs, restart all Content Servers running against the repository.

To create an EMC Centera store:

1. Access the New EMC Centera Store - Info page:
 - a. Connect to a repository to create a Centera store.
 - b. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
 - c. Click **File > New > EMC Centera Store**.
The **New EMC Centera Store - Info** page is displayed.
2. Type the name and a description of the new Centera store.

3. In the **Plugin Name** section, select **Default Plugin** or **Select Plugin**.

- Select **Default Plugin** to set a null ID (0000000000000000) in the a_plugin_id property of the EMC Centera store object.
- Select the **Select Plugin** radio button to use the default CSEC plug-in.

To use a plug-in other than the default CSEC plug-in, click the **Select Plugin** link, locate the plug-in in the repository, select it, and click **OK**.

When a repository is created, a default plug-in object for CSEC is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in [Creating or modifying plug-ins, page 418](#) to create a new plug-in object with the content of the plug-in object set as follows:

- Windows: %DM_HOME%\bin\emcplugin.dll
- Solaris, AIX, and Linux: \$DM_HOME/bin/libemcplugin.so
- HP-UX: \$DM_HOME/bin/libemcplugin.sl

4. Click **Edit** to add or modify storage parameters for the Centera store.

Use the instructions in [Defining the storage parameters for an EMC Centera store, page 405](#) to add or modify storage parameters for the Centera store.

5. Select **Enable Content Compression** to compress all content in the store.

This option is only available in 5.3 SP1 and later repositories where Content Storage Services is enabled.

6. Select **Configure Retention Information** to enable content retention. When selected, the system automatically selects and inactivates the **Event Based Retention** checkbox.

Note: The options to configure retention information for Centera stores differ if you do not connect to a version 6 or later repository.

- a. **Retention Attribute Name:** Type the retention attribute name. The value entered must *not* be one of the values specified as a content attribute name.

- b. **Fixed Retention:** Select to choose how the value of the retention property is set:

- **Choose a retention period:** Select to set a period of days as the retention period for all content in the Centera store. Next, select the date and time for the default retention.
- **Choose default retention days:** Select and then type the number of retention days.

Both default retention date and default retention days can be specified. If both are specified, the default retention days will take precedence over default retention date. If default retention date is selected but no value is specified, the system will ignore the retention date option.

- c. **Event Based Retention:** When Configure Retention Information is selected, the system automatically selects and inactivates this checkbox to prevent changing the event based retention option status.

- d. **Application Provides Retention:** Select to require that a client application supply the retention date when content is saved to the Centera store.

7. To add other content properties, click **Add**.

- a. Type the name of a content attribute.

The content attribute name can be an arbitrary name. It does not have to correspond to any existing properties of the objects whose content is stored in the Centera store.

- b. Type a description.
 - c. Click **OK**.
 - d. Repeat steps a to c as required.
8. Click **Finish**.

Modifying an EMC Centera store

Use the instructions in this section to modify an EMC Centera store.

A default retention period is optionally available with Content Server 5.3 SP3 and later. When modifying a Centera store in a 5.3 SP3 repository for the first time, the system asks if you want to upgrade. The upgrade runs a method that adds a new property, `default_retention_days`, to the store object type definition. After the method runs, restart all Content Servers running against the repository.

To modify an EMC Centera store:

1. Access the EMC Centera Store Properties - Info page:
 - a. Connect to a repository where the Centera store is located.
 - b. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
 - c. Select a Centera store and select **View > Properties > Info**.
To locate the store faster, filter the list by selecting **EMC Centera Store** from the drop-down list.
2. Change the properties of the store. [Properties of an EMC Centera store, page 408](#) contains information about the fields.
3. Click **OK** when finished or click **Cancel**.

Defining the storage parameters for an EMC Centera store

Use the instructions in this section to add or modify storage parameters for the EMC Centera store.

To define the storage parameters for an EMC Centera store:

1. Access the **Storage Parameters** page:
 - a. Access the **Storage** list page:
 - i. Connect to a repository where the Centera store is located.
 - ii. Navigate to **Administration > File Management > Storage**.
The **Storage** list page is displayed.

- b. Access the EMC Centera store **Info** page:
 - To create a Centera store, select **File > New > EMC Centera Store** to access the **New EMC Centera Store - Info** page.
 - To modify a Centera store, select a Centera store and then select **View > Properties > Info** to access the **EMC Centera Store Properties - Info** page.

To locate the store faster, filter the list by selecting **EMC Centera Storage** from the drop-down list.
 - c. In the **Storage Parameters** section, click **Edit** to access the **Storage Parameters** page.
2. In the **Enter new value** field, type the connection string for the EMC Centera storage system.



Caution: If entering multiple parameters, the connection string must be in the first position.

The connection string format is:

IP_address|hostname{, IP_address|hostname}?Centera_profile

where:

- *IP_address* is the IP address of the Centera host.
- *hostname* is the host name of the Centera machine.
- *Centera_profile* is a full-path specification of a Centera profile.

The path must be accessible from the Content Server host machine and the specified directory must be readable by the Content Server installation owner.

If configuring Centera clusters, the connection string has a format in which you identify primary and secondary Centera clusters for one or more Content Servers:

server_config_name="primary=cluster_id,secondary=cluster_id[?Centera_profile"]{,server_config_name="primary=cluster_id,secondary=cluster_id[?Centera_profile"]}

where:

- The primary *cluster_id* is the name or IP address of the Centera cluster to which the Content Server will write.
- The secondary *cluster_id* is the name or IP address of the Centera cluster from which the Content Server will read if it cannot read from the specified primary cluster.

Including a Centera profile is optional. The storage parameter property has a length of 1024 characters. Assign names to the Centera cluster nodes that are short enough to allow the full connection string to fit within the property.

Refer to the Documentum Content Server Version 6.5 Release Notes for complete information.

3. Click **Add** to move the value to the **Storage Parameters** section.
4. Set optional storage parameters.

- To enable embedded blob use, enter the following parameter:

pool_option:embedded_blob:size_in_KB

where *size_in_KB* is the maximum size in kilobytes of the content that you want to store as embedded blobs. For example, if you want to store all content that is 60 KB or smaller as embedded blobs, set the storage parameter value as:

```
pool_option:embedded_blob:60
```

- To set the C-clip buffer size, enter the following parameter:

```
pool_option:clip_buffer_size:integer
```

where *integer* is an integer number representing the number of kilobytes. For example, to set the buffer size to 200 KB, set the storage value parameter as:

```
pool_option:clip_buffer_size:200
```

5. In the Storage Parameters section, you can do any of the following:

- To move an optional storage parameter up or down in the list, select it and then click the up or down arrow. The connection string must be in the first position.
- To modify the connection string or a parameter, select it and then click **Edit**. The entry moves to the **Enter new value** field. After modifying the entry, click **Add**. Use the up or down arrows to reposition the modified entry.
- To delete a parameter, select it and then click **Remove**.

6. When finished, click **OK**.

Defining the content attributes saved in an EMC Centera store

EMC Centera stores allow you to save up to 62 metadata values with each piece of content saved in the system. Use these instructions to add and describe the attributes.

To define the content attributes saved in an EMC Centera store:

1. Access the EMC Centera Store Properties - Info page:
 - a. Connect to a repository where the Centera store is located.
 - b. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
 - c. Select a Centera store and select **View > Properties > Info**.
To locate the store faster, filter the list by selecting **EMC Centera Storage** from the drop-down list. Please note that the filtered results will show the type as **dm_ca_store**.
2. Click **Add**.
The **Content Attribute** page is displayed.
3. Type the name of an attribute.
The attribute name can be an arbitrary name. It does not have to correspond to any existing properties of the objects stored in the Centera store.
4. Type a description.
5. Click **OK**.
6. Repeat steps 3 to 5 as required.
7. Click **OK**.

Properties of an EMC Centera store

Some of the fields discussed in this table are only available or visible when you modify an existing EMC Centera store. Others are only available when creating an EMC Centera store.

Table 47. Properties of an EMC Centera store

Field label	Value
Name	The name of the EMC Centera store.
Description	The description of the EMC Centera store.
Plugin Name	<p>The name of the plug-in for the EMC Centera store. Options are:</p> <ul style="list-style-type: none"> • Default Plugin: Select to set a null ID (0000000000000000) in the a_plugin_id property of the EMC Centera store object. • Select Plugin: Select to use the default CSEC plug-in. <p>When a repository is created, a default plug-in object for CSEC is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in Creating or modifying plug-ins, page 418 to create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> — Windows: %DM_HOME%\bin\emcplugin.so — HP-UX: \$DM_HOME/bin/libemcplugin.sl
Storage Parameters	<p>Click Edit to add or modify storage parameters for the Centera store.</p> <p>Use the instructions in Defining the storage parameters for an EMC Centera store, page 405 to add or modify storage parameters.</p>
Enable Content Compression	If selected, all content in the EMC Centera store will be compressed.
	This option is only available in 5.3 SP1 and later repositories with Content Storage Services enabled.

Field label	Value
Configure Retention Information	If selected, content retention is enabled.
	If selected, the system automatically selects and inactivates the Event Based Retention checkbox.
	Note: The options to configure retention information for EMC Centera stores differ if you do not connect to a version 6 or later repository.
Retention Attribute Name	The name of the retention attribute. The value entered must not be one of the values specified as a content attribute name.
Fixed Retention	When selected, the Choose default retention date and Choose default retention days checkboxes are enabled. The Fixed Retention checkbox is enabled when the Configure Retention Information checkbox is selected.
Choose a default retention date	Select to set a period of days as the retention period for all content in the EMC Centera store. Next, select the date and time for the default retention.
	This checkbox is enabled only when the Fixed Retention checkbox is selected.
Choose default retention days	Select and then type the number of retention days.
	Both default retention date and default retention days can be specified. If both are specified, the default retention days will take precedence over default retention date. If default retention date is selected but no value is specified, the system will ignore the retention date option.
Event Based Retention	This checkbox is enabled only when the Fixed Retention checkbox is selected.
	When Configure Retention Information is selected, the system automatically selects and inactivates this checkbox to prevent changing the event based retention option status.
Application Provides Retention	Select to require that a client application supply the retention date when content is saved to the EMC Centera store.
Add	Click to access the Content Attribute page to add other content properties.

Field label	Value
Content Attribute Name	If content attributes have been configured for the object, their names will be listed here.
Content Attribute Description	If content attributes have been configured for the object, their descriptions will be listed here.

NetApp SnapLock stores

A Network Appliance SnapLock (NetApp SnapLock) store stores large amounts of unchanging data such as email archives. NetApp SnapLock is a licensed software that provides storage level retention capability through the creation of Write Once Read Many (WORM) volumes on Network Appliance storage systems. These WORM volumes enable users to prevent altering or deleting content until a specified retention date. NetApp SnapLock does not have advanced retention management features such as retention hold, event based retention, or privileged delete, which is available on an EMC Centera store. You can define a retention date or, with Content Server 5.3 SP6 or later, a retention period for the content in a NetApp SnapLock store. You can also enable content compression for a SnapLock store.

There are two types of NetApp SnapLock stores:

- SnapLock Compliance store handles data retention to meet SEC regulations.
- SnapLock Enterprise store handles data retention to help customers meet their self-regulated date retention requirements.

Refer to the SnapLock documentation provided by Network Appliance for more information about the two types of stores.

SnapLock requires:

- A Content Server version 5.3 SP6 or later
- A NetApp SnapLock license
- A SnapLock storage device
- An EMC connector license

Click these links for more information on:

- [Creating NetApp SnapLock stores, page 411](#)
- [Modifying a NetApp SnapLock store, page 412](#)

The Content Management chapter in the *Content Server Administration Guide* contains additional information about NetApp SnapLock stores.

Creating NetApp SnapLock stores

To create a NetApp SnapLock store, you must:

- Have a license for NetApp SnapLock.
- Have an EMC connector license.
- Enable the feature with the license key in the Content Server software installation containing the repository for which you are creating the SnapLock store.
- Know the directory path of the SnapLock storage system.

A repository can have multiple SnapLock stores. For ease of administration, maintenance, and management, it is recommended that you use the same plug-in for all the SnapLock stores.

To create a NetApp SnapLock store:

1. Access the New SnapLock Store - Info page:
 - a. Connect to a repository to create a SnapLock store.
 - b. Select **Administration > File Management > Storage**.
The **Storage** list page appears.
 - c. Click **File > New > NetApp SnapLock Store**.
The **New SnapLock Store - Info** page is displayed.
2. Enter general information about the SnapLock store:
 - a. **Name:** Type the name of the new SnapLock store.
 - b. **Description:** Optionally, type a description for the SnapLock store.
 - c. **Plugin Name:** Select one of the following for the plug-in information:
 - **Default Plugin:** Select to set a null ID (0000000000000000) in the a_plugin_id property of the SnapLock store object.
 - **Select Plugin:** Select to use the default Snaplock connector plug-in.
To use a plug-in other than the default Snaplock connector plug-in, click the **Select Plugin** link, locate the plug-in in the repository, select it, and click **OK**.

When a repository is created, a default plug-in object for SnapLock is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in [Creating or modifying plug-ins, page 418](#) to create a new plug-in object with the content of the plug-in object set as follows:

 - Windows: %DM_HOME%\bin\emcplugin.dll
 - Solaris, AIX, and Linux: \$DM_HOME/bin/libemcplugin.so
 - HP-UX: \$DM_HOME/bin/libemcplugin.sl
 - d. **Snaplock Volume Path:** Type the directory path of the SnapLock storage system. The first character of the path must be / for UNIX (NFS) or \ for Windows (CIFS).
 - e. **Enable Content Compression:** Select to compress all content in the store.
This option is only available in 5.3 SP1 and later repositories where Content Storage Services is enabled.

3. Enter retention information for the SnapLock store:
 - a. **Configure Retention Information:** Select to enable content retention. When selected, the system automatically selects and inactivates the **Event Based Retention** checkbox.
Note: The options to configure retention information for SnapLock stores differ if you do not connect to a version 6 or later repository.
 - b. **Retention Attribute Name:** Type the retention attribute name. The value entered must *not* be one of the values specified as a content attribute name.
 - c. **Fixed Retention:** Select to choose how the value of the retention property is set:
 - **Choose a default retention date:** Select to set a period of days as the retention period for all content in the SnapLock store. Next, select the date and time for the default retention.
 - **Choose default retention days:** Select and then type the number of retention days.

Both default retention date and default retention days can be specified. If both are specified, the default retention days will take precedence over default retention date. If default retention date is selected but no value is specified, the system will ignore the retention date option.
 - d. **Application Provides Retention:** Select to require that a client application supply the retention date when content is saved to the SnapLock store.
4. Click **OK**.

Modifying a NetApp SnapLock store

Use the instructions in this section to modify a NetApp SnapLock store.

To modify a NetApp SnapLock store:

1. Access the NetApp SnapLock Store Properties - Info page:
 - a. Connect to a repository where the SnapLock store is located.
 - b. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
 - c. Select a SnapLock store and select **View > Properties > Info**.
To locate the store faster, filter the list by selecting **NetApp SnapLock Store** from the drop-down list. Please note that the filtered results will show the store type as **dm_ca_store**.
2. Change the properties of the store.
3. Click **OK** when finished or click **Cancel**.

Properties of a NetApp SnapLock store

Some of the fields discussed in this table are only available when creating a NetApp SnapLock store.

Table 48. Properties of a NetApp SnapLock store

Field label	Value
Name	The name of the NetApp SnapLock store. After the store is created, you cannot modify the name.
Description	The description of the NetApp SnapLock store.
Plugin Name	<p>The name of the plug-in for the NetApp SnapLock store. Options are:</p> <ul style="list-style-type: none"> • Default Plugin: Select to set a null ID (0000000000000000) in the a_plugin_id property of the NetApp SnapLock store object. • Select Plugin: Select to use the default Snaplock Connection plug-in. <p>When a repository is created, a default plug-in object is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Use the instructions in Creating or modifying plug-ins, page 418 to create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> — Windows: %DM_HOME%\bin\emcplugin.so — HP-UX: \$DM_HOME/bin/libemcplugin.sl
Snaplock Volume Path	The directory path of the NetApp SnapLock storage system.
Enable Content Compression	If selected, all content in the NetApp SnapLock store will be compressed.
Configure Retention Information	<p>This option is only available in 5.3 SP1 and later repositories with Content Services enabled.</p> <p>If selected, content retention is enabled.</p> <p>If selected, the system automatically selects and inactivates the Event Based Retention checkbox.</p> <p>Note: The options to configure retention information for NetApp SnapLock stores differ if you do not connect to a version 6 or later repository.</p>
Retention Attribute Name	The name of the retention attribute. The value entered must not be one of the values specified as a content attribute name.
Fixed Retention	Select to choose how the value of the retention property is set.

Field label	Value
Choose default retention date	Select to set a period of days as the retention period for all content in the NetApp SnapLock store. Next, select the date and time for the default retention.
Choose default retention days	Select and then type the number of retention days.
	Both default retention date and default retention days can be specified. If both are specified, the default retention days will take precedence over default retention date. If default retention date is selected but no value is specified, the system will ignore the retention date option.
Application Provides Retention	Select to require that a client application supply the retention date when content is saved to the NetApp SnapLock store.

Mount points

A mount point object represents a directory that is mounted by a client. It is a useful way to aggregate multiple locations that must be mounted.

To create a new mount point, you must define the name and file system path of the mount point and designate preferred aliases for UNIX, Windows, and Macintosh clients.

For instructions on creating or modifying mount points, refer to [Creating or modifying mount points, page 414](#).

Creating or modifying mount points

Use these instructions to create a mount point object.

To create or modify a mount point object:

1. Connect to a repository.
2. Select **Administration > File Management > Storage**.
The Storage list page is displayed.
3. Access the Info page:
 - To create a new mount point object, select **File > New > Mount Point** to access the **New MountPoint - Info** page.
 - To modify an existing mount point object, select the correct mount point and then select **View > Properties > Info** to access the **MountPoint Properties - Info** page.
4. Complete or modify the fields on the Info page.

[Table 49, page 415](#) describes the mount point properties.

5. Click OK.

Table 49. Properties of a mount point

Field label	Value
Name	The name of the mount point object. Some names, such as "events" or "common," are reserved for Content Server use.
Host Name	The hostname for the machine on which this directory resides.
File System Path	The location of the directory or file represented by the location object. The path syntax must be appropriate for the operating system of the server host. For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.
Security	The security level for this directory location. Options are: <ul style="list-style-type: none"> • Public Open • Public • Private The default value is Private.
Unix Preferred Alias	Set to the directory name used to mount the directory.
Macintosh Preferred Alias	Set to the volume name chosen for the mounted directory.
Windows Preferred Alias	The mounted directory's volume name is set when the directory is exported through the file-sharing system. It is the name that will appear in the Chooser for that directory. Set to the alias drive letter used to mount the directory.
Comments	For example, t:\ or k:\ Any comments regarding this mount point.

Locations

The directories that a Content Server accesses are defined for the server by location objects. A location object can represent the location of a file or a directory.

For information on creating or modifying locations, refer to [Creating or modifying locations, page 416](#).

Creating or modifying locations

Use the instructions in this section to create or modify location objects.

A location object contains a file system location of a specific file or directory. The server uses the information in location objects to find the files and directories that it needs. Create the directory on the file system before creating a location object.

To create or modify locations:

1. Connect to a repository.
2. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
3. Access the Info page:
 - To create a new location, select **File > New > Location** to access the **New Location - Info** page.
 - To modify an existing location, select the correct location, and then select **View > Properties > Info** to access the **Location Properties - Info** page.
4. Complete or modify the fields.
[Table 50, page 416](#) describes the location object properties.
5. Click **OK**.

Table 50. Properties of location objects

Field label	Value
Name	The name of the location object. Some names, such as "events" or "common," are reserved for Content Server use.
Choose a Mount Point for this Location	(Optional) The mount point underneath which this location resides. The name of the mount point object that describes the mount point.

Field label	Value
Mount Point Path	If you selected Choose a Mount Point for this Location, select a mount point path. Options are: Existing: Select and then select NULL or share from the drop-down list box. Create Mount Point Path: Select and then navigate to a file system location for the mount point.
File System Path	The location of the directory or file represented by the location object. The path syntax must be appropriate for the operating system of the server host. For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.
Path Type	Indicates whether the location points to a directory or file.
Security Type	The security level for the directory or file. Valid values are: <ul style="list-style-type: none">• publicopen• public• private If the security type is not set, the default value is the security level of the referencing object, such as an associated storage object.

Plug-ins

A plug-in is a shared library (on UNIX or Linux systems) or DLL file (on Windows systems) for retrieving content when an external store is in use.

You must create the plug-in. To assist you, Documentum provides code for sample plug-ins in the DM_HOME/unsupported/plugins directory. The API interface between the shared library or DLL and the server consists of C functions for the plug-in library. The functions are described in detail in the Functions for Creating Plug-in Libraries chapter in the *Content Server API Reference Manual*.

For information on creating or modifying plug-ins, refer to [Creating or modifying plug-ins, page 418](#).

Creating or modifying plug-ins

Use these instructions to create the plug-in object that represents the plug-in.

To create or modify a plug-in object:

1. Connect to a repository.
2. Select **Administration > File Management > Storage**.
The **Storage** list page is displayed.
3. Access the Info page:
 - To create a new plug-in, select **File > New > Plug-in** to access the **New Plug-in** page.
 - To modify an existing plug-in, select the correct plug-in and then select **View > Properties > Info** to access the **Plug-in Properties - Info** page.
4. Complete or modify the fields.
The plug-in object properties are described in [Table 51, page 418](#)
5. Click **OK**.

Table 51. Properties of plug-in objects

Field label	Value
Name	The name of the plug-in object.
Hardware Platform	Designate the hardware platform on which the plug-in can run: <ol style="list-style-type: none">1. Click Edit.2. type a hardware type on which the plug-in can run.3. Click Add.4. When all types are entered, click OK.
Operating System	Designate the operating systems on which the plug-in can run: <ol style="list-style-type: none">1. Click Edit.2. type an operating system on which the plug-in can run.3. Click Add.4. When all types are entered, click OK.

Field label	Value
Type	Select a file type. Options are: <ul style="list-style-type: none"> • DLL (Windows) • SO (Solaris) • SL (HP-UX)
Usage	Type a comment on how the plug-in is used.

Assignment policies

Assignment policies are sets of rules that DFC-based applications apply to determine the correct file store, EMC Centera store, or NetApp SnapLock store for each new content file added to the repository. (Thumbnail stores and streaming stores are of the file store type.) Assignment policies are associated with object types and are represented in the repository by persistent objects. An assignment policy's permission set must grant at least READ permissions to World. To create assignment policies, a user must have the user privilege level of System Administrator or Superuser. For complete information on storage and content management, refer to the *Content Server Administration Guide*.

Assignment policies are a feature of Content Storage Services (CSS). To move content files that are already in a repository to the correct file store or retention store (EMC Centera or NetApp SnapLock), create a migration policy. For information on migration policies, refer to [Migration policies, page 429](#). CSS is available only where the CSS license key was provided during Server configuration.

Assignment policies are applicable only to SysObjects and SysObject subtypes. A particular assignment policy can be associated with multiple object types. A particular object type can have only one associated assignment policy. To view the assignment policies associated with types, refer to [Viewing assignment policies, page 376](#).

The DFC policy engine applies the assignment policies. Any client application built on DFC applies assignment policies automatically if CSS is enabled in the repository.

Assignment policies are inherited and only one policy can be associated with an object type. When a new content file is added to the repository, the assignment policy engine determines whether the file's object type has an active associated assignment policy. If there is no active assignment policy for the type, the assignment policy engine determines whether the type's supertype has an active associated assignment policy. This process continues until the assignment policy engine arrives at the SysObject type. If there is an active assignment policy for the file's type or a supertype, the policy is applied and the file is stored according to the conditions of the assignment policy. If no policy is found or if none of the rules match in an applicable policy, the default algorithm for determining the correct storage area is used. If none of the rules match in the applicable assignment policy, the policy engine does *not* further search the type hierarchy. For complete information on the default algorithm for determining storage, refer to the *Content Server Administration Guide*.

Assignment policies consist of rules that define the criteria for storing content files in the correct storage area. There are two types of rules: standard and custom.

Standard rules determine storage area based only on an object's format and content size. These are properties of the content object (dmr_content object). Standard rules have from one to five criteria

that are entered using drop-down lists. For example, a standard rule might require that content files of the format gif with content size between 50,000 bytes and 100,000 bytes be stored in filestore02.

Custom rules are entered into a text box. There are no restrictions on the number of conditions in a custom rule. Custom rules can be based on the values of any standard or custom SysObject property, provided those values are present before an object is saved. The properties and values are specified using methods available on the SysObject, such as `getString()`, `getInt()`, or `getRepeatingString()`. Custom rules follow the Java syntax for any conditional statements in the rule. For examples of custom rules, refer to [Examples of custom assignment policy rules, page 427](#). For assistance in creating, implementing, or debugging custom rules, contact Documentum Professional Services or Documentum Developer support.

There is no syntactical difference between the two types of rules. During rule validation, a standard rule is translated into the same syntax used for custom rules.

Assignment policies are applied only to new content files, whether they are primary content files or renditions. An assignment policy is applied when the content file is first saved or imported into the repository. An assignment policy is also applied when a new version of a document is created, because versioning creates a new content file. When a document is checked out and checked in and a new version results, the policy is applied to the new version of the content file. If an existing document is modified and saved as the same version of the document, an assignment policy is applied if one exists. If you modify an existing documents properties and save the changes without checking out and versioning the document, a policy is not invoked. The content is saved into its current storage location.

Under the follow conditions, assignment policies are not applied or enforced:

- An application sets the `a_storage_type` SysObject property.

If `a_storage_type` is set by an application, assignment policies do not execute for any of the primary content pages (content added using a Setfile). Documentum client applications do not generally set this property.

- The application specifies the storage location for a secondary rendition during an `addrendition` call.

If a storage location is already provided, the policy engine does not execute the policy for this particular secondary rendition.

- Assignment policies are not enabled.
- The DFC policy engine is turned off.
- Assignment policies are enabled but a policy does not exist for an object type or for any of the types supertypes.
- A document does not satisfy any of the conditions in the applicable policy.
- The content is replicated (content associated with a replica object).
- The content is loaded into a repository with dump and load.
- The content generated by a refresh API.

An assignment policy's rules are applied in the order in which they are listed within a policy. If a rule is met, the remaining rules are ignored. To match a rule, all conditions in the rule must be satisfied.

If the assignment policy engine encounters an error in a rule at runtime (for example, if a property name is invalid), the assignment policy engine returns an error and the save operation

on the document or object fails. This behavior can be overridden by setting the following DFC client-preference flag in the dfc.properties file on the application server host where Webtop or Documentum Administrator is installed:

```
dfc.storagepolicy.ignore.rule.errors=true
```

If this flag is set to **true**, the assignment policy engine ignores the faulty rule and attempts to apply the next rule in the policy.

The default value of the dfc.storagepolicy.ignore.rule.errors flag is **false**.

The assignment policy list page displays a list of all assignment policies in the current repository.

The following information is displayed for each policy:

- Policy name
- A brief description of the policy
- Whether the policy is currently Active or Inactive
- The object types to which the policy applies

Click the **Name**, **Description**, or **Status** links to sort the list. To display All, Active, or Inactive policies, make a selection from the drop-down list. To jump to policies whose names begin with a particular letter, click that letter. To change the number of policies displayed, select a new number from the **Show Items** drop-down list.

Click the following links for help with:

- [Viewing a list of assignment policies, page 422](#)
- [Creating assignment policies, page 422](#)
- [Viewing or modifying the properties of an assignment policy, page 424](#)
- [Modifying the permissions of an assignment policy, page 424](#)
- [Properties of an assignment policy, page 424](#)
- [Examples of custom assignment policy rules, page 427](#)
- [Associating an assignment policy with an object type, page 427](#)
- [Deleting assignment policies, page 428](#)
- [Setting or updating a retention date or retention period for documents or other objects, page 428](#)

Creating or modifying assignment policies

Click the links below for information on creating or modifying assignment policies:

- [Creating assignment policies, page 422](#)
- [Viewing or modifying the properties of an assignment policy, page 424](#)

Viewing a list of assignment policies

You can view a list of all assignment policies defined for a particular repository and select any of the listed policies for viewing or modifying properties. For complete instructions for viewing or modifying assignment policies, refer to [Viewing or modifying the properties of an assignment policy, page 424](#).

To view a list of assignment policies in a repository:

1. Connect to a repository.
2. Select **Administration > Storage Management > Assignment Policies**.
The **Assignment Policies** list page is displayed.

Creating assignment policies

To create an assignment policy, you must have the role of Administrator or, if there are no Administrators in the repository, the user privilege level of System Administrator or Superuser. Policies can only be created in repositories where Content Storage Services is enabled.

To create an assignment policy:

1. Access the New Assignment Policy - Info page:
 - a. Connect to a repository to create an assignment policy.
 - b. Select **Administration > File Management > Assignment Policies**.
The **Assignment Policies** list page is displayed. This page lists all existing assignment policies in the repository.
 - c. Click **File > New > Assignment Policy** to create an assignment policy.
The **New Assignment Policy - Info** page for a new assignment policy is displayed.
2. Type a name and a description for the new assignment policy.
The name must be unique in the repository and can be modified after the policy is saved.
3. Select a **Status**.
The default status is **Inactive**. Select **Active** to enable the policy and automatically validate the rule syntax. The validation process does not check whether property names in the rules are valid.
4. If the policy is created in the inactive state, optionally clear the **Validate all of the rules defined for this policy** checkbox.
The default is selected. If the policy is created in the active state, the checkbox is selected and grayed out.
5. Select the object types to which the policy applies.
A policy can be applied to multiple object types. If the chosen object type has subtypes, the policy is inherited automatically at runtime by the subtypes, except those subtypes that are already associated with a different assignment policy.
 - a. Click **Select**.

- A list of SysObject subtypes is displayed on the **Choose a type** page, including custom types.
- b. Choose the object types to which the policy applies and click >.
 - c. Click **OK** to return to the New Assignment Policy - Info page.
6. To create standard rules, select **Standard Rule (Maximum of 5 Criteria)**.
- Standard rule is selected by default. A policy can have up to five rules, which can be any combination of standard and custom rules. Each rule can have up to five criteria.
- a. On the first drop-down list, select **Format** or **Content Size (in bytes)**.
 - b. If you selected **Format**, select an operand (**is** or **is not**) and click **Select** to access the Choose a format page, then choose a format and click **Ok** to return to the New Assignment Policy - Info page.
 - c. If you selected **Content Size (in bytes)**, select an operand from the drop-down list and type a value (in bytes) in the text box.
 - d. To add additional conditions to the rule, click **Add Criteria** and repeat steps a through c.
A standard rule can have up to five criteria.
 - e. To remove a condition, click **Remove**.
 - f. Select a storage area from the **Then** drop-down list.
 - g. To end the process of creating a rule without completing the rule, click **Cancel Rule**.
 - h. When the rule is complete, click **Insert Rule**.
The rule is displayed in the list of rules.
 - i. To add additional standard rules, repeat steps a through h.
7. To create custom rules, click **Custom Rules**.
- a. Type the rule in the text box.
For more information on custom rules and examples of custom rule syntax, refer to [Examples of custom assignment policy rules, page 427](#).
 - b. Click **Insert Rule**.
The rule is displayed in the rules list.
 - c. To delete text that is typed in the text box, click **Cancel Rule**.
 - d. To add more rules, repeat steps a through c.
A policy can have up to five rules.
8. If necessary, delete or change rules, or change the order of the rules.
- To delete an existing rule, select the rule and click **Remove**.
 - To change an existing rule, select the rule and click **Edit**, modify the rule, then click **Update Rule**.
 - To change the order in which rules occur in the policy, select a rule and click **Up** or **Down**.
The rules in a policy are evaluated in order when a content file is saved. When a rule matches, the remaining rules are ignored.
9. Click **Finish** to create the policy or **Cancel** to exit without creating the policy.

Viewing or modifying the properties of an assignment policy

Use these instructions to view or modify the rules, object types, and other values defined for an assignment policy.

To modify an existing policy, you must have the role of Administrator or, if there are no Administrators in the repository, the user privilege level of System Administrator or Superuser. Policies can only be used in repositories where Content Storage Services is enabled.

To view or modify the properties of an existing assignment policy:

1. Access the Assignment Policy Properties - Info page for an existing assignment policy:
 - a. Connect to a repository where the assignment policy resides.
 - b. Select **Administration > Storage Management > Assignment Policies**.
The **Assignment Policies** list page is displayed. This page displays a list of all assignment policies in the current repository.
 - c. Select the assignment policy and then select **View > Properties > Info**.
The **Assignment Policy Properties - Info** page for the policy is displayed.
2. View or modify the values for the assignment policy.
[Properties of an assignment policy, page 424](#) provides information about the assignment policy properties.
3. When you finish viewing or modifying the policy's properties, click **OK** to save changes.

Modifying the permissions of an assignment policy

Use these instructions to modify the permissions of an assignment policy. An assignment policy's permission set must grant at least READ permissions to World.

To modify the assignment policy permissions:

1. Connect to a repository where the assignment policy resides.
2. Select **Administration > Storage Management > Assignment Policies**.
The **Assignment Policies** list page is displayed. This page displays a list of all assignment policies in the current repository.
3. Select the assignment policy and then select **View > Properties > Permissions**.
The **Properties: Permissions** page for the assignment policy is displayed.

Properties of an assignment policy

This section displays the New Assignment Policy - Info page for an assignment policy and describes the assignment policy properties.

Click the links below for information on creating or modifying assignment policies:

- [Creating assignment policies, page 422](#)
- [Viewing or modifying the properties of an assignment policy, page 424](#)

Figure 19. New Assignment Policy - Info page

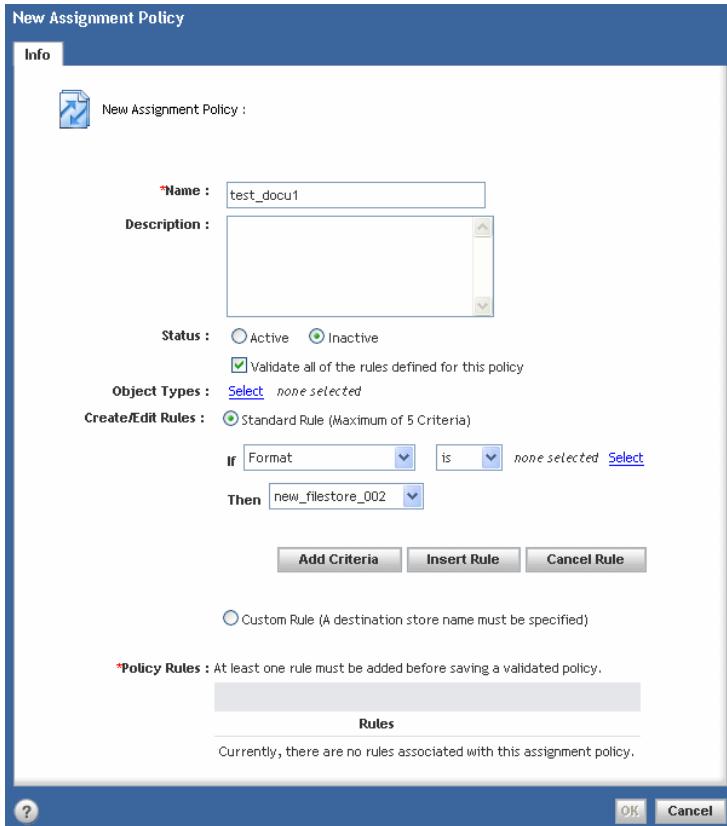


Table 52. Properties of an assignment policy

Field label	Value
Name	Displays the name of the assignment policy, which must be unique in the repository. You can change the name of the policy after creating it.
Description	An optional text field for a short description of the policy.

Field label	Value
Status	<p>Select a status for the policy:</p> <ul style="list-style-type: none"> • Active: Policy is enabled and will automatically validate the rule syntax. The validation process does not check if property names in the rules are valid. • Inactive: Policy is disabled. May optionally be validated if you select the Validate all of the rules defined for this policy checkbox. <p>The status of a new policy is inactive by default.</p>
Validate all of the rules defined for this policy	<p>Select to validate the policy's rules when you save a new or modified policy to the repository. When selected, rules are validated when Insert Rule is clicked.</p> <p>When Status is set to Inactive, you can specify whether or not to validate the rules.</p> <p>When Status is set to Active, the policy is always validated by default.</p>
Object Types	<p>Lists the different object types to which the policy applies.</p> <p>Click the Select link to associate additional SysObject subtypes with the policy.</p> <p>A single policy can be associated with multiple object types. However, each object type can be associated only with a single assignment policy.</p> <p>If you select an object type that has subtypes, the policy is inherited at runtime by the type's subtypes, unless an assignment policy is already associated with a particular subtype.</p>
Create/Edit Rules	<p>Select a radio button to indicate which rule type to create or edit:</p> <ul style="list-style-type: none"> • Select Standard Rule to choose the criteria for a new rule from the drop-down menus. Specify up to five conditions for each rule. • Select Custom Rule to type the syntax for a custom rule in the text box. For information about creating custom rules, see Examples of custom assignment policy rules, page 427. <p>To add a new rule to the policy, click Insert Rule.</p>

Field label	Value
	A policy contains one to a maximum of five rules.
Policy Rules	Displays the existing rules defined for this policy. Click a rule to select it, then rearrange the order in which the rules are executed by clicking the Up and Down links. Edit or delete a rule by clicking the associated Edit and Remove links.

Examples of custom assignment policy rules

Custom rules define assignment policies based on values of an object's properties. Specify these properties in the rule using the methods available on DFC's IDfSysObject, such as **getString()**, **getInt()**, or **getRepeatingString()**.

Custom rules follow Java syntax for the conditional statement in the rule. The following are examples of valid custom rules:

Example 13-1. Custom Rules for Assignment Policies

Example Rule 1:

```
sysObj.getString("owner_name").equals("JSmith") --> filestore_02
```

Example Rule 2:

```
sysObj.getString("subject").equals("Policies and Procedures") &&
sysObj.getOwnerName().equals("JSmith") --> filestore_03
```

Example Rule 3:

```
sysObj.getString("subject").equals("smith") &&
sysObj.getOwnerName().equals("john") --> filestore_03
```

Note that --> is correct and syntactically required.

For assistance in creating, implementing, or debugging custom rules, please contact Documentum Professional Services or Documentum Developer support.

Associating an assignment policy with an object type

Assignment policies are inherited and only one policy can be associated with an object type. Use these instructions to associate an existing assignment policy with an object type. To associate a new assignment policy with an object type, use the instructions in [Creating assignment policies, page 422](#).

To associate an assignment policy with an object type:

1. Access the Assignment Policy Properties - Info page for an existing assignment policy:
 - a. Connect to a repository where the assignment policy resides.

- b. Select **Administration > Storage Management > Assignment Policies**.
The **Assignment Policies** list page is displayed. This page lists all assignment policies in the current repository.
 - c. Select the assignment policy to associate with an object type and then select **View > Properties > Info**.
The **Assignment Policy Properties - Info** page for the policy is displayed.
2. Click the **Select** link in the **Object Types** section to access the Choose a type page.
 3. Select the object type(s) and click the add arrow.
 4. Click **OK**.
The Assignment Policy Properties - Info page for the assignment policy appears and displays the new object type(s) for the policy.
 5. Click **OK**.
The Assignment Policies list page appears and displays the new object type(s) for the assignment policy.

Deleting assignment policies

Use these instructions to delete assignment policies.

To delete an assignment policy:

1. Connect to a repository where the assignment policy resides.
2. Select **Administration > Storage Management > Assignment Policies**.
The **Assignment Policies** page is displayed. This page lists all assignment policies in the repository.
3. Select the checkboxes next to the assignment policies to be deleted.
4. Select **File > Delete**.
5. Click **OK** or **Finish**.
 - Click **OK** to delete one policy.
 - Click **Finish** to delete multiple policies.

Setting or updating a retention date or retention period for documents or other objects

An EMC Centera store or NetApp SnapLock store is retention-enabled when a default retention date is required for all objects saved to that store.

You can assign specific retention dates for content stored in a retention-enabled store. A retention date is the date to which the content file must be retained. If a retention date is defined for content in

the storage system, the file cannot be removed from the repository until that date. For example, if you set the retention date for an object to February 15, 2011, the content cannot be removed until that date.

When a retention date is set for an object, it is set for all renditions associated with page 0 (zero) of the object. Content Server moves the selected object and all of its associated renditions to a retention-enabled storage area. If there are multiple retention-enabled storage areas in the repository, you must select the target storage area. To set a retention date, you must belong to the Webtop administrator role and have at least WRITE permission on the object, and the Centera or SnapLock store must be retention-enabled.

You can alternatively assign a *retention period* for content stored in a retention-enabled store. A retention period is the amount of time for which the content must be retained. If a retention period is defined, you cannot remove the file from the repository until that period has expired. For example, if the retention period is set to five years and the current date is January 1, 2007, the content file cannot be removed before January 1, 2012.

To set or update a retention period or retention date for a document or other repository object:

1. Navigate to the cabinet or folder containing the object for which you want to specify a retention date.
2. Select the object, then select **Tools > Set Retention Date**.
The **Set Retention Date** page is displayed.
3. To set a retention period for the primary content and renditions associated with page 0 of this object, select **Retention Period**, type a number in the text box, and choose **Dates or Years** from the drop-down list.
4. To set a retention date, select **Retention Date**, click the calendar button associated with the **Retention Date** field, and select the retention date for the primary content and renditions associated with page 0 of this object.
5. If the repository has more than one retention-enabled store, select the name of a storage area from the pull-down menu on the **Retention Enabled Store** field.
6. Click **OK**.

Migration policies

Migration policies move content files from one storage area to another, based on the rules (conditions) defined when creating the policy. Files are selected for migration based on format, content size, or date criteria. The target storage area of a migration policy can be a file store or a retention store (EMC Centera or NetApp SnapLock). Rules can be standard rules, created by making choices from drop-down lists, or they can be custom rules, which use DQL predicates. Custom rules can select content to migrate from dm_sysobject, its subtypes, and dmr_content objects. SysObject subtypes are not supported prior to Documentum version 6.

Migration policies are jobs that call the dm_MoveContent method, which executes the MIGRATE_CONTENT administration method. The conditions are stored as job arguments. A Content Storage Services (CSS) license is required to create content migration jobs. CSS is enabled using a license key when Content Server is installed or when the Server Configuration Program

is used to update the server installation. (Another feature of CSS is assignment policies, which determine where content files are stored when saved in a repository. For information on creating assignment policies, refer to [Assignment policies, page 419](#).)

To sort the Migration Policies list page, click the **Name**, **Description**, **Job Type**, **Last Run**, **State**, or **Status** columns. To display a different number of migration policies per page, select a number from the drop-down list.

Click the links for help with:

- [Creating migration policies, page 430](#)
- [Setting the rules of a migration policy, page 434](#)
- [Viewing or modifying migration policies, page 436](#)
- [Deleting migration policies, page 436](#)

Creating migration policies

Use the instructions in this section to create a migration policy. Migration policies can be created and used only in repositories where Content Storage Services is enabled.

To create migration policies:

1. Access the New Migration Policy - Info page for a new migration policy.
 - a. Connect to a repository to create a migration policy.
 - b. Select **Administration > Storage Management > Migration Policies**.
The **Migration Policies** list page appears.
 - c. Select **File > New > Migration Policy**.
The system displays the New Migration Policy - Info page.
2. Enter information on the **New Migration Policy - Info** page.
 - a. **Name**: Type the name of the job.
 - b. **Job Type**: Optionally, enter a type of job.
The job type is displayed in a drop-down list on the Jobs list page and can be used to sort jobs.
 - c. **Trace Level**: Select a trace level from 0 (no tracing) to 10 (a debugging level of tracing).
 - d. **Designated Server**: Select a server from the drop-down list. The list displays all servers running against the repository of which Documentum is aware.
 - e. **State**: Select a state for the policy. Options are *Active* and *Inactive*.
 - f. **Deactivate on Failure**: Select to deactivate the job after a run fails to execute correctly.
 - g. **Run After Update**: Select to run the job immediately after you save it.
 - h. **Save Job if Invalid**: Select to save the job even if it is invalid.
 - i. Click **Next** to access the New Migration Policy - Schedule page.
3. Enter scheduling information on the **New Migration Policy - Schedule** page.

- a. **Start Date and Time:** Designate a start date and time for the job. The default is the current date and time.
 - b. Designate how often and at what interval the job runs.
 - **Repeat:** Select a unit of time.
 - **Frequency:** Type how often the job is invoked.

For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
 - c. **End Date and Time:** Designate an end date and time for the job or select **after** to indicate a number of invocations after which the job becomes inactive.

The default end date is 10 years from the current date and time.
 - d. If you selected **after**, then optionally, type a continuation interval.

The default is zero. Most jobs do not require this field to be set. Use this field only if a job needs to pause, then resume at a later time.
 - e. Click **Next** to access the New Migration Policy - Rules page.
4. Enter information on the **New Migration Policy - Rules** page.
- a. **Simple selection:** Select to use drop-down lists to define migration conditions.
 - i. To migrate objects of a particular format, select **format**, click the **Select** link and then select the correct format.
 - ii. To migrate objects according to creation date, choose **Created** and an operand, then type a number of days.

The number of days is always in relation to the date the job runs. The operands are:

 - **Exactly**, which selects objects created exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created on June 5.

 - **More than**, which selects objects created more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created before June 5.

 - **Less than**, which selects objects created less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created after June 5.
 - iii. To migrate objects according to date modified, choose **Modified** and an operand, then type a number of days.

The number of days is always in relation to the date the job runs. The operands are:

 - **Exactly**, which selects objects modified exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified on June 5.

- **More than**, which selects objects modified more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified before June 5.

- **Less than**, which selects objects modified less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified after June 5.

- iv. To migrate objects according to date accessed, choose **Accessed** and an operand, then type the size in number of days.

The number of days is always in relation to the date the job runs. The operands are:

- **Exactly**, which selects objects accessed exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed on June 5.

- **More than**, which selects objects accessed more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed before June 5.

- **Less than**, which selects objects accessed less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed after June 5.

- v. To migrate objects according to size, choose **Size** and an operand, then type a number of bytes.

- vi. **Renditions to include:** If you selected *created*, *modified*, or *accessed*, select whether to migrate **Primary** or **Secondary** renditions or both.

- b. **DQL query selection:** Select to type conditions into a text field.

Custom rules can select content to be migrated from dm_sysobject, its subtypes, and dmr_content objects. SysObject subtypes are not supported prior to Documentum 6.

- i. Select one of the following:

- **Move specified type:** Select to migrate the content associated with SysObjects (dm_sysobject) and its subtypes. When selected, you must also select to migrate primary or secondary renditions, or both.
- **Move content objects only:** Select to migrate the content associated with content objects (dmr_content).

- ii. **Where:** Type a rule into the text box.

Specify a DQL predicate and whether the predicate runs against content associated with SysObjects, its subtypes, or content objects.

- iii. **Renditions to include:** If you selected **Move specified types**, select to migrate **Primary** or **Secondary** renditions or both.
- c. **Target Store:** Select a target storage area.
This is the destination storage area to which the content files migrate. The list includes the repository's file stores and retention stores (EMC Centera and NetApp SnapLock).
- d. **Batch Size:** Type the number of content files to include in a single transaction during the migration operation.
The default value is 500.
- e. **Maximum Count:** Type the maximum number of content files to transfer.
To specify an unlimited number of documents, type a zero [0] or leave the field blank.
- f. Optionally, enter a value in the **Content Migration Threads** field to indicate the number of internal sessions to use to execute the migration policy. The default value is 0, indicating that migration will execute sequentially.
- Note:**
- This field displays only if you have a Content Storage Services license and the license is enabled on the Content Server.
 - The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config).
- g. Click **Next** to access the New Migration Policy - SysObject page.
5. Enter information on the **New Migration Policy - SysObject** page.
- a. **Title:** Type the title.
- b. **Subject:** Type the subject.
- c. **Keywords:** Click **Edit** to access the Keywords page:
 - To add a keyword, type a new keyword in the **Enter new value** box and click **Add**.
 - To remove a keyword, select the keyword and click **Remove**.
 - To change the order in which keywords are listed, select the keyword and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The system displays the New Migration Policy - SysObject page.
- d. **Authors:** Click **Edit** to access the Authors page:
 - Type a new author in the **Enter new value** box and click **Add**.
 - To remove an author, select the name and click **Remove**.
 - To change the order in which authors are listed, select the name and click **Move Up** or **Move Down**.
 - Click **OK** to save the changes or **Cancel** to abandon the changes.The system displays the New Migration Policy - SysObject page.

- e. **Owner Name:** Click **Edit** to access the Choose a user page:
 - Select an owner.
 - Click **OK**.The system displays the New Migration Policy - SysObject page.
 - f. **Show More:** Click to view more sysobject properties about the migration policy.
6. Click **Finish**.

Setting the rules of a migration policy

Use the Rules tab to define which documents are migrated by a migration policy. Rules can be standard rules, created by making choices from drop-down lists, or they can be custom rules, which use DQL predicates. Custom rules can select content to be migrated only from dm_sysobject and dmr_content objects. SysObject subtypes are not supported.

To set the rules of a content migration job:

1. Select **Simple selection** to use drop-down lists to define migration conditions.
 - a. To migrate objects of a particular format, select **format**, click the **Select** link and then select the correct format.
 - b. To migrate objects according to creation date, choose **Created** and an operand, then type a number of days.

The number of days is always in relation to the date the job runs. The operands are:

 - **Exactly**, which selects objects created exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created on June 5.

 - **More than**, which selects objects created more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created before June 5.

 - **Less than**, which selects objects created less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were created after June 5.
 - c. To migrate objects according to date modified, choose **Modified** and an operand, then type a number of days.

The number of days is always in relation to the date the job runs. The operands are:

 - **Exactly**, which selects objects modified exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified on June 5.

- **More than**, which selects objects modified more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified before June 5.

- **Less than**, which selects objects modified less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were modified after June 5.

- d. To migrate objects according to date accessed, select **Accessed** and an operand, then type the size in number of days.

The number of days is always in relation to the date the job runs. The operands are:

- **Exactly**, which selects objects accessed exactly the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed on June 5.

- **More than**, which selects objects accessed more than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed before June 5.

- **Less than**, which selects objects accessed less than the number of days you type before the job runs.

For example, if you type 5 days and the job runs on June 10, objects are selected that were accessed after June 5.

- e. To migrate objects according to size, select **Size** and an operand, then type a number of bytes.
- f. **Renditions to include**: If you selected *created*, *modified*, or *accessed*, select whether to migrate **Primary** or **Secondary** renditions or both.

2. Select **DQL query selection** to type conditions into a text field.

Custom rules can select content to be migrated from dm_sysobject, its subtypes, and dmr_content objects. SysObject subtypes are not supported prior to Documentum 6.

- a. Select one of the following:

- **Move specified type**: Select to migrate the content associated with SysObjects (dm_sysobject) and its subtypes. When selected, you must also select to migrate primary or secondary renditions, or both.
- **Move content objects only**: Select to migrate the content associated with content objects (dmr_content).

- b. **Where**: Type a rule into the text box.

Specify a DQL predicate and whether the predicate runs against content associated with SysObjects, its subtypes, or content objects.

- c. **Renditions to include:** If you selected **Move specified types**, select to migrate **Primary** or **Secondary** renditions or both.
3. Select a **Target Store** storage area.
This is the destination storage area to which the content files migrate. The list includes the repository's file stores and retention stores (EMC Centera and NetApp SnapLock).
4. In the **Batch Size** field, type the number of content files to include in a single transaction during the migration operation.
The default value is 500.
5. Type the maximum number of content files to transfer in the **Maximum Count** field.
To specify an unlimited number of documents, type a zero [0] or leave the field blank.
6. Optionally, enter a value in the **Content Migration Threads** field to indicate the number of internal sessions to use to execute the migration policy. The default value is 0, indicating that migration will execute sequentially.
Note:
 - This field displays only if you have a Content Storage Services license and the license is enabled on the Content Server.
 - The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config).
7. Click **OK** to save the changes or **Cancel** to exit without saving.

Viewing or modifying migration policies

Use these instructions to view or modify a migration policy.

To view or modify a migration policy:

1. Connect to a repository.
2. Navigate to **Administration > Storage Management > Migration Policies**.
The system displays the **Migration Policies** list page. This page lists all migration policies in the repository.
3. Select the migration policy whose properties you want to view or modify and then select **View > Properties > Info**.
The system displays the **Migration Policy Properties - Info** page.
4. Modify any property or the rules of a migration policy.
5. Click **OK** to save the changes or **Cancel** to exit without saving the changes.

Deleting migration policies

Use these instructions to delete migration policies.

To delete a migration policy:

1. Connect to a repository.
2. Navigate to **Administration > Storage Management > Migration Policies**.
The **Migration Policies** list page is displayed. This page lists all migration policies in the repository.
3. Select the migration policies to delete.
4. Select **File > Delete**.
5. Click **OK** or, to delete all selected policies, **Finish**.

Chapter 14

Content Delivery

Documentum Interactive Delivery Services (IDS) and Documentum Interactive Delivery Services Accelerated (IDSx) enable publishing and delivery of content directly from a repository to a website. Any content can be published and updated as documents are revised in the repository. Document versions and formats to publish can also be specified. You can indicate when to publish a document and when to remove it from the website. Publication can occur on demand or automatically on a schedule. Using Interactive Delivery Services (IDS), you can choose to ingest content back to the repository.

IDSx provides a new feature for replication. IDSx can replicate content and metadata that are published on IDSx staging target to multiple replication targets. Replication process can occur through Content Server jobs or on demand. Using the Replication tab, which is in the content delivery configuration in Documentum Administrator, you can configure multiple replication targets for an IDSx staging target.

IDSx offers a bi-directional capability of delivering (publish/replicate) content to a target and also pulling content back to the repository. This is known as Ingestion. Ingestion is a process that pulls content from the staging target and/or replication targets back to the repository.

You can select to ingest content using the Advanced and the Replication tabs in Documentum Administrator.

To publish, IDSx must be installed on the computer where the repository is hosted (the source machine) and on the website host (the target machine). To replicate content, IDSx target software must be installed on all the replication targets.

All content that are published on IDSx staging target can be replicated. IDSx uses accelerated data transfer technology for faster file transfer.

Refer to [Creating content delivery configurations, page 442](#) for more information on replication.

The *Interactive Delivery Services Accelerated Installation Guide* and *Interactive Delivery Services Accelerated User Guide* documentation provides additional information about Interactive Delivery Services Accelerated (IDSx).

The *Interactive Delivery Services Installation Guide* and *Interactive Delivery Services User Guide* documentation provides additional information about Interactive Delivery Services (IDS).

Content delivery configuration is controlled by three objects. The `scs_admin_config` object at Administration/Content Delivery/IDS Administration contains attributes that apply to *all* delivery configurations in a given repository. The `dm_webc_config` and `dm_webc_target` objects at

Administration/Content Delivery/IDS Configurations contain arguments that apply to individual content delivery configurations.

Many attributes can be set for either an individual content delivery configuration, or all configurations in a repository. When an attribute appears in both IDS Administration and IDS Configurations, the value of the attribute in IDS Configurations overrides the value of the attribute in the scs_admin_config object at IDS Administration.

A content delivery configuration defines the objects to be published, the publishing folder for publication, and the version and format of the objects to be published. It also defines the directory on the target machine where the objects are placed after they are transferred from the source machine, and contains other information necessary for transferring the export data set.

To publish, IDS must be installed on the computer where the repository is hosted (the source machine) and on the website host (the target machine). Configuration information for the target is contained in the agent.ini file on the target host; refer to the *Interactive Delivery Services Installation Guide* for information pertaining to this initialization file.

The IDS Configuration Template stores default values that you can use to create new content delivery configuration. Access the template from the Interactive Delivery Services Configuration list page.

On the Interactive Delivery Services Configuration list page, sort the content delivery configurations in the current repository by clicking the following links:

- **Name:** The object name of the content delivery configuration.
- **Source Folder:** The repository publishing folder.
- **Target Host:** The computer to which documents are published.
- **Published Version:** The document version that is published.
- **Connection:** The connection type (secure or nonsecure).
- **State:** Represents whether the delivery configuration is active (True) or inactive (False).

To show more than the default 10 items, select a different number from the **Show Items** drop-down list. To filter the items displayed, select a different value in the unlabeled drop-down list. To view content delivery configurations whose names begin with a particular letter, click that letter. To jump to a particular configuration, type the first few letters of its object name in the **Starts With** field and click **Go**.

Click the links below for information and instruction for:

- Locating content delivery configurations, [page 441](#)
- Creating or modifying content delivery configurations, [page 441](#)
- Creating content delivery configurations, [page 442](#)
- Modifying content delivery configurations, [page 446](#)
- Creating or modifying the advanced properties of a content delivery configuration, [page 448](#)
- Creating or modifying replication settings for a content delivery configuration, [page 450](#)
- Creating or modifying extra arguments for a content delivery configuration, [page 452](#)
- Content delivery configuration fields, [page 463](#)
- Deleting content delivery configurations, [page 470](#)
- Testing content delivery configurations, [page 470](#)

- Duplicating a content delivery configuration, page 471
- Deactivating a content delivery configuration, page 472
- Publishing objects, page 472
- Content delivery configuration results, page 474
- Content delivery logs, page 474
- About effective labels, page 475

Locating content delivery configurations

Use these instructions to locate the correct content delivery configuration.

To locate content delivery configurations:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations** to access the Interactive Delivery Services Configuration list page.
If there are no content delivery configurations, the page displays the message No Content Delivery Configuration objects in the repository.
3. Locate the correct content delivery configuration.
 - To view active content delivery configurations, select **Active** from the drop-down list.
 - To view all content delivery configurations, select **All** from the drop-down list.
 - To view content delivery configurations whose names start with a particular letter, click the letter.
 - To jump to a particular content delivery configuration, type its name in the search box and click **Go**.
 - To sort the content delivery configurations displayed, click **Name, Source Folder, Target Host, Published Version, Connection, or State**.

Creating or modifying content delivery configurations

Click the links for information on:

- Creating content delivery configurations, page 442
- Modifying content delivery configurations, page 446
- Creating or modifying the advanced properties of a content delivery configuration, page 448
- Creating or modifying replication settings for a content delivery configuration, page 450

- Creating or modifying extra arguments for a content delivery configuration, page 452
- Content delivery configuration fields, page 463

Creating content delivery configurations

Use these instructions to create content delivery configurations in Documentum Administrator. You must have Superuser privileges to create a content delivery configuration. The user authentication is mandatory in IDSx. All fields required for publishing are on the New Content Delivery Configuration- Info page.

The [Content delivery configuration fields, page 463](#) section contains additional information about fields on the content delivery configuration pages.

To create a content delivery configuration:

1. Log in to the repository.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The **Interactive Delivery Services Configuration** list page appears. If there are no content delivery configurations, the page displays the message No Content Delivery Configuration objects in the repository.
3. Do one of the following:
 - a. Select the IDS Configuration Template and then select **File > Save As** to access the New Content Delivery Configuration - Info page.
The IDS Configuration Template stores default values that you can use to create new content delivery configurations.
 - b. Select **File > New > Content Delivery Configuration** to access the New Content Delivery Configuration - Info page.

4. Enter content delivery configuration information on the New Content Delivery Configuration - Info page.

All fields on this page are required for publishing. The [Content delivery configuration fields, page 463](#) section contains additional information about each field.

a. Repository Settings

- **State:** To create the content delivery configuration in an inactive state, select **Inactive**. The default state is **Active**.
- **Configuration Name:** Type the name of the configuration.
- **Publishing Folder:** Click **Select** to select a publishing folder, which is the root folder of the folder to publish.
- **Version:** Type the document version to publish.

Specify a version number or a symbolic label such as CURRENT or DRAFT. If you specify a symbolic label, the case must match the label's case in the repository. To allow documents with different version labels to be published, specify ANY VERSION.

b. **Target Host Settings**

- **Target Host Name:** Type the name of the host to which this configuration publishes. This is the target host, a host where the IDS/IDSx target software is installed.
- **Target Port:** Type the port on the target host where IDS/IDSx listens for connections from the source host. This must be the port designated when the target software was installed.
- **Target UDP Port:** Type the UDP port on the target host which is used for accelerated file transfer. Use unique UDP port for each IDSx configurations, irrespective of using the same or a different IDSx target.

Note: The Target UDP Port option is available only in **IDSx**.

- **Connection Type:** Select a secure or nonsecure connection. This is the type of connection used for connections from the source host to the target host. The default is **Secure**.
- **Target Root Directory:** Type the full path of the target root directory.

This directory on the IDS/IDSx target host is where IDS/IDSx places the content files and metadata for publication to the website. During initial publication or a full refresh, the contents of the target root directory are deleted. Ensure that the correct directory is designated as the target root directory.

If you change the target directory after the initial publishing event for the configuration, republish the configuration using the Full Refresh option.

5. Click **Next** to complete additional content delivery configuration fields on the New Content Delivery Configuration - Advanced page.
6. Enter additional content delivery configuration information on the **New Content Delivery Configuration - Advanced** page. The [Content delivery configuration fields, page 463](#) section contains additional information about each field.

a. **Property Export Settings**

- **Add properties as HTML Mega tags:** Select to add properties to HTML documents as META tabs.
- **Export Properties:** Select to export properties.

If selected and you want to include the properties of objects that lack associated content files, select **Include contentless properties**.

If you select **Include contentless properties** and you want to include the properties of folders, select **Include folder properties**.

- **Additional Properties:** To include properties other than the default properties, click **Select Attributes** to access the Choose an attribute page and select an object type from the drop-down list. The default object type is dm_sysobject; only subtypes of dm_sysobject can be published.
- **Property Table Name:** Type the target host property table name, which is required if you selected **Export Properties**.

b. Content Selection Settings

- **Formats:** Select the formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.
- **Effective Label:** To control publishing by date, type an effective label. Section [About effective labels, page 475](#) contains additional information about effective labels.
- To enable global publishing, select **Global Publishing Enabled**.
- If you are using Web Publishing, select a **Website Locale**.

If a document exists in more than one translation in the publishing folder, the locale code indicates which translation to publish and also points to the Web Publisher rules that define the second and subsequent choices of translation to publish.

If you do not use Web Publisher or if your publishing folder is not configured for multilingual publishing, the drop-down list does not appear.

c. Miscellaneous Settings

- **Export Directory:** Select an export directory. The default is a subdirectory of \$DOCUMENTUM/share/temp. When you execute a publishing operation, the directory \$DOCUMENTUM/share/temp/web_publish is created.

On Windows, the length of the repository path to an object to publish, plus the length of the object name, plus the length of the export directory on the Content Server host is limited to 255 characters. There is no length limitation on UNIX.

- **Ingest Directory:** Select an ingest directory. The default is a subdirectory of \$DOCUMENTUM/share/temp. You can choose a different directory by clicking **Select Directory**.
- **Trace Level:** Select a trace level. The trace levels correspond to the trace levels available using the Trace API methods. The default value is 0.
- **Web Server URL Prefix:** Type the Web Server URL Prefix. This is the URL to the target root directory and is required if using Web Publisher.

Note: **Web Server URL Prefix** is not applicable to replication targets.

d. Synchronization Settings

- **Transfer is to live website:** Select to enable online synchronization and indicate you are publishing to a live website.
- **Online Synchronization Directory:** Type the online synchronization directory to use on the target host. The online synchronization directory must be on the same drive as the target root directory. If you do not specify an online synchronization directory, IDS uses a default directory.

Note: Online synchronization is not available for replication targets.

- **Pre-Synch Script on Target:** Type the name of a presync script to run a script on the target host before updating the website. The string consisting of the name of the script plus any arguments you pass must not exceed 48 characters in length.
- **Post-Synch Script on Target:** Type the name of the post-sync script to run a script on the target host after the website is updated. The string consisting of the name of the script plus any arguments you pass must not exceed 48 characters in length.

- e. **Ingest Settings**
 - **Ingest:** Select this option if you want to ingest content from the target to the repository.
 - **Target Ingest Directory:** Enter the directory path of the target from where content will be ingested.
 - f. **Transfer Authentication Settings**
 - **Enable system authentication on target:** Select to use system authentication on the target host.

Note: The Enable system authentication option is not available for replication.
 - **Username and Password:** Type the username and password for the transfer user.
 - **Domain:** If the target host is on Windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.
7. Click **Next** to access the **New Content Delivery Configuration - Replication** page.
- Note:** The **New Content Delivery Configuration - Replication** page is available only in **IDSx**.
8. **Replication Target Host Settings**
 - **Target Host Name:** Type the name of the host to which this configuration replicates. This is the replication target host, a host where the **IDSx** target software is installed.
 - **Target Port:** Type the port of the replication target host where **IDSx** listens for connections from the source host. This must be the port designated when the target software was installed.
 - **Target UDP Port:** Type the UDP port on the target host which is used for accelerated file transfer. Use unique UDP port for each **IDSx** configurations, even if you are using the same or a different **IDSx** target.
 - **Connection Type:** Select a secure or nonsecure connection. This is the type of connection used for connections from the source host (Staging Target) to the target host (Replication Target). The default is **Secure**.
 - **Target Root Directory:** Type the full path of the target root directory.

This directory on the **IDSx** replication target host is where **IDSx** places the content files and metadata for publication to the website. During initial replication or a full refresh, the contents of the target root directory are deleted. Ensure that the correct directory is designated as the target root directory.

If you change the target root directory after the initial replication event for the configuration, replicate the configuration again in order to synchronize the target root directory.
- **Export Properties:** You can select this checkbox to export properties to the replication target.
 - **Property Table Name:** Type the target host property table name, which is required if you selected **Export Properties**.
 - **Ingest:** Select this option if you want to ingest content from the replication target to the repository.
 - **Target Ingest Directory:** Enter the directory path of the replication target from where content will be ingested.

9. Transfer Authentication Settings

- **User Name** : Type the user name for the data transfer.
- **Password** : Type the password for the data transfer.
- **Domain**: If the target host is on Windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.
- **addReplicationTarget**: Click this link to add another replication target.

Note: You can add multiple replication targets.

10. Click **Next** to access the **New Content Delivery Configuration - Extra Arguments** page.
11. Click **Edit** on the **New Content Delivery Configuration - Extra Arguments** page to access the **extra_arguments** page.
 - a. In the **Enter new value** box, type an argument for the content delivery configuration. For example, type *mail_notification_on success* or *mail_notification_user documentum*.
 - b. Click **Add** to move the extra argument to the right side.
 - c. Click the **Move Up** or **Move Down** buttons to rearrange the order of the extra arguments.
 - d. Select an extra argument on the right side and then click **Remove** to delete it.
 - e. Click **OK** to return to the New Content Delivery Configuration- Extra Arguments page.
12. Click **OK** to save the content delivery configuration or click **Cancel**.
The Interactive Delivery Services Configuration list page appears.

Modifying content delivery configurations

Use these instructions in this section to modify a content delivery configuration. You can change any of the properties for a content delivery configuration. When you access a content delivery configuration, the following information about the configuration appears:

Table 53. Content delivery configuration information

Label	Information
Initial Publishing Date	The date documents were first published using this configuration.
Refresh Date	The date of the last successful full refresh of the content delivery configuration.
Last Increment Date	The date of the last successful incremental publish event for the content delivery configuration.
Increment Count	The number of successful incremental updates since the initial publish operation or last full refresh.

Label	Information
Publishing Status	Indicates whether the last publishing event succeeded or failed.
Event Number	Unique number generated internally for each publishing operation.

To modify a content delivery configuration:

1. Connect to the repository from which you are publishing.
 2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The Interactive Delivery Services Configuration list page appears.
 3. Select the content delivery configuration to change and then select **View > Properties > Info**.
The Content Delivery Configuration - Info page appears.
 4. Modify any fields on the **Content Delivery Configuration - Info** page.
Section [Content delivery configuration fields, page 463](#) contains information about the fields on the Content Delivery Configuration - Info page.
 5. Do one of the following:
 - Click the **Advanced** tab to modify additional content delivery configuration fields on the Content Delivery Configuration - Advanced page.
 - Click **OK** to save the content delivery configuration changes and return to the Interactive Delivery Services Configuration list page.
 - Click **Cancel** to return to the Interactive Delivery Services Configuration list page without saving any changes to the content delivery configuration.
 6. If you clicked the **Advanced** tab, modify fields on the Content Delivery Configuration - Advance page.
Section [Content delivery configuration fields, page 463](#) contains information about the fields on the Advance page.
 7. If you clicked the **Replication** tab, modify fields on the Content Delivery Configuration - Replication page.
Section [Content delivery configuration fields, page 463](#) contains information about the fields on the Replication page.
- Note:** The Replication tab is available only in **IDSx**.
8. Do one of the following:
 - Click the **Extra Arguments** tab to access the Content Delivery Configuration - Extra Arguments page.
 - Click **OK** to save the content delivery configuration changes and return to the Content Delivery Configuration list page.
 - Click **Cancel** to return to the Content Delivery Configuration list page without saving any changes to the content delivery configuration.
 9. If you clicked the **Extra Arguments** tab, click the **Edit** button on the Content Delivery Configuration - Extra Arguments page.

The **extra_arguments** page appears.

- a. In the **Enter new value** box, type an argument for the content delivery configuration.
For example, type *mail_notification_on success* or *mail_notification_user documentum*.
 - b. Click **Add** to move the extra argument to the right side.
 - c. Click the **Move Up** or **Move Down** buttons to rearrange the order of the extra arguments.
 - d. Select an extra argument on the right side and then click **Remove** to delete it.
 - e. Click **OK** to return to the New Content Delivery Configuration - Extra Arguments page.
10. Do one of the following:
- Click **OK** to save the content delivery configuration changes and return to the Interactive Delivery Services Configuration list page.
 - Click **Cancel** to return to the Interactive Delivery Services Configuration list page without saving any changes to the content delivery configuration.

Creating or modifying the advanced properties of a content delivery configuration

Use the instructions in this section to create or modify the content delivery configuration properties on the New Content Delivery Configuration - Advanced or Content Delivery Configuration - Info page. The instructions assume you connected to a repository and navigated to the Advanced page for a content delivery configuration. [Creating content delivery configurations, page 442](#) contains instructions on connecting to a repository and navigating to the Advanced page.

To create or modify the advanced properties of a content delivery configuration:

1. Enter additional content delivery configuration information on the Advanced page. Section [Content delivery configuration fields, page 463](#) contains information about the fields on the Advanced page.
 - a. **Property Export Settings**
 - **Add properties as HTML Mega tags:** Select to add properties to HTML documents as META tabs.
 - **Export Properties:** Select to export properties.
If selected and you want to include the properties of objects that lack associated content files, select **Include contentless properties**.
If you select **Include contentless properties** and you want to include the properties of folders, select **Include folder properties**.
 - **Additional Properties:** To include properties other than the default properties, click **Select Attributes** to access the Choose an attribute page and select an object type from the drop-down list. The default object type is dm_sysobject; only subtypes of dm_sysobject can be published.
 - **Property Table Name:** Type the target host property table name, which is required if you selected **Export Properties**.

b. **Content Selection Settings**

- **Formats:** Select the formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.
- **Effective Label:** To control publishing by date, type an effective label. Section [About effective labels, page 475](#) contains additional information about effective labels.
- To enable global publishing, select **Global Publishing Enabled**.
- If you are using Web Publishing, select a **Website Locale**.

If a document exists in more than one translation in the publishing folder, the locale code indicates which translation to publish and also points to the Web Publisher rules that define the second and subsequent choices of translation to publish.

If you do not use Web Publisher or if your publishing folder is not configured for multilingual publishing, the drop-down list does not appear.

c. **Miscellaneous Settings**

- **Export Directory:** Select an export directory. The default is a subdirectory of \$DOCUMENTUM/share/temp. When you execute a publishing operation, the directory \$DOCUMENTUM/share/temp/web_publish is created.

On Windows, the length of the repository path to an object to publish, plus the length of the object name, plus the length of the export directory on the Content Server host is limited to 255 characters. There is no length limitation on UNIX.

- **Ingest Directory:** Select an ingest directory. The default is a subdirectory of \$DOCUMENTUM/share/temp. You can choose a different directory by clicking **Select Directory**.
- **Trace Level:** Select a trace level. The trace levels correspond to the trace levels available using the Trace API methods. The default value is 0.
- **Web Server URL Prefix:** Type the Web Server URL Prefix. This is the URL to the target root directory and is required if using Web Publisher.

Note: **Web Server URL Prefix** is not applicable to replication targets.

d. **Synchronization Settings**

- **Transfer is to live website:** Select to enable online synchronization and indicate you are publishing to a live website.
- **Online Synchronization Directory:** Type the online synchronization directory to use on the target host. The online synchronization directory must be on the same drive as the target root directory. If you do not specify an online synchronization directory, IDS uses a default directory.
Note: Online Synchronization is not available for replication targets.
- **Pre-Synch Script on Target:** Type the name of a presync script to run a script on the target host before updating the website. The string consisting of the name of the script plus any arguments you pass must not exceed 48 characters in length.
- **Post-Synch Script on Target:** Type the name of the post-sync script to run a script on the target host after the website is updated. The string consisting of the name of the script plus any arguments you pass must not exceed 48 characters in length.

e. **Ingest Settings**

- **Ingest:** Select this option if you want to ingest content from the target to the repository.
- **Target Ingest Directory:** Enter the directory path of the target from where content will be ingested.

f. **Transfer Authentication Settings**

- **Enable system authentication on target:** Select to use system authentication on the target host.
Note: The Enable System Authentication option is not available for replication.
- **Username and Password:** Type the username and password for the transfer user.
- **Domain:** If the target host is on Windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.

2. Click **Previous**, **Finish**, or **Cancel**.

- Click **Previous** to return to the Info page.
- Click **Finish** to save the content delivery configuration and return to the Interactive Delivery Services Configuration list page.
- Click **Cancel** to return to the Interactive Delivery Services Configuration list page without saving the content delivery configuration.

Creating or modifying replication settings for a content delivery configuration

Use the instructions in this section to create or modify the replication settings for a content delivery configuration property. The instructions assume you connected to a repository and navigated to the New Content Delivery Configuration- Replication or Content Delivery Configuration - Replication

page for a content delivery configuration. Section [Creating content delivery configurations, page 442](#) contains instructions on connecting to a repository and navigating to the Replication page.

1. Replication Target Host Settings

- **Target Host Name:** Type the name of the host to which this configuration replicates. This is the replication target host, a host where the IDSx target software is installed.
- **Target Port:** Type the port of the replication target host where IDSx listens for connections from the source host. This must be the port designated when the target software was installed.
- **Target UDP Port:** Type the UDP port on the target host which is used for accelerated file transfer. Use unique UDP port for each IDSx configurations, even if you are using the same or a different IDSx target.
- **Connection Type:** Select a secure or nonsecure connection. This is the type of connection used for connections from the source host (Staging Target) to the target host (Replication Target). The default is **Secure**.
- **Target Root Directory:** Type the full path of the target root directory.

This directory on the IDSx replication target host is where IDSx places the content files and metadata for publication to the website. During initial replication or a full refresh, the contents of the target root directory are deleted. Ensure that the correct directory is designated as the target root directory.

If you change the target root directory after the initial replication event for the configuration, replicate the configuration again in order to synchronize the target root directory.

- **Export Properties:** You can select this checkbox to export properties to the replication target.
- **Property Table Name:** Type the target host property table name, which is required if you selected **Export Properties**.
- **Ingest:** Select this option if you want to ingest content from the replication target to the repository.
- **Target Ingest Directory:** Enter the directory path of the replication target from where content will be ingested.

2. Transfer Authentication Settings

- **User Name :** Type the user name for the data transfer.
- **Password :** Type the password for the data transfer.
- **Domain:** If the target host is on Windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.
- **addReplicationTarget:** Click this link to add another replication target.

Note: You can add multiple replication targets.

Creating or modifying extra arguments for a content delivery configuration

Use the instructions in this section to create or modify the extra arguments for a content delivery configuration property.

The instructions assume you connected to a repository and navigated to the New Content Delivery Configuration- Extra Arguments or Content Delivery Configuration - Extra Arguments page for a content delivery configuration. Section [Creating content delivery configurations, page 442](#) contains instructions on connecting to a repository and navigating to the Extra Arguments page.

To create or modify extra arguments:

1. On the New Content Delivery Configuration- Extra Arguments or Content Delivery Configuration - Extra Arguments page, click **Edit**.
The **extra_arguments** page appears.
2. In the **Enter new value** box, type an argument for the content delivery configuration.
For example, type *mail_notification_on success* or *mail_notification_user documentum*.
3. Click **Add** to move the extra argument to the right side.
4. Click the **Move Up** or **Move Down** buttons to rearrange the order of the extra arguments.
5. Select an extra argument on the right side and then click **Remove** to delete it.
6. Click **OK** to return to the New Content Delivery Configuration- Extra Arguments or Content Delivery Configuration - Extra Arguments page.

For information on extra arguments, see [Extra arguments, page 452](#).

Extra arguments

The following table describes the extra arguments for a content delivery configuration.

Table 54. Extra arguments

Key	Description	Default Value(s)
use_docbase_formats	Determines whether the default file format extensions set in the repository are used when files are published. FALSE overrides the default file format extensions set in the repository. TRUE or no setting uses the extensions set in the repository format objects.	TRUE

Key	Description	Default Value(s)
use_text_file_extensions	When set to TRUE, text files that do not have a .txt extension in the object name are published with the .txt extension. For example, if a text file MyFile is published and the parameter is set to TRUE, the file is published as MyFile.txt. If the parameter is set to FALSE, the default value, the file is published as MyFile.	FALSE
agent_connection_timeout	The timeout interval in seconds for the IDS publish method's connection to the target host. For example, to wait 90 seconds:	120
	<pre>agent_connection_ timeout=90</pre>	
	If the publishing operation takes longer, Documentum Administrator displays an error message and the publishing log files record that the publishing operation failed.	
connect_thread_timeout	The timeout interval in seconds for the end-to-end tester's connection to the target host. For example, to wait 90 seconds:	30
	<pre>connect_thread_ timeout=90</pre>	
lock_sleep_interval	The number of seconds for which IDS waits for a webc lock object to be unlocked. For example, to wait 90 seconds:	10
	<pre>lock_sleep_interval=90</pre>	

Key	Description	Default Value(s)
lock_retry_count	How many times IDS checks whether the webc lock object is unlocked. The value of this key multiplied by the value of lock_sleep_interval controls the total amount of time for which IDS waits to lock a configuration with a lock object. Since the default lock_sleep_interval value is 10 seconds, IDS retries for a total of 300 seconds (5 minutes) by default.	30
lock_exitifbusy_flag	Whether IDS exits or retries when it finds a webc lock object locked. TRUE causes IDS to exit.	TRUE
disable_dctm_tag	Whether you want the Documentum META tag to appear when you use META tag merging.	TRUE
trace_passwords	Whether passwords appear in debug tracing output. FALSE causes passwords to be omitted from debug tracing output. TRUE causes passwords to be included in debug tracing output.	FALSE
error_threshold	The number of errors allowable on the source side during a single full-refresh, incremental, or force-refresh publishing operation.	0
max_cached_ssl_sockets	The number of cached SLL sockets between source and all targets that are retained for reuse. Does not restrict the maximum number of SLL sockets that can be open at one time. Used only in the scs_admin_config object in the IDS Administration sub-node.	30

Key	Description	Default Value(s)
publish_contentless_documents	Whether documents can be published that do not have associated content files. TRUE causes publication of documents without associated content files. FALSE causes documents without associated content files not to be published. Note: This option can also be selected on the Advanced tab of the content delivery configuration.	FALSE
publish_folder_properties	Whether folder properties can be published. TRUE causes folder properties to be published. FALSE causes folder properties not to be published. If set to TRUE, requires that publish_contentless_documents is also set to TRUE. Note: This option can also be selected on the Advanced tab of the content delivery configuration.	FALSE
compression	Whether file compression is enabled. TRUE causes files to be compressed. FALSE disables file compression.	TRUE
min_size_worth_compressing	The threshold in bytes beneath which compression of a particular file does not yield performance gains	5000
max_entries_per_zipfile	The number of files whose size is below min_size_worth_compressing that are collected in a zip file for transfer to the target host.	128
extensions_to_compress	The file types to compress, by file extension.	html, jhtml, shtml, phtml, xhtml, htm, jht, sht, asp, jsp, xml, css, txt
publish_source_version_labels	When set to TRUE, all values of the r_version_label attribute are published to the repeating attribute table.	FALSE

Key	Description	Default Value(s)
mssql_store_varchar	Microsoft SQL Server database only. When set to TRUE, string attributes are stored in the source catalog database and target database as varchar rather than nvarchar.	FALSE
store_log	When set to true, you cannot publish multibyte data. Whether to store log files in the repository. TRUE causes logs to be stored in the repository. FALSE causes logs not to be stored in the repository.	TRUE
method_trace_level	The log is not stored in the repository for a single-item publishing operation when method_trace_level is set to 0.	0
export_threshold_count	The level of tracing output. 0 is the lowest level of tracing and 10 is the highest level of tracing.	100
use_format_extensions	Indicates the number of items the export operation exports at one time.	FALSE
	Use with format key to check for valid format extensions.	
	If use_format_extensions is set to FALSE, files are published with the format extensions defined in the repository for the format.	
	If use_format_extensions is set to TRUE and a particular extension is defined as valid for a particular format, files of that format with that extension are published with the extension.	
	If use_format_extensions is set to TRUE and a particular extension is <i>not</i> defined as valid for a particular format, files of that format with that extension are published with	

Key	Description	Default Value(s)
format	the format extensions defined in the repository for the format.	
force_serialized	Use with use_format_extensions key. Takes the format: <i>format.format_name=semicolon-separated_extensions</i>	FALSE
sourceAttrsOnly	When set to TRUE, single-item publishes are performed serially rather than in parallel.	
additionalMetatagFileExts	By default, on each publish IDS creates a properties.xml file, which contains <i>all</i> the attributes of the objects published. If sourceAttrsOnly is set, IDS writes only the default attributes and any additional attributes that are published to the XML file. <ul style="list-style-type: none">• r_object_id• r_modified_date• object_name• i_chronicle_id• r_version_label• content_id• i_full_format• r_folder_path Allows exported attributes to be added as metatags to file formats with the extensions asp, jsp, jht, and sht. Add them as a semicolon-separated list: <i>additional_metatag_extensions=asp;jsp;jht;sht</i>	NO default value.

Key	Description	Default Value(s)
export_relations	When set to TRUE and attributes are published, relation objects (dm_relation objects) are published to a database table on the target.	FALSE
clean_repeating_table_noAttrs	Deprecated.	
export_media_properties	When set to true, attributes of the dmr_content object and dm_format object are exported and published to the target.	FALSE
additional_media_properties	When export_media_properties is set to true, used to specify additional attributes of dmr_content and dm_format objects to be published. The format is a semicolon-separated list:	FALSE
	<pre>additional_media_ properties=type1. attribute1;type2. attribute2</pre>	
For example:		
	<pre>additional_media_ properties=dmr_content. x_range;dmr_content.z_ range</pre>	
exclude_folders	A semicolon-separated list of absolute repository paths, indicates the folders to be excluded from a publishing operation. When set, content files and attributes from folders indicated are not published.	
For example:		
	<pre>exclude_folders=/acme. com/images;/acme.com/ subdir</pre>	
pre_webroot_switch_script	A script to be run before online synchronization takes place. For more information, refer to "Scripts run before or after the Webroot Switch" in the <i>Interactive Delivery Services User Guide</i> .	

Key	Description	Default Value(s)
post_webroot_switch_script	A script to be run after online synchronization takes place. For more information, refer to “Scripts run before or after the Webroot Switch” in the <i>Interactive Delivery Services User Guide</i> .	
full_refresh_backup	When set to TRUE, the content files and database tables on the target host are backed up before the synchronization phase in a full-refresh publishing operation.	FALSE
exclude_formats	Takes a semicolon-separated list of format extensions and excludes content files with those extensions from publishing. For example to exclude .xml and .wml files:	Not set
check_valid_filename	If this parameter is set to TRUE, then the filename is checked for Windows illegal characters. Illegal characters are replaced as specified by the filename_replace_char parameter.	TRUE (Windows only); FALSE for all other O/S
	The default value of check_valid_filename is TRUE if the IDS source is on Windows; the default is set to FALSE for all other operating systems. This parameter should be used if the target is on a Windows host and the source is not on Windows.	
filename_replace_char	Windows only. Used in conjunction with check_valid_filename. Defines the character to use to replace invalid characters in file names on Windows. For example:	_ (underscore)

Key	Description	Default Value(s)
sync_on_zero_updates	When set to TRUE, database updates are made and pre- and post-synch scripts are run even if there is no new data to publish from the repository.	FALSE
transform_type	Used with Web Publisher Page Builder only.	absolute
	Determines whether links in HTML pages are resolved at publication time to absolute or relative paths. Valid values are absolute and relative.	
ingest_workflow	Used with Content Delivery web service only. Specifies a custom workflow to be used with the ingest operation. Refer to the <i>Documentum Enterprise Content Services 6.5 Reference Guide</i> for details about this web service.	
	Note: This argument can be set at the repository (IDS Administration) level only. You cannot specify different ingest workflows for individual content delivery configurations.	
wan_acceleration_ssh_port	This is the TCP Port required for accelerated data transfer authentication. If the SSH port has to be changed, check the SSH service configuration (sshd_config) for windows for changing the default port.	22
	The default value is applicable to all publishing configurations and can be overridden for each publishing configuration, by setting this as an extra argument for publishing.	
wan_acceleration_disabled	This parameter is used to disable the accelerated data transfer and use HTTP for file transfer.	False

Key	Description	Default Value(s)
wan_acceleration_policy	<p>This parameter defines the policy used for accelerated data transfer.</p> <ul style="list-style-type: none"> • ADAPTIVE/FAIR (A): When set to this value, the file transfer monitors and adjusts the transfer rate to fully utilize the available bandwidth to the maximum limit. When there is congestion due to other file transfers, this mode shares bandwidth for other flows and utilizes a fair rate of transfer. In this mode, both the maximum and minimum transfer rates are required. • FIXED (F): When set to this value, the file transfer happens at a specified target rate, irrespective of the actual network capacity. In this mode, a maximum transfer rate is required. • TRICKLE/STEALTH (T): When set to this value, the file transfer uses the available bandwidth to the maximum rate. When there is congestion due to other file transfers, the transfer rate is reduced down to the minimum rate. 	A
min_file_transfer_rate	This is the minimum file transfer rate	0Mbps
max_file_transfer_rate	This is the maximum file transfer rate	1000Mbps
wan_acceleration_log_details	The file transfer process status are captured in the content delivery log files	FALSE

Key	Description	Default Value(s)
wan_acceleration_file_checksum	<p>This parameter is used to resume file transfer when there is a failure.</p> <ul style="list-style-type: none"> • FILE_ATTRIBUTES: When set to this value, checks for the file size of both files. If the file size is the same, then transfer does not take place. 	OFF
decision_commit_rollback	<p>This parameter is used to set the threshold value for transaction capability. For example, if there are 10 replication targets, and if the DCR value reads as:</p> <pre data-bbox="649 1332 894 1396">decision_commit_ rollback 6</pre> <p>implies that if replication operation succeeds on a minimum of 6 replication targets, then a decision is taken to commit (File System and RDBMS) the changes performed by the replication operation.</p> <p>If the <i>number_of_failures</i> value is greater than the <i>decision_commit_rollback</i> value, a rollback is initiated on the replication targets.</p>	NA

Key	Description	Default Value(s)
	The value assigned to this attribute must be a positive integer.	
tc_file_size	The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i> .	100 MB
	When the size of the files replicated exceeds <i>tc_file_size</i> , transaction capability feature is disabled. The units is specified in MB.	
	The value assigned to this attribute must be a positive integer.	
tc_file_count	The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i> .	500
	When the number of files replicated exceeds <i>tc_file_count</i> , transaction capability feature is disabled.	
	The value assigned to this attribute must be a positive integer.	

Content delivery configuration fields

The following tables contain details about fields on the following pages that are used to create or modify content delivery configurations:

- New Content Delivery Configuration- Info page
- New Content Delivery Configuration- Advanced page
- New Content Delivery Configuration - Replication page
- Content Delivery Configuration - Info page
- Content Delivery Configuration - Advanced page
- Content Delivery Configuration - Replication page

Table 55. Content delivery fields - Info page

Field label	Value
State	Select Active to indicate using this content delivery configuration is active. The default state is Active. Select Inactive to deactivate the configuration.
Configuration Name	Identifies the publishing configuration. The name appears in the list of existing configurations and the name of log files applying to the configuration.
Publishing Folder	The root repository folder from which you are publishing. The root folder and all subfolders are published.
	If you change this setting after the initial publication, you must re-publish the configuration using the Full Refresh option.
Version	Defines which version of the document to publish. If unspecified, the default is the CURRENT version.
	If you change this setting after you publish the configuration initially, you must republish the configuration using the Full Refresh option.
Target Host Name	Identifies the target host machine to which documents are published. This is the target host, a host where the Interactive Delivery Services (IDS) target software is installed.
Target Port	The port number of the website's host machine to use for connections. This must be the port designated when the target software was installed.
Connection Type	May be Secure or Non-secure . This is the type of connection used for connections from the source host to the target host. The default is Secure .
Target Root Directory	The physical directory on the target host where the transfer agent places the export data set for publication. Also known as the webroot. If you change this setting after the initial publishing event for the configuration, you must re-publish the configuration using the Full Refresh option.
	CAUTION: During initial publication or a full refresh, the contents of the target root directory

Field label	Value
	are deleted. Ensure that you designate the correct directory as the target root directory.

Table 56. Content delivery fields - Advanced page

Field label	Value
Add properties as HTML Meta Tags	If selected, the system inserts document properties into HTML content files as META tags on the target host.
Export Properties	If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.
Include contentless properties	If selected, the system exports a default set of properties for each published document.
Include folder properties	If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.
Additional Properties	If selected, documents in the publishing folder that without an associated content file are published. Only the properties associated with the contentless document are published.
	By default, this option is not selected and is enabled only if Export Properties is also selected.
	If selected, folder properties are published to the website. This option is enabled only if Include contentless properties is also selected.
	Identifies additional properties to export to repository on target host. If Export Properties is selected, IDS exports a set of default properties for each published document.
	If this setting changes after initial publishing event for the configuration, republish using the Full Refresh option.
	Click Select Attributes to identify additional properties to export.

Field label	Value
Property Table Name	The name to use when creating the database tables on the target host. Specify a table name if Export Properties is selected. The table name must not exceed 28 bytes.
Formats	If this setting changes after initially publishing the configuration, republish the configuration using the Full Refresh option.
Effective Label	The content formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.
	If this setting changes after publishing the configuration initially, republish the configuration using the Full Refresh option.
Export Directory	This field is used in conjunction with the a_effective_label document property to filter documents for publication. If Effective Label is specified, only documents with a matching a_effective_label value are examined as possible candidates for publication. If unspecified, all documents are examined as possible candidates.
	If this setting changes after initially publishing the configuration, you must republish the configuration using the Full Refresh option.
Ingest Directory	The name of the local directory on the Content Server host where documents are placed after they are exported from the repository.
	The default is a subdirectory of \$DOCUMENTUM/share/temp. When executing a publishing operation, the directory \$DOCUMENTUM/share/temp/web_publish is created.
	On Windows, the length of the repository path to an object to publish, plus the length of the object name, plus the length of the export directory on the Content Server host is limited to 255 characters. There is no length limitation on UNIX.
	The name of the directory on the source where the documents are placed after being pulled from the target directory. The default is a subdirectory of \$DOCUMENTUM/share/temp. You can choose a different directory by clicking Select Directory .

Field label	Value
Trace Level	<p>Defines a tracing level for IDS operations. The trace levels correspond to the trace levels available using the Trace API methods. The default value is 0.</p>
Global Publishing Enabled	<p>Enables the global publishing feature of Web Publisher. Replaces the <code>global_publishing</code> extra argument that was added manually to the content delivery configuration in prior versions.</p>
Website Locale	<p>Web Publisher only. Site Caching Services 4.3 and above only. Interactive Delivery Services 6.5 SP2 only. Replaces the <code>global_locales</code> extra argument that was added manually to the content delivery configuration in prior versions. Select a locale from the drop-down list. If using Web Publisher and a document exists in more than one translation in the publishing folder, the locale code indicates which translation to publish and also points to the Web Publisher rules that define the second and subsequent choices of translation to publish.</p>
	<p>The drop-down list contains choices only when you are using Web Publisher and the publishing folder is configured for multilingual use.</p>
	<p>If you do not use Web Publisher or if your publishing folder is not configured for multilingual publishing, the drop-down list does not appear.</p>
Web Server URL Prefix	<p>This is the URL to the target root directory and is required if using Web Publisher.</p>
	<p>For example, if the target root directory is <code>d:\inetpub\wwwroot\webcache</code> and the website host is on a computer <code>host_name</code>, set the Web Server URL Prefix to <code>http://host_name/webcache</code>.</p>
	<p>Note: Web Server URL Prefix is not applicable to replication targets.</p>

Field label	Value
Transfer is to live website	<p>If selected, Interactive Delivery Services attempts to minimize user interruptions during publishing. Leave cleared if users do not have access to the site during publishing operations.</p>
Online Synchronization Directory	<p>If this setting changes after initial publication, republish the configuration using the Full Refresh option.</p>
Pre-Synch Script on Target	<p>The directory on the target host to be used as temporary storage for the backup copy of the Interactive Delivery Services repository during online updates. This must be specified if Transfer is to live website is selected.</p>
Post-Synch Script on Target	<p>If this setting changes after you publish the configuration initially, republish the configuration using the Full Refresh option.</p>
Ingest	<p>The name of a script, located in the target host's product/bin directory, to run before publishing takes place. If online synchronization is enabled, the script runs before online synchronization occurs. There is a 48-character limit for information typed into this field.</p>
Target Ingest Directory	<p>The name of a script located in the target host's product/bin directory to be run after publishing occurs. If online synchronization is enabled, the script runs after online synchronization takes place. There is a 48-character limit for information typed into this field.</p>
Enable system authentication on target	<p>Select this option if you want to ingest content from the target to the repository.</p>
User Name	<p>Select this option if you want to ingest content from the target to the repository.</p>
Password	<p>Enter the directory path of the target from where the content will be ingested.</p>
Confirm Password	<p>Select to require a transfer username and password for authentication. Not selected means the transfer username and password are not required for authentication before a data transfer occurs.</p>
Domain	<p>Identifies the user whose account will be used by the transfer agent to connect to the target host.</p>
	<p>The password for the user specified in User Name.</p>
	<p>Enter the password again for confirmation.</p>
	<p>Identifies the domain of the user specified in User Name.</p>

Table 57. Content delivery fields - Replication page

Field label	Value
Target Host Name	Identifies the target host machine to which documents are published. This is the replication target host, a host where the Interactive Delivery Services Accelerated (IDSx) target software is installed.
Target Port	The port number of the website's host machine to use for connections. This must be the port designated when the replication target software was installed.
Target UDP Port	The UDP port on the target host which is used for accelerated file transfer. Unique UDP port has to be used for every IDSx configurations, irrespective of using the same or different IDSx targets.
Connection Type	May be Secure or Non-secure . This is the type of connection used for connections from the source host to the target host. The default is Secure .
Target Root Directory	The physical directory on the target host where the transfer agent places the export data set for publication. Also known as the webroot. If you change this setting after the initial publishing event for the configuration, you must replicate the configuration again in order to synchronize the target root directory.
Export Properties	You can select this checkbox to export properties to the replication target.
Property Table Name	Type the target host property table name, which is required if you selected Export Properties .
Ingest	Select this option if you want to ingest content from the replication target to the repository.
Target Ingest Directory	Enter the directory path of the source where the content will be stored.

Field label	Value
User Name	Enter the user name for the data transfer.
Password	Enter the password for the data transfer.
Domain	If the target host is on windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.
addReplicationTarget	Adds multiple replication targets.

Deleting content delivery configurations

If a content delivery configuration is no longer needed, you can delete it. To stop publishing using the configuration, make the content delivery configuration inactive. Section [Deactivating a content delivery configuration, page 472](#) provides instructions on how to deactivate a publishing configuration.

To delete a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations** to access the Interactive Delivery Services Configuration list page.
3. Select the content delivery configuration to delete and then select **File > Delete**.
The system displays a delete confirmation page.
4. Click **OK** or **Cancel**.
 - Click **OK** to delete the content delivery configuration.
 - Click **Cancel** to return to the Interactive Delivery Services Configuration list page without deleting the configuration.

Testing content delivery configurations

After creating a content delivery configuration, test it by running the end-to-end tester, which simulates a publishing operation without publishing any documents. The end-to-end tester tests all parameters set in a publishing configuration and ensures that IDS/IDSx can make the necessary connections to the database and target host.

The end-to-end tester creates a log file in the repository whether the test fails or succeeds. View the resulting log file after running the tester. If the test fails, examine the log file to determine which

element of your IDS/IDSx installation is not working. You can read the file from Documentum Administrator or retrieve it directly from the repository where IDS/IDSx log files are stored in the /System/Sysadmin/Reports/Webcache folder.

To test a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The Interactive Delivery Services Configuration list page appears.
3. Select the content delivery configuration to test and then select **Tools > End to End Test**.
The **End to End Configuration** page appears.
4. On the End to End Configuration page, select a trace level and then click **OK** to run the end-to-end test.
The **Content Delivery Configuration Publish Result** page appears.
5. Click the link to access the **Content Delivery Configuration Log** page to view the publishing log.
6. Click **OK** to return to the Content Delivery Configuration Publish Result page.
7. Click **OK** again to return to the Interactive Delivery Services Configuration page.

Duplicating a content delivery configuration

Create a new content delivery configuration by duplicating and then modifying a content delivery configuration that is thoroughly tested and successfully used in production. The IDS Configuration Template stores default values that you can use to create new content delivery configurations.

To duplicate a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The Interactive Delivery Services Configuration list page appears.
3. Select the content delivery configuration to duplicate and then select **File > Save as**.
The **New Content Delivery Configuration - Info** page for the new content delivery configuration appears. The object name of the configuration defaults to
`Copy [1] of configuration_name`
where `configuration_name` is the name of the original configuration.
4. Modify fields that need to be changed on the New Content Delivery Configuration - Info, New Content Delivery Configuration- Advanced, New Content Delivery Configuration - Replication, and New Content Delivery Configuration - Extra Arguments pages.
Note: New Content Delivery Configuration - Replication page is available only in **IDSx**.
Section [Content delivery configuration fields, page 463](#) contains information about each field on these pages.
5. If you export properties, ensure that you change the table name for the exported properties.
6. Click **OK**.

The new configuration is saved and the Interactive Delivery Services Configuration list page appears.

Deactivating a content delivery configuration

To suspend publishing operations without deleting the content delivery configuration, deactivate it using the instructions in this section.

To deactivate a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The **Interactive Delivery Services Configuration** list page appears.
3. Select the correct content delivery configuration and then select **File > Properties > Info**.
The **Content Delivery Configuration - Info** page appears.
4. Select **Inactive** in the **Repository Settings** section.
The **Content Delivery Configuration - Info** page appears.
5. Click **OK**.
The Interactive Delivery Services Configuration list page appears.

Publishing objects

Use the instructions in this section to manually run a publishing job from the Interactive Delivery Services Configuration list page. To publish on a schedule, use the instructions in [Creating jobs, page 268](#) to modify the job that was automatically created for the publishing configuration.

To publish from a content delivery configuration:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The **Interactive Delivery Services Configuration** list page appears.
3. Select the correct content delivery configuration and then select **Tools > Publish**.
The **Content Delivery Configuration Publish** page appears.
4. Select the required options on the **Content Delivery Configuration Publish** page:
 - **Refresh entire site:** Select to force a full refresh publish.
A full refresh deletes and republishes all content and drops and recreates the database tables.
 - **Recreate property schema:** Select to destroy and recreate the database tables on the target host.
Using this option forces a full-refresh publish.
 - **Update property schema:** Select to update the database tables with schema changes, but without republishing all content files and metadata.

- **Launch the process asynchronously:** Select to refresh the screen before publishing is complete.

If you do not select Launch process asynchronously, the screen does not refresh before publishing is completed and your browser may time out.

- **Trace Level:** Select a trace level.

5. Click **OK**.

If you selected **Refresh entire site or Recreate property schema**, a warning message appears.

6. Click **OK**.

The publishing job runs and the results are displayed. Note that it may take several minutes for the publishing log to be available from Documentum Administrator.

To replicate from a content delivery configuration

1. Connect to the repository from which you are replicating.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The **Interactive Delivery Services Configuration** list page appears.
3. Select the correct content delivery configuration and then select **Tools > Replicate**.
The **Content Delivery Configuration Replicate** page appears.
4. Select a trace level.
5. Click **OK**.

The replication job runs and the results are displayed in the **Content Delivery Configuration Replicate Result** page. In this page, you can also click the link available to view the logs. Note that it may take several minutes for the Replication log to be available from Documentum Administrator.

To ingest from a content delivery configuration

1. Connect to the repository from which you are replicating.
 2. Navigate to **Administration > Content Delivery > IDS Configurations**.
The **Interactive Delivery Services Configuration** list page appears.
 3. Select the correct content delivery configuration and then select **Tools > Ingest** or right-click on the content delivery configuration and then select **Ingest**.
The **Content Delivery Configuration Ingestion** page appears.
 4. Select a trace level.
 5. Click **OK**.
- The **Content Delivery Configuration Ingestion Result** page appears. In this page, you can also click the link available to view the logs. Note that it may take several minutes for the Ingestion log to be available from Documentum Administrator.

Content delivery configuration results

This page indicates whether a publishing or a replication operation succeeded or failed. For details on the publishing operation, on the *content delivery configuration publish result* page, click the links to view the publishing logs. Similarly, for details on the replication operation, click the links on the *content delivery configuration replicate result* page to view the replication logs. After viewing the log, click **OK** or **Cancel** to close the log, then click **OK** or **Cancel** to return to the **Interactive Delivery Services Configuration** list page.

Interactive Delivery Services version 6x can be configured for email notification of content delivery configuration results. Refer to *Interactive Delivery Services User Guide* and *Interactive Delivery Services Accelerated User Guide* for more information.

Content delivery logs

Each publishing operation or end-to-end test generates a log file. View these files to determine whether publishing succeeded and to diagnose problems when a publishing operation fails. To navigate from the publishing log list page, click the **Content Delivery** breadcrumb.

This section contains the following topics:

- [Viewing content delivery logs, page 474](#)
- [Deleting content delivery logs, page 474](#)

Viewing content delivery logs

Each publishing event or publishing test generates a log file. Review the file after publishing or testing a content delivery configuration to determine if the operation succeeded.

To view publishing logs:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
3. Select the correct content delivery configuration and then select **View > Logs**.
4. Click the name of the log you want to view.
5. Click **OK**.

Deleting content delivery logs

After you examine logs or as they accumulate in the repository, you may want to delete them. Use these instructions for deleting content delivery logs.

To delete publishing logs:

1. Connect to the repository from which you are publishing.
2. Navigate to **Administration > Content Delivery > IDS Configurations**.
3. Select the correct content delivery configuration and then select **View > Logs**.
4. Select the logs to delete.
5. Select **File > Delete**.

The log file is deleted.

About effective labels

Use *effective labels* to enable IDS to determine which documents to publish based on effective and expiration dates.

The effective label specified in a content delivery configuration allows IDS to determine when to publish a particular document and when to delete it from the website. IDS does this by examining the repeating properties `a_effective_label`, `a_effective_date`, and `a_expiration_date`, which are properties of the `dm_sysobject` type. These properties are inherited by all subtypes of `dm_sysobject`.

Each `a_effective_label` corresponds to a matching `a_effective_date` and `a_expiration_date`. Because these are repeating properties, you can specify multiple effective labels, effective dates, and expiration dates for each document. IDS looks for the effective and expiration dates matching a particular effective label, and uses the dates to determine when to publish a document and when to withdraw the document from the website.

For example, a document might have the effective label, effective date, and expiration date properties set as follows:

Table 58. Using effective labels

<code>a_effective_label</code>	<code>a_effective_date</code>	<code>a_expiration_date</code>
DRAFT	03/05/08	03/15/08
REVIEW	03/16/08	03/26/08
COMMENT	03/27/08	04/10/08
APPROVED	04/10/08	04/10/09

Setting the document's effective label to REVIEW means the document will be published on March 16, 2008 and removed from the website on March 26, 2008. Setting the effective label to APPROVED means the document will be published on April 10, 2008 and withdrawn on April 10, 2009.

Documents whose effective label does not match the effective label set in the content delivery configuration are published regardless of the values set for effective date and expiration date.

Chapter 15

Indexing Management

This chapter contains information and instructions for administering full-text indexing in repositories. A full-text index is an index on the properties and content files associated with your documents or other SysObjects or SysObject subtypes. Full-text indexing enables the rapid searching and retrieval of exact text strings within content files and properties.

Full-text indexes are created by software components separate from Content Server. The index agent prepares documents for indexing and the index server creates indexes and responds to queries from Content Server. For information on installing the index agent and index server, refer to the *Content Server Full-Text Indexing Installation Guide*. For general information on full-text indexing, refer to the *Content Server Administration Guide*.

You must have System Administrator or Superuser privileges to start and stop index agents or index servers, or disable index agents, and to manage index queue items. You must have System Administrator or Superuser privileges to edit the properties of the index agent configuration object and other full-text configuration objects. Click the links below for topics on:

- [Index agents and index servers, page 478](#)
 - [Starting and stopping index agents, page 479](#)
 - [Starting and stopping index servers, page 479](#)
 - [Suspending and resuming index servers, page 480](#)
 - [Reindexing index servers, page 480](#)
 - [Disabling index agents, page 481](#)
 - [Enabling index agents, page 481](#)
 - [Verifying indexing actions, page 482](#)
 - [Viewing or modifying index agent properties, page 482](#)
 - [Viewing index server properties, page 482](#)
 - [Viewing index server logs, page 483](#)
- [Managing index queue items, page 483](#)
 - [Resubmitting individual objects, page 484](#)
 - [Resubmitting all failed queue items, page 485](#)
 - [Removing queue items by status, page 485](#)
 - [Removing queue items, page 485](#)

- [Viewing queue items associated with an object, page 486](#)
- [Creating a new indexing queue item, page 486](#)

Index agents and index servers

The Index Agents and Index Servers list page shows the index agents and index servers associated with the repository to which you are currently connected.

The index agent exports documents from a repository and prepares them for indexing. A particular index agent runs against only one repository. This page displays the index server with which an index agent is associated.

The index server creates full-text indexes and responds to full-text queries from Content Server.

This section contains information about the following:

- Starting, stopping, suspending, and resuming the index agent and index server
- Reindexing index servers
- Disabling index agents
- Viewing index server properties
- Viewing or modifying index agent properties

You must have System Administrator or Superuser privileges to perform these tasks.

If the repository has a high-availability indexing configuration running, in which multiple, redundant index agents and index servers are installed and multiple, redundant indexes are maintained, the paired index agents and index servers are displayed together, listed under the name of the index.

If the repository has a high-availability indexing configuration running, in which multiple, redundant index server and index agents are installed and multiple, redundant indexes are maintained, the index agents and index servers are displayed on the Index Agents and Index Servers list page. The default names are:

- For the first index, *repositoryname_ftindex_00*
- For the first index server, FAST Fulltext Engine Configuration 00
- For the first and all subsequent index agents, *hostname_IndexAgent1*
- For the next index, *repositoryname_ftindex_01*
- For the next index server, FAST Fulltext Engine Configuration



Caution: Stopping an index server or index agent interrupts full-text indexing operations, including updates to the indexes and querying the indexes.

Click the links for instructions to perform the following tasks:

- [Starting and stopping index agents, page 479](#)
- [Starting and stopping index servers, page 479](#)
- [Suspending and resuming index servers, page 480](#)

- Reindexing index servers, page 480
- Disabling index agents, page 481
- Enabling index agents, page 481
- Verifying indexing actions, page 482
- Viewing or modifying index agent properties, page 482
- Viewing index server properties, page 482
- Viewing index server logs, page 483

Starting and stopping index agents

Use these instructions to stop a running index agent or start an index agent that is stopped.

If the index server is stopped and you try to start its associated index agent, you are asked whether you want to also start the index server. If the status of the index server is **Not Responding**, you cannot start or stop the index server, but you can start or stop the associated index agent.

An index agent that is disabled cannot be started and is not started automatically when its associated Content Server is started. You must enable the index agent first. For information on enabling a disabled index agent, refer to [Enabling index agents, page 481](#). If the index agent's status is **Not Responding**, examine the machine on which it is installed and ensure that the software is running.



Caution: Stopping the index agent interrupts full-text indexing operations, including updates to the index and queries to the index. An index agent that is stopped does not pick up index queue items or process documents for indexing.

To start or stop an index agent:

1. Connect to the repository as a user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index agent.
4. To start the index agent, select **Tools > Start**.
5. To stop the index agent, select **Tools > Stop**.
6. Confirm that you want the index agent started or stopped.
The index agent's status changes to running or stopped.

Starting and stopping index servers

Use these instructions to stop a running index server or start an index server that is stopped. If you stop an index server, its associate index agent is also stopped, and you are informed that the index agent will be stopped as well.

If the index server's status is **Not Responding**, attempt to retrieve and examine the logs, using the instructions in [Viewing index server logs, page 483](#). If you cannot retrieve the logs, examine the machine on which the index server is installed and determine whether it is running.

When you stop the index server, wait a few minutes before attempting to restart it.



Caution: Stopping the index server interrupts full-text indexing operations, including updates to the index and queries to the index.

To start or stop an index server:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index server.
4. To start the index server, select **Tools > Start**.
5. To stop the index server, select **Tools > Stop**.
6. Confirm that you want the index server started or stopped.
The index server's status changes to running or stopped.

Suspending and resuming index servers

Use these instructions to suspend a running index server and resume an index server that is suspended.

To suspend and resume an index server:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index server.
4. To suspend the index server, select **Tools > Suspend Server**.
5. To resume the index server, select **Tools > Resume Server**.
6. Confirm that you want the index server suspended or resumed.

Reindexing index servers

An existing index may become corrupted because of disk failure or corruption, host failure, or the unexpected shutdown of the index server. When the index is corrupted, you might want to reindex the repository. Reindexing the repository rebuilds the existing index by replacing entries in the index.

Use these instructions to reindex an index server.

To reindex an index server:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index server.
4. To reindex the index server, select **Tools > Reindex Server**.
5. Confirm that you want the index server reindexed.

Disabling index agents

An index agent that is disabled cannot be started and is not started automatically when its associated Content Server is started. You can disable an index agent only after it has been stopped. To start a disabled index agent that is not running, you must enable the index agent first, using the instructions in [Enabling index agents, page 481](#).

You may wish to disable an index agent if the computer on which the index server is installed has had a hardware failure or if the index agent itself has failed.

To disable an index agent:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index agent.
4. If the index agent is running, select **Tools > Stop**.
5. Select **Tools > Disable**.
6. Confirm that you want the index agent disabled.

The index agent's status changes to disabled.

Enabling index agents

An index agent that is disabled cannot be started (if it is stopped) and is not started automatically when its associated Content Server is started. You must first stop the index agent if it is running. Use these instructions to enable a disabled index agent.

To enable a disabled index agent:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the correct index agent.
4. If the index agent is running, select **Tools > Stop**.
5. Select **Tools > Enable**.

6. Confirm that you want the index agent enabled.
The index agent's status changes to running.
7. Restart the index agent.

Verifying indexing actions

You are asked to confirm stopping, starting, suspending, resuming, and reindexing index agents or index servers, and enabling or disabling index agents. The confirmation page displays the action you requested. Click **OK** to continue with the action or **Cancel** to stop the action.

Viewing or modifying index agent properties

Use these instructions to view the properties of an index agent. You can modify the following index agent properties, but it is recommended that you do not change the values:

- Exporter Thread Count

This is the number of concurrent exporter threads run by the index agent. The default value is 3. If you change the exporter thread count, you must restart the index agent for the change to take effect.

- Polling Interval

This is the frequency, in seconds, at which the index agent polls for queue items. The default value is 60.

All other properties are read-only.

To view or modify index agent properties:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select the index agent and then select **File > Properties**.
4. If required, modify the exporter thread count or polling interval properties.
It is recommended that you do not modify the default values.
5. Click **OK** to save the changes or **Cancel** to exit without saving.

Viewing index server properties

You cannot modify the properties of an index server. To view the properties of an index server, click the **Info** icon. The following properties are displayed:

- The index server name

This is the object name of the configuration object.

- The name of the host on which the index server is running
- The base port number used by the index server

The default value is 13000.

- Collection name

The name of an index collection, which typically contains the index data for a particular repository.

- Description

A description of the collection, including the repository for which the collection contains the index data.

- Cluster

The search cluster to which the collection belongs. The default name is webcluster.

- Pipeline

The document processing pipeline for a particular collection. The default value is DFTXML.

For 5.3 repositories with the indexing software installed, only one row is displayed because a 5.3 index server managed only one collection. In 5.3 SP1 and later repositories, an index server can manage multiple collections.

Viewing index server logs

You can view the logs produced by the index server.

To view the logs of an index server:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Agents and Index Servers**.
3. Select an index server.
4. Select **View > Get Index Server Logs**.
A zip file containing the logs is produced.
5. Save the zip file to the local drive.
6. Unzip the compressed file and view the logs.

Managing index queue items

Creating, versioning, or deleting a SysObject or SysObject subtype creates a queue item indicating that the full-text indexes must be updated to account for the changes. The index agent reads items from the queue and ensures that the required index updates take place.

If the repository's indexing system runs in a high-availability configuration, with multiple index agents and index servers, each index agent/index server pair supports its own index. Creating,

versioning, or deleting a SysObject or SysObject subtype creates a queue item for each pair and each index is updated.

This page lists index queue items for the current repository. To sort the queue items, click the **Object ID**, **Object Name**, **Object Type**, **Task Status**, **Acquired by**, or **Creation Date** links. The **Object Name** and **Object ID** columns list the object name and object ID of the object to be indexed, not the index queue item. If you click the Info icon for a queue item, the properties of the object to be indexed are displayed, not the queue item's properties.

If the indexing system is in a high-availability configuration, the name of each index is displayed at the top of this page and only the queue items for one index at a time are displayed. To change which index's queue items are displayed, click the name of index.

To change the number of queue items displayed, select a different number in the **Show Items** drop-down list.

By default, the list page displays failed queue items. To filter the queue items by status, choose the appropriate status on the drop-down list:

- **Indexing Failed**, which is the default status displayed

If indexing failed, information about the error is displayed in red under the queue item's name and other properties.

- **All**, which displays all current queue items in the repository
- **Indexing in Progress**, which indicates that the object is being processed by the index agent or index server
- **Awaiting Indexing**, which indicates that the index agent has not yet acquired the queue item and started the indexing process
- **Warning**, which indicates that the index agent encountered a problem when it attempted to start the indexing process for the object

If indexing generated a warning, information about the problem is displayed in red under the queue item's name and other properties.

Queue items that have failed indexing can be resubmitted individually, or all failed queue items can be resubmitted with one command.

Click the links for information on the following topics:

- [Resubmitting individual objects, page 484](#)
- [Resubmitting all failed queue items, page 485](#)
- [Removing queue items by status, page 485](#)
- [Removing queue items, page 485](#)
- [Viewing queue items associated with an object, page 486](#)
- [Creating a new indexing queue item, page 486](#)

Resubmitting individual objects

You can resubmit individual objects for indexing.

To resubmit individual objects:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Queue**.
3. If the repository's indexing system is installed in a high-availability configuration, ensure that the index queue for the correct index is selected.
4. Choose an object.
5. Select **Tools > Resubmit Queue Item**.

Resubmitting all failed queue items

You can resubmit for indexing all documents that failed indexing. This menu choice executes the `mark_for_retry` administration method. If the indexing system is installed in a high-availability configuration, all failed queue items for all indexes are resubmitted.

To resubmit all objects that failed indexing:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Queue**.
3. Select **Tools > Resubmit all failed queue items**.

Removing queue items by status

Use these instructions to remove index queue items by status.

To remove queue items by status:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Queue**.
3. If the repository's indexing system is installed in a high-availability configuration, ensure that the index queue for the correct index is selected.
4. Select **Tools > Remove Queue Items by Status**.
5. Select the correct status.

Removing queue items

Use these instructions to remove queue items from the indexing queue. Note that if a queue item has already been acquired by the index agent, it cannot be removed from the indexing queue.

To remove queue items:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to **Administration > Indexing Management > Index Queue**.
3. If the repository's indexing system is installed in a high-availability configuration, ensure that the index queue for the correct index is selected.
4. Select the queue items.
5. Select **Tools > Remove queue items**.

Viewing queue items associated with an object

From a repository's cabinets, you can view the index queue items associated with a particular object.

To view the queue items associated with an object:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to the object in the repository's cabinets.
3. Select the object.
4. Select **Tools > View Queue Items**.
The queue items are displayed for the selected index queue.
5. If the repository's indexing system is installed in a high-availability configuration, optionally click the links for each index queue.

Creating a new indexing queue item

You can create a queue item to submit a particular SysObject for indexing.

To create a queue item and submit and a particular object for indexing:

1. Connect to the repository as user who has System Administrator or Superuser privileges.
2. Navigate to the object in the repository's cabinets.
3. Select the object.
4. Select **File > New > Create queue item**.
The index queue and new queue item are displayed.

5. If the repository's indexing system is installed in a high-availability configuration, optionally click the links for each index queue.

Chapter 16

Content Transformation Services Administration

This chapter explains how to perform administration tasks for Content Transformation Services (CTS) products using Documentum Administrator.

Content Transformation Services (CTS) is the name for the architecture behind the Documentum products Document Transformation Services, Advanced Document Transformation Services, Regulatory Publishing Transformation Services, Media Transformation Services and a number of add on components that work in synch with those products. The Content Transformation Services Administration component appears in Documentum Administrator if at least one Content Transformation Services product instance is installed and configured on a repository. This check is done through executing the DQL/DFC call to find the presence of at least one `cts_instance_info` object in the repository.

Although you are always connected to a single repository in Documentum Administrator, there could be multiple CTS instances polling the repository. All CTS instances polling the repository are displayed when you select the Content Transformation Services group in the Administration node. You must select at least one CTS instance before you can perform any administration tasks on it.

Links to CTS administration tasks are available in the Administration Node. If a CTS instance has been configured for the current repository, all tasks are contained within a Content Transformation Services group on the main Administration page.

Click the links below for information and instructions on:

- [Changing the CTS user, page 489](#)
- [Configuring a CTS instance, page 490](#)
- [Viewing a CTS log file, page 493](#)
- [Viewing details of a CTS instance, page 494](#)
- [Controlling your CTS instance, page 494](#)
- [CTS reporting, page 496](#)

Changing the CTS user

This feature allows you to change the user name that a CTS instance uses to log in to the repository. This utility queries the repository for a list of applicable users (with at least Superuser or System

Administrator privilege) and displays them in a list. To change the CTS user, the user's password is required.

To change the user name used by the CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance from the list of available instances.
5. Click **Tools > Content Transformation Services > Change User**.
6. Select a user name that is available for the repository from the **User name** drop-down.
7. Enter the user's password in the **Password** field.
8. Enter the user's password again in the **Confirm Password** field.
9. Enter the user's domain in the **Domain** field if it is required on your system.
10. Click **OK**.

Configuring a CTS instance

This feature allows you to update some of the CTS configuration parameters.

The following tasks are possible through the Configure CTS instance screen:

- [Changing the polling interval, page 490](#)
- [Changing the logging level, page 491](#)
- [Changing the System Operator, page 491](#)
- [Changing the notification setting, page 492](#)
- [Changing the maximum number of queue items, page 492](#)
- [Changing the queue item expiry, page 493](#)

Changing the polling interval

The polling interval is the amount of time in seconds that the instance will wait between polls. This should not be less than 2 seconds.

To change the polling interval of a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to configure from the list of available instances.

5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, enter a number to represent the polling interval in the **Polling interval** field.
The minimum interval time is 2 seconds.
7. Click **OK**.

Changing the logging level

The logging level value controls how much information will be recorded in the CTS log files.

Note: As more information is logged (that is, a higher logging level), it affects both the application's performance as well as the amount of storage space on the CTS host.

The available (log4j) logging levels are as follows:

- **ERROR** Includes error events that may still allow the application to continue running.
- **DEBUG** Includes fine-grained informational events that are most useful when debugging an application.
- **WARNING** Includes potentially harmful situations.
- **INFO** Includes informational messages that highlight the progress of the application at coarse-grained level.

To change the logging level of a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, select a value for the new logging level from the **Logging Level** drop down.
7. Click **OK**.

Changing the System Operator

The System Operator is the name of the user that receives messages from an instance of CTS.

To change the operator used by an instance of CTS:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.

4. Select the CTS instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, select a user name from the **Operator** drop down.
7. Click **OK**.

Changing the notification setting

The notification setting controls whether notifications (both successful notifications and notifications of errors or warnings) should be sent to each individual user requesting a transformation through a CTS product.

To change the notification setting for an instance of CTS:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, select either **YES** or **NO** in the **Send Notification** drop down.
7. Click **OK**.

Changing the maximum number of queue items

The value for a maximum number of queue items controls how many items the CTS instance adds for processing each time it polls the queue. The default is 10 items.

To change the maximum number of queue items for a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, enter a number to represent the maximum number of queue items for the CTS instance in the **Max Queue Items to Sign Off** field.
7. Click **OK**.

Changing the queue item expiry

The queue item expiry is the amount of time an item will be sitting on a queue before being deleted from the queue. You must also indicate the measurement of time you wish to use. Use 's' to indicate intervals in seconds, 'm' for minutes, 'h' for hours and 'd' for days. For example, a value of 2 m indicates that an item is removed from the queue when 2 minutes passes from the time it was originally created until the time of the poll.

To change the queue item expiry:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to configure from the list of available instances.
5. Click **Tools > Content Transformation Services > Configure**.
6. In the Configure CTS instance screen, enter a number to represent the queue item expiry time in the **Max Queue Item Age** field.
7. Select a time measurement value from the drop down.
8. Click **OK**.

Viewing a CTS log file

Log files are created for each CTS product and component. The contents and detail level of each log file depend on the log file setting you have chosen for the CTS instance (see [Changing the logging level, page 491](#)).

The log files screen lists available log files on the CTS host and allows you to choose a log file for viewing. The selected log file opens in a new window.

To view a CTS log file:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to view log files for from the list of available instances.
5. Click **Tools > Content Transformation Services > View Log File**.
6. In the Log File List screen, navigate through the list to locate a log file you wish to view. Select the log file checkbox and click **OK**.

The selected log file opens in a new window.

Viewing details of a CTS instance

The CTS instance details screen does not allow you to perform any updates for the instance it is merely informative. It lists some crucial information with regards to a CTS instance, such as:

- **Product** Possible values include Document Transformation Services, Advanced Documentation Transformation Services, Regulatory Publishing Transformation Services, Media Transformation Services, Audio/Video Transformation Services, and Medical Imaging Transformation Services.
- **Version** The version number of each product.
- **Hostname** The name of the host machine for each product.
- **Status** The current status (Running or Stopped).
- **Started On** The time and date that this instance was last started.

The number of queued items and the number of items processed by the CTS instance are displayed in the top right corner of the screen.

In addition, some information about the Plug-ins that are installed with this instance are provided. This includes the Plug-in name, a description of the Plug-in, and its status.

To view details for a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to view details for and select **View > Properties**.
5. The details for the selected CTS instance are displayed.
When you are finished viewing the details, click **Close**.

Controlling your CTS instance

CTS administration allows you to view some details about a CTS instance, such as the products running on the instance and details about those specific products. The CTS instance details screen also allows you to select a particular CTS product and either start, stop, or refresh it.

You can also start, stop, and refresh an entire CTS instance through easily accessible menu items.

The following tasks are possible through the Control CTS Service screen:

- [Stopping the CTS service, page 495](#)
- [Starting the CTS service, page 495](#)
- [Refreshing the CTS service, page 495](#)

Stopping the CTS service

You can stop a CTS service when the instance is currently running. Any items that are currently in the processing queue are removed.

To stop a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to stop from the list of available instances.
5. Do one of the following:
 - Click **Tools > Content Transformation Services > Stop**.
 - Select the CTS instance that you want to stop from the list of available instances and select **View > Properties**.

On the CTS Instance Details screen, click **Stop**.

The Status for the CTS instance changes to Stopped.

Starting the CTS service

You can start a CTS service when the instance is currently stopped. The CTS instance activated date and time is refreshed to show the correct date and time of activation.

To start a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to start from the list of available instances.
5. Do one of the following:
 - Click **Tools > Content Transformation Services > Start**.
 - Select the CTS instance that you want to start from the list of available instances and select **View > Properties**.

On the CTS Instance Details screen, click **Start**.

The Status for the CTS instance changes to Running.

Refreshing the CTS service

Refreshing a CTS instance forces it to re-initialize its configuration files without stopping and starting the service. This is typically used after updating some of the CTS configuration files. The CTS

instance activation date and time is refreshed to show the correct date and time of activation. The CTS queue is unaffected by a refresh.

To refresh a CTS instance:

1. Connect to the repository where the CTS instance is located.
2. Click the **Administration** node.
3. Click the **CTS Instances** node or link.
4. Select the CTS instance that you want to refresh from the list of available instances.
5. Do one of the following:
 - Click **Tools > Content Transformation Services > Refresh**.
 - Select the CTS instance that you want to refresh from the list of available instances and select **View > Properties**.
On the CTS Instance Details screen, click **Refresh**.
6. You may receive an Instance Refresh notification. Selecting **Do not show this again** will prevent this screen from appearing in the future. Click **Ok** to proceed with the refresh.
The CTS instance is refreshed.

CTS reporting

CTS reporting allows you to monitor your CTS product activities. Data such as number of transformation requests in a time frame, number of successful transformations, number of failed transformations, errors, and file sizes can all be used to monitor the success and usage of your CTS products.

This information is contained in a table on the repository. At regular intervals, or when the table reaches a certain size, the data is copied to an archive table and the main table is cleared. This allows for better CTS performance on your repository.

To enable or disable CTS reporting, refer to the Administration Guide for your CTS product.

This section contains the following topics:

- [Configuring CTS reporting, page 496](#)
- [Viewing archived CTS reporting data, page 497](#)

Configuring CTS reporting

Report configuration is performed on a repository. This means that all CTS instances that are configured for the current repository will follow this configuration.

To configure CTS reporting:

1. Connect to the repository where one or more CTS instances have been configured.
2. Click the **Administration** node.

3. Click the **CTS Reporting Configuration** node or link.
4. Configure the values as required:
 - **Archiving Interval** refers to the number of days between archiving. The default value is 1, meaning the table data is archived daily.
 - **Archiving Data Size** refers to the number of rows in the table before the table data is archived. The default value is 10,000.
 - **Archiving Monitor Interval** refers to the number of seconds between checks to the archiving interval and data size. The default value is 60, meaning the monitor will check every 60 seconds to see if either the archiving interval value or the archiving data size has been met. When either of the conditions has been met, the reporting data is archived.
5. Click **OK**.

Viewing archived CTS reporting data

Archived CTS reporting data is viewable only through Documentum Digital Asset Manager. When a user enters start and end times, Digital Asset Manager returns reporting data that is applicable to that reporting period. The data is viewable as a Microsoft Excel spreadsheet.

Regular users can view their own CTS reporting data. Administrator users can view all CTS reporting data.

To view archived CTS reporting data:

1. Login to the repository you want to view data for, using Digital Asset Manager.
2. Select **Tools > Transformation Report**.
3. Enter a value for the **Report Name**. This can be any name, and will be used to name the Excel spreadsheet file. An object ID will be appended to the Report Name.
4. Enter a **Start Time** and **End Time** for the reporting period you wish to view.
5. Click **OK**.

An Excel spreadsheet opens, containing the data for the selected reporting period.

Chapter 17

Content Intelligence Services

Content Intelligence Services (CIS) is an EMC Documentum product that automatically categorizes documents based on an analysis of their content or their metadata. Use the items under the Content Intelligence node to:

- Create the taxonomy of categories into which CIS assigns documents.
- Identify the property rules and the keywords and phrases that the Content Intelligence Services server (CIS server) uses as evidence terms to determine whether a document belongs to a category or not.
- Select documents for CIS processing and set the processing schedule.
- Review and approve the automatic categorization of documents.
- Manually categorize documents.

This chapter explains how to configure CIS and categorize documents using Documentum Administrator. The *Content Intelligence Services Installation Guide* provides information on the installation of the CIS server.

The *Content Intelligence Services Administration Guide* provides information about the option to import predefined taxonomies from specially formatted XML files, then manage them with Documentum Administrator.

Understanding Content Intelligence Services

Content Intelligence Services organizes documents into *categories* that are maintained in a taxonomy. A taxonomy is a hierarchical set of categories used to organize content in the repository based on a set of criteria different from the cabinet and folder structure. This alternate organization, often based on the subject matter of the content, provides a place for users to look for all content related to common topics of interest.

For example, suppose that the folders in repository cabinets organize objects based on which department created the content or on the document type, such as Press Releases in one folder and Product Design Specifications in another folder. A user looking for all available information about a particular product including documents from multiple departments, and both press releases and design specifications needs to look in all folders that could possibly include objects related to that topic. With product-based categories, the user can look in a single category to find all documents related to the product, while the documents themselves remain filed in the original folders.

Content Intelligence Services can assign documents to relevant categories based on a semantic analysis of their content. When you define your corporate taxonomy, you identify key words and phrases associated with each category. CIS uses these words and phrases as *evidence terms*: when the server processes a document, it assigns the document to categories based on the evidence terms it finds in the content.

For example, the definition of a category called Internet Service Provider might identify the acronym ISP and the names of specific ISP vendors as evidence terms. When CIS server analyzes a document and finds the words ISP and Earthlink in the content, it determines that the document belongs in the category Internet Service Provider.

When required, you can also configure CIS to classify documents based on the property values (document metadata). In this case, documents are assigned according to the values of the repository attributes. This may be an essential condition for documents to match with a category.

As CIS server processes a document, it determines the document's *confidence score* for each category in the taxonomy. The confidence score reflects how much evidence CIS server found to indicate that the document belongs in the category. If the document's score for a category exceeds a predefined high threshold, CIS server assigns the document to that category. If the confidence score falls just short of the threshold, CIS server can provisionally assign the document to the category as a Pending candidate. The user who owns the category must review pending document candidates before they are fully categorized.

When a document is assigned to a category, it can be linked to the folder associated with the category. Depending on how you configure CIS, it may also add the category names to an attribute of the document.

Content Intelligence Services also supports *manual categorization*, where users (rather than CIS server) manually assign documents to categories. Just as with automatic CIS server processing, category assignments can be used to link documents into a searchable hierarchy of category folders, add the category names to a document attribute, or both. You can specify whether manually assigned documents require review from the category owner before they are fully assigned.

Categorizing documents

The primary steps involved in Content Intelligence Services processing are:

- Choose how category assignments are reflected in the repository
- Create a taxonomy of categories
- Provide evidence terms for each category
- Submit documents for categorization
- Review and approve the proposed categorization

The first three steps are setup tasks that you perform as part of configuring Content Intelligence Services and infrequently after that. The remaining steps represent the day-to-day operation of Content Intelligence Services.

Choosing categorization options

You can decide how to reflect category assignments in the repository. Content Intelligence Services can record category assignments in two ways:

- **Link to Folders:** CIS maintains a set of folders whose names and hierarchy correspond to the categories in the taxonomy. When a document is categorized, CIS creates a relationship between the document and the category. When users view the category folder in DA, they see the assigned documents, but the documents are not linked into the folder in the same way documents are linked into folders in other parts of the repository. When you select this option, however, CIS creates a full link between the document and the folder in addition to its normal assignment relation.
- **Assign as Attributes:** When a document is categorized, CIS writes the names of assigned categories in the attributes of the document. The category class definition specifies which document attribute is updated.

You can configure CIS to record category assignments in both of these ways, one of them, or neither. If neither Link to Folders or Assign as Attributes is active, Webtop users and Documentum Desktop users are not able to see the category assignments.

Note: You should select these options only when you know you need the functionality they provide. Default CIS processing is adequate in most cases.

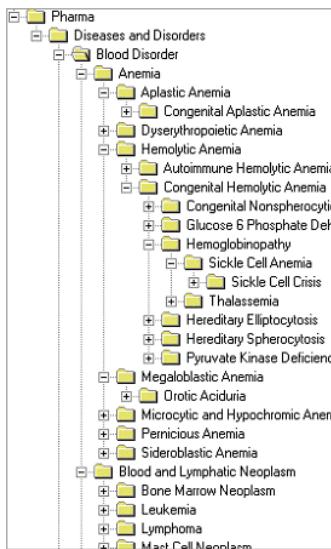
For information about setting CIS configuration options, see [Modifying Content Intelligence Services configuration, page 508](#).

Creating taxonomies and categories

The most critical factor in the success of a Content Intelligence Services implementation is defining categories appropriate for the documents to be organized. The categories need to be relevant to the documents, and the relationship between categories needs to be clear enough for users to easily determine which category will contain the content they are looking for. For automatic processing, each category needs to include specific, unambiguous evidence terms that CIS server can use to accurately assign documents to the category.

CIS categories are arranged into hierarchical structures known as *taxonomies*. When you create categories, you define their position in the taxonomy, the property rules that a document must meet in order to be assigned to each category, and the evidence terms the words and phrases that CIS server uses to understand the document content and determine which categories each document belongs in. The structure of the taxonomy determines the relationships between the categories and provides the tree structure that users navigate to locate documents. A category can appear in more than one place in a single taxonomy, or in multiple taxonomies.

A taxonomy organizes categories into a conceptual hierarchy. Typically, the categories below a given node in the taxonomy have a kind of or narrower term relationship to the parent node: in the figure below, for instance, Anemia is a kind of Blood Disorder, and Aplastic Anemia and Hemolytic Anemia are kinds of Anemia (and by extension kinds of Blood Disorders).

Figure 20. Partial pharmaceutical taxonomy

Taxonomies can organize content based on industry-standard classifications or a custom classification. For example, the partial pharmaceutical taxonomy shown in the figure classifies concepts according to the nature of the disorder using industry-standard Medical Subject Headings (MeSH) classification.

Content Intelligence Services includes several pre-built starter taxonomies that you can import then adapt to your situation. These taxonomies are XML files in taxonomy exchange format (TEF), which you can import then manage in Documentum Administrator. If none of them are a close match, you can build taxonomies from scratch using Documentum Administrator or TEF.

If you plan to process documents from multiple subject areas, you can create separate taxonomies for each area. One advantage to separate taxonomies is that they can be maintained separately by different subject matter experts.

[Building taxonomies, page 509](#) provides information about creating taxonomies and defining categories. The *Content Intelligence Services Administration Guide* provides information about importing TEF taxonomies.

Providing category evidence

Category definitions include evidence, which tell CIS server what words and phrases are likely to appear in documents that belong in the category. This section includes information about:

- [Confidence values and document scores, page 502](#)
- [Stemming and phrase order, page 504](#)
- [Category links, page 505](#)

Confidence values and document scores

Each category definition lists the words and phrases that serve as evidence that a document belongs in the category. These words and phrases are called *evidence terms*. When CIS server analyzes a

document, it reviews all the content of the document, looks for these terms, and determines whether to score a hit based on which terms it finds. Based on the number of hits, CIS server calculates a *document score* for each category.

Each evidence term in the category definition has a *confidence value* assigned to it. The confidence value specifies how certain CIS server can be about scoring a hit for a document when it contains the term. For example, if a document includes the text IBM, CIS server can be nearly certain that the document relates to the category International Business Machines. Therefore, the confidence level for the term IBM is High.

Other pieces of evidence may *suggest* that the category might be appropriate. For example, if a document includes the text Big Blue, CIS server cannot be certain that it refers to International Business Machines. The confidence level is Low, meaning that CIS server should score a hit for the category International Business Machines only if it encounters the text Big Blue *and* other evidence of the same category in the document.

You can also *exclude* evidence terms. For example, suppose you have a category for the company Apple Computers. The term Apple is certainly evidence of the category. However, if the term fruit appears in the same document, you can be fairly sure that Apple refers to the fruit and not the company. To capture this fact, you would add fruit as excluded evidence term to the Apple Computers category.

Finally, you can define terms as *required* terms. In this case, the document must contain at least one Required term. If only Required terms are defined for the category, then only one is sufficient to assign the document to the category. If the evidence terms are not only Required terms, then the document must contain one Required term and have a confidence score high enough for the category.

The confidence values for evidence terms are integers between 0 and 100.

When you set confidence values in Documentum Administrator, you can choose a predefined confidence level or enter a number directly. The predefined values are:

- **High:** Equivalent to the confidence level 75.
- **Medium:** Equivalent to the confidence level 50.
- **Low:** Equivalent to the confidence level 15.
- **Supporting:** This evidence by itself does not cause CIS server to score a hit for a document. However, it increases the confidence level of other evidence found in the same document.
- **Exclude:** If one of the evidence terms found in a document has this confidence level, then the document will never be assigned to this category.
- **Required:** These terms are must-have terms but they are not taken into account for the document's score.

If the resulting score exceeds or meets the category's on-target threshold, CIS server assigns the document to the category. If the score is lower than the on-target threshold but higher than or equal to the candidate threshold, CIS server assigns the document to the category as a Pending candidate; the category owner must review and approve the document before the assignment is complete. If the score falls below the candidate threshold, CIS server does not assign the document to the category.

Stemming and phrase order

CIS server linguistic analysis module uses *stemming* to recognize related words and treat them as a single evidence term. Stemming means extracting the common root, or stem, from expressions that differ only in their grammatical form. For example, the words parked, parks, and parking share the same stem (park), and CIS server recognizes them as four instances of the same evidence term rather than as four different terms.

You may want certain evidence terms not be stemmed. For example, if you define the term Explorer as in Microsoft Internet Explorer, you do not want CIS server to recognize other forms of the word as the same term. When you turn off stemming, CIS server looks for an exact match with the defined term. In our example, CIS server would consider the word explorers as a separate term. Turning off stemming for a term means that CIS server will not recognize even the plural form of a noun or different forms of the same verb. When you turn off stemming, make sure you explicitly add as terms all of the forms you want CIS server to recognize.

Another example is when you want CIS server to treat different forms of the same stem as separate terms; for example, if you want to use provider and provide as evidence of different categories.

CIS provides out-of-the-box stemming capability for the English language. To use the stemming option for other languages, you need to install language dictionaries, as described in the *Content Intelligence Service Administration Guide*.

Setting the language used for the stemming

The language used for the stemming can be defined either for the documents, for the categories, or for both of them.

When you specify the language of a document, the text of the document is analyzed and stemmed according to this language. Then the result of the analysis is compared with the evidence terms of categories of the same language or which language is not defined. Note that defining a language for a category acts as a filter: *a document will never be assigned to a category of a different language*.

To set the language for the documents that you want to classify, you can either set it for every document or for an entire document set. When a language is set for a document set, it prevails over the language set for individual documents. This prevents from classification errors if the document language is not correctly set. Note that you can only select one language per document. If the document set is made of many documents in different languages, then the language must be set at the document level and not at the document set level. When no language is defined for the documents or for the document sets, if the stemming is activated, the language used is the one defined in the CIS server configuration. The *Content Intelligence Service Administration Guide* describes how to set the default language for CIS server.

You can also define the language of the categories used for the classification. The language can be set for every category or for the entire taxonomy. If the language of a category is not specified, then the language of the taxonomy is used, it does not inherit the language of the parent category, if any. When no language is defined, the language used is the one defined in the CIS server configuration. You also have the possibility to define the language as “Any language”, this means that documents in any language —that is, in different languages— can be assigned to this category.

The following languages are available for the stemming option: English, French, German, Italian, Portuguese, Spanish, Danish, Dutch, Finnish, Swedish, Norwegian Bokmal, and Norwegian Nynorsk.

Activating the stemming

Stemming can be activated at different levels:

- In the category class definition, you can choose to use the stemming on the category names. If you select Use stemming in the category class definition, then it will be the default value for all categories created from this category class.
- In the category definition, you can choose to override the default option inherited by the category class. You can either select or deselect the stemming option.
- For each evidence term (keywords or phrases), you can choose to use the stemming. This option is automatically disabled and grayed out if you selected Any language as the category language.

Retaining the phrase order

When you enter a multi-word phrase as evidence, CIS server by default looks for an exact match with the phrase. If you select the **Recognize words in any order** checkbox, CIS server looks for all of the words in the phrase in the same sentence regardless of their order.

Category links

Categories can include other categories as evidence: when a document is assigned to one category, CIS server can use that assignment as evidence for a related category. For example, when a document is assigned to the category Documentum Content Intelligence Services, you might want it also assigned to the category Documentum. Rather than entering the evidence separately in both categories, you enter it for the category where it makes sense, then tell CIS server to consider documents assigned to that category as candidates for the second category as well. To accomplish this, you link the category Documentum Content Intelligence Services into an evidence set for the category Documentum. Like all evidence, category link evidence has a confidence value associated with it, telling CIS server how much to add to the document's overall score for the current category when the document is assigned to the linked category.

There are three types of category links:

- Explicit category links, for which you identify the category to link into the evidence for this category
- Parent links, for which CIS links all of this category's parent categories into its set of evidence terms
- Child links, for which CIS links all children of this category into its set of evidence terms

Category classes can specify that CIS include Parent or Child links automatically. If a category belongs to a class where these options are set, the evidence for the category will include these links even though they do not appear in the category definition itself.

Submitting documents for categorization

Documents can be submitted to CIS server for categorization in two ways:

- Users of Documentum WDK-based applications, such as Webtop and Web Publisher, can select documents from the repository and submit them for categorization.
- Administrators can create document sets that query the repository for a group of documents and submit them for categorization. A document set can include a repeating schedule that specifies how often it runs its query and submits any new or revised documents to CIS server.

[Submitting documents to CIS server, page 531](#) provides information about submitting documents on demand. [Processing documents, page 528](#) provides information about creating and using document sets.

Reviewing proposed categorizations

When you create a taxonomy, you identify a *category owner* for each category. The category owner is the person or the list of persons responsible for making sure that documents assigned to the category truly belong in the category.

For details about reviewing categorized documents, see [Reviewing categorized documents, page 532](#).

Setting up Content Intelligence Services

The procedure below provides an overview of the steps necessary to get Content Intelligence Services up and running.

Note: CIS server needs to be running when you set up CIS in DA. See *Content Intelligence Services Administration Guide* for details about starting CIS server.

1. Install Content Intelligence Services according to the instructions in the *Content Intelligence Services Installation Guide*.
2. Configure the repositories for Content Intelligence Services, as described in [Configuring Content Intelligence Services, page 507](#).
3. Design and create taxonomies, as described in [Building taxonomies, page 509](#).
4. Synchronize the taxonomies with CIS server.

Synchronizing a taxonomy copies the latest category and taxonomy definitions to CIS server. See [Synchronizing taxonomies, page 527](#).

5. Identify a set of test documents and check them into a folder in the repository.

The set of documents should include representatives of the various types of documents you will be processing with Content Intelligence Services. You will use the documents to test and fine-tune the category definitions.

6. Create a document set that selects the test documents.

For details about creating document sets, see [Defining document sets, page 529](#).

7. Run a test run of the document set and review the resulting categorizations.

For information about test processing, see [Test processing and production processing, page 528](#).

8. Adjust the category definitions as necessary to refine the results.

If CIS does not assign some documents to the categories you expect it to, you may need to revise the evidence associated with the categories. If a document appears in a category it should not, it means that the evidence for that category is too broad: consider adding additional terms. If a document does not appear in a category that it should, it means that the evidence is too restrictive.

When you make changes to category definitions, do not forget to synchronize the taxonomy with CIS server; see [Synchronizing taxonomies, page 527](#).

9. Clear the test assignments, then repeat steps 7 and 8.

Clearing the previous assignments enables you to run the test again. For information about clearing assignments, see [Clearing assignments, page 533](#).

10. When CIS server is categorizing the test documents correctly, run the test again using a different set of documents.

Repeat steps 5 through 9. Running the test with a new set of documents helps confirm that the category definitions are tuned correctly for the complete range of documents, not just for the particular test document set.

11. Synchronize taxonomy in production mode, and run the document set in production mode. You can also schedule the document set run.

12. Bring the taxonomies online.

Set the taxonomy status to online to make it available to users. Users can submit documents for categorization and view category assignments through Documentum Webtop. See [Managing taxonomies, page 526](#).

Configuring Content Intelligence Services

Before using Content Intelligence Services to categorize documents, you must:

- [Enable CIS functionality in the repository whose documents will be processed](#)
- [Set CIS configuration options for the repository](#)

Enabling Content Intelligence Services

Before you can use Content Intelligence Services, you must activate the CIS-related objects in the repositories to which you want to apply CIS processing.

Note: You must be logged in as a user with superuser privileges to enable CIS processing. If you do not have sufficient access, the CIS options do not appear.

To enable CIS functionality for a repository:

1. Navigate to **Administration > Content Intelligence** for the repository you want to process documents from.
2. Click the **Enable repository for category assignments** link.
The **Enable Repository for Content Intelligence** page appears.
3. Enter the path to the cabinet or folder under which taxonomy and category folders appear.
When you create taxonomies and categories, Documentum Administrator creates corresponding folders, one folder for each taxonomy and category with the same hierarchical relationships.
When the [Link to Folders](#) option is active, CIS links categorized documents into the folders corresponding to their assigned categories.
The default location for these folders is in a cabinet named **Categories**.
4. Enter the path to the system folder where Content Intelligence administrative information will be stored. The default path is **/System/Application/CI**.
5. Enter the host names for the production CIS server and the test CIS server. The host name is made of the IP address or DNS name followed by the port number (optional), for example:

192.168.1.250:18460

Default port number is **18460**.

You can define the host names using an IPv6 addresses. When using an IPv6 address, with or without a specific port number, it must be enclosed by square brackets, for example:

[2001:0db8:0:0:0:0:1428:57ab]

[2001:0db8:0:0:0:0:1428:57ab]:5678

CIS enables you to categorize documents in production mode or test mode; see [Test processing and production processing, page 528](#) for details. Although you can use the same CIS server for both production and testing, separate servers are recommended for better performance and availability.

The specified CIS server(s) need be running when you enable the repository.

6. Enter the User Name and password for the CIS server to connect to the repository. The authentication against the repository is required when retrieving documents and assigning documents to categories.
7. Click **OK**.
8. Set the CIS processing options for the repository.

For details, see [Modifying Content Intelligence Services configuration, page 508](#).

Modifying Content Intelligence Services configuration

The Configuration for Content Intelligence page enables you to modify how CIS records category assignments as well as the host names for the CIS servers that process documents from this repository. For an overview of the categorization options, see [Choosing categorization options, page 501](#).

You must be a member of the `ci_taxonomy_manager_role` to configure CIS.

To modify CIS configuration for a repository:

1. Navigate to **Administration** node.
2. In the **Content Intelligence Services** box on the right, click the link **Configure CIS**.
The Configuration for Content Intelligence page appears.
3. Update the host names, and optionally the port numbers, of the CIS production and test servers if necessary.

CIS allows you to categorize documents in production mode or test mode; see [Test processing and production processing, page 528](#) for details. Although you can use the same CIS server for both production and testing, separate servers are recommended for better performance and availability.

The specified CIS server(s) need be running when you configure the repository.

4. Specify whether CIS links assigned documents into a corresponding category folder. This option is not selected by default.

If you do not select the **Link assigned documents into category folders** option, category assignments are not returned as search results, and Documentum Webtop users can view assignments only if you assign them as attributes.

Note: Selecting this option affects system performance during document processing and classification. Do not select it unless you need the functionality it provides.

5. Specify whether CIS adds assigned category names to document attributes by selecting or not the **Update document attributes with category assignments** option . This option is selected by default.

Which attributes CIS updates is determined by the category classes of each category; see [Defining category classes, page 510](#)

6. Enter the Documentum User Name and password for CIS server to use when connecting to this repository.

Select a user account that has appropriate permissions for retrieving documents to process and assigning documents to categories.

7. Click **OK** to validate.

Building taxonomies

The term *taxonomy* refers to two related items in Content Intelligence Services. In most situations it refers to the hierarchy of categories that divide up a particular subject area for content. For example, the term is used in this sense when you refer to the Human Resources taxonomy or the Pharmaceutical taxonomy. A taxonomy in this sense has a root level and any number of categories as direct and indirect children.

Content Intelligence Services also uses the term *taxonomy* to refer to the Documentum object that serves as the root level of the hierarchy. Taxonomy objects represent the top level, much as a cabinet represents the top level of a hierarchy of folders.

The organizational structure of a taxonomy determines the navigation path that users follow to locate documents in the category as well as certain types of inheritance: a category inherits some

default values from the taxonomy definition and can inherit evidence from its children categories, its parent category, or any other category.

Taxonomies consist of three types of Documentum objects:

- **Taxonomy objects** represent the root of a hierarchical tree of categories. The definition of a taxonomy sets default values for its categories and can include property conditions that documents must meet in order to be assigned to categories in the taxonomy. No documents are assigned directly to the root of the taxonomy.
- **Categories** are the headings under which documents are classified. The definition of a category includes the evidence that CIS server looks for in document content to determine whether it belongs in the category.
- **Category classes** define general types of categories. Every category is assigned to a class, which specifies the default behavior of the category.

In addition to building taxonomies using Documentum Administrator, you can import pre-built taxonomies from XML files in taxonomy exchange format (TEF). The *Content Intelligence Services Administration Guide* provides more information about importing taxonomies.

Defining category classes

Each category is part of a category class. The properties of a category class determine the default behavior of categories belonging to the class. Individual categories can override the default behavior. For details about the evidence-handling options, see [Providing category evidence, page 502](#). If you are using the [Assign as Attributes](#) option to write category assignments into each document's attributes, the category class identifies which attribute CIS writes the category names into.

CIS includes one category class by default, named Generic. In many instances, you can configure this category class and use it for all of your categories. You need to create additional category classes only when you need to assign category information to a different attribute or use different rules for generating category evidence.

You can also [delete category classes](#), but you must first reassign all categories to use another category class. You can reassign the categories on the page that displays when you delete the class.

To create or modify a category class:

1. Navigate to **Administration > Content Intelligence > Category Classes**.
A list page appears, showing the available category classes.
2. Select **File > New > Category Class** to create a new category class, or click the  icon next to the category class whose properties you want to set.
The properties page for category classes appears. It has two tabs, one for general category class information and the other for default values.
3. Enter a name and description for the category class.
The name appears in the list of category classes that displays when creating categories. If you are editing an existing category class, the name is read only. The description enables you to enter more descriptive information about the category class.
4. Identify the document attribute into which CIS writes the names of assigned categories.

The classification attribute must be an existing attribute for the object type of documents that will be assigned to categories of this class, and it must be a repeating value attribute, for example, **keywords**. Category names are written into the attribute only if this option is active; see [Modifying Content Intelligence Services configuration, page 508](#) for information about setting the option. Note that the current values of the selected attribute are erased by CIS and replaced by the result of the new categorization. Therefore, end users should not edit this attribute manually.

5. Click the **Default Values** tab.

You use this page to set the default behavior for categories of this class. When you assign a category to this class, the category will use the values from the class unless the user who creates the category changes the option on the New Category screen.

6. Specify how CIS treats the category name as an evidence term for the category.

- a. To have CIS adding the category name as an evidence term, select the **Include Category Name as evidence term** checkbox. If you deselect this option, the next two options are not relevant and are grayed out. Skip to step 7.
- b. To activate the **stemming** option on the category name, select the **Use stemming** checkbox.
- c. To enable the words in multi-word category names to appear in any order, select the **Recognize words in any order** checkbox. When the checkbox is not selected, CIS server recognizes the category name only if it appears exactly as entered.

7. Set the default rules for using evidence from child or parent categories.

When a document is assigned to one category, CIS server can use that assignment as evidence that the document also belongs in a related category. This type of evidence propagation is most common between categories and their parent or children categories. See [Category links, page 505](#) for more information.

- a. To use evidence from parent or child categories by default, select the **Use evidence from child/parent** checkbox. Deselect the checkbox to avoid evidence propagation.
- b. From the drop-down list associated with the checkbox, select **child** to use evidence from child categories as evidence for the current category or **parent** to use evidence from parent categories.

8. Click **Finish** to close the properties page.

To delete category classes:

When you delete a category class already used for existing categories, you are prompted to reassign the categories to another category class.

1. Navigate to **Administration > Content Intelligence > Category Classes**.
A list page appears, showing the available category classes.
2. Select the category classes you want to delete.
3. From the **File** menu, select **Delete**.
A confirmation message appears, asking you to confirm that you want to delete the category class.
4. For category classes that are assigned to existing categories, select an alternate category class for the categories.

When a category class is still in use, the confirmation message page enables you to select which of the remaining category classes is assigned to categories that currently use the deleted class. Choose the class from the **Update categories to use the category class** drop-down list.

5. Click **OK** to delete the category class.

Defining taxonomies

You need to create a taxonomy object before you can create any of the categories in the hierarchy. The taxonomy object sets certain default values for the categories below it.

Since the taxonomy object is the root of a complete hierarchy of categories, it is the object that you work with when performing actions that affect the entire hierarchy, such as copying the latest definitions to CIS server (synchronizing) or making the hierarchy available to users (bringing the taxonomy online). For information about these operations, see [Managing taxonomies, page 526](#).

Every CIS implementation needs to have at least one taxonomy to use for analyzing and processing documents. Depending on the types of documents being categorized, you may want to create multiple taxonomies. Generally you want one taxonomy for each distinct subject area or domain. One advantage to separate taxonomies is that they can be maintained separately, by different subject matter experts, for example.

The Properties page for a taxonomy object can have two or three tabs:

- The **Attributes** tab displays the basic information about the taxonomy, most of which was entered when the taxonomy was created.
- The **Property Rules** tab lists conditions that documents must meet before CIS server will assign them to any category under this taxonomy.
- The **Select Taxonomy Type** tab is displayed if category or taxonomy is subtyped. Using this, you can create your own subtype.

Note: If there are no subtypes, then the **Select Taxonomy Type** tab will not be displayed.

To create or modify a taxonomy:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. To display only taxonomies that you own or only online taxonomies, choose one of the options from the drop-down list in the upper right corner of the list page.
3. Select **File > New > Taxonomy** to create a new taxonomy. To modify a taxonomy, select it and then go to **View > Properties > Info**.
The properties page for taxonomies appear.
4. In the **Select Taxonomy Type** tab, select the taxonomy type from the drop down list to create a subtype.
Click **Next** to proceed or click **Attributes** tab.
Attributes page displays the non-editable subtype of the taxonomy.
5. Enter a name, title, and description for the taxonomy. Only the taxonomy name is mandatory and it must be unique. The title is not mandatory and it is not necessarily unique.

By default, the taxonomy name is the text that appears in the list of taxonomies. However, it is possible to display the taxonomy title instead of the taxonomy name, the procedure [To display the object titles instead of the object names; page 520](#) describes how to switch from the category and taxonomy names to the category and taxonomy titles.

6. Click the **Select owner** link and choose the taxonomy owner. The taxonomy owner can be a person, a list of persons, or groups.

7. Choose the default category class from the drop-down list.

The selected class appears as the default category class when you create categories in this taxonomy. See [Defining category classes, page 510](#) for information about category classes.

8. Select the taxonomy language. The selected language must match with the language of the documents that you want to classify. If the language is different, the documents will never be assigned to a category of this taxonomy.

If the language of a category is not defined, the language set for the taxonomy is used. If no language is set for the taxonomy, CIS server default language is used.

Select **Any language** in the drop down list to match any document's language. For example, you can use this option if you don't plan to activate the stemming and thus, evidence terms are valid in any language, such as patterns for social security numbers or acronyms like EMC. If the option Any language is selected, then it is not possible to use the stemming on the evidence terms of this taxonomy. The Use stemming option in the evidence term definition is then disabled and grayed out.

9. Specify whether the taxonomy is online or offline.

An online taxonomy is available for users to browse and assign documents to. A new taxonomy is offline until you explicitly put it online by selecting **Online** from the **State** drop-down list.

Typically you want to keep the taxonomy offline until you have completed testing it.

10. Set the default on-target and candidate thresholds.

The on-target and candidate thresholds determine which documents CIS server assigns to a category during automatic processing. When a document's confidence score for the category meets or exceeds the on-target threshold, CIS server assigns it to the category. When the score meets or exceeds the candidate threshold but does not reach the on-target threshold, CIS server assigns the document to the category as a candidate requiring approval from the category owner. See [Confidence values and document scores, page 502](#) for details.

The threshold values for the taxonomy object set the default threshold values for categories in this taxonomy. The default values are 80 for the on-target threshold and 20 for the candidate threshold.

11. For previously saved taxonomies, review the synchronization state of the taxonomy.

If the taxonomy has never been synchronized, the status is **Unknown**. See [Synchronizing taxonomies, page 527](#) for information about synchronization.

The synchronization state is not displayed when you are creating a new taxonomy.

12. Click **OK** to close the properties page, or click the **Property Rules** tab to specify criteria that all documents in this taxonomy must meet.

Add property rules to the taxonomy if you want to define rules specific to document attributes. For help using the **Property Rules** tab, see [Defining property rules, page 521](#).

13. Click **OK** to close the properties page.

14. To create or modify the categories in the taxonomy, see [Defining categories, page 518](#) for information about defining categories.
15. To synchronize the taxonomy if you have made any changes to it or its categories, see [Synchronizing taxonomies, page 527](#) for information about synchronization.

Creating subtypes for a taxonomy or for a category

Sub-typing feature enables you to add your own attributes to the dm_object (dm_taxonomy for taxonomies or dm_category for categories) and create a sub-type for that object. You can create a subtype or multiple subtypes by editing/adding the attributes of objects with the tools such as TEF, DA and Web Publisher. The subtype created resides in the repository data dictionary. They inherit the ACL settings from dm_category and dm_taxonomy.

Using Documentum Administrator and TEF, you can create a custom tab for the subtype. For more information refer to [Creating custom tab for the subtype, page 514](#)

Creating custom tab for the subtype

You must use Documentum Application Builder to create the custom tab for a category subtype's attributes. You can configure the Documentum Adminstrator's tab using Documentum Application Builder. After configuring the Documentum Administrator's tab, you can create a custom tab for their subtypes.

If customization for a subtype is not available, Documentum Administrator will use the closest super-type settings that are available for a particular subtype.

Example 17-1. Example 1

MyCat1 is a subtype of Category.

If Documentum Administrator is not customized to recognize MyCat1, it reads MyCat1 as a default category.

Example 17-2. Example 2

MyCat1 is a subtype of Category.

MyCat2 is a subtype of MyCat1.

If Documentum Administrator is not customized to recognize MyCat2, then it reads MyCat2 as MyCat1. If MyCat1 is also not customized, then DA reads MyCat1 and MyCat2 as individual categories.

To create custom tabs for a category subtype's attributes, use the Display Configuration tab in Documentum Application Builder. Using this, you can configure Documentum Administrator tab as needed.

To create custom tab for the subtype:

1. Open the Documentum Application Builder.
2. In the DocApp Explorer, double-click the object types name to open the type editor, and select the Display Configuration tab.

Tip: Tip: Each row in the Scope field represents one scope. A scope does not have a name and is instead identified by its set of scope definitions.

To know more about the scope field, refer to “*Working with Object Types*” in *Documentum Application Builder User Guide*

3. To create and modify tabs on which to display the attributes, perform these actions in the Display Configuration List:

Note:

- The object types parents tabs are inherited. Adding, deleting, editing tabs, or changing the order of the tabs breaks inheritance—that is, changes made to the parents tabs will not be reflected in this types tabs.
- In Desktop, a type attributes Attribute Category field values are used as long as you have not broken inheritance with the parent types display configuration or if a display configuration is not specified for either the type or its parent.
- Tab names are also localizable.
- Web Publisher does not have tabs, so it displays the display configurations as sections on the same page.
- For WDK applications, to display attributes (particularly mandatory ones) on the object properties Info page, specify the Info category.

To add a new tab:

- a. Click **Add**.
- b. Enter a new tab name or choose one of the defaults from the drop-down list.
- c. To add the tab to all EMC Documentum clients, check **Add to all applications**. This tab is shared between all application and any changes to it are reflected in all applications.
- d. Click **OK**.

Note: When you create tabs with identical names in different applications, DAB creates new internal names for the second and subsequent tabs by appending an underscore and integer (for example, dm_info_0) because the internal names must be unique for a type. The identical names are still displayed because they are mapped to their corresponding internal names. When you change locales, DAB displays the internal names, because you have not specified a name to be displayed in that locale. It is recommended that you change them to more meaningful names in the new locales.

Using one of the defaults automatically creates a tab with an identical name, because the default is already used by another application.

Checking **Add to all applications** results in only one tab being created—not several tabs with different internal names and identical display names—and all display names are mapped to that one tab.

- To remove a tab, select the tab name and click **Remove**.
- To rename a tab, select the tab name and click **Rename**.
- To change the order in which tabs are displayed, select the tab and click the up and down arrows.

4. To modify the attributes displayed on a tab, perform these actions in the Attributes in Display Configuration:
 - a. In the Display Configuration List, select the tab in which the attributes you want to modify are displayed. The attributes that are currently displayed on the tab are shown in the Attributes in Display Configuration text box.
 - b. Click **Edit**
 - c. To specify which attributes are displayed on the tab and how they are displayed, perform these actions in the Display Configuration dialog box:
 - To display attributes on the tab, select the attribute in the Available attributes text box and click **Add**.
 - To delete attributes from the tab, select the attribute in the Current attribute list text box and click **Remove**.
 - To change the order in which the attributes are displayed on the tab, select the attribute in the Current attribute list text box and click up or down arrows.

Note: Although you can change the order in which attributes are displayed on a tab in the Desktop Properties dialog box, you cannot change the tab order (that is, the sequence in which you can move the cursor from field to field by pressing the Tab key).

- To display a separator between two attributes, select the attribute above which you want to add a separator and click **Add Separator**.
- To delete a separator between two attributes, select the separator and click **Remove Separator**.

If you have more attributes than can fit on a tab, force some attributes to be displayed on a secondary page in Webtop, select the attribute and click **Make Secondary**.

Note: Desktop does not use this setting. A vertical scrollbar is used when all attributes cannot be displayed in the dialog box at the same time.

To move a secondary attribute back onto the primary tab, select the attribute and click **Make Primary**.

Creating subtype instances

Use Documentum Administrator to create new instances of taxonomies and categories.

To create subtype instances:

1. Click **File > New > Category** or **File > New > Taxonomy**.

When a new instance is created, Documentum Administrator launches the Info screen for the new object. You can customize Documentum Administrator to create subtype instances which is similar to category/taxonomy creation.

The info screen enables you to view and edit attributes of a particular taxonomy or category.

2. Enter a name, title, and description for the category. Only the category name is mandatory and it must be unique. The title is not mandatory and it is not necessarily unique.

By default, the category name is the text that appears in the list of categories and is the name of the folder created to correspond to this category. However, it is possible to display the category title instead of the category name, the procedure [To display the object titles instead of the object names; page 520](#) describes how to switch from the category and taxonomy names to the category and taxonomy titles.

Note: You cannot use the same name for two categories in the same category class. It is generally a good idea to use unique names for all categories regardless of their category class, so that users can distinguish the categories when their names are written in document attributes. You may, however, use the same title for multiple categories.

3. Click the **Select owner** link and choose the owner of this category.

The standard page for selecting user(s) or group(s) appears. The category owner is the user who can approve or reject documents assigned to the category as a candidate requiring approval from the category owner; see [Reviewing categorized documents, page 532](#) for information about the document review process. The user you select is added to the ci_category_owner_role automatically, giving him or her access to the category through Documentum Administrator.

4. Choose the category class from the drop-down list.

The **category class** determines default behavior for the new category as well as the document attribute to which CIS server adds the category name if you are using the [Assign as Attributes](#) option.

5. Enter on-target and candidate thresholds.

The on-target and candidate thresholds determine which documents CIS server assigns to a category during automatic processing. When a document's confidence score for the category meets or exceeds the on-target threshold, CIS server assigns it to the category. When the score meets or exceeds the candidate threshold but does not reach the on-target threshold, CIS server assigns the document to the category as a candidate requiring approval from the category owner. See [Confidence values and document scores, page 502](#) for details.

The default values come from the definition of the taxonomy you selected in order to navigate to this category.

6. Click **OK** to create subtype instance.

To create an instance of a taxonomy or category subtype:

1. Click the **CustomProp** tab to create a custom tab for the subtypes.
2. Enter the custom type for the subtype.
3. Click **OK** to close the properties page, or click the **Property Rules** tab to specify criteria that all documents in this taxonomy must meet.
Add property rules to the taxonomy if you want to apply a specific criteria to all documents before they are considered for categorization in this taxonomy. For help using the **Property Rules** tab, see [Defining property rules, page 521](#).
4. Click **OK** to close the properties page.

Defining categories

When you create a category, you define its position in the hierarchy of categories by navigating into the category that you want to be its parent. The category inherits default values for most of the required attributes from the [taxonomy object](#) at the top of the hierarchy.

The procedure below describes how to create a category and set its basic properties. For information about providing the evidence that CIS server uses to identify documents that belong in the category, see [Setting category rules, page 520](#).

To create a category:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. To display only taxonomies that you own or only online taxonomies, choose one of the options from the drop-down list in the upper right corner of the list page.
3. Select a taxonomy and navigate to the location where you want the category to appear.
The right pane should display the contents of the category that will be the new category's parent.
4. From the menu, select **File > New > Category**.

The properties page for categories appears with three tabs

5. If subtypes have been created, in the **Select Category Type** tab, select the category type from the drop down list to create a subtype.
Click **Next** to proceed or click **Attributes** tab. If no subtypes have been created, directly go to the **Attributes** tab.

Attributes page displays the non-editable subtype of the category.

6. Enter a name, title, and description for the category. Only the category name is mandatory and it must be unique. The title is not mandatory and it is not necessarily unique.

By default, the category name is the text that appears in the list of categories and is the name of the folder created to correspond to this category. However, it is possible to display the category title instead of the category name, the procedure [To display the object titles instead of the object names:, page 520](#) describes how to switch from the category and taxonomy names to the category and taxonomy titles.

Note: You cannot use the same name for two categories in the same category class. It is generally a good idea to use unique names for all categories regardless of their category class, so that users can distinguish the categories when their names are written in document attributes. You may, however, use the same title for multiple categories. For example, if you want a Marketing category in the North America taxonomy and another in the Europe taxonomy, name the categories Marketing (North America) and Marketing (Europe), but use the title Marketing for both. Their position in the hierarchy is sufficient to allow users to distinguish them when navigating.

7. Click the **Select owner** link and choose the owner of this category.

The standard page for selecting a user appears. The category owner is the user who can approve or reject documents assigned to the category as a candidate requiring approval from the category owner; see [Reviewing categorized documents, page 532](#), for information about the document review process. The user you select is added to the ci_category_owner_role automatically, giving him or her access to the category through Documentum Administrator.

8. Select the category class from the drop-down list.

The **category class** determines default behavior for the new category as well as the document attribute to which CIS server adds the category name if you are using the [Assign as Attributes](#) option.

9. Select the category language. The selected language is used to filter the documents that you want to classify. If the language is different, the documents will never be assigned to the category.

If the language of a category is not defined —and whatever the language of the parent category, if any— the language set for the taxonomy is used. If no language is set for the taxonomy, CIS server default language is used.

Select **Any language** in the drop down list to match any document's language. For example, you can use this option if you don't plan to activate the stemming and thus, evidence terms are valid in any language, such as patterns for social security numbers or acronyms like EMC. If the option **Any language** is selected, then it is not possible to use the stemming on the evidence terms of this category. The **Use stemming** option is then disabled and grayed out.

10. Enter on-target and candidate thresholds.

The on-target and candidate thresholds determine which documents CIS server assigns to a category during automatic processing. When a document's confidence score for the category meets or exceeds the on-target threshold, CIS server assigns it to the category. When the score meets or exceeds the candidate threshold but does not reach the on-target threshold, CIS server assigns the document to the category as a candidate requiring approval from the category owner. See [Confidence values and document scores, page 502](#) for details.

The default values come from the definition of the taxonomy you selected in order to navigate to this category.

11. Specify how CIS treats the category name as an evidence term for the category.

- a. To have CIS adding the category name as an evidence term, select the **Include Category Name as evidence term** checkbox. If you deselect this option, the next two options are not relevant and are grayed out.
- b. To activate the **stemming** option on the category name, select the **Use stemming** checkbox. This option is automatically disabled and grayed out if you selected Any language as the category language.
- c. To enable the words in multi-word category names to appear in any order, select the **Recognize words in any order** checkbox. When the checkbox is not selected, CIS server recognizes the category name only if it appears exactly as entered.

12. Set the default rules for using evidence from child or parent categories.

When a document is assigned to one category, CIS server can use that assignment as evidence that the document also belongs in a related category. This type of evidence propagation is most common between categories and their parent or children categories. See [Category links, page 505](#) for more information.

- a. To use evidence from parent or child categories by default, select the **Use evidence from child/parent** checkbox. Deselect the checkbox to avoid evidence propagation.
- b. From the drop-down list associated with the checkbox, select **child** to use evidence from child categories as evidence for the current category or **parent** to use evidence from parent categories.

13. Click **CustomProp** tab to create a custom tab for the subtypes.

14. If the customization for a subtype is not available, Documentum Administrator will use the closest supertype settings that are available for a particular subtype. For more information , refer to [Creating custom tab for the subtype, page 514](#) .

15. Enter the custom type for the subtype.

16. Click **OK**.

The property page closes, and the category appears in the list.

17. Set the category rules.

For details, see [Setting category rules, page 520](#).

Displaying object titles

You have the possibility to display the object title instead of the object names for the taxonomy, category and document objects.

If all titles are defined (for taxonomies, categories, *and* documents), it allows to display the title, which can be more user-friendly, instead of the name, which is used as an identifier.

Note that you cannot choose to display only category titles, or only document titles. The switch works on all objects at once. If the title is not defined for all objects then the column will be empty. In this case, you can display both columns, side by side.

To display the object titles instead of the object names:

1. Locate the taxonomies_component.xml file under the <DA webapp directory>\webcomponent\config\admin\taxonomies directory.
2. Locate the <showobjectname> property.
 - Set the property to **true** to display the category name (default option).
 - Set the property to **false** to display the category title.
3. Save the file.
4. Restart Apache Tomcat service to apply the modification.

Setting category rules

A category's rules determine what documents are assigned to it. The rules fall into two major categories:

- *Property rules*, which set conditions that a document must meet in order to be considered for assignment to the category
- *Evidence*, which list the words, phrases or patterns that CIS server looks for to indicate that a document belongs in the category

Property rules specify category rules based on attributes of the document; evidence specifies category rules based on the content of the document. If the category definition only contains evidence terms then a document must contain these evidence terms to be assigned to the category. If the category definition only contains property rules, then the document or its attributes must meet the conditions

set by the property rules. If the category definition only both evidence terms and property rules, then both must be satisfied for a document to be assigned.

The evidence terms that can be defined in Documentum Administrator for a category can also be divided into two categories:

- *Simple terms* are the key words and phrases for the category, each of which by itself is a good indicator of category membership
- *Compound terms* are groups of words and phrases that work together to indicate category membership. No one term in the group has a high enough confidence value to assign a document to the category, but the presence of multiple terms can cause the total confidence score to cross the on-target threshold.

For many categories, only simple terms are required. As a general practice, we recommend adding only simple terms when you first define a category. You can add compound terms when you are refining your categories to make more subtle discriminations as a result of testing.

Note: Patterns cannot be defined in Documentum Administrator, the *Content Intelligence Services Administration Guide* describes how to define patterns.

To set the rules for a category:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. Navigate to the category whose rules you want to set.
3. Click the  icon in the **Rules** column.
The rules page for the category appears. The right pane of the screen displays property rules for the category; the left pane displays the evidence for the category.
4. Set any property rules based on document attributes.
See [Defining property rules, page 521](#) for details.
5. Define the evidence for the category.
The evidence for a category is divided into simple terms and compound terms. When defining a new category, we recommend adding simple terms; see [Defining simple evidence terms, page 524](#) for details.
See [Defining compound evidence terms, page 537](#) for information about creating compound terms.

Defining property rules

The Rules Summary page for a category shows the rules that CIS server uses to determine which documents it assigns to the category. While evidence terms specify what words and phrases need to appear in the content of a document, property rules define other property conditions, not related to the content, that documents must meet in order to be assigned to the category. The property conditions are based on the repository attributes of the documents. If a document does not meet the defined property conditions, CIS server does not assign it to the category.

The Property rules can be used in conjunction with evidence terms; but they can also be used on their own to assign documents. This way, you can assign documents to categories based on the documents' property values, without even considering the documents' content.

You can also define property rules for a taxonomy as a whole. Any property rule associated with the taxonomy applies to every category within the taxonomy. The taxonomy-level rules appear on the rules page for the category with the taxonomy name displayed in the title of the box.

To set property rules that documents must meet:

1. From the [Property Rules](#) page, click the **Edit** link in the **Category Property Rule** box.
The Property Rules page appears.
2. To require assigned documents to come from a specific folder, click the **Select folder** link next to **Look in:** and navigate to the folder.
When you click **OK** after selecting the folder, the folder appears next to the **Look in** label.
3. To require assigned document to have a particular object type, click the **Select type** link next to **Type:** and select the object type. The default object type is `dm_sysobject`. If you have created custom object types, [To display or hide an attribute:, page 524](#), describes how to make custom object types available in the CIS component.
When you click **OK** after selecting the object type, the type name appears next to the **Type** label.
4. To assign documents based on their attributes, select the **Properties** checkbox and enter the criteria used to qualify documents.
 - a. Select whether all criteria should be met:
 - **ALL** indicates that all rules must be satisfied to assign the document.
 - **ANY** means that the document can be assigned when only one rule is satisfied.By default, all property rules must be satisfied.
 - b. Select the repository attribute whose value you want to test. The list of attributes differs according to the selected object type. If you have created custom attributes, [To display or hide an attribute:, page 524](#), describes how to display custom attributes.
 - c. From the drop-down list in the middle, select the operator that will be used to compare the selected attribute with the test value.
The available operators differ depending on the type of the attribute you selected in the previous step. For example, for a Boolean attribute, the two operators are **equal** and **not equal** and the possible values are **true** or **false**.
The operators **contains** and **does not contain** are only available for string attributes.

The operators **greater than** or **less than** can be used to select string values alphabetically. For example, the string ABD is greater than ABC. You can then assign documents using their title, their author or any other string attribute by alphabetical order, such as: all documents with an author name greater than A and less than C (note that in this case, words starting with C are ignored).

- d. Enter the value to test against in the text box on the right. Values are not case sensitive and accents are ignored.

To define a rule on the Format attribute, you must enter the value as it appears in the document's Property page. For example, to match documents whose format is Microsoft Word Office Word Document 8.0-2003 (Windows), enter the value **msw8**.

To define a rule on any date attribute, the corresponding value should comply to Documentum date standards. [Table 59, page 523](#) demonstrate possible date formats (non-exhaustive list).

Table 59. Date formats for property rules

Date format	Example
mm/dd/yy	02/15/1990
mon dd yyyy	Feb 15 1990
mm/yy	02/90
dd/mm/yyyy	15/02/1990
yyyy/mm	1990/02
yy/mm/dd	90/02/15
yyyy-mm-dd	1990-02-15
dd-mon-yy	15-Feb-90
month yyyy	February 1990
month dd yy	February 15 90
month, yyyy	February, 1990
month dd, yyyy	February 15, 1990

Note that property rules on a date attribute do not take into account the time (hours, minutes, seconds).

- e. To add an additional condition, click the **Add Property** button and repeat steps b through d.
5. Click **OK** to return to the rules page.

Displaying attributes in Property rules

You may need to modify the type list or the attribute list for property rules, to select which attributes you want to display for the property rules.

By default, all the attributes of the selected object type are available, excepted attributes beginning with r_, a_, or i_, such as r_modified_date or a_content_type. To hide attributes that are visible by default, you need to add them to an exclusion list. To make available attributes that are hidden by default, you need to add them to an inclusion list.

Custom types created from dm_sysobject or dm_document object type automatically inherit of the same searchable attributes. The attributes available or excluded for the dm_sysobject or dm_document object types are also available or excluded for the derived object.

The following procedure describes how to display or hide attributes.

To display or hide an attribute:

1. Navigate to C:\Program Files\Apache Software Foundation\Tomcat 5.0\webapps\da\webcomponent\config\admin\category.
2. Open the qualiferrules_component.xml file.
3. Under the <attribute_list> element, you can add an entry for the type whose attribute display you want to modify.

For example:

```
<attribute_list>
  <type id='my_custom_type'>
```

Two <type id> elements already exist for the dm_sysobject and dm_document object types.

4. Under the <type id> element, add the new attributes that should or should not appear in the drop-down menu, respectively in the <exclusion_attributes> and <inclusion_attributes> elements. By default, all the attributes of the selected object type are available; to hide them, add them to the exclusion list.

Attributes that are hidden by default begin with r_, a_, or i_; to make them available, add them to the inclusion list.

For example:

```
<attribute_list>
  <type id='my_custom_type'>
    <exclusion_attributes>
      <attribute>my_custom_attribute1</attribute>
      <attribute>my_custom_attribute2</attribute>
    <exclusion_attributes>
    <inclusion_attributes>
      <attribute>my_custom_attribute3</attribute>
    <inclusion_attributes>
  </type>
</attribute_list>
```

Defining simple evidence terms

The **Simple Terms** box displays words and phrases that are good indicators of category membership individually. Each term has an associated confidence value, which indicates how certainly CIS server can infer the appropriateness of the category when the term appears in a document. For simple terms, the confidence value is generally High. See [Providing category evidence, page 502](#) for more information.

A newly defined category may have one simple term already defined: the name of the category. The category name may appear as text or as the keyword @implied; either option means that CIS server treats the category name as a simple evidence term. The category name or @implied appears if the category class for this category has the **Generate evidence from category name** option set; see [Defining category classes, page 510](#).

If you find during testing that a particular simple term is causing CIS server to assign too many documents to the category, you can convert the simple term into a compound term that is more discriminating. To convert a simple term into a compound term, click the **Add additional terms** link

next to the term that you want to change and follow the instructions in [Defining compound evidence terms, page 537](#).

To define the properties of a category evidence term:

1. Click the **Add a new simple term** link to add a new term, or click the  icon next to a term you want to modify.
The Evidence page appears. For a new term, the **Use stemming** and **Recognize words in any order** checkboxes are set to the default values from the category class for this category.
2. To use a word or phrase as evidence for the category, click the **Keyword** option button and enter the word or phrase in the adjacent text box.
A keyword is a text string that CIS server looks for in the documents it processes.
3. To include another category as evidence for this category, click the **Category** option button and identify the category to use as evidence for this category.
A category link tells CIS server to use the evidence of another category as part of the definition of this category.
 - To use this category's parent category, select **Parent** from the drop-down list.
 - To use this category's children categories, select **Child**.
 - To link to a selected category, select **Category**, then click the **Select category** link that appears to the right of the drop-down list and select the related category from the page that appears.
- See [Category links, page 505](#) for more information about the types of category link.
4. Specify whether CIS server uses **stemming** on the evidence term by selecting or deselecting the **Use stemming** checkbox. This option is automatically disabled and grayed out if you selected Any language as the category language.
5. If the evidence term is a multi-word phrase, specify whether CIS server recognizes the words in any order by selecting or deselecting the **Recognize words in any order** checkbox.
If the checkbox is not selected, CIS server recognizes the phrase only when the words appear in exactly the order they are entered here.
6. Assign a confidence value for the evidence term.
The system assigns High confidence to the term by default, and we recommend this confidence value for most simple terms. To specify a different value:
 - a. Deselect the **Have the system automatically assign the confidence (HIGH) for me** checkbox.
A pair of option buttons appear for setting the confidence level.
 - b. To select one of the system-defined confidence levels, click the **System Defined Confidence Level** button and select a level from the drop-down list box. The system-defined levels are described in [Confidence values and document scores, page 502](#).
 - c. To set a custom confidence level, click the **Custom Confidence Level** button and enter a number between 0 and 100 in the text box.
7. Click **OK** to close the Evidence page.
The evidence term appears in the **Simple Terms** box.
8. Repeat steps 1 to 7 for each simple term.

Managing taxonomies

When you create a taxonomy, it is offline by default. Offline taxonomies are available under the **Administration > Content Intelligence** node for designing and building, but are not available for users to see. To make the taxonomy available to users, you bring it online.

When CIS server categorizes documents, it uses taxonomy and category definitions that are stored locally on the CIS server host machine. Whenever you create or modify any part of a taxonomy, you need to update the taxonomy definition on the CIS server machine. This process is called *synchronization*.

Both of these operations are available for complete taxonomies only, not individual categories or portions of the hierarchy.

This section includes information about these taxonomy management processes:

- [Making taxonomies available, page 526](#)
- [Synchronizing taxonomies, page 527](#)
- [Deleting taxonomies, page 528](#)

Making taxonomies available

When you create a taxonomy, it has an offline status. An offline taxonomy is available through Documentum Administrator, but is not visible to end-users via Webtop. (You can perform test categorizations with an offline taxonomy; see [Test processing and production processing, page 528](#).) Offline status enables you to build, test, and revise the taxonomy before making it available to end-users.

When you bring it online, the taxonomy, its categories, and categorized documents appear to users under the Categories node.

To make a taxonomy available to users in Webtop:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. Select the taxonomy you want to make available then go to **View > Properties > Info**.
3. The properties page for the taxonomy appears, select the Attributes tab.
4. Select **Online** from the **State** drop-down list box.
5. Click **OK**.
The taxonomy now appears to users under the Category node and is available for categorization.

To make a taxonomy unavailable to users in Webtop:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. Select the taxonomy you want to take offline then go to **View > Properties > Info**.

3. The properties page for the taxonomy appears, select the Attributes tab.
4. Select **Offline** from the **State** drop-down list box.
5. Click **OK**.

The taxonomy is no longer visible to users. Existing documents remain in the categories.

Synchronizing taxonomies

The taxonomy and category definitions you create are saved in the repository. When CIS server automatically categorizes documents, it refers to copies of these definitions. Whenever you create or modify any part of a taxonomy, you need to copy the updates from the repository to the CIS server. The process of copying taxonomy and category definitions from the repository to CIS server is called *synchronization*. Updates to the taxonomy are not reflected in automatic processing until you synchronize them.

Note: If any of the categories in a taxonomy include links to categories in other taxonomies, both taxonomies must be synchronized to avoid possible errors.

To synchronize a taxonomy definition:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.

A list of the existing taxonomies appears.

2. Select the taxonomy you want to synchronize.

3. Select **Tools > Content Intelligence > Synchronize**.

The Synchronize page appears. If you selected multiple taxonomies, the page will appear once for each selected taxonomy.

4. Select which CIS servers you want to synchronize with.

You can categorize documents in production mode or test mode, providing a separate CIS server host for each mode; see [Test processing and production processing, page 528](#) for details. Select the checkbox for the production server, the test server, or both. CIS will copy the latest taxonomy definitions to the selected server(s).

5. Click the **OK** button to start the synchronization.

If you selected multiple taxonomies at step 2, a **Next** button appears in place of the **OK** button until you have selected servers for each taxonomy. The synchronization for all selected taxonomies occurs together.

The synchronization process starts, and the list of taxonomies reappears. If you receive any errors or warnings, refer to the error log on CIS server for details. See the *Content Intelligence Services Administration Guide* for information.

6. To check the status of the synchronization process, click the **View Jobs** button at the bottom of the page.

When the synchronization is complete, a message indicating its success or failure is sent to your Documentum Inbox.

Deleting taxonomies

When you delete a taxonomy, it removes all categories within that taxonomy except for categories that are linked into other taxonomies. All assignments to those categories are also removed, although the documents themselves are not.

To delete a taxonomy:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. Select the taxonomy you want to delete.
3. Select **File > Delete**.
A message page appears asking you to confirm that you want to delete the taxonomy.
4. Click **OK** to remove the taxonomy.

Processing documents

When your taxonomies and their category definitions are in place, you are ready to categorize documents. Content Intelligence Services supports both automatic categorization, where CIS server analyzes documents and assigns them to appropriate categories, and manual categorization, where a person assigns documents to categories.

Documentum Administrator enables you to review the results of either type of categorization, and to manually adjust them if necessary. For documents that CIS server could not definitively assign to particular categories, category owners use Documentum Administrator to approve or reject the candidate documents.

Click the links below for more information about processing documents:

- [Test processing and production processing, page 528](#)
- [Defining document sets, page 529](#)
- [Submitting documents to CIS server, page 531](#)
- [Assigning a document manually, page 532](#)
- [Reviewing categorized documents, page 532](#)

Test processing and production processing

You can submit documents to CIS server in *test* mode or *production* mode. You choose the mode when you define the document set.

In test mode, CIS server performs its analysis to categorize the submitted documents, but it does not make any of the permanent updates that you want it to make when you put Content Intelligence Services into production. You use test mode to refine and validate your category definitions. After reviewing the results of a test run, you can [clear the proposed categorizations](#), update the category

definitions, and run the test again. When CIS server is properly categorizing documents, you can bring the taxonomy online to put it into production.

In production mode, CIS server updates documents and the repository based on the results of its categorization. The nature of the updates depends on which configuration options are active: if Link to Folders is active, CIS server links documents into the folders corresponding to the categories, and if Assign as Attribute is active, CIS server writes the name of the assigned categories into each document's attributes. See [Choosing categorization options, page 501](#) for information about these options, and [Modifying Content Intelligence Services configuration, page 508](#) for details about how to set them.

You can perform test processing on a separate CIS server from your production server. Offloading test processing from the production server prevents your tests from competing for resources with the production system. See [Modifying Content Intelligence Services configuration, page 508](#) for information about specifying the test and production servers.

You can view the documents assigned to a category either after a test processing or after a production processing.

To switch from production view to test view

1. Navigate to the category for which you want to see the assigned documents. (Do not select the category.)
2. Select **View > Page View > Test view** to display the results of the category assignments after a test run.
3. Repeat the previous step but selecting **Production view** to go back to the production view.

Defining document sets

Documents are submitted to CIS server by means of *document sets*. A document set is a collection of documents that are sent to CIS server together, and which CIS server processes in the same way. The document set can retrieve all documents from a specified folder or be automatically applied to documents that users submit for categorization.

Once you have created and run a document set, the Properties page for the document set includes status information on the Last Run tab.

To create or modify a document set:

1. Navigate to **Administration > Content Intelligence > Document Sets**.
A list of the existing document sets appears.
2. Select **File > New > Document Set** to create a new document set, or select the document set you want to modify then select **View > Properties > Info**.
The properties page for document sets appears.
3. Enter a name and description for the document set.
Use a descriptive name that will enable you to distinguish it from other document sets. You may want the name to reflect the documents included in the set.

4. Select the document set language. The selected language must match with the language of the categories and taxonomies used for the classification. The documents will never be assigned to a category of a different language.
If the language of the document set is not defined, the language set for the document is used. If no language is set for the document, CIS server default language is used.
5. Click the **Document Set Builder** tab.
You use the controls on this tab to create the query used to retrieve documents for processing.
6. To include documents from a specific folder, click the **Select** link next to **Look in:** and navigate to the folder containing the documents to process.
When you click **OK** after selecting the folder, the folder appears next to the **Look in** label.
7. To specify the object type of the documents selected for processing, click the **Select** link next to **Type:** and select the object type.
When you click **OK** after selecting the object type, the type name appears next to the **Type** label.
8. The **Properties** checkbox is already selected to assign documents based on their attributes. Enter the criteria used to select documents.
 - a. Select an attribute whose value you want to test.
The drop-down list on the left displays the attributes of the object type you selected at step 6.
 - b. From the drop-down list in the middle, select the operator to use to compare the selected attribute to the test value.
The available operators differ depending on the attribute you selected in the previous step.
 - c. Enter the value to test against in the text box on the right.
 - d. To add an additional condition, click the **Add Property** button and repeat steps a through c.
The document set will include only those documents whose attributes meet all of the conditions.
9. Click the **Processing** tab.
You use the controls on this tab to specify when the documents in this document set are submitted to CIS server for processing and whether they are processed in test or production mode.
10. By default, the schedule is set to **Inactive**. To define a schedule, set the document set schedule to **Active**.
An active document set is run according to its defined schedule. An inactive document set is not run, and the remaining scheduling controls are grayed out.
11. For active document sets, specify when the documents in the set should be submitted to CIS server for processing.
 - a. Click the calendar icon next to the **Start Date** field to select the day on which the documents will be first submitted to CIS server.
 - b. Set the time of day for the first run by selecting numbers from the **Hour**, **Minute**, and **Second** drop-down lists.
The **Hour** setting uses a 24-hour clock.
 - c. Specify how often this document set submits documents to CIS server by entering a number in the **Repeat** box and picking the units (minutes, hours, days, weeks, or months) from the drop-down list.

- Each time the document set runs, it submits only new or revised documents to CIS server.
12. Click one of the **Processing Mode** option buttons to indicate whether to run this document set in production mode or test mode.
See [Test processing and production processing, page 528](#) for information about production and test modes. Selecting the mode also determines which CIS server processes the document set: the production server or the test server.
 13. If you chose **Test** at step 11, click **Select Taxonomy** and select a taxonomy to run the test against.
For a test run, you can have CIS server only consider the categories in the taxonomy you are testing. The taxonomy does not need to be online. For a production run, all synchronized taxonomies are used for the classification.
 14. Click **OK** to close the properties page.
 15. Synchronize the document set to copy changes to CIS server.
 - a. Select the document set you want to synchronize.
 - b. Select **Tools > Content Intelligence > Synchronize**.
The Synchronize page appears. **CIS servers to Update** shows which CIS server will be updated based on the processing mode for this document set.
 - c. Click the **OK** button to start the synchronization.
If you receive any errors or warnings, refer to the error log on CIS server for details.
 16. To check the status of the synchronization process, click the **View Jobs** button at the bottom of the page.
When the synchronization is complete, a message indicating its success or failure is sent to your Documentum Inbox.
 17. To view the documents that the document set will submit to CIS server, click the name of the document set on the list page.
Documentum Administrator runs the query from the Document Set Builder tab and displays the documents in the result set.
Note: Deleting a document from this page removes it from the repository, not simply from the document set.

Submitting documents to CIS server

There are two ways to submit documents to CIS server for automatic categorization.

When you submit one or more documents for automatic categorization, the documents are added to a queue awaiting CIS server processing. They are processed as CIS server retrieves documents from its queue.

To submit a document for CIS server processing:

1. Select the document you want classify.
2. Select **Tools > Submit for Classification**.

To submit a set of documents for CIS server processing:

1. Navigate to **Administration > Content Intelligence > Document Sets**.
A list of the existing document sets appears.
2. Select the document set you want to run.
You can only select one document set at a time. If you select multiple sets, the **Start Processing** menu option is grayed out. However, several document sets can be processed at the same time.
3. Select **Tools > Content Intelligence > Start Processing**.
4. Enter a name for the run.
The name enables you to identify this run in the log files.
5. Click **OK** to submit the documents for processing.
To review the status of a processing run, open the properties page for the document set and click the **Last Run** tab. For a greater level of detail, check the CIS server log files; see the *Content Intelligence Services Administration Guide*.

Assigning a document manually

This sections describes how to manually assign a document from a cabinet folder to a category.

CIS server must be configured to Production mode.

To manually assign a document:

1. Navigate to a cabinet and select the document to assign.
2. Select **Edit > Add To Clipboard**.
3. Navigate to the category to which you want to assign the document in the node **Administration > Content Intelligence > Taxonomies**). If not already done, turn page view into **Production view**.
The list of documents belonging to the selected category in **Production view** is displayed.
4. Select **Edit > Assign here**. The document is assigned to the category, its status is set to *assigned_manual*.
If the option **Link assigned documents into category folders** is enabled, a relationship is created between the document and the category folder corresponding to the selected category.
If the option **Update document attributes with category assignments** is enabled, the name of the category is added as a value of the keyword attribute for the document.

Reviewing categorized documents

The My Categories page provides direct access to the categories for which you are the owner. From the My Categories page, you can view all documents assigned to the categories you own, or you can display just those documents assigned to the category with a status of Pending. As the category owner, you are responsible for approving or rejecting Pending documents.

Documents receive Pending status when the [confidence score](#) that CIS server assigns to the document is higher than the category's candidate threshold but less than its on-target threshold. When you approve or reject a Pending document assignment, CIS server saves this information and does not ask you to approve or reject it again (unless you [clear assignments](#)).

To review candidate documents:

1. Navigate to **Administration > Content Intelligence > My Categories**.

A list of the categories for which you are the category owner appears. The total number of candidate (Pending) documents for the category appears in the right column.

Note: The My Categories list displays all categories at the same level. To view categories in their proper hierarchical position, navigate to the categories from **Administration > Content Intelligence > Taxonomies** rather than choosing **My Categories**.

2. Select **My Categories with pending documents** from the drop-down list in the upper right. With this option selected, the list displays only categories that have Pending documents.
3. Click the category **Name** to display the complete list of documents assigned to the category, or click the value in the **Total Candidates** column to display only the Pending documents. The list of assigned documents and their assignment status appears.
4. Select the checkbox next to the candidate document to select it.
5. To approve the document in this category, select **Tools > Content Intelligence Approve** and click **OK** on the confirmation page that appears. If you are only viewing the Pending documents, the approved document disappears from the current view because it is no longer a candidate.
6. To reject the suggested categorization, select **Tools > Content Intelligence > Reject Candidate** and click **OK** on the confirmation page that appears.. The document disappears from the current view because it is no longer a candidate.
7. Repeat steps 3 through 6 for each candidate document in categories for which you are the category owner.

Clearing assignments

You can clear assignments at the taxonomy level or a category level. You can choose to clear only the documents in that category, or in the category and all of its children.

You can also clear the assignments for all documents belonging to a document set or for a single document.

Clearing assignments is most common when running in [test mode](#). If you clear assignments made in production mode, any record of the category owner's approval or rejection of a proposed assignment is also lost. As a result, CIS server may ask the category owner to approve or reject category assignments again.

To remove assignments of all documents in a taxonomy or category:

1. Navigate to **Administration > Content Intelligence > Taxonomies**. A list of the existing taxonomies appears.

2. Navigate to the category whose assignments you want to clear and select it.
3. Select **Tools > Content Intelligence > Clear Assignments**.
4. Select which types of assignments to clear.
 - a. Click one of the **Clear assignments with status** option buttons to indicate whether to clear all assignments, only pending assignments, or only complete assignments.
 - b. Click one of the **Clear assignments with type** option buttons to indicate whether to clear test assignments, active assignments, or both.
5. To clear the assignments in all subcategories, select the **Include subcategories?** checkbox.
If the checkbox is not selected, only assignments in the current category are cleared.
6. Click **OK**.

To remove assignments of all documents in a document set:

1. Navigate to **Administration > Content Intelligence > Document Sets**.
A list of the existing document sets appears.
2. Navigate to the document set whose assignments you want to clear and select it.
3. Select **Tools > Content Intelligence > Clear Assignments**.
4. Select which types of assignments to clear.
 - a. Click one of the **Clear assignments with status** option buttons to indicate whether to clear all assignments, only pending assignments, or only complete assignments.
 - b. Click one of the **Clear assignments with type** option buttons to indicate whether to clear test assignments, active assignments, or both.
5. Click **OK**.

To remove the assignment for a selected document:

1. Navigate to **Administration > Content Intelligence > Taxonomies**.
A list of the existing taxonomies appears.
2. Navigate to the document whose assignment you want to clear and select it by clicking the checkbox next to its name.
3. Select **Tools > Content Intelligence > Clear Assignments**.

Refining category definitions

When you have created your taxonomy and provided evidence terms for each category, the next step is to test how well the category definitions guide CIS server in categorizing documents.

Compile a set of test documents and submit them to CIS server. The test set should include representatives of the various types of documents you will be processing with Content Intelligence Services. When processing is complete, review the resulting categorization. If CIS server does not

assign some documents to the categories you expect it to, you may need to revise the category thresholds or the evidence associated with the categories.

If a document appears in a category it should not, it means that the evidence for that category is too broad: consider adding additional terms. If a document does not appear in a category that it should, it means that the evidence is too restrictive.

The rule of thumb is: Make the category definition simple and test it with your documents. If it works in most cases leave it alone. If there are problems recognizing a category and more differentiating data is necessary, then use compound terms as described in the topics of this section.

This section provides tips for refining category definitions to make more subtle discriminations where necessary. The main topics are:

- [Using compound terms, page 535](#)
- [Selecting terms, page 536](#)
- [Modifying category and taxonomy properties, page 536](#)
- [Defining compound evidence terms, page 537](#)

It is also possible to define patterns to match specific terms like phone numbers or social security numbers. The *Content Intelligence Services Administration Guide* provides the detailed procedure for defining patterns.

Using compound terms

CIS server determines whether to assign a document to a category by adding together the [confidence values](#) assigned to the individual pieces of evidence in the category definition. For some categories, there may be multiple, separate collections of evidence that should lead CIS server to assign a document to the category. You can define categories that have multiple *evidence sets*, each of which represents an independent means of recognizing the category.

An evidence set is a collection of terms that CIS server uses together as evidence of a particular concept. You can create multiple evidence sets in order to define separate sets of terms. Confidence levels are not combined across evidence sets.

When you define a category in Documentum Administrator, the first evidence set consists of simple terms, each of which by itself is a good indicator of category membership. A simple term can be a single word or a multi-word phrase, and is typically assigned a confidence value of High. The list of simple terms represents the keywords and phrases for the category, and for many categories it is the only evidence required.

When you are tuning your categories to make more subtle distinctions, you can add compound terms to the category definition. A compound term is a collection of words and phrases that work together to indicate category membership. Each word or phrase typically has a confidence value of Low, Supporting, or Exclude. No one term from the collection has a high enough confidence value to assign a document to the category, but the presence of multiple terms can cause the total confidence score to cross the on-target threshold. The main difference between a compound term and a list of simple terms is the confidence value of each term. The section [Confidence values and document scores, page 502](#) provides information about how to define confidence values.

CIS server treats each compound term as an independent evidence set. That is, you can think of each compound term as an independent definition of the category evidence. A document is assigned to the category only if its cumulative score from any one compound term (or the list of simple terms) exceeds the threshold.

See [Defining compound evidence terms, page 537](#) for details about creating compound terms.

Selecting terms

The biggest challenge when defining categories is selecting the proper terms to serve as evidence for them. If you define a category using only terms that are unique to that category, CIS server will not recognize the category in documents that relate to it in an indirect way. On the other hand, if you choose common words as evidence terms, CIS server may recognize the category when the document does not in fact belong in it.

The challenge is to create category definitions that are just complete enough to trigger category recognition without introducing ambiguity. It is just as important to keep misleading terms out of category definitions as it is to make sure that all viable terms are included. You might think that OR is a viable term as part of the definition of Oregon, but OR crops up in so many other contexts that OR should not be part of the definition of Oregon.

Note: CIS server is not case sensitive for evidence terms. OR matches OR, Or, and or.

Using common words as evidence terms

The easiest categories to define are those having proper nouns as evidence terms. Defining the category for International Business Machines Corporation is intuitive: you would naturally include features such as IBM and variations on the company name.

More complex category definition techniques are required when the proper noun denoting a category is made up of several commonly occurring words. Defining a category such as Internet Service Provider means you have to clearly specify what CIS server should not recognize as a valid term as well as what it should recognize. Internet Service Provider is a name made up of three frequently encountered words, and CIS server needs to recognize all three words in the correct context to correctly assign a document to the category.

A correct definition uses both simple terms and a compound term. The list of simple terms contains obvious and unique synonyms, such as ISP. The compound term includes each word of the phrase Internet Service Provider as an Supporting term: no evidence is enough until all three terms are found in a document.

Modifying category and taxonomy properties

The options on this page are the same as those for [creating a new taxonomy](#).

If CIS server is not assigning documents properly to a category, you may need to change the on-target or candidate thresholds. If documents appear in the category that should not, you may need to

increase the thresholds; if documents that should appear in the category do not, you may need to lower the thresholds. If the category owner is required to approve too many documents, you can lower the on-target threshold while leaving the candidate threshold unchanged.

To update category or taxonomy properties:

1. Navigate to the category whose properties you want to update. Select the category and then select **View > Properties > Info**.
2. The Properties page appears, select the Attributes tab.
3. Update the title and description for the category if necessary.
4. To change the category owner, click the **Select owner** link and choose the new owner.

The standard page for selecting a user appears. The category owner is the user who can approve or reject documents assigned to the category as a candidate requiring approval from the category owner; see [Reviewing categorized documents, page 532](#) for information about the document review process.

5. To change the category class, choose the category class from the drop-down list.
The **category class** determines default behavior for the new category as well as the document attribute to which CIS server adds the category name if you are using the [Assign as Attributes](#) option.
6. Update the on-target and candidate thresholds.

The on-target and candidate thresholds determine which documents CIS Server assigns to a category during automatic processing. When a document's confidence score for the category meets or exceeds the on-target threshold, CIS server assigns it to the category. When the score meets or exceeds the candidate threshold but does not reach the on-target threshold, CIS server assigns the document to the category as a candidate requiring approval from the category owner. See [Confidence values and document scores, page 502](#) for details.

7. Click **OK**.

The property page closes.

Defining compound evidence terms

A compound term is a collection of words and phrases that work together to indicate category membership. None of the words by themselves are enough for CIS server to confidently assign a document to the category, but when they appear in combination it adds to the confidence score. See [Using compound terms, page 535](#) for more information.

When a category definition includes multiple compound terms, each one defines a collection of evidence used together to set a document's score. Confidence levels are not combined across compound terms.

If you find during testing that a particular simple term is causing CIS server to assign too many documents to the category, you can convert the simple term into a compound term that is more discriminating. To convert a simple term into a compound term, click the **Add additional terms** link next to the term that you want to change and follow the instructions in the procedure below.

To create a new compound evidence term:

1. Navigate to the category whose evidence you want to update and click the  icon to display the rules page.
2. Click the **Add new compound evidence** link to add a completely new compound term, or click the **Add additional term** link next to a simple term that you want to convert into a compound term. The Evidence page appears. It looks the same as the Evidence page for a simple term, except that **Prev**, **Next**, and **Finish** buttons appear in place of the **OK** button at the bottom of the page. These buttons enable you to navigate between the Evidence pages for each of the terms that make up the compound term.
3. Set the evidence properties for one of the simple terms in the compound term.

Follow steps 1 through 6 of [the procedure for defining a simple term](#). The only difference when defining part of a compound term is that the default system-assigned confidence level is Low.

4. Click **Next** and repeat step 3 to add additional terms, or click **Finish** (or **OK** if you are converting a simple term) to complete the compound term.

When you click **Next**, another instance of the Evidence page appears. The page title shows which term you are now defining and the total number of evidence terms in the compound term (**Compound Evidence Term X of Y**).

When you click **Finish** or **OK**, the individual terms of the compound term appear on a list page.

Click the **Back to Rules Summary** link to display again the Rules page of the category.

To modify a compound term:

1. Click the  icon next to the compound term you want to modify.
A list page appears with each individual term in the compound in a separate row.
2. To modify a term in the compound, click the  icon next to the term and change its evidence properties.
Follow [the procedure for defining a simple term](#).
3. To add an additional term to the compound, select **File New Evidence** and set the evidence properties for the new term.
Follow [the procedure for defining a simple term](#). The only difference when defining part of a compound term is that the default system-assigned confidence level is Low.
4. To remove one or more terms from the compound, select the checkboxes next to the terms and select **File > Delete**.

If removing the selected terms will result in only a single term remaining, a page appears asking whether you want to convert the remaining term to a simple term or delete it as well.

Resource Management

Use the Administration > Resource Management navigation in Documentum Administrator to monitor and configure Documentum system resources in the Documentum environment.

When you first navigate to Resource Management, the system displays the Resource Agents list page. From this list page you can:

- Add new resource agents.
- Delete existing resource agents.
- Access the Resource Agent Properties - Info page to view or modify properties for resource agents.
- Access the Resources on Agent list page for a specific resource agent.

For more information about the Resource Agents list page, go to [Managing resource agents, page 540](#).

Click the links below for information and instructions on:

- [Understanding Resource Management, page 540](#)
- [Managing resource agents, page 540](#)
 - [Adding resource agents, page 541](#)
 - [Viewing or modifying resource agent properties, page 542](#)
 - [Resource agent authentication failure, page 542](#)
 - [Deleting resource agents, page 543](#)
- [Managing resource properties, page 543](#)
 - [Managing general information for resources, page 544](#)
 - [Managing resource attributes, page 545](#)
 - [Managing resource operations, page 546](#)
 - [Starting operations, page 546](#)
 - [Viewing resource notifications, page 547](#)
 - [Viewing the Notification page, page 547](#)

- [Viewing resource logs, page 548](#)
- [Monitoring resources, page 549](#)

Understanding Resource Management

The Resource Management node provides an interface for viewing and managing Documentum resources exposed in the Documentum environment as Java Management Beans (MBeans). Documentum Administrator maintains the list of resource agents, which includes the information necessary to access a resource agent. The resource agent information is stored in the ResourceAgentsRegistry in the global registry.

Users access the MBean resources in the distributed network through a resource agent (JMX agent) to obtain a list of available MBean resources that they can manage. The Resource Management node displays a list of the resource agents; however, only a system administrator can create, delete, or update resource agents.

A resource agent may require authentication to access its resources (MBeans). Documentum Administrator will first attempt to authenticate the user using the current session login information. If that fails, then Documentum Administrator prompts for a username and password.

Click the links below for information and instructions for:

- [Managing resource agents, page 540](#)
 - [Adding resource agents, page 541](#)
 - [Viewing or modifying resource agent properties, page 542](#)
 - [Resource agent authentication failure, page 542](#)
 - [Deleting resource agents, page 543](#)
- [Managing resource properties, page 543](#)
 - [Managing general information for resources, page 544](#)
 - [Managing resource attributes, page 545](#)
 - [Managing resource operations, page 546](#)
 - [Starting operations, page 546](#)
 - [Viewing resource notifications, page 547](#)
 - [Viewing the Notification page, page 547](#)
 - [Viewing resource logs, page 548](#)
 - [Monitoring resources, page 549](#)

Managing resource agents

Select the Resource Management node (Administration > Resource Management) to access the Resource Agents list page. The resource agent information is stored in the ResourceAgentsRegistry in

the global registry. If no resource agents are configured in the global registry, the Resource Agents list page displays a message that no items were found.

System administrators can add, delete, and edit resource agents. A resource agent may require authentication to access its resources (MBeans). Documentum Administrator will first attempt to authenticate the user using the current session login information. If that fails, then Documentum Administrator prompts for a username and password.

From the **Resource Agents** list page, you can:

- Add resource agents.
- Access the Resource Agent Properties - Info page to view or modify resource agent properties.
- Delete resource agents.
- Access the Resources on Agent list page for a specific resource agent.

For more information, refer to:

- [Understanding Resource Management, page 540](#)
- [Adding resource agents, page 541](#)
- [Viewing or modifying resource agent properties, page 542](#)
- [Resource agent authentication failure, page 542](#)
- [Deleting resource agents, page 543](#)

Adding resource agents or modifying agent properties

Click the links below for information and instructions on:

- [Adding resource agents, page 541](#)
- [Viewing or modifying resource agent properties, page 542](#)

Adding resource agents

You must be a system administrator to add resource agents.

To add a resource agent:

1. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
2. Select **File > New > Resource Agent** to access the **New Resource Agent - Info** page.
3. Enter properties for the new resource agent:
 - a. **Name:** Type the name of the resource agent.
 - b. **JMX Service URL:** Type the JMX URL used to connect to the resource agent.
 - c. **Test:** Click to contact the resource agent at the specified URL.
The test is successful if it contacted the resource agent at the specified URL.

The test fails and the system displays the Resource Agent Authentication page if it was unable to contact the resource agent. Verify that the URL, username, and password information are correct.

- d. **Description:** Type a short description of the resource agent.
 - e. **Default Polling Interval:** Type a polling interval time.
The system checks the status of resources on this agent every x milliseconds. The default is set at 5000 milliseconds.
4. Click **OK** when you have completed entering the properties for the new resource agent or click **Cancel** to return to the Resource Agents list page without saving any information.

Viewing or modifying resource agent properties

You must be a system administrator to modify resource agents.

To view or modify resource agent properties:

1. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
2. Select the resource agent whose properties you want to view or modify.
3. Select **View > Properties > Info** to access the **Resource Agent Properties - Info** page to view or modify the properties for a resource agent.
4. View or modify resource agent properties:
 - a. **Name:** The name of the resource agent.
 - b. **JMX Service URL:** The JMX URL used to connect to the resource agent.
 - c. **Test:** Click to contact the resource agent at the specified URL.
The test is successful if it contacted the resource agent at the specified URL.
The test fails and the system displays the Resource Agent Authentication page if it was unable to contact the resource agent. Verify that the URL, username, and password information are correct.
 - d. **Description:** The short description of the resource agent.
 - e. **Default Polling Interval:** The polling interval time.
This checks the status of resources on this agent every x milliseconds. Default is set at 5000 milliseconds.
5. Click **OK** when you have completed viewing or modifying the properties for the resource agent or click **Cancel** to return to the Resource Agents list page without saving any changes.

Resource agent authentication failure

The Resource Agent Authentication page appears when an attempt to contact the resource agent fails. Verify that the URL, username, and password information for the resource agent are correct.

Deleting resource agents

You must be a system administrator to delete resource agents.

To delete a resource agent:

1. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
2. Select the resource agents that to delete.
3. Select **File > Delete** to delete the resource agents.
The system displays the **Delete Resource Agent(s)** page.
4. Click **OK** (or **Finish** for multiple agents) on the Delete Resource Agent(s) page to delete the resource agents, or click **Cancel** to return to the Resource Agents list page without deleting the resource agents.

Managing resource properties

The Resources on Agent list page displays MBean resources for a selected resource agent. Select a resource to display the properties of the resource, such as attributes, operations, notifications, and a log file, if defined.

- The Resource Properties - Info page displays key information about the resource. The polling interval defines the frequency to poll the resource for activity. This is not used in the current release.
- The Resource Properties - Attributes page displays the resource attributes. Writeable attributes provide an input control to update the attribute value. Attribute changes will be updated on the resource by clicking the **Save Changes** or **OK** button.
- The Resource Properties - Operations page displays the operations that can be performed. Selecting an operation displays the operations dialog, which enables you to enter any required data, perform the operation, and view the results (if the operation has results).
- The Resource Properties - Notifications page displays the resource notifications you are subscribed to.
- The Resource Properties - Log page enables you to:
 - Specify the log level for tracing.
 - Specify the log level of messages.
 - Specify the number of viewable log file lines.
- The <MBean name> Monitor page displays information for resource types that have been configured for the server monitor interface.

To view resources on the resource agent:

1. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
2. Select the resource agent to view or modify.
3. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.

From the Resources on Agent list page, you can drill down to see information regarding the resource agent.

Click the links below for information and instructions on:

- Managing general information for resources, [page 544](#)
- Managing resource attributes, [page 545](#)
- Managing resource operations, [page 546](#)
- Starting operations, [page 546](#)
- Viewing resource notifications, [page 547](#)
- Viewing the Notification page, [page 547](#)
- Viewing resource logs, [page 548](#)
- Monitoring resources, [page 549](#)

Managing general information for resources

The Resource Properties - Info page contains general information about the resource, such as the name, status, resource agent, domain and node, and type. You can also select an interval to check the status of resources on the resource property.

To manage general information for resources:

1. Navigate to the Resource Properties - Info page:
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select the resource agent to view.
 - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
 - Note:** If the MBean server named in the JMX Service URL field on the Resource Agent Properties - Info page is not available, the system displays an error message instead of the Resources on Agent list page.
 - d. Highlight the resource to view.
 - e. Select **View > Properties > Info** to access the **Resource Properties - Info** page.
2. View general information about the resource:
 - a. **Name:** Name of the resource

- b. **Status:** Status of the resource.
 - c. **Resource Agent:** Name of the resource agent.
 - d. **Domain/Node:** Name of the domain or node path.
 - e. **Type:** The resource type, such as Configuration.
 - f. **Description:** Description of the resource.
3. Enter a **Polling Interval** to check the status of resources on this resource property.
If you change the polling interval on the Resource Properties - Info page, it will override the default polling interval setting on the resource agent. Default is set at 1000 milliseconds.
 4. Click **OK** to save changes and return to the Resource on Agent list page or click **Cancel** to return to the Resources on Agent list page without saving any changes.

Managing resource attributes

The Resource Properties - Attributes page displays the attributes for an MBean. If the MBean enables you to update the attributes, then the system displays an input control. The MBean resource will validate the new data values.

To manage resource attributes:

1. Navigate to the Resource Properties - Attributes page:
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select the resource agent to view.
 - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
 - d. Select the resource to view.
 - e. Select **View > Properties > Attributes** to access the Resource Properties - Attributes page.
2. View or modify the MBean attributes:
 - a. **Name:** Name of the attribute.
 - b. **Description:** Description of the attribute.
 - c. **Value:** Attributes may be read-only or editable.
3. Click **Refresh** to refresh the list of attributes and their values.
4. If you changed any values, click **Save Changes** to update the resource with the new values; otherwise the changes will be lost.
5. Click **OK** to save changes and return to the Resources on Agent list page or click **Cancel** to return to the Resources on Agent list page without saving any changes.

Managing resource operations

The Resource Properties - Operations page displays the operations that can be performed. Selecting an operation displays the Start Operations dialog, which enables you to enter required data (if required) and perform the operation.

To manage resource operations:

1. Navigate to the Resource Properties - Operations page:
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select the resource agent to view.
 - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
 - d. Select the resource that you want to view.
 - e. Select **View > Properties > Operations** to access the **Resource Properties - Operations** page.
2. Click a link in the **Name** column to access the **Start Operation** page.
3. On the Start Operation page, enter parameters (if required) and click **Start Operation**.
4. Click **Close** on the Start Operation page to return to the Resource Properties - Operations page.
5. Click **OK** or **Cancel** to return to the Resources on Agent list page.

Starting operations

After clicking on an operation name on the Resource Properties - Operations page, the system displays the Start Operations page. If the operation requires parameters, then parameter input fields will be displayed. Enter parameters (if required) and click **Start Operation**.

Table 60. Start Operation page properties

Field label	Value
Operation	Name of the operation
Description	Description of the operation.
Resource	Name of the resource.
Agent	Name of the resource agent.
Domain	Domain for the resource agent.
Parameters	The system will display input control fields if parameters are defined for the operation.
Start Operation	Click to invoke the operation. The dialog box remains open until you click Close .

Field label	Value
Status	After the operation runs, displays that the operation completed or displays an error message, if one is provided.
Return Value	Displays the return value of the operation, if it has one.
Close	Close the dialog and return to the Resource Properties - Operations page.

Viewing resource notifications

The Resource Properties - Notifications page displays the resource notifications you subscribe. These notifications are sent only while you are viewing the resource properties.

To view resource notifications:

1. Navigate to the Resource Properties - Notifications page:
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select the resource agent to view.
 - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
 - d. Select the resource to view.
 - e. Select **View > Properties > Notifications** to access the **Resource Properties - Notifications** page.

The notifications shown on the Resource Properties - Notifications page occurred since you viewed the properties for this resource. Click the **Log** tab for events that occurred prior to this session.
2. Click **Refresh** to refresh the list with notifications that occurred while viewing the resource.
3. Click an item in the **Message** column to view the **Notification** page, which provides additional information about the notification for the resource.
4. Select **Subscribe** to listen for and display notifications from the resource.
5. Click **OK** or **Cancel** to return to the Resources on Agent list page.

Viewing the Notification page

After clicking on an item in the **Message** column on the Resource Properties - Notifications page, the system displays the Notification page.

Table 61. Fields on the Notification page

Field label	Value
Message	Notification message.
Occurred	Time notification occurred.
Resource	Name of the resource.
Agent	Name of the resource agent.
Domain	Domain for the resource agent.
Close	Close the dialog and return to the Resource Properties - Notifications page.

Viewing resource logs

The Resource Properties - Log page displays log file information for the resource if it is supported by the MBean resource.

To view resource logs:

1. Navigate to the Resource Properties - Log page:
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select the resource agent to view.
 - c. Select **View > Resources on Agent** to access the **Resources on Agent** list page that displays the resources for the selected resource agent.
 - d. Select the resource to view.
 - e. Select **View > Properties > Log File** to access the **Resource Properties - Log** page.

The system displays the log file name and size that the server returned.
2. Click **Download** to download the log file.
 This opens a standard browser Download dialog with the log file as the download target.
3. Select a **Log Level**.
 If a list of levels is published by the resource, the system displays the list of published severity levels, ranked by severity level. If no severity levels are published by the resource, the system displays all.
4. In the **View Logged Events** section, select what and how you want to view the logged events:
 - a. Select a **Severity** type to view.
 - b. Select to view the **First** or **Last** logged events and then select the number of lines to display, or select **All** to display all logged events.
5. Click **Go** to fetch the logged events from the log file using the selected criteria.
6. Click **OK** or **Cancel** to return to the Resources on Agent list page.

Monitoring resources

The <MBean name> Monitor page displays information for resource types that have been configured for the server monitor interface. The monitor interface is available only for these MBean types:

- AcsServerMonitorMBean
- AcsServerConfigMBean
- JmxUserManagementMBean
- IndexAgent

To monitor resources:

1. Access the <MBean name> Monitor page.
 - a. Navigate to **Administration > Resource Management > Resource Agents** to access the **Resource Agents** list page.
 - b. Select a resource agent and then select **View > Resources on Agent** to access the **Resources on Agent** list page.
 - c. Select a resource and then select **View > Monitor** to access the <MBean name> **Monitor** page.

Note: The Monitor menu option is available only for specific MBean types that have been configured for the server monitor interface.

2. Click **Refresh** to refresh all attributes, including writeable ones.
3. View the attributes in the **Properties** section.

You can modify the contents in the Properties section if the attributes are writeable. Click **Save Changes** to update the attributes on the MBean. After saving the changes, the system displays a message in the Notifications section if the MBean has the notifications implemented.

4. Click an operation button.
The **Start Operations** page appears where you can enter date (if required) and perform the operation.
5. View the information in the **Notifications** section.
6. View the information in the **View Logged Events** sections.
This section displays the logged events if the MBean implements these methods.

7. Click **Close** to exit and return to the Resource Agents list page.

Manual configuration steps for monitoring resources

This section details the manual configuration steps for monitoring resources.

To manually configure:

1. The following changes are required in
`\app\webcomponent\config\admin\resourcemanagement\resources\mbeanresourceslist_component.xml`.
Add the JMXBeans to the <mbeantypes> node list.

Example 18-1.

```
<mbeantypes>
<!--name denotes the exact name of MBean-->
<mbeantype name='IndexAgent'>
<!--onclickcomponent specifies the component to be invoked-->
<onclickcomponent>mbeanresourcemonitordialogcontainer</onclickcomponent>
</mbeantype>
</mbeantypes>
```

2. The following changes are required in
\\app\\webcomponent\\config\\admin\\resourcemanagement\\resources\\mbeanresourcemonitor_component.xml.

Add the JMXBeans to the <mbeantypes> node list.

Example 18-2.

```
<mbeantypes>
  <!--name denotes the exact name of the MBean-->
  <mbeantype name='IndexAgent'>
    <!--attributes are the list of the attributes that need
        to be exposed in the monitor user interface-->
    <attributes>
      <attribute>Status</attribute>
      <attribute>Mode</attribute>
      <attribute>...</attribute>
    </attributes>
    <!--operations are the list of the operations that need to be exposed
        in the monitor user interface. launchcomponent=true will launch the
        operations user interface in a new window. Also if the operation
        requires user input, then the user interface automatically opens in a
        new window-->
    <operations>
      <operation launchcomponent='false'>Start</operation>
      <operation launchcomponent='true'>downloadLogFile</operation>
      <operation launchcomponent='true'>...</operation>
    </operations>
    <!--notifications are the list of notifications, ideally the
        empty list will capture all notifications.-->
    <notifications>
      </notification></notification>
    </notifications>
    <!--refreshinterval denotes the interval in miliseconds for the
        monitor user interface to be refreshed. Ideal value should be 10sec.-->
    <refreshinterval>10000</refreshinterval>
  </mbeantype>
</mbeantypes>
```


Chapter 19

Administrator Access

This chapter discusses administrator access sets in Documentum Administrator. Administrator access sets enable organizations to configure access to administrative functions by role.

This chapter cover the following topics:

- [Understanding administrator access sets, page 553](#)
- [Creating administrator access sets, page 555](#)
- [Viewing or modifying administrator access sets, page 555](#)
- [Deleting administrator access sets, page 556](#)
- [Properties on the administrator access set pages, page 557](#)

Understanding administrator access sets

The administrator access functionality enables access to Administration nodes based on roles. The nodes, such as Basic Configuration, User Management, Job Management, and Audit Management, provide access to different repository and server functions.

Note: Administrator Access functionality is available only on Documentum 6 and later repositories.

Use the Administration > Administrator Access navigation to access the Administrator Access Sets list page. Administrators with Superuser privileges and client capability of Coordinator or greater can access the Administrator Access node to create new administrator access sets, view or modify the properties of existing administrator access sets, or delete administrator access sets.

Administrator access set definitions reside in the global registry and associate nodes to roles and then group the functionality exposed through Documentum Administrator to a role. For example, a User Manager role associated with a corresponding administrator access set may enable access to the User Management node. Users associated with the User Manager role can access the User Management node to manage users, groups, roles, and sessions in the repository.

Administrator access sets do not conflict with Content Server privileges; object level and user level permissions and permission sets take precedence over administrator access sets. Even if a user has access to a node, that user may not have the proper permissions to do anything.

Non-superusers logging in to Documentum Administrator who do not belong to any administrative role with a corresponding administrator access set will not see any administration nodes. The exceptions to this rule are:

- The Groups node is enabled for users with Create Group privileges.
- The Types node is enabled for users with Create Type privileges.

Non-superusers defined in any administration access set will see only the nodes they are configured for.

Administrators with Superuser privileges and client capability of coordinator or greater can access and manage (create, edit, and delete) administrator access set configurations. Superusers are immune from the effects of an administrator access set. For example, if a Superuser is assigned to a role with an administrator access set such as a Audit Manager, the Superuser continues to see the full Administration node tree, including the Administrator Access node.

The following example illustrates access to Administration nodes using administrator access sets and roles:

1. Create an AuditManager role.
2. Create an administrator access set to map AuditManager role to the Audit Management node.
3. If a user logs in to Documentum Administrator and:
 - Belongs to the AuditManager role and is not a Superuser, the user sees only the Audit Management node.
 - Does not belong to any role and is not a Superuser, the user will not see any administration nodes.
 - Is a Superuser, the user sees all nodes under the Administration node and also sees the Administrator Access node.

The list of available roles is retrieved from the repository to which the administrator is connected. To ensure that administrator access sets function correctly across an application, the roles associated with the administrator access sets must exist in all repositories. For example, if Repository1 has role ABC, then Repository2 must also have role ABC defined. If the assigned role is missing in the connecting repository, the administrator access set does not take effect for the missing role. If the role does not exist in the connected repository, Documentum Administrator displays the role on the Administrator Access Set Properties - Info page with a message in red font that the role is not defined in the repository. Documentum Administrator enables an administrator to save an administrator access set containing inactive or missing roles.

Note: The following Administration nodes are currently not available for the administrator access set functionality:

- Work Queue Management
- Distributed Content Configuration
- Privileged Clients

The User Management chapter provides information on setting up roles. The Documentum Administrator Deployment Guide contains information on how to enable or disable the administration access set functionality.

Creating or modifying administrator access sets

Click the links for information on:

- [Creating administrator access sets, page 555](#)
- [Viewing or modifying administrator access sets, page 555](#)

Creating administrator access sets

Use the instructions in this section to create new administrator access sets.

To create administrator access sets:

1. Connect to a repository with Superuser privileges and client capability of Coordinator or greater.
2. Navigate to **Administration > Administrator Access**.
The **Administrator Access Sets** list page appears.
3. Select **File > New > Administrator Access Set**.
The **New Administrator Access Set - Info** page appears.
4. Enter information about the new administrator access set:
 - **Name:** Type a unique name for the administrator access set.
After creating and saving an administrator access set, the name cannot be modified.
 - **Description:** Optionally, type a description for the administrator access set.
 - **Nodes:** Select the checkboxes to designate the nodes that users with this role can access.
At least one checkbox must be selected for an administrator access set.
 - **Assigned Role:** Click **Select** to access the **Choose a role** page to associate a role with the administrator access set.
The assigned role must be unique for an administrator access set.
- Properties on the administrator access set pages, page 557 provides additional information about the field properties on the New Administrator Access Set - Info page.
5. Click **OK** to save the new administrator access set or click **Cancel** to exit without saving any changes.
The system displays the **Administrator Access Sets** list page.

Viewing or modifying administrator access sets

Use the instructions in this section to view or modify administrator access sets.

To view or modify administrator access sets:

1. Connect to a repository with Superuser privileges and client capability of Coordinator or greater.
2. Navigate to **Administration > Administrator Access**.
The **Administrator Access Sets** list page appears.
3. Select an administrator access set and then select **File > Properties > Info**.
The system displays the **Administrator Access Set Properties - Info** page.
4. View or modify information about the administrator access set:
 - **Name:** View the unique name for the administrator access set.
After creating and saving an administrator access set, the name cannot be modified.
 - **Description:** Optionally, type or modify a description for the administrator access set.
 - **Nodes:** Select or clear the checkboxes to designate the nodes that users with this role can access.
At least one checkbox must be selected for an administrator access set.
 - **Assigned Role:** Click **Select** to access the **Choose a role** page to associate a role with the administrator access set.
The assigned role must be unique for an administrator access set.

[Properties on the administrator access set pages, page 557](#) provides additional information about the field properties on the Administrator Access Set Properties - Info page.

5. Click **OK** to save the modified administrator access set or click **Cancel** to exit without saving any changes.
The **Administrator Access Sets** list page appears.

Deleting administrator access sets

Use the instructions in this section to delete administrator access sets.

To delete administrator access sets:

1. Connect to a repository with Superuser privileges.
2. Navigate to **Administration > Administrator Access**.
The Administrator Access Sets list page appears.
3. Select an administrator access set and then select **File > Delete**.
The **Delete Administrator Access Set** page appears.
4. Click one of the following:
 - **OK** to delete the object.
 - **Finish** to delete multiple objects.
 - **Cancel** to exit without deleting any administrator access sets.

The **Administrator Access Sets** list page appears.

Properties on the administrator access set pages

This section:

- Shows the Administrator Access Set Properties - Info page.
- Describes the fields on the New Administrator Access Set - Info and Administrator Access Set - Info pages.

Figure 21. Administrator Access Set Properties - Info page

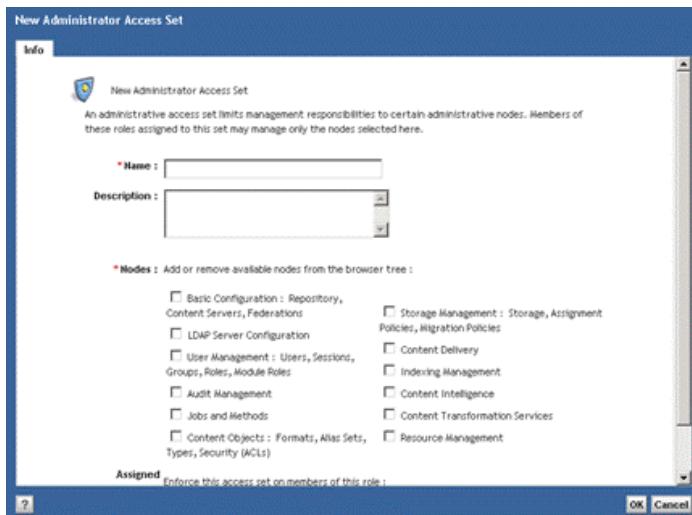


Table 62. Administrator access sets page properties

Field label	Value
Name	Name of the administrator access set. The administrator access set name must be unique. After creating and saving an administrator access set, the name cannot be modified.
Description	Description of the administrator access set.
Nodes	Select the checkboxes to designate the nodes that users with this role can access. At least one checkbox must be selected for an administrator access set.

Assigned Role	Indicates the role assigned to the administrator access set. If the role does not exist in the connected repository, Documentum Administrator displays the role in a red font on the Administrator Access Set Properties - Info page.
	The assigned role must be unique for an administrator access set. If the assigned role is not unique for an administrator access set, the system displays a message: Duplicate Assigned Role, please choose another.
	The system does not require assigning a role to an administrator access set. You can save an administrator access set that contains an inactive or missing role. This is useful during the initial setup of your system, or if there is no one at the time to fill an administrative role but you want to have the settings available for later.
Select	Click to access the Choose a role page to select a role for the administrator access set.
OK	Click to save the modifications to the administrator access set and return to the Administrator Access Sets list page.
Cancel	Click to return to the Administrator Access Sets list page without saving any changes.

Chapter 20

Privileged Clients

This section discusses managing privileged client permissions and privileges through Documentum Administrator.

The Privileged Client list page lists DFC clients that have been created in the repository that you are logged into. Each DFC client object has a corresponding certificate object that stores the public key of that DFC client.

From the Privileged Clients list page you can:

- View the existing list of DFC clients, their client IDs, hostname, and whether the DFC clients are approved to perform privileged escalations.
- Approve a DFC client to perform privileged escalations.
- Deny a DFC client from performing privileged escalations.
- Delete a DFC client and its certificate that it uses.

The Manage Clients locator page displays the list of DFC clients created in the repository. When an administrator selects one or more DFC clients on the Manage Clients page and clicks OK, a DFC client object is created in the logged in repository. The public key certificate is also copied to the local repository.

Approving or denying privilege escalations

This section discusses approving or denying a DFC client to perform privilege escalations.

To approve or deny privilege escalations

1. Navigate to **Administration > Privileged Clients** to access the **Privileged Clients** list page.
2. If the DFC client does not appear on the **Privileged Clients** list page, click **Manage Clients** to access the **Manage Clients** page.
 - a. Optionally, enter the name, or a portion of the name of the DFC client.
 - b. Click **Go**.
The system displays all registered DFC clients matching the criteria that you entered.
 - c. Select the registered DFC clients that you want to perform privilege escalations on.
 - d. Click **>**.

- The selected DFC clients will move to the right side.
- To remove any DFC clients from the right side, select them and then click <.
- e. Click **OK** to return to the Privileged Clients list page.
 3. To approve a DFC client that appears on the Privileged Clients list page, select it and then select **Tools > Approve Privilege**.
 4. To deny a DFC client that appears on the Privileged Clients list page, select it and then select **Tools > Deny Privileges**.

Table 63. Privileged Clients list page properties

Field label	Value
Client Name	The name of the DFC client.
Client ID	The ID of the DFC client.
Host Name	Name of the machine where the DFC client is running.
Approved	Indicates if the given DFC client is approved to perform privilege escalations.
Manage Clients	Click to access the Manage Clients page to select DFC clients that are registered in the global registry.

Selecting registered DFC clients

On the Manage Clients page, select DFC clients that are registered in the global registry to be moved to the logged-in repository.

1. Navigate to **Administration > Privileged Clients** to access the **Privileged Clients** list page.
 2. Click **Manage Clients** to access the **Manage Clients** page.
- Note:** The Manage Clients button is disabled if a global registry is not configured or is unavailable.
3. Optionally, enter the name, or a portion of the name of the DFC client.
 4. Click **Go**.
- The system displays all registered DFC clients that match the criteria that you entered.
5. Select the registered DFCs that you want to perform privilege escalations on.
 6. Click >.
- The selected DFC clients will move to the right side.
- To remove any DFC clients from the right side, select them and then click <.
7. Click **OK** to return to the Privileged Clients list page.

Deleting a DFC and its certificate

Use the instructions in this section to delete a DFC client and the certificate that it uses, unless that certificate is used by another DFC client.

Deleting a DFC certificate.

1. Navigate to **Administration > Privileged Clients** to access the **Privileged Clients** list page.
2. Select a DFC client and then select **Tools > Remove from List**.

Chapter 21

Content Services for SAP Web Administrator

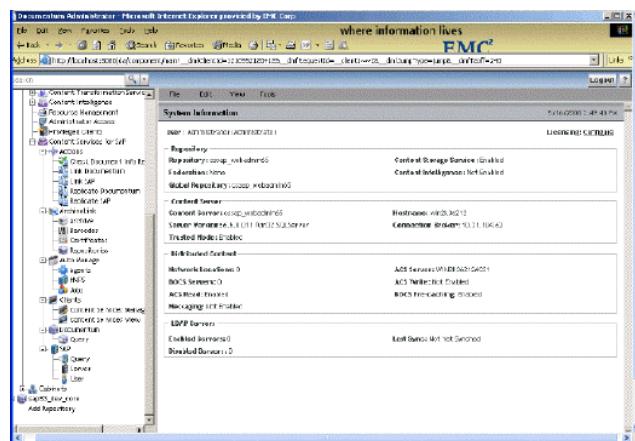
Content Services for SAP Web Administrator (WebAdmin) is a browser-based tool hosted within the Documentum Administrator that you can use to configure and administer Archive Services for SAP (AS SAP) and Content Services for SAP (CS SAP).

Understanding the Enterprise Integrations node of the WebAdmin GUI

The CS SAP WebAdmin module and Documentum Administrator must be installed before CS SAP WebAdmin will be accessible through the Documentum Administrator. Complete CS SAP installation information is in the *EMC Documentum Content Services for SAP Version 6.5 Installation Guide*.

After you have logged in to Documentum Administrator and the System Information page appears, you can select and expand the Content Services for SAP Web Administration node located under the Administration node on the left-hand tree.

Figure 22. WebAdmin - initial page



The Content Services for SAP Web Administration node contains the following subnodes when CS SAP is installed:

- Actions
- ArchiveLink
- Auto Manage
- Clients
- Documentum
- SAP

Each subnode contains additional subnodes used to perform CS SAP functions:

- The *Actions* subnode lets you create Content Services Actions which perform document linking, data replication, and integrity checking functions.
- The *Archive Link* subnode lets you configure archives, Barcodes for Archive Link, and certificate management.
- The *Auto Manage* subnode lets you set up the Agent Services, configure Jobs to run the Agent services and monitor the progress of jobs.
- The *Clients* subnode lets you configure Content Services for the Content Services Manage and Content Services View client applications.
- The *Documentum* subnode lets you define Documentum Queries.
- The *SAP* subnode lets you define SAP Queries and configure SAP Servers and Users to be used by Content Services.

Configuring Connections to SAP

Before you can use Content Services Archive or Agent functionality, you must first configure the SAP server and user information in CS SAP.

In order to communicate with both SAP and Documentum, CS SAP must know the server and user login details for each system. The Documentum login parameters are specified when the Archive or Agent services are created, as described in [Configuring, viewing, and editing archives, page 566](#) and [Creating, viewing, and editing an Agent, page 601](#). When CS SAP connects to Documentum Content Server, it reads the SAP server and user configuration parameters from the repository.

CS SAP was designed so that you can configure multiple SAP servers and users. This allows CS SAP to be used across multiple SAP application servers.

Create a specific user in your SAP system for use with CS SAP.

The procedures in this section describe how to configure SAP servers and SAP users that will be used by the WebAdmin application to access SAP.

Creating, viewing, and editing connections to an SAP server

To create, view, or edit connections to an SAP server:

1. Connect to WebAdmin.
2. Click to expand the **SAP** subnode and select the **Server** subnode.
The **Server** screen appears.
3. Select **File > New > SAP Server** from the menu at the top of the **Server** screen.
The **SAP Server Properties** screen appears.
4. Type a name for the Server in the **New Server Name:** field.
5. Do one of the following:
 - If you want to log in to an SAP server:
Type the hostname or IP address for the server. When an SAP router is used, fill in the complete SAP router string in the following format:
`/H/router1/H/<host_name_or_IP_address>`
 - If you want to log in to an SAP group, which is associated with an SAP R/3 server, type the following in this field:
`MSHOST=<message_server_host> R3NAME=<SAP_system_ID> GROUP=<SAP_group>`
6. Type the system name and number in the appropriate fields.
7. Select **Enable load balancing**, if required.
8. Click **OK** to save the SAP server configuration.

Creating, viewing, and editing an SAP user

To create, view or edit an SAP user:

1. Connect to WebAdmin.
2. Click to expand the **SAP** subnode and select the **User** subnode.
The **SAP User** screen appears.
- Note:** To enable worklist and links creation in CS SAP Webadmin, the recommended authorization profiles for SAP users are:
 - SAP_ALL
 - SAP_NEW
3. Select **File > New > SAP User** from the menu at the top of the **SAP User** screen.
The **SAP User Properties** screen appears.
4. Enter the new username in the **New User Name:** field.
5. Enter the user ID the **User ID:** field.
6. Enter a password for the user.

Note: From version 6.0, CS SAP supports case-sensitive passwords when connecting to SAP ECC 6.0 or later. Ensure that the CS SAP user password you enter exactly matches the SAP user password.

When using CS SAP 6.0 and later to connect to an older SAP system:

- The user password entered in CS SAP must be all uppercase
 - or
 - The kernel patch in SAP note 792850 must be applied to support case-sensitive passwords
7. Enter the client number.
 8. Select the language for the user from the **Language:** list box.
 9. Click **OK** to save the SAP user configuration.

Configuring HTTP Archiving Services

CS SAP does not include the HTTP archiving services component; this component has been moved to Archive Services for SAP (AS SAP). The instructions contained in this section are relevant only if you have parallel installations of CS SAP and AS SAP in your environment.

SAP must be configured to work with CS SAP. Information about configuring SAP using SAPGUI is in the *EMC Documentum Content Services for SAP Configuration Guide*.

Configuring, viewing, and editing archives

SAP uses named “logical archives” as a mechanism to specify target storage. Installations will typically have a number of “archives” relating to different types of information which will be archived. For example:

- Archive AA may be used to archive printlists from SAP. As an administrator, you may want to configure the system to store printlists within the Documentum Content Server folder /SAP/Printlists.
- Archive BB may be used to archive outgoing documents from SAP. As an administrator, you may want to configure the system to store outgoing documents within the Documentum Content Server folder /SAP/Outgoing.

WebAdmin allows you to specify rules for how to handle archived documents/data from SAP. As shown above, this may be simply to store different types of information in different locations for better housekeeping. However, it may also be desirable to specify access permissions, initiate workflows, or define whether received documents should be rendered into formats such as HTML and PDF.

All configuration objects created in WebAdmin are stored within the Documentum Content Server. For example, each archive configuration, such as AA, BB, can be found in the Documentum Server folder /System/DocLink/SAP/Archive.

Before configuring an archive in WebAdmin, you must first create the archive in SAP. When this has been done, WebAdmin can be used to mirror the SAP configuration and define Documentum Content Server specific configuration options.

To configure, view, or edit archives:

1. Connect to WebAdmin.
2. Click to expand the **ArchiveLink** subnode and select the **Archive** subnode.
The **Archive** screen appears.
3. Select **File > New > Archive** from the menu at the top of the Archive screen.
The **Properties** screen appears.
4. Enter the archive name in the **Archive Name:** field.
You can use names up to 30 character in length for archives, when supported by SAP.
5. The following parameters can be configured.

Table 64. Valid entries

Fieldname	Description
Archive ID	Name of the SAP archive using a two-letter string. The installation script creates a sample archive named 'AA'.
SAP Document Type	Set to NONE (HTTP provided).
Documentum Type	Specifies the Documentum document type. .
Workflow	Set to No Workflow.
Attribute Map	The attribute map is used to define the Documentum attributes of an archived document.
Filtering	There is a special attribute "FOLDER" that can be configured. If nothing is specified, the document is stored in the default cabinet. To specify the folder path, use the same format string as for the Agent attribute maps. Example: "FOLDER="/SAP/Archive/AA".
Custom Filter	Specifies a server method that is executed when a document is stored. This allows you to filter attributes and to do additional tasks when a document is saved.
Built-in Filter	Allows you to specify what filters are applied to convert the ALF format into XML for output to PDF, ASCII, or HTML.
Service-based business objects (SBO)	Allows you to customize archived object behavior, as described in Specifying a custom filter .

These items are further explained in the following sections.

6. Click **OK** to save the archive configuration.

Deleting archived and linked documents

In a repository, if you delete version 1.0 of a document that is linked to SAP or archived from SAP, the link to SAP is also deleted. This is because the dm_relation object which creates the link to SAP is deleted when the parent object (which is always version 1.0) is deleted.

We recommend that you do not delete the original version of objects that are linked to SAP if you want to maintain their link to SAP. If you need to delete version 1.0 of a document, but want to keep the link to SAP, after deleting the document, you must relink the object to SAP, outside of CS SAP.

Configuring the repository document type

The value of the Document Type field defines the object type used to store the document in the repository. The default format is sap_archive. This object type must be a sub-type of dm_document, for example, dm_doc_ebr.

If you use filters that extract additional attributes, this parameter must be set to the corresponding Documentum document type.

Specifying a custom filter

(Optional) Type the name of a custom filter here.

A custom filter is usually a Docbasic or Java program that is stored as content of a specific method (dm_method) or an SBO. For example, a custom filter may parse the archived file and extract attributes from the document content. The attributes are then passed back to the Content Services Archive software and stored as custom attributes. Or, a custom filter can create queries to attach other documents (such as SOPs) as virtual components to the archived document.

Custom filters have to be marked with a leading exclamation mark if they are external executables and not dm_methods. The complete path to the executable has to be provided after the exclamation mark.

For example:

```
!C:\production\extract_keys.exe
```

SBO custom filters must be marked with a leading exclamation mark and pound sign (!#).

For example:

```
! #mySBOName
```

More information is in [Customizing archives using service-based business objects](#).

Specifying a built-in filter

Using existing Documentum filters, you can define additional actions performed when a PrintList is archived. The following filters are currently implemented:

- *make_pdf*: A PDF rendition is generated by the Content Services software and added to the archived PrintList. To create a PDF rendition, you may want to define parameters to control how the rendition is formatted.
- *make_text*: An ASCII text rendition is generated by the Content Services Archive software and added to the archived PrintList.
- *make_html*: An HTML rendition is generated by the Content Services Archive software and added to the archived PrintList.

Implementing external filters

The filter mechanism allows you to customize Content Services Archive. You can write a filter program that parses the file to be archived and extracts special attributes for storage with the archived document.

The filter can be written in any programming or scripting language, such as Docbasic, C, C++, Perl, and JDK. It must be configured in the document profile with the Custom Filter Method parameter as described in [Specifying a custom filter](#). The filter gets a number of arguments on the command line and it writes the result back to the Content Services Archive process. For performance reasons, the filter does not need to access the repository (but it is possible if really needed).

The filter is called with the following command line parameters:

```
path dm_doc_type dm_archive object_id repository_name repository_user  
repository_password
```

The parameters are:

- *path*: Full path of the ASCII text rendition of the file to be archived. Example: '/tmp/S567378.txt'.
- *dm_doc_type*: SAP document type for which this filter is defined. Example: 'ALF'.
- *dm_archive*: SAP archive ID. Example: 'AA'.
- *object_id*: Document ID of the document created in the repository. Example: '09001edc800003af'.
- *repository_name*: Name of the current repository. This parameter is used when the filter has to connect to the repository.
- *repository_user*: Name of the repository user.
- *repository_password*: Password for the repository user.

The filter passes the result back simply by writing to the standard output. Additionally, it must return 0 (zero) when the program exits, as shown in this table.

Table 65. External filters

Language	Syntax
Docbasic	print...

Language	Syntax
C	fprintf(stdout,"...")
C++	cout << "..."
Java	

The following parameters allow the filter to pass results back to Content Services Archive:

- *set,<any attribute name>,<value>*: Defines an attribute with a given value. The attribute must exist for the object type used. By default the object type is 'dm_document'. If additional attributes must be stored, you must define a new sub-type of 'dm_document' and define that the attributes the filter uses. Use the configuration parameter 'SAP Obj Type' when using a filter with different object types.

Example: 'set,object_name,PI Sheet 4711'

- *virtual,<obj type> where <qualification>*: Allows you to specify a query that selects documents to attach to the archived document as virtual components.

Example: ' virtual,dm_document where title like 'SOP 4711%'

- *error,<error message>*: If the filter wants to report an error. We recommend storing the error on the first line of the file. The error message is written to the log file and the operator is notified.

Example: 'error,Cannot open file'

Example: PI sheet

This example creates a custom filter which extracts specific attributes from archived documents. This example uses the PI Sheet filter that was installed with the Content Services Archive software. It assumes that a second filter was installed for Inspection Lots. This filter looks similar to the PI Sheet filter, but is not explained here. This example is already installed and configured so it is not required to perform the steps explained here.

The purpose of the following customization is to extract some document attributes from an archived PI sheet. These document attributes will enable standard Documentum queries to find the PI sheet again.

The first few lines of the archived PI sheet appear as follows:

```
-----
PI sheet      : 1000000000000002128
Proc. order   : YMM_14
Plant         : 0001
CntlRecDestin. : 01
Operating grp. : GROUP 1
Dest.type     : 1
Test          :
Status         : 00005
Created on    : 05.01.1996
                  : 10:22:36
Changed on    : 05.01.1996
-----
```

To create a customized PI sheet filter:

1. Define a new document type named dm_pi_sheet.

This new document type defines the attributes you wish to extract. The document type is defined with the following DQL statement:

```
CREATE TYPE dm_pi_sheet (
    proc_order char(32), plant char(32), ctrl_rec_dest char(32),
    operating_grp char(32), dest_type char(32), status char(32)
) WITH SUPERTYPE dm_document
```

2. Create a filter that parses the PI Sheet and defines the attributes in Docbasic:

```
Sub GetMatch(l1 As String, match As String, delimiter As String, ByRef res As String)
If InStr(l1, match) = 1 Then
    pos = InStr(l1, delimiter)
    If pos > 0 Then
        fld$ = Mid$(l1, pos + 2)
    res = Trim$(fld$)
    End If
End If
End Sub

Sub Filter(arg_path As String, arg_dm_doc_type As String,_
arg_dm_archive As String,_
arg_obj_id As String, arg_docbase As String,_
arg_user As String, arg_passwd As String)
' open file and get values into variables
file% = FreeFile
Open arg_path For Input As file%
Count = 0
Do While Not EOF(file%)
' read each line and try to find values
    Line Input #file%, l1$
    GetMatch l1$, "PI sheet", ":", pi_sheet$
    GetMatch l1$, "Proc. order", ":", proc_order$
    GetMatch l1$, "Plant", ":", plant$
    GetMatch l1$, "CntlRecDestin.", ":", ctrl_rec_dest$
    GetMatch l1$, "Operating grp.", ":", operating_grp$
    GetMatch l1$, "Dest.type", ":", dest_type$
    GetMatch l1$, "Status", ":", status$
' definitions must be within the 20 first lines
    Count = Count + 1
    If (Count > 20) Then
        Exit Do
    End If
Loop
'write attributes and content to stdout
Print "set,object_name," + pi_sheet$
Print "set,proc_order," + proc_order$
Print "set,plant," + plant$
Print "set,ctrl_rec_dest," + ctrl_rec_dest$
Print "set,operating_grp," + operating_grp$
Print "set,dest_type," + dest_type$
Print "set,status," + status$

Exit Sub
End Sub
```

3. Create a method named dm_filter_pisheet with the following DQL statement:

```
CREATE dm_method OBJECT set object_name='dm_filter_pisheet',
```

```
set method_verb='dmbasic -eFilter',set timeout_min=30,
set timeout_max=604800,set timeout_default=86400,
set run_as_server=TRUE,set use_method_content=TRUE,
set method_type='dmbasic'
```

4. Use the object ID of the created method and store the Docbasic file with the following API methods.

The DQL statement in the previous step returned the object ID of the method created:

```
setfile,c,<ID of dm_method>,<Docbasic path>,crtext
save,c,<ID of dm_method>
```

5. In WebAdmin, create an archive named PI. Define this archive to use folder /SAP/PI Sheets.

Using this archive from SAP ensures that all PI Sheets are stored in this folder.

6. Configure the archive PI in SAP.

Make sure PI Sheets are archived to this archive.

7. Create a profile object (dm_al_profile) called ALF-PI:

This profile is applied when a document of the SAP document type 'ALF' is archived to the archive 'PI':

- a. Define Document Type as 'dm_pi_sheet'.
- b. Define Document Format and SAP Retrieve Format as 'sap_print_list'.
- c. Activate the Built-In Filter parameter as 'make_pdf' or 'make_html' if required.
- d. Define Custom Filter Method as 'dm_filter_pisheet'.

Note: This step is very important.

8. Test your customized filter by archiving a PI Sheet.

Check attributes and renditions to verify that the filter implementation worked correctly.

Customizing archives using service-based business objects

Documentum Business Objects are designed to provide modular business logic to the presentation layer by hiding the underlying docbase schema and by using Documentum core services, facilitating customization of object behavior without modifying any existing application built on DFC.

Service-based business objects (SBOs) are generalized objects that provide a specific service that may operate on different Documentum object types or other business objects, and are not tied to a specific Documentum object type. Each service-based business object provides a generalized interface to a group of related operations that need to be performed. The operations may not need access to a docbase, however, content management services are the focus of Documentum Business Objects.

The archiving operation can be customized using a custom filter, such as an SBO. To enable Documentum archiving customization using SBOs, an archive configuration can specify an SBO as a

custom filter. Archive Services will dynamically execute a method “doArchive (IDfPersistentObject obj, String archiveID) throws DfException” which should be defined in the SBO:

1. The SBO must have a method void doArchive (IDfPersistentObject pobj, String archiveID) throws DfException.
2. The message returned to SAP http response, in the event of any error while executing the archive customization method, should be returned by doArchive(..) method in the exception message.
3. The call to doArchive(..) runs within the context of an archiving transaction and AS SAP will do a commit() when SBO doArchive(..) is successfully executed.
4. The SBO module need not handle any function for session management for the SessionManager passed by AS SAP. For example: Transactions, Session creation, or release. SBOs can obtain session by calling getSessionManager(), getSession(), or just getSession().
5. SBOs should not release the session obtained by session management described in step 4. However, if any session manager or session is created in SBO explicitly, SBO has the responsibility to release it.
6. AS SAP will pass the IDfPersistentObject corresponding to the archived object to doArchive(..) method of the SBO. Also the archive ID will be passed (if it is an archive config object).
7. AS SAP will set the SessionManager corresponding to credentials specified in docbase configuration for the docbase to the SBO.

Customizing archives using SBOs

To customize platforms using service-based business objects (SBOs):

1. Connect to WebAdmin.
2. Click to expand the **ArchiveLink** subnode and select the **Archive** subnode.
The **Archive** screen appears.
3. Select **File > New > Archive** from the menu at the top of the Archive screen.
The Properties screen appears.
4. Enter the SBO service name, prefixed with !# in the custom filter text box, and click **OK**.
Archive a document to the content repository from SAP.
The customized functionality implemented in SBOs doArchive() method executes.

Managing temporary disk space in the CS SAP host

When an SAP archive file is accessed, CS SAP fetches the file to the local disk, and then starts streaming the content back to SAP. These locally cached files are managed by DMCL, and an algorithm implemented in DMCL determines when the files are cleaned up. If dmcl.ini is not configured appropriately, the disk may reach its default maximum capacity at some point. In order to avoid choking the disk space with these temporary files, modify the **local_diskfull_limit** attribute of the dmcl.ini file.

The **local_diskfull_limit** attribute specifies the maximum disk space assigned for storing locally cached files, and is expressed as a percentage between 1 and 100. For more information on

specifying appropriate values for the `local_diskfull_limit` attribute, refer to Support Note 77053 in the EMC Documentum Support Center (<http://softwaresupport.emc.com>).

To configure when EMC Documentum should warn you about an impending shortage of disk space, modify the `local_diskfull_warn` attribute. This attribute is expressed as a percentage between 1 and 100.

Configuring HTTP barcodes for archive linking

In the HTTP archive scenario, Agent services process “barcoded documents” and link them to SAP.

A typical scenario for implementing barcode support is in “late archiving with barcodes.”

Note: Ensure that barcodes are available for linking:

- The image is scanned.
- The barcode is recognized (by third-party software).
- The barcode is stored as a number in an object attribute (by third-party software).

To configure HTTP barcodes for archive linking:

1. Connect to WebAdmin.
2. Click to expand the **ArchiveLink** subnode and select the **Barcodes** subnode.
The **Barcodes** screen appears.
3. Select **File > New > Barcode** from the menu at the top of the **Barcode** screen.
The **Barcode Properties** screen appears.
4. Select the document type from the **Choose a Document Type:** list box.
5. Select the barcode storage attribute from the **Barcode stored in attribute:** list box.
6. Select the archive for use from the **Archive to use:** list box.
7. Click **OK** to save the barcode configuration.

Configuring HTTP certificates for archive linking

To configure HTTP certificates for archive linking:

1. Connect to WebAdmin.
2. Click to expand the **ArchiveLink** subnode and select the **Certificates** subnode.
The **Certificates** screen appears.
3. Select **File > New > Certificate** from the menu at the top of the **Certificates** screen.
The **Certificates Properties** screen appears.
4. Right-click on a certificate and select **Properties** from the sub-menu.
Selecting **Delete** removes the Certificate from the CS SAP repository
5. Select **Activate** or **Deactivate** from the **Status:** list box.

6. Select a certificate expiration date from the **Expiration:** calendar menu and list boxes.
7. Click **OK** to save the certificate configuration.

Configuring HTTP repositories for archive linking

To configure HTTP repositories for archive linking:

1. Connect to WebAdmin.
2. Click to expand the **ArchiveLink** subnode and select the **Repositories** subnode.
The **Repositories** screen appears.
3. Select **File > New > Repository** from the menu at the top of the **Repository** screen.
The **Repository Properties** screen appears.
4. Enter the connection information for the new repository, as follows:
Repository Name: Name of the new repository
User Name: User name associated with the user of the new repository
User Password: User password associated with the user name of the user of the new repository
Domain: Domain in which the new repository resides
5. Enter the connection information for the global repository associated with the new repository, as follows:
User Name: User name associated with the user of the global repository
User Password: User password associated with the user name of the user of the global repository
Domain: Domain in which the global repository resides
6. Click **OK** to save the new repository configuration.

Configuring the Agent Component

The Agent component substantially improves productivity, information integrity, and information availability by automating the linking process between SAP objects and documents, and the maintenance of those links. For example:

- Attribute information from scanned invoices can be automatically replicated from SAP to Documentum, providing non-SAP users with searchable access to invoices without having to learn SAPGUI.

The Agent component provides an automatic means of linking and replicating objects in SAP and Documentum.

Note: This feature is part of License Key 2 and will not be available if you have purchased License Key 1.

There are three parts to the Agent component known as Actions, Agents, and Jobs. Actions define what has to be done.

There are five types of Actions:

1. Linking SAP objects to Documentum objects.
2. Linking Documentum objects to SAP objects.
3. Replicating SAP objects into a Documentum repository.
4. Replicating Documentum objects into SAP.
5. Checking the integrity of the linked objects in SAP and Documentum.

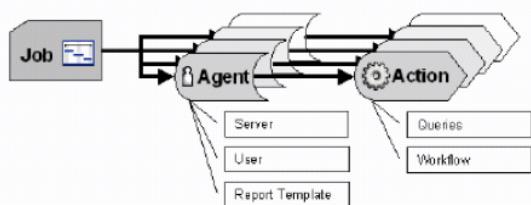
All actions use queries and workflows to perform these tasks.

Agents run the actions. The Agent defines on what machine and with which user an action is carried out as well as what the report that is generated looks like.

Jobs are scheduled events that can start Agents. There can be multiple Agents attached to a Job that are run one after the other. The job defines when the Agents have to run, according to a specified schedule.

This illustration shows the relationship between these parts.

Figure 23. Agent services



Configuring queries

Actions depend on queries to identify objects that need to be linked or replicated. The queries can be made on SAP or Documentum systems.

SAP queries

In order to test SAP queries, at least one SAP user and one SAP server have to be configured.

This specifies a query that identifies all SAP objects that must be linked to a dynamic Documentum query or to a repository folder. The query is either a query through SAP CAD Interface, PLM Interface, or a BAPI or SAP table query.

Creating, viewing, and editing an SAP query

To create, view, or edit a new query:

1. Connect to WebAdmin.
2. Click to expand the **SAP** subnode and select the **Query** subnode.
The **Query** screen appears.

3. Select **File > New > SAP Query** from the menu at the top of the **Query** screen.
The **SAP Query Properties** screen appears.
4. Enter the query name in the **Query Name:** field.
5. Choose an SAP query type from the **SAP Query Type:** list box. Your choices are described in the table below.

Table 66. Query types

Old interface Query types (for SAP R/3 version 4.6c)	New interface Query types (for SAP R/3 version 4.7 and 4.6c)
Document info record	No Object PLM (Formerly Document info record)
Equipment by short text	Equipment by short text PLM
Functional location by text	Functional location by text PLM
Material by description	Material by description PLM Note: The Material by description PLM query type has three query conditions: <ol style="list-style-type: none"> 1. MATERIALSHORTDESCSEL_low 2. MATERIALSHORTDESCSEL_Sign 3. MATERIALSHORTDESCSEL_Option All three query conditions are required if the query is to return a result.
Archive data	Archive data
Cost center	Cost center
Financial document	Financial document
Personnel links	Personnel links
Personnel master	Personnel master
Purchasing document	Purchasing document
Customer	Customer Table PLM
Print list	Print list
Vendor	Vendor Table PLM
WBS Element	WBS Element PLM
Asset Master	Asset Master GetList PLM

6. Build the query condition.

For each query condition you want to define:

- a. Choose a parameter from the **Query Condition composer:** list box and enter a value for the parameter in the text box.
- b. Click the down arrow to add the parameter and value to the **Query Condition:** field.

Note: Highlight an entry in the Query Condition field and click 'x' to delete an entry.

- c. Continue to choose parameters and enter values to build the query condition.

Note: The conditions are AND linked.

7. Click **OK** to save SAP Query configuration.

The Query screen reappears with the newly created SAP query.

8. Highlight the newly created SAP query and select File > Test from the menu at the top of the Query screen.

9. Choose a Server and a User on which to test the query, and click the test button.

Note: You must save any amendments before you implement any changes made. If the query execution on the SAP System takes too long, WebAdmin can receive a timeout.

The window shows the test results and is blank until the query results are returned.

Documentum queries

This specifies a query that selects the complete set of objects to be linked. The query can be any valid DQL query that selects at least the r_object_id and the object_name as well as one or several attributes that contain the SAP object information.

Creating, viewing, and editing a Documentum query

To create, view, or edit a new query:

1. Connect to WebAdmin.
2. Click to expand the **Documentum** subnode and select the **Query** subnode.
The **Documentum Query** screen appears.
3. Select File > New > **Documentum Query** from the menu at the top of the **Documentum Query** screen.
The **Documentum Query Properties** screen appears.
4. Enter a name for the query in the **Name:** field.
5. Enter a DQL statement for the query in the **Query:** field.

You can use the \$ARG expression when defining the DQL statement. For example:

```
select r_object_id,object_name from dm_document where object_name ='$ARG1'...
```

See [Creating, viewing, and editing SAP to Documentum links, page 583](#) for details of the \$ARG expression.

6. Click **Execute** at the far right of the **Query:** field.
The query executes.
7. Click **OK** to save Documentum Query configuration.
The Documentum Query screen reappears with the newly created Documentum query.

8. Highlight the newly created Documentum query, right-click, and select Properties from the sub-menu.

The **Query Properties** screen appears.

9. Click **Execute** at the far right of the **Query:** field.

The query executes.

Restricting SAP query results by EMC Documentum query results

Restrict the results of an SAP query by the results of an EMC Documentum query by defining an optional parameter to the SAP query type, **sap_query_plm_type_table**.

1. In the **custom.xml** file for the SAP query type, **sap_query_plm_type_table**, add a query parameter **\$DQL**:

```
<?xml version="1.0"?>
<REQUEST ON_ERROR="abort" NOTE="put your own methods inside this request">
    <OBJECT_CREATE ON_EXIST="version">
        <API_CONFIG TYPE="sap_query_plm_type_table" CLASS="sap">
            <ATTRIBUTE NAME="object_name" IS_KEY="true">
                EKPO_Table PLM
            </ATTRIBUTE>
            ...
            <ATTRIBUTE NAME="query_parameters" IS_REPEATING="true">
                <VALUE>Client=MANDT</VALUE>
                <VALUE>Document_Number=EBELN</VALUE>
                <VALUE>Item_Number=EBELP</VALUE>
                <VALUE>$DQL=</VALUE>
            </ATTRIBUTE>
            ...
        </API_CONFIG>
    </OBJECT_CREATE>
</REQUEST>
```

2. Extract the contents of dmei_custom_installer.zip into a temporary folder.
3. Locate the **dfc.properties** file in the temporary folder and edit the file with the Documentum Foundation Class directory information.
4. Locate the **installer.properties** file in the temporary folder and edit the file with the following:

Value	Definition
user.language	The default is en_US (English).
docbase.name	Name of the repository that you want to configure.
docbase.user.name	Type dm_doclink_sap or workaround ID.
domain	Name of the domain in which the repository is located.
custom.xml.path	The custom XML file path.

5. Locate the **log4j.properties** file in the temporary folder and edit to change the directory location of the log files.

Note: By default, log files are generated in the current (temporary) folder.

6. Issue the following command from the command line to run the custom XML file installer:

```
java -jar dmei_custom_installer.jar
```

Note: The file dmei_custom_installer.jar is in the temporary folder where you extracted the contents of the dmei_custom_installer.zip file.

7. Enter the password for the repository specified in the dfc.properties file.

File processing begins and the message **Processing Successfully Completed!** appears when processing completes.

You have now added the **\$DQL** parameter to the SAP query type, **sap_query_plm_type_table**.

Note: If the **Processing Failed!** message appears, look in the log files to determine the problem with the custom.xml file installation.

A DQL query can be provided as value for the **\$DQL** parameter created previously.

To assign a DQL query as value for the \$DQL parameter for the SAP query type, sap_query_plm_type_table:

1. Connect to WebAdmin.
2. Click to expand the **SAP** subnode and select the **Query** subnode.
The SAP Query screen appears.
3. Select File > New > SAP Query from the menu at the top of the Query screen.
The Properties screen appears.
4. Enter a query name in the **Query Name:** field.
5. From the **SAP Query Type** drop-down list, select **EKPO_Table PLM**.
6. From the **Query Condition Composer** drop-down list, select **\$DQL**.
7. Type a DQL query as value for this parameter.

Example 21-1.

\$DQL=select item_id from sap_abc_document where sap_document_number IS NULL

8. Click the down arrow to add the parameter and value to the **Query Condition:** field.

9. In the **Condition Composer**, compose another condition as follows:

Item_number=\$item_id

10. Click the down arrow to add the parameter and value to the **Query Condition:** field.

11. Click OK to save the query.

SAP queries can now be restricted by selecting query conditions based on values obtained from the \$DQL query result set.

Testing queries with \$ARG# statements

By configuring a Documentum Query with Arguments (\$ARG#) in the DQL statement, the query can be used later for Link Actions.

The \$ARG# variable has to be numbered, for example \$ARG1, \$ARG2. The variable can be used as a placeholder that will be resolved during runtime.

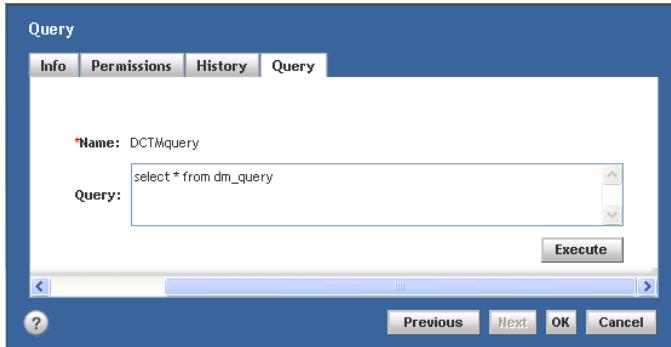
```
select r_object_id, object_name from dm_document where object_name ='$ARG1'
```

This query will select all documents of type dm_document, where the object name equals a given substitute for the argument with the number 1. An explanation on how these queries can be used for a link action is in [Creating, viewing, and editing SAP to Documentum links, page 583](#).

When testing, the query will be parsed for occurrences of \$ARG# and the user will be prompted to enter a substitution for every argument found.

When all arguments are replaced according to the string, the final query that is about to be tested will be shown.

Figure 24. Query test



Support for \$TODAY in FromDate parameter for sap_query_type_rfc query type

CS SAP supports \$TODAY in FromDate parameter for sap_query_type_rfc query type.

In order to download selected SAP object keys from transaction **oa01** (RFC ARCHIV_GET_CONNECTIONS), SAP makes the selection based on the current date. This allows SAP to select a dataset limited by the amount of archived files produced in a day, in addition to a given Business Object Type or Archive Type.

\$TODAY parameter can be specified in **FromDate** parameter in **Condition Composer**.

To select all BKPF-linked documents archived in the last 3 days, use a query of type “Financial document”. This uses **sap_query_type_rfc** to call **ARCHIV_GET_CONNECTIONS**:

1. Connect to WebAdmin.
2. Click to expand the **SAP** subnode and select the **Query** subnode.
The **SAP Query** screen appears.
3. Select **File > New > SAP Query** from the menu at the top of the Query screen.
The **Properties** screen appears.
4. Enter a query name in the **Query Name:** field.
5. From the **SAP Query Type** drop-down list, select **Financial document**.
Financial document is of query type **sap_query_type_rfc**.
6. From the **Query Condition Composer** drop-down list, select **FromDate**.
7. Type the following value for this parameter:
\$TODAY-3

8. Click the down arrow to add the parameter and value to the **Query Condition:** field.

The query would be as follows:

```
FromDate=$TODAY-3
```

Example 21-2.

If this query was executed on October 17, 2005, then the symbolic value is expanded to 20051017-3 = 20051014. This query instructs **ARCHIV_GET_CONNECTIONS** to select data of the last 3 days only.

9. Click **OK** to save the query.

Linking objects

Agent services make use of the SAP DMS interface to perform linking of objects from Documentum into SAP. The DMS interface was originally built to integrate CAD applications into an SAP system. Subsequently, SAP expanded the DMS interface to include integrations with Product Lifecycle Management (PLM) systems. The PLM Interface is the “next generation” of the DMS interface and greatly enhances its functionality.

A set of API functions called the “CAD Interface” allow you to access SAP server version 4.6c from external applications like the Agent services or CAD Systems.

The “PLM Interface” is comprised of a set of API functions and allows you to access the SAP server from external applications like the Agent services or PLM Systems, like Documentum. With the PLM Interface you can access SAP server version 4.7 and 4.6c. In addition to accessing the content on your SAP 4.7 server, the PLM Interface enables you to get editable copies of it, and check it into and out of your Documentum repository.

In order to link from objects in SAP to objects held in Documentum, the SAP DMS creates objects in SAP called Document Info Records (DIRs).

A DIR is created in SAP for every document released from Documentum. The DIR contains several attributes like description, document ID, document version, and a reference to a specific Documentum object in the Documentum repository.

The SAP client application (SAPGUI) can launch an external application for specific content or carrier types (in SAP terminology). These external applications include Content Services View installed on workstations running SAPGUI.

When a document previously released from Documentum into SAP is viewed, Content Services View is launched and the information stored in the DIR is passed to this application. With this information, the Documentum Content Server is queried and the requested document is retrieved and displayed with a viewer application on the SAP workstation.

Document linking actions allow you to specify attributes for the DIR using the “Rule Composer.” The rule composer allows you to specify the following attributes for a DIR:

- DocumentNumber: SAP DIR number. A document number specified by the Agent could be, for example, "DocumentNumber=\"%s\",i_chronicle_id." This must be a unique number.
- DocumentDescription: Description attribute of DIR. A value must be defined. Example: "DocumentDescription=\"%s\",object_name." If not specified the object name is used by default.

- DocumentType: SAP document type (for example "DocumentType="DOC"). The default is "DRW."

Note: Since the PLM type objects are usually drawings, a default value of "DRW" is used. You can always override this setting in the Query Conditions field of the SAP Query Composer, as described in [Creating, viewing, and editing an SAP query, page 576](#).

Example 21-3.

You can assign the value of DocumentType as DES for a DES document type.

For all document types, you can set the value of DocumentType as one of the following:

- DocumentType=*
- DocumentType=

In this case, no value has been assigned to the parameter. The value for the parameter has been set to blank.

- DocumentStatus: An SAP Document Status can be specified =PI. This is mandatory for PLM-based SAP object types.

Creating, viewing, and editing SAP to Documentum links

In the following example you want to link all materials within SAP that have a description starting with "pump*" to a document in the repository with the same object_name as the material's description.

You will need to create:

- An SAP Query "Select all pumps" which selects materials with the following condition:

```
Description = pump*
```

This query (Querytype: Material by Description) returns the following attributes:

```
Description, Type, Industry, Material
```

- Documentum Query "FindObjectName" which selects objects of type dm_document where the object_name equals "\$ARG1":

```
Select r_object_id, object_name from dm_document where object_name = '$ARG1'
```

- Link SAP Action "Link query to pumps" uses both queries ("Select all pumps" and "FindObjectName") and has the following map rules:

\$ARG1	= Material
DocumentType	= "DRW"
DocumentDescription	= "Documents for %s", Material

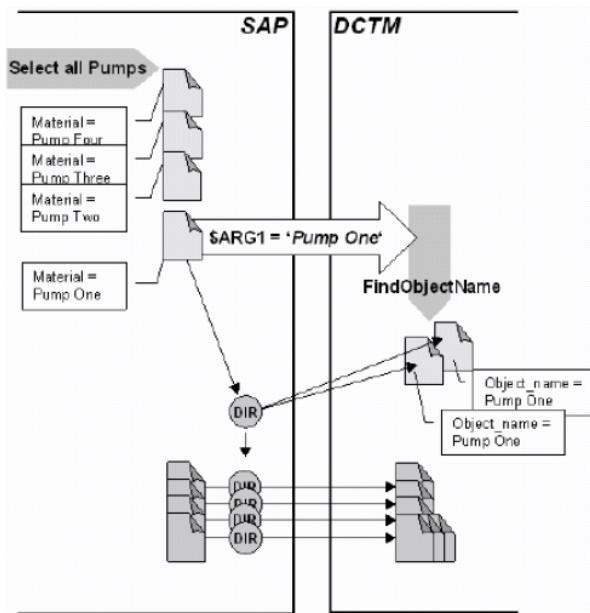
The result is:

The Link SAP action runs "Select all pumps" (SAP Query), returning a number of SAP material objects with their description matching "pump*".

For each object returned, the content of attribute “Material” is passed as a substitution for “\$ARG1” to “FindObjectName” (DCTM Query). Assuming the attribute “Material” of the first object is “Pump One”, the action continues as follows:

- “FindObjectName” selects a number of documents [1..n] with an object_name that equals “Pump One.”
- The DIR is created for the current SAP object with links to the documents in the repository named “Pump One.”
- The additional DIR attributes are assigned according to the map rules. The DocumentType is “DRW” and the DocumentDescription is “Documents for Pump One.”
- This loop will be repeated for each object returned by “Select all pumps” (SAP Query), thereby establishing the goal.

Figure 25. Linking result



To configure a Link SAP to Documentum action, you will need a Documentum Query and a previously configured SAP Query. In order to specify a workflow, it has also to be previously defined.

To create, view, or edit SAP to Documentum links:

1. Connect to WebAdmin.
2. Click to expand the **Actions** subnode and select the **Link SAP** subnode.
The **Link SAP** screen appears.
3. Select **File > New > Link SAP** from the menu at the top of the Link SAP screen.
The **Link SAP Properties** screen appears.
4. Enter an action in the **Action:** field.
5. Choose the SAP system from the **SAP System Type:** list box.
6. Choose the Documentum query from the **Documentum Query:** list box.

7. Choose the SAP query from the **SAP Query:** list box.
8. Link Workflow is set to No Workflow.
9. Check **Verify object links**, if required.
10. Use the Map Rule Composer for each rule you want to define:
 - a. Choose the variable from the **Variables** list box.
 - b. Enter the format of the variable in the **Format** field.
 - c. Choose the parameter required from the list box and click the up arrow to add the parameter to the **Parameters** field.

The up arrow also alters the format string by adding %s at the end.

The attribute map allows you to specify the following:

DIR attributes: When a document is released to SAP, an SAP DIR is created for it. Values can be set for DocumentType, DocumentDescription, DocumentNumber, and DocumentStatus. For example, the rule Document Description = "Document for %s", Material will build a DIR description containing the Material attribute from the SAP object returned by the SAP query chosen.

\$ARG#s: In order for the SAP object to be linked to a Documentum object, Content Services must be able to find the related object in the repository. Here you specify the substitution for an \$ARG# in the DQL statement of the Documentum query. In this way a lookup into Documentum is defined which identifies the object(s) which the SAP object should be linked to.

 - d. Click the down arrow to add the rule to the **Defined Map Rules:** field.
11. Click **OK** to save the SAP to Documentum link configuration.

Creating, viewing, and editing Documentum to SAP links

This action links specific documentum objects to SAP objects. When configured and executed using the Auto Manage function, this action works as follows:

- Reads the Agent configuration object to retrieve the SAP connection parameters.
- Connects to SAP.
- Executes the Documentum Query.
- Each returned object is then processed as follows:
 - The Attribute Map is used to find the specific related SAP object.
 - If the SAP object is found, then CS SAP checks to see if this object is already linked. If it is not linked, then a DIR is created in SAP. The attribute map is used to set the DIR attributes.

In the following example you want to link all sub-folders of the folder /SAP/Material to a Material in SAP where the material attribute matches the folder name.

You will need to create/configure:

- A Documentum Query "SelectMaterialFolders" selects objects of type dm_folder where the folder's location has to be /SAP/Material:

```
select r_object_id,object_name from dm_folder where folder('/SAP/Material')
```

- “Material Master” is the SAP Object Type that you want to link to your material folders. This SAP Object Type has the following attributes:

MaterialType, Material, Industry, BaseUnit, Description, Pant

These attributes are shown with the prefix “key” in the map rules, indicating that they can be used as search conditions in the generated SAP Query.

- Link Documentum Action “Link material folders” has the following map rules:
-

key.Material	= "%s", object_name
DocumentType	= "DRW"
DocumentDescription	= "Document folder for %s", object_name

The action will link the following version and format of the folders:

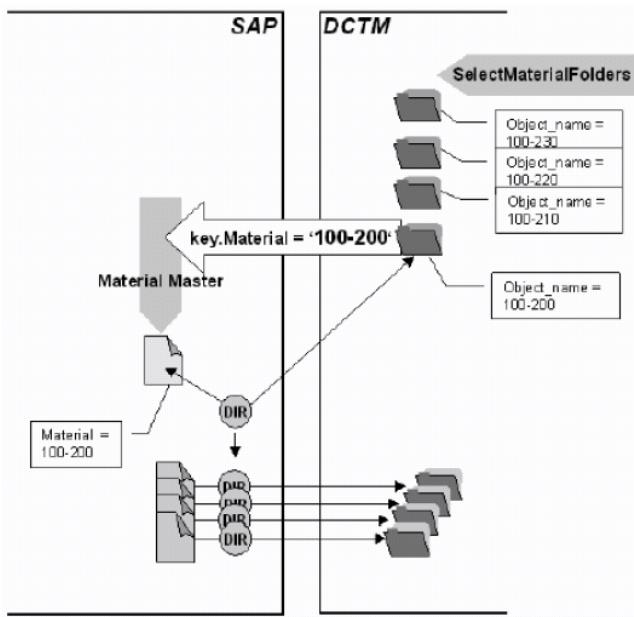
Format:	Best Format
Version:	Current Version

The result is:

The Link Documentum action runs “SelectMaterialFolders” (Documentum Query), returning a number of folders in the folder /SAP/Material.

For each folder returned, the content of attribute “object_name” is passed to an SAP query for SAP object type Material Master as condition for the attribute Material. Assuming the attribute “object_name” of the first folder is “100-200”, the action continues as follows:

- The created SAP Query for “Material Master” selects one object [1] with the attribute Material matching “100-200.”
- Then the DIR is created for the current folder and the selected SAP objects, using the defined version and format.
- The additional DIR attributes are assigned according to the map rules. The DocumentType is “DRW” and the DocumentDescription is “Document folder for 100-200.”
- This loop will be repeated for each folder returned by “SelectMaterialFolders” (Documentum Query), thereby establishing the objective.

Figure 26. Linking result

To configure a Link Documentum to SAP action, you will need a previously configured Documentum Query. In order to specify a workflow it has also to be previously defined.

To create, view, or edit Documentum to SAP links:

1. Connect to WebAdmin.
2. Click to expand the **Actions** subnode and select the **Link Documentum** subnode.
The **Link Documentum** screen appears.
3. Select **File > New > Link Documentum** from the menu at the top of the Link Documentum screen.
The **Link Documentum Properties** screen appears.
4. Enter an action name **Action:** field.
5. Choose the SAP system from the **SAP System Type:** list box.
6. Choose the SAP object from the **SAP Object Type:** list box.
7. Choose the Documentum Query from the **Documentum Query:** list box.
8. Link Workflow is set to No Workflow.
9. Select **Verify object links**, if required.
10. Define the binding rules.
 - a. Choose the format from the **Format:** list box.
Enter which document format/rendition should be released to SAP. Best Format and Primary Content Format are configured using CS SAP WebAdmin as described in [Configuring the Manage and View Components](#).
 - b. Choose the version of the document that should be released and the version required from the list box to the right of the **Version:** field, and then click the arrow to add that version to the **Version:** field.

Choose a specific version label, such as "DRAFT", or use a keyword like dms_selected_version or dms_all_versions. If all versions are released to SAP, then the CS SAP Viewer will display a list of all possible document versions.

11. Use the Rule Composer to define each Attribute Map:

- a. Choose a variable from the **Variables** list box.
- b. Enter the format of the variable in the **Format** field.
- c. Choose the parameter from the list box below the **Parameters** field, and click the up arrow to add the parameter to the **Parameters** field.
The up arrow also alters the format string by adding %s at the end.
- d. Click the down arrow to add the rule to the **Defined Map Rules** field.

The attribute map allows you to specify the following:

- **DIR attributes:** When a document is released to SAP, an SAP DIR is created for it. Values can be set for DocumentType, DocumentDescription, DocumentNumber, and DocumentStatus. For example, the rule **Document Description = "Related SOP for %s"**, object_name will build a DIR description containing the object_name attribute from the Documentum document.
- **Lookup Key Values:** In order for the Documentum object to be linked to an SAP object, Content Services must be able to find the related object in SAP. Here you specify a lookup into SAP which identifies the single object which the document should be linked to. For example, key.Material="%s", object_name will instruct Content Services to link the Documentum object to an SAP material which has the material name equal to the Documentum object_name.

12. Click **OK** to save the Documentum to SAP link configuration.

Automated early archiving using the Agent component

The Agent component can now be used to automate the movement of incoming TIFF images to SAP work items. This is done by configuring a Link Documentum action using parameters similar to the following example:

```
SAP Object Type = Image assign sap workflow  
Dctm Query = SelectInvoiceFolders
```

Create a Documentum Query that returns the object name and object ID of the documents to be sent to SAP, for example, "select r_object_id,object_name from sap_invoice where folder('/SAP/Invoices')."

```
Key.DocumentType=ZFIINVOICE  (enter your custom SAP document type for  
incoming TIFF images)  
Key.Objecttype=BKPF    (enter your SAP object type)  
Key.ArchiveId=Q2  
Key.Drl=Drl
```

Arbitrary parameters when starting an SAP workflow

Content Services for SAP expands the customizing options described above in "Automated Early Archiving Using the Agent component" similar to the 'Image assign sap workflow' action. When creating a custom BAPI, based on the ARCHIV_PROCESS_RFCINPUT function, define optional parameters to be passed to the DOCUMENT_DATA table parameter.

Add an attribute name to appear in the WebAdmin attribute map to a name on the lines of DOCUMENT_DATA-<paramname>; for example, DOCUMENT_DATA-DESCRIPTION, to the "sap_container" attribute. The mapped value is added in the DOCUMENT_DATA table with NAME=<paramname>.

For example, the addition of the attribute name, DESCRIPTION, to the following line:

```
<VALUE>Description=DOCUMENT_DATA-DESCRIPTION</VALUE>
```

and the following mapping:

```
"Description" -> "Object ID: %s, r_object_id"
```

adds a line like the following:

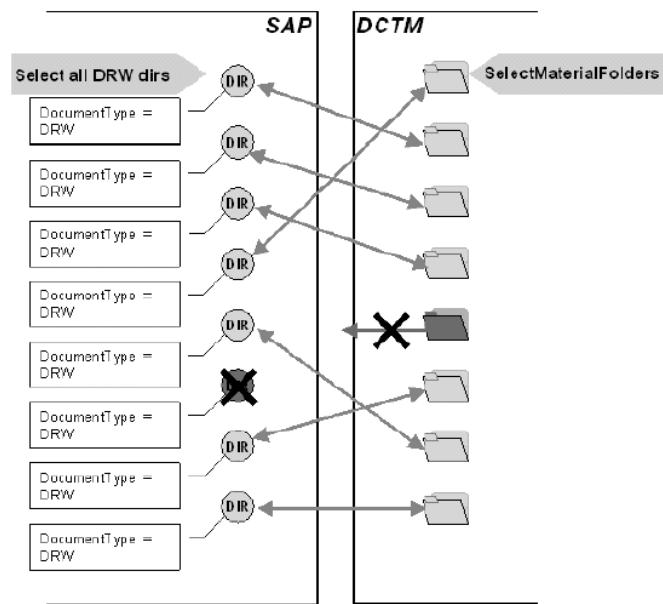
```
NAME=DESCRIPTION, WERT=Object ID: 09f97a8d8000e658
```

to the DOCUMENT_DATA table parameter.

Checking the integrity of linked documents

After the Agent has automatically linked the SAP and Documentum object, it is technically possible to manually edit or delete DIRs in SAP. It is therefore possible to change/delete links from SAP without receiving a notification of this within Documentum. To help ensure the integrity of the links between SAP and Documentum, it is possible to write a rule to perform an integrity check between the two systems. *Content Services for SAP does not attempt to fix problems: it just reports them.*

The aim of this action is to generate a report that details any mismatches between Documentum and SAP. The action builds two lists and looks to see whether there is a Documentum object, such as a document, folder, or query, related to each retrieved DIR. In the end, all DIRs that have no Documentum object linked to them are listed in a report. If there is no DIR for a Documentum object, the relation to this object is listed in a report. This is shown in the following illustration.

Figure 27. Integrity checking

Note: To configure a Check DIR action, you will need a Documentum query and an SAP query, both previously configured.

To check integrity of objects in both systems:

1. Connect to WebAdmin.
2. Click to expand the **Actions** subnode and select the **Check Document Info Records** subnode. The **Check Document Info Records** screen appears.
3. Select **File > New > Check Document Info Records** from the menu at the top of the Check Document Info Records screen. The **Check Document Info Records Properties** screen appears.
4. Enter an action name in the **Action:** field.
5. Choose the Documentum query from the **Documentum Query:** list box.
6. Choose the SAP query from the **SAP Query:** list box.
7. Click **OK** to save the DIR check.

Replication of information between Documentum and SAP

CS SAP provides a facility for maintaining the integrity of documents held in SAP with those stored in Documentum.

Replication is the duplication of data held in one system into another system.

The replication process, once started updates all objects not matching the set conditions and not yet updated.

Replicating SAP objects

Replication creates images of SAP objects in Documentum. For example, you may want to replicate invoice information into archived images in Documentum.

In the following example you want to replicate all pumps within SAP as folders in the /SAP/Material folder (in the Documentum repository) in order to store additional documents to each pump in that folder. Replicating here means, that the folder should have the same attributes, as the actual SAP object has, in order to be able to search for a specific pump in the repository as well. When the folders are generated you would be able to link them back to the SAP pump objects.

You will need to create/configure:

- An SAP Query “Select all pumps” selects materials with the following condition:

```
Description = pump*
```

This query (Querytype: Material by Description) returns the following attributes:

```
Description, Type, Industry, Material
```

- Documentum Object Type “dm_folder” is the Documentum Object Type that you want to represent the SAP pumps in the repository.
- Replicate SAP Action “Replicate material folder” has the following rules:

The *Object Key* rules are used to check whether there is a dm_folder object with the path /SAP/Material and the object_name matching the material attribute of the current pump object in SAP.

object_name	= "%s", Material
FOLDER	= "/SAP/Material"

The *Update Condition* rules are used to check whether the attributes of the folder have to be updated (only validated if “update object” is checked). Here you only update the folder if the title of the folder is empty.

The *Map Rules* are used to define the mapping of the SAP attributes to the Documentum attributes.

object_name	= "%s", Material
title	= "%s", Description
FOLDER	= "/SAP/Material"

The result is:

The Replicate SAP action runs “Select all pumps” (SAP Query), returning a number of SAP material objects with their description matching “pump*”.

For each object returned, the Replication action checks whether the dm_folder object already exists. Assuming the attribute Material of the first pump is “Pump One” the query looks like this:

```
Select r_object_id from dm_folder where object_name = 'Pump One'  
and folder('/SAP/Material')
```

If the folder does not exist (no record returned), the action checks whether it should create one (“create object” is checked). Otherwise it checks the update condition (“update object” is checked). In this case, the action looks for whether the title of the returned dm_folder is empty.

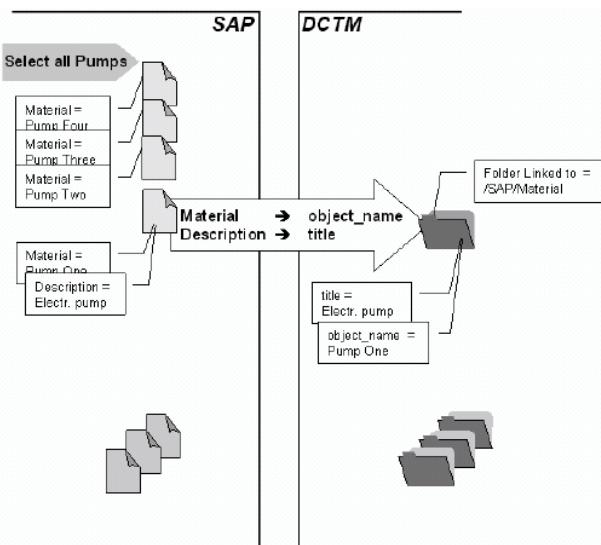
If the folder has to be created or updated, the action maps the SAP attributes to the specified Documentum attributes.

Object_name	= "Pump One"
Title	= "Electr. Pump"
FOLDER	= "o" "t"

Note: FOLDER is a special attribute since it does not really exist. The action creates the dm_folder object in the specified repository folder if a creation is necessary.

This loop will be repeated for each object returned by “Select all pumps” (SAP Query), thereby establishing the goal.

Figure 28. Replication result



To configure a Replicate SAP action, you will need a previously configured SAP query. In order to specify a workflow it has also to be previously defined.

To replicate SAP objects in Documentum:

1. Connect to WebAdmin.
2. Click to expand the **Actions** subnode and select the **Replicate SAP** subnode.
The **Replicate SAP** screen appears.
3. Select **File > New > Replicate SAP** from the menu at the top of the Replicate SAP screen.
The **Replicate SAP Properties** screen appears.
4. Enter an action name in the **Action:** field.

5. Choose the SAP system from the **SAP System Type**: list box.
6. Choose the Object type from the **Object Type**: list box.
7. Choose the SAP query from the **SAP Query**: list box.
8. **Link Workflow** is set to No Workflow.
9. Select **Update Object**, if required.
10. Select **Create Object**, if required.
11. For eachObject Key, Update Condition, and Map Rule you want to define:
 - a. Choose the variable from the **Variable** list box.
 - b. Enter the format of the variable in the **Format** field.
The entry is altered with %s automatically added at the end.
 - c. Choose the parameter required from the list box below the **Parameters** field, and click the up arrow to add the parameter to the **Parameters** field.
 - d. Click **ADD** to add the rule to the **Object Key**, **Update Condition**, and\or **Map Rules** fields.
12. Click **OK** to save the action.

Replicating Documentum objects

In the following example, you want to update the Status of Document Info Record (DIR) attribute in SAP to reflect a change in the status of the Documentum object. Replication in this example means updating SAP objects, not creating new ones. This example can be found as a configuration object in WebAdmin, called Update DIR status. We will execute a Documentum query and update the related DIRs to reflect a change in document status.

You will need to create/configure:

- A Documentum Query “SelectMaterialFolders” selects objects of type dm_folder where the folder’s location has to be /SAP/Material:


```
select r_object_id,object_name from dm_folder where folder('/SAP/Material')
```
- An SAP Object Type: “Document info record” is the SAP Object Type that you want to update in SAP.
- Replicate Documentum Action “Update DIR status” has the following rules:

The *Object Key* rules are used to check whether there is an SAP object for the current dm_folder with the document number attribute matching the folder’s object_ID.

DocumentNumber	= "%s", r_object_id
DocumentType	= "DRW"
DocumentPart	= "000"
DocumentVersion	= "00"

The *Update Condition* rules are used to check whether the attributes of the SAP object have to be updated (only validated if “update object” is checked.) This means we update the DIR only if its status is “AA”.

DocumentStatus = “AA”

The *Map Rules* are used to define the mapping of the Documentum attributes to the SAP attributes.

DocumentStatus = “IA”

The Replicate Documentum action runs “SelectMaterialFolders” (Documentum Query), returning the sub folders of /SAP/Material.

For each folder returned, the Replication action checks whether the corresponding Material Master object exists in SAP. If it does, the DocumentStatus attribute for the DIR will be checked to see if it is “AA.” If it is, the status will be updated to “IA.”

To replicate Documentum objects in SAP:

1. Connect to WebAdmin.
2. Click to expand the **Actions** subnode and select the **Replicate Documentum** subnode.
The **Replicate Documentum** screen appears.
3. Select **File > New > Replicate Documentum** from the menu at the top of the **Replicate Documentum** screen.
The **Replicate Documentum Properties** screen appears.
4. Enter an action name **Action:** field.
5. Choose the SAP system from the **SAP System Type:** list box.
6. Choose the SAP object from the **SAP Object:** list box.
7. Choose the Documentum query from the **Documentum Query:** list box.
8. **Link Workflow** is set to No Workflow.
9. Select **Update object**, if required.
10. Select **Create object**, if required.
11. For the Object Key, Update Condition, and each Map Rule you want to define:
 - a. Choose the variable from the **Variables** list box.
 - b. Enter the format of the variable in the **Format** field.
The entry is altered with %s automatically added at the end.
 - c. Choose the parameter required from the list box below the **Parameters** field, and click the up arrow to add the parameter to the **Parameters** field.
 - d. Click **ADD** to add the rule to the **Object Key**, **Update Condition**, and \or **Map Rules** fields.
12. Click **OK** to save the action.

Replicating custom DMS attributes from EMC Documentum to SAP

Documentum Administrator allows you to replicate custom DMS attributes from EMC Documentum to SAP.

This section contains the following topics:

- [Configuring classification attributes for sap_query_type_plm query types, page 595](#)
- [Replicating custom DMS attributes to SAP custom tables, page 597](#)

Configuring classification attributes for sap_query_type_plm query types

Documentum Administrator supports custom DMS classification attributes. Custom DMS classification attributes can be set for the **CLASSIFICATIONVALUES** and **CLASSALLOCATIONS** table parameters of **BAPI_DOCUMENT_CHANGE/CREATE**.

To configure classification values for sap_query_type_plm query types:

1. Browse to the directory where you extracted the contents of the CS SAP installer archive, and open the **custom.xml** file for editing.
2. In the **custom.xml** file, use the following convention to configure the **sap_query_type_plm** query type to the corresponding custom DMS classification attributes:

```
<VALUE><VariableName>=CHARACTERISTICVALUES.<CLASSTYPE>.<CLASSNAME>
<CHARACTERISTICNAME>, <DELETIONFLAG>, <SIZE> </VALUE>
```

For example, you can set classification values and class allocations as follows:

```
<VALUE>Instruction=CHARACTERISTICVALUES.017.SPEC_APPEARANCE.
CHARNAME_INSTRUCTION,0,30</VALUE>
```

A sample **sap_query_type_plm** definition would be as follows:

```
<?xml version="1.0"?>
<REQUEST ON_ERROR="abort">
<OBJECT_CREATE ON_EXIST="version">
    <API_CONFIG TYPE="sap_query_type_plm" CLASS="sap">
        <ATTRIBUTE NAME="object_name" IS_KEY="true">Document Info Record
        PLM</ATTRIBUTE>
        <ATTRIBUTE NAME="function_module_create">BAPI_DOCUMENT_CREATE
        </ATTRIBUTE>
        <ATTRIBUTE NAME="function_module_update">BAPI_DOCUMENT_CHANGE
        </ATTRIBUTE>
        <ATTRIBUTE NAME="sap_object_type"></ATTRIBUTE>
        <ATTRIBUTE NAME="query_parameters" IS_REPEATING="true">
            <VALUE>DocumentType=DOCUMENTDATA.DOCUMENTTYPE,3</VALUE>
            <VALUE>Description=DOCUMENTDATA.DESCRIPT_D,40</VALUE>
            <VALUE>DocumentNumber=DOCUMENTDATA.DOCUMENTNUMBER,25</VALUE>
            <VALUE>DocumentVersion=DOCUMENTDATA.DOCUMENTVERSION,2</VALUE>
            <VALUE>DocumentPart=DOCUMENTDATA.DOCUMENTPART,3</VALUE>
            <VALUE>DataCarrier1=DOCUMENTDATA.DATA_CARR,2</VALUE>
            <VALUE>WSApplication1=DOCUMENTDATA.DISPLAY_APPL,10</VALUE>
            <VALUE>DocFile1=DOCUMENTDATA.ORIGINAL,255</VALUE>
            <VALUE>STATUSEXTERN=DOCUMENTDATA.DOC_STATUS,2</VALUE>
            <VALUE>USERDEFINED1=DOCUMENTDATA.USERDEFINED1,14</VALUE>
            <VALUE>USERDEFINED2=DOCUMENTDATA.USERDEFINED2,14</VALUE>
            <VALUE>USERDEFINED3=DOCUMENTDATA.USERDEFINED3,14</VALUE>
            <VALUE>USERDEFINED4=DOCUMENTDATA.USERDEFINED4,14</VALUE>
            <VALUE>Laboratory=DOCUMENTDATA.LABORATORY,3</VALUE>
```

```

<VALUE>HostName=HOSTNAME, 20</VALUE>
<VALUE>Color=CHARACTERISTICVALUES.017.SPEC_APPEARANCE.
    CHARNAME_COLOR, 0, 30</VALUE>
<VALUE>Instruction=CHARACTERISTICVALUES.017.SPEC_APPEARANCE.
    CHARNAME_INSTRUCTION, 0, 30</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="parameter_defaults" IS_REPEATING="true">
    <VALUE>DocumentType=DRW</VALUE>
    <VALUE>DocumentVersion=00</VALUE>
    <VALUE>DocumentPart=000</VALUE>
    <VALUE>DataCarrier1=DOCUMENTUM</VALUE>
    <VALUE>WSApplication1=DCM</VALUE>
    <VALUE>SPEC_INSTRUCTION=DEFAULT_VALUE</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="result_parameters" IS_REPEATING="true">
    <VALUE>DocumentNumb=DOCNUMBER, 25</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="key_attributes" IS_REPEATING="true">
    <VALUE>DocumentType=DOCUMENTTYPE, 0, 3</VALUE>
    <VALUE>DocumentNumber=DOCUMENTNUMBER, 3, 25</VALUE>
    <VALUE>DocumentPart=DOCUMENTPART, 30, 3</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="methods" IS_REPEATING="true">
    <VALUE>Create</VALUE>
    <VALUE>Update</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="result_table">DOCUMENTSTRUCTURE, 64</ATTRIBUTE>
</API_CONFIG>
</OBJECT_CREATE>
</REQUEST>

```

3. Extract the contents of **dmei_custom_installer.zip** into a temporary folder.
4. Locate the **dfc.properties** file in the temporary folder and edit the file with the Documentum Foundation Class directory information.
5. Locate the **installer.properties** file in the temporary folder and edit the file with the following:

Value	Definition
user.language	The default is en_US (English).
docbase.name	Name of the repository that you want to configure.
docbase.user.name	Type dm_doclink_sap or workaround ID.
domain	Name of the domain in which the repository is located.
custom.xml.path	The custom XML file path.

6. Locate the **log4j.properties** file in the temporary folder and edit to change the directory location of the log files.

Note: By default, log files are generated in the current (temporary) folder.

7. Issue the following command from the command line to run the custom XML file installer:

```
java -jar dmei_custom_installer.jar
```

Note: The file **dmei_custom_installer.jar** is in the temporary folder where you extracted the contents of the **dmei_custom_installer.zip** file.

8. Enter the password for the repository specified in the **dfc.properties** file.

File processing begins and the message Processing Successfully Completed! appears when processing completes.

You have configured classification values for sap_query_type_plm query types; Documentum Administrator can now replicate custom DMS attributes of a document from EMC Documentum to SAP.

The classification values that you configured here are accessible from the **Rule Composer** section of the **Link Documentum** and **Replicate Documentum** tabs in WebAdmin.

Note: If the Processing Failed! message appears, look in the log files to determine the problem with the custom.xml file installation.

Replicating custom DMS attributes to SAP custom tables

Documentum Administrator supports replicating DMS classification attributes from EMC Documentum to SAP custom tables.

To replicate custom DMS attributes to SAP custom tables:

1. Start SAP GUI and connect to an SAP R/3 system.
 2. In the command field, execute the **/se80** transaction code.
 3. Use the options available in the **Object Navigator** page to define a custom SAP table.
- Definition of a sample custom SAP table is as follows.

Field	Element	Type	Length	Description
MANDT	MANDT	CLNT	3	Client
DOKAR	DOKAR	CHAR	3	Document Type
DOKNR	DOKNR	CHAR	25	Document Number
DOKTL	DOKTL_D	CHAR	3	Document Part
DOKVR	DOKVR	CHAR	2	Document Version
DOKDSR	DOKDSR	CHAR	25	Document Description

4. Browse to the directory where you extracted the contents of Documentum Administrator's installer archive, and open the **custom.xml** file for editing.
5. In the **custom.xml** file, specify entries that correspond to the definition of the custom table you created in step 2.

The emphasized portion of the following sample snippet (from a **custom.xml** file) indicates how the entries in the **custom.xml** file correspond with the definition of the sample custom SAP table shown in step 2:

```
<?xml version="1.0"?>
<REQUEST ON_ERROR="abort">
<OBJECT_CREATE ON_EXIST="version">
    <API_CONFIG TYPE="sap_query_type_plm" CLASS="sap">
        <ATTRIBUTE NAME="object_name" IS_KEY="true">Document Info Record
        PLM</ATTRIBUTE>
        <ATTRIBUTE NAME="function_module_create">BAPI_DOCUMENT_CREATE
        </ATTRIBUTE>
        <ATTRIBUTE NAME="function_module_update">BAPI_DOCUMENT_CHANGE
    </API_CONFIG>
</OBJECT_CREATE>
<REQUEST>
```

```

</ATTRIBUTE>
<ATTRIBUTE NAME="sap_object_type"></ATTRIBUTE>
<ATTRIBUTE NAME="query_parameters" IS_REPEATING="true">
    <VALUE>DocumentType=DOCUMENTDATA.DOCUMENTTYPE,3</VALUE>
    <VALUE>Description=DOCUMENTDATA.DESCRIPT_D,40</VALUE>
    <VALUE>DocumentNumber=DOCUMENTDATA.DOCUMENTNUMBER,25</VALUE>
    <VALUE>DocumentVersion=DOCUMENTDATA.DOCUMENTVERSION,2</VALUE>
    <VALUE>DocumentPart=DOCUMENTDATA.DOCUMENTPART,3</VALUE>
    <VALUE>DataCarrier1=DOCUMENTDATA.DATA_CARR,2</VALUE>
    <VALUE>WSApplication1=DOCUMENTDATA.DISPLAY_APPL,10</VALUE>
    <VALUE>DocFile1=DOCUMENTDATA.ORIGINAL,255</VALUE>
    <VALUE>StatusExtern=DOCUMENTDATA.DOC_STATUS,2</VALUE>
    <VALUE>UserDefined1=DOCUMENTDATA.USERDEFINED1,14</VALUE>
    <VALUE>UserDefined2=DOCUMENTDATA.USERDEFINED2,14</VALUE>
    <VALUE>UserDefined3=DOCUMENTDATA.USERDEFINED3,14</VALUE>
    <VALUE>UserDefined4=DOCUMENTDATA.USERDEFINED4,14</VALUE>
    <VALUE>Laboratory=DOCUMENTDATA.LABORATORY,3</VALUE>
    <VALUE>HostName=HOSTNAME,20</VALUE>
    <VALUE>Color=CHARACTERISTICVALUES.017.SPEC_APPEARANCE.
        CHARNAME_COLOR,0,30</VALUE>
    <VALUE>Instruction=CHARACTERISTICVALUES.017.SPEC_APPEARANCE.
        CHARNAME_INSTRUCTION,0,30</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI>=
        ZCUSTOM_BAPI.BAPI_NAME,30</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Table>=
        ZCUSTOM_BAPI.TABLE_NAME,30</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Client>=
        ZCUSTOM_BAPI.BAPI_CLIENT,3</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Document_Type>=
        ZCUSTOM_BAPI.BAPI_DOCUMENTTYPE,3</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Document_Number>=
        ZCUSTOM_BAPI.BAPI_DOCUMENTNUMBER,25</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Document_Part>=
        ZCUSTOM_BAPI.BAPI_DOCUMENTPART,3</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Document_Version>=
        ZCUSTOM_BAPI.BAPI_DOCUMENTVERSION,2</VALUE>
    <VALUE><Meaningful_Display_Name_for_Custom_BAPI_Document_Description>=
        ZCUSTOM_BAPI.BAPI_DOCUMENTDESCRIPTION,25</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="parameter_defaults" IS_REPEATING="true">
    <VALUE>DocumentType=DRW</VALUE>
    <VALUE>DocumentVersion=00</VALUE>
    <VALUE>DocumentPart=000</VALUE>
    <VALUE>DataCarrier1=DOCUMENTUM</VALUE>
    <VALUE>WSApplication1=DCM</VALUE>
    <VALUE>SPEC_INSTRUCTION=DEFAULT_VALUE</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="result_parameters" IS_REPEATING="true">
    <VALUE>DocumentNumb=DOCNUMBER,25</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="key_attributes" IS_REPEATING="true">
    <VALUE>DocumentType=DOCUMENTTYPE,0,3</VALUE>
    <VALUE>DocumentNumber=DOCUMENTNUMBER,3,25</VALUE>
    <VALUE>DocumentPart=DOCUMENTPART,30,3</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="methods" IS_REPEATING="true">
    <VALUE>Create</VALUE>
    <VALUE>Update</VALUE>
</ATTRIBUTE>
<ATTRIBUTE NAME="result_table">DOCUMENTSTRUCTURE,64</ATTRIBUTE>
</API_CONFIG>
</OBJECT_CREATE>
</REQUEST>

```

6. Extract the contents of **dmei_custom_installer.zip** into a temporary folder.

7. Locate the **dfc.properties** file in the temporary folder and edit the file with the Documentum Foundation Class directory information.
8. Locate the **installer.properties** file in the temporary folder and edit the file with the following:

Value	Definition
user.language	The default is en_US (English).
docbase.name	Name of the repository that you want to configure.
docbase.user.name	Type dm_doclink_sap or workaround ID.
domain	Name of the domain in which the repository is located.
custom.xml.path	The custom XML file path.

9. Locate the **log4j.properties** file in the temporary folder and edit to change the directory location of the log files.

Note: By default, log files are generated in the current (temporary) folder.

10. Issue the following command from the command line to run the custom XML file installer:

```
java -jar dmei_custom_installer.jar
```

Note: The file **dmei_custom_installer.jar** is in the temporary folder where you extracted the contents of the **dmei_custom_installer.zip** file.

11. Enter the password for the repository specified in the **dfc.properties** file.

File processing begins and the message **Processing Successfully Completed!** appears when processing completes.

Note: If the **Processing Failed!** message appears, look in the log files to determine the problem with the **custom.xml** file installation.

CS SAP is now configured to replicate custom DMS attributes of a document from EMC Documentum to SAP custom tables.

The classification values that you configured here are accessible from the **Rule Composer** section of the **Link Documentum** and **Replicate Documentum** tabs in WebAdmin.

Note: Special processing rules are defined for the following attributes:

- DOCUMENT_TYPE
- DOCUMENT_NUMBER
- DOCUMENT_PART
- DOCUMENT_VERSION

The values for these attributes can be set to the corresponding values for the SAP DIR object that is created or updated. Invoke the special processing rules by setting the following symbolic values.

Attribute	Symbolic value
Document Type	@DOCTYPE
Document Number	@DOCNUMBER
Document Part	@DOCPART
Document Version	@DOCVERSION

Depending on your requirements, set these symbolic values in the **Rule Composer** section of the **Link Documentum** and **Replicate Documentum** tabs in WebAdmin.

Note: To use the zcustom BAPI, map the zcustom BAPI and zcustom table name using the rule composer in WebAdmin. The zcustom table name is the name of the parameter for the zcustom BAPI and not the name of the table itself.

Working with the FILTER attribute

The FILTER attribute is a symbolic target that specifies an external command line to run when creating links.

The FILTER attribute conforms to the following syntax:

<Path> <Arg1> <Arg2> <ArgN> <r_object_ID> <Repository> <User Name> <Password>

The parameters used in the syntax are described in the following table:

Parameter	Description
Path	Fully qualified path to an executable.
Arg1, Arg2,...ArgN	Arbitrary parameters as defined by your filter program.
r_object_id	r_object_id of the current object.
Repository	Name of the repository where you would like to run the executable.
User Name	Username used to connect to the repository.
Password	Password that corresponds to the username described in this table.

You can use these parameters to pass additional values to the external filter; use the **printf() -format** string for this purpose.

If the execution is successful, the external filter returns 0 as the exit code; if unsuccessful, it returns a non-zero value as the exit code.

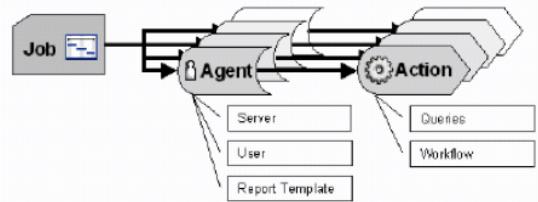
Using Auto Manage to execute CS SAP actions

Jobs can be made to run automatically at regular intervals by creating an Agent to run a defined action:

- Jobs run Agents.
- Agents execute actions.
- Actions perform linking, replication, or integrity checking.

Job progress and status can be monitored.

The following illustration shows the relationship between these parts.

Figure 29. Agent services

Creating, viewing, and editing an Agent

Agents run actions and define on which server and what user an action will run. If an action was meant to run on several servers, each server has to have an Agent configured. You should be careful choosing an SAP user since the Agent will run the action with the access rights this user has on the SAP Server defined in the Agent.

Additionally a report template can be configured, defining how the Agent's report file is displayed. The reports are stored in /System/sysadmin/Reports on the Documentum repository running the job that invokes the Agent.

The report format is XML. The template can be any file with a "<DM_XML_INCLUDE>" tag that will be replaced with the XML-report generated by the Agent.

Note: The XML-report has no XML header tag [<?xml version="1.0"?>] New report template files have to be stored in /System/Content Services/DCTM/Template/Report.

To configure an Agent, you will need a previously configured Action as well as a previously defined SAP Server and SAP user.

To create, view, or edit an Agent:

1. Connect to WebAdmin.
2. Click to expand the **Auto Manage** subnode and select the **Agents** subnode. The **Agents** screen appears.
3. Select **File > New > Agent** from the menu at the top of the Agent screen. The **Agent Properties:** screen appears.
4. Enter a name for the Agent in the **New Agent Name:** field.
5. Choose the SAP system type from the **SAP System Type:** drop-down list.
6. Choose the action required by the Agent from the **Action:** drop-down list.
7. Choose the SAP server where the Agent is running from the **SAP Server:** drop-down list.
8. Choose the SAP user with the rights to run the Agent from the **SAP User:** drop-down list.
9. Click **OK** to save the Agent configuration.

Auto Manage notification

You can create jobs and send a notification to a group of users. However, when you select a group or user, the application tries to load all the users in the repository; as a result, a page timeout occurs or the application stops responding unless you create a **Group** in Documentum Administrator, and associate users to this group.

Registering and HVP worker

To register an HVP worker, you will need a previously configured Action as well as a previously defined SAP Server and SAP user.

To register HVP worker:

1. Connect to WebAdmin.
2. Click to expand the **Auto Manage** subnode and select the **HVPS** subnode.
The **HVPS** screen appears.
3. Select **File > New > Register HVP Worker** from the menu at the top of the HVPS screen.
The **Register Worker:** screen appears.
4. Enter a name for the Worker in the **Name:** field.
5. Enter the web address for the Worker in the **Worker URL:** field.
6. Click **Edit** in the **Capabilities:** field.
The **hvp_capabilities** Web Page Dialog appears.
7. Enter a new capability in the Enter new value: box and click Add to add the capability to the **hvp_capabilities** list box.
Select a capability and use up and down to arrange capabilities in the desired order. Use Edit and Delete to update or remove capabilities.
8. Click **OK** to save the capability configuration.
You are returned to the **Register Worker** screen.
9. Select **Is Available:** if required.
10. Click **OK** to save the Worker registration information.

Creating, viewing, and editing SAP jobs

There are two running modes available for a job. When started in “execute job” mode, the job is actually executed. If the job runs in “write job’s report” mode, only the report is written and no objects are actually altered. This mode is recommended to test jobs before changing any data.

The Trace Level defines the granularity of the Logfile written when executing the job.

Note: There is a difference between a Report and a Logfile. In the report there are messages from the Agents/actions. The Logfile contains the messages of the Job, failure reasons for example.

It is helpful to have a description of the job, explaining what the job is meant to do.

A job can be scheduled to start on a defined date (Activation Date) and to expire on a defined date (Expiration Date). The format of the date is “day, month, year” and the format of the time is “hours: minutes: seconds.” The activation date can be copied to the expiration date with the arrow button on the right side of the expiration date row.

The frequency of invoking the job can be defined with an interval. The interval consists of a number and a measurement. The following measurements are available:

- Minute(s)
- Hour(s)
- Day(s)
- Week(s)
- Month(s)
- Years(s)
- Day of the week
- Day of the month
- Day of the year

There can be a number of runs defined, deactivating the job after having completed the defined number of runs. If 0 is defined, the job runs with no limitations.

To configure a Job, you will need a previously configured Agent.

To create, view, or edit jobs:

1. Connect to WebAdmin.
2. Click to expand the **Auto Manage** subnode and select the **Jobs** subnode.
The **Jobs** screen appears.
3. Select **File > New > Job** from the menu at the top of the **Jobs** screen.
The **New Job** screen appears with four tabs across the top.
4. In the **Info** tab:
 - a. Enter a job name in the **Name:** field.
 - b. Enter a job type in the **Job Type:** field.
 - c. Select a trace level for the job in the **Trace Level:** list box.
 - d. Select **Active** or **Inactive**, if required.
 - e. Select **Deactivate upon failure**, **Run after Update**, or **Save if invalid**, if required.
 - f. Click **Next** or **Schedule** to continue the job configuration.
5. In the **Schedule** tab:
 - a. Select a job start date and time with the **Start Date And Time:** calendar pop-up and time list boxes.
 - b. Select a metric for job to repeat in the **Repeat:** list box.

- c. Enter how often the job will repeat in the **Frequency:** list box.
 - d. Select a job end date and time with the **End Date And Time:** calendar pop-up and time list boxes, or enter a specific number of time for the job to run.
 - e. Click **Next** or **Method** to continue the job configuration.
6. In the **Method** tab:
- a. Click the select method link for **Method Name**, select a method from the list, and click **OK**.
 - b. Click the edit link for **Arguments:** enter the argument in the **Enter new value:** field, click **Add** to add the value to the **Method Arguments:** field, and click **OK**.
Or click **Pass standard arguments** to accept the default arguments.
 - c. Click **Next** or **SysObject Info** to continue the job configuration.
7. In the **SysObject Info** tab:
- a. Enter a title for the system object.
 - b. Enter a subject for the system object.
 - c. Click the edit link for **Keywords**, enter the keyword in the **Enter new value:** field, click **Add** to add the value to the **Keywords:** field, and click **OK**.
 - d. Click the edit link for **Authors**, enter the author name(s) in the **Enter new value:** field, click **Add** to add the value to the **Authors:** field, and click **OK**.
 - e. Click the edit link for **Owner Name**, select an owner from the list, and click **OK**.
 - f. Click the edit link for **Version Label**, enter the version in the **Enter new value:** field, click **Add** to add the value to the **Version Label:** field, and click **OK**.
 - g. Click the **Show More\Hide More** toggle for additional object owner properties.
 - h. Click **Next** or **Sap Job** to continue the job configuration.
8. In the **SAP Job** tab:
- a. Select job agents from the **Agents:** list box.
 - b. Click **Add** to add the agent to the **Agents to Run** field.
Use the up and down arrows to adjust the order that agents run.
9. Click **Finish** to save the Job configuration.
The newly created job appears in the **Jobs** screen.

Performing job maintenance

To perform additional job maintenance options:

1. Connect to WebAdmin.
2. Click to expand the **Auto Manage** subnode and select the **Jobs** subnode.
The **Jobs** screen appears showing the job **Object Name**, job **Last Completion** run, and the current **State** of the job.
3. Right-click on the desired job and select:

Properties — to make adjustments to the job settings.

Run — to immediately run the job.

Refresh — to refresh the Jobs screen.

View Job Report — to view a report of the job run

View Trace File — to view a report based on the trace level set for the job run

Delete — to delete the job and all its settings

The *EMC Documentum Content Server User Guide* and *EMC Documentum Content Server Reference Manual* have more information on job status attributes [dm_job].

Configuring the Manage and View Components

The Manage component supports Documentum Administrator's certified SAP DMS and PLM interfaces. This functionality requires the Desktop Client, and thereby, a Documentum Foundation Suite license, to operate.

This section describes how to set the defaults for the Manage component and the configuration of the View component.

Configuring the Manage component

To configure the Manage component:

1. Connect to WebAdmin.
2. Click to expand the **Clients** subnode and select the **Content Services Manage Type Defaults** subnode.
The **Content Services Manage Type Defaults** screen appears.
3. Select **File > New > Content Services Manage Type Default** from the menu at the top of the **Content Services Manage Type Defaults** screen.
The **Content Services Manage Type Defaults Properties** window appears.
The field names are described in the following table.

Table 67. Parameters

Field name	Description
Document Type	Name of the Documentum object type you want to configure. Enter dm_document to define default settings for all document types. If not explicitly configured, the document type is automatically inherited by all sub-types of this document type.

Field name	Description
SAP Document Type	<p>Defines which SAP document type is assigned to the DIR created in SAP. This parameter cannot be selected by the user. Default value is DRW if no value is entered in this field. Verify that the type defined in this field exists in SAP.</p>
	<p>Note: Since the PLM type objects are usually drawings, a default value of "DRW" is used. You can always override this setting in the Query Conditions field of the SAP Query Composer, as described in Creating, Viewing, and Editing an SAP Query.</p>
Description Attribute	<p>Example 21-4. You can assign the value of DocumentType as DES for a DES document type.</p> <p>For all document types, you can set the value of DocumentType as one of the following:</p> <ul style="list-style-type: none"> • DocumentType=* • DocumentType= <p>In this case, no value has been assigned to the parameter. The value for the parameter has been set to blank.</p> <p>Defines the name of the attribute that contains the description value. This value can subsequently be modified by the user. For example, a description of object_name specifies that the object name is stored in the DIR. This attribute is mandatory. Default value if not configured is object_name.</p>
Version Label\Required Version	<p>Defines a set of version labels required for releasing a document to SAP. Manage does not allow you to link an object that does not match one of the configured values. For example, entering RELEASED into this field means that released documents require a version label of RELEASED in the document version attribute. By default, this feature is turned off when this attribute field is empty.</p>

Field name	Description
Status Label\Required Status	Defines the status flags that a document must have before it can be released to SAP. Manage does not allow you to link an object that does not match the status configured in this attribute. For example, if you define the Required Status as Released, Manage requires that the a_status attribute in the document to also have a value of Released. By default, this feature is turned off when this attribute field is empty.
Folder path in Docbase\Required Folder	Defines one or several folders that the document must be linked to before it can be released to SAP. Manage does not allow you to link an object that does not exist in one of the configured folders. For example, a value of '/SOP/Released' entered in this field requires that released objects be located in this folder. By default, this feature is turned off when this attribute field is empty.
Available Formats\Possible Format	Defines the set of content types from which the user can select. These content types must be present in the object when released to SAP. The first item is the preferred one. The set of Possible Formats is mapped to the list of currently available formats retrieved from the object. The default is that all renditions and the primary content type are displayed if this field is left empty. The recommended value for this field is primary content type. Special values that may be entered for this field include dms_object_content, which selects the primary content type, and dms_best_format, which forces the viewer to decide what format to use.
Version Label\Possible Version	Defines the set of versions from which the user can select. These versions must be present in the object when released to SAP. The first item is the preferred one. The set of Possible Versions is mapped to the list of currently available versions retrieved from the object. By default, this feature is turned off when this attribute field is empty.

4. Enter the mnemonic for the SAP document type.
5. Choose the Description Attribute from the drop-down list.

6. For each of the Required Version Label, Status Label, and Folder Path in repository, enter the required value and click on the corresponding right arrow to add the value to the list.
7. For each Possible format, choose the Available Format from the drop-down list and click the right arrow to add it to the Possible Format list.
8. Enter a Possible Version Label and click the right arrow to add it to the Possible Version list.
Note: You can rearrange the order of these items with the up/down arrow or delete them with the delete button.
9. Click **OK** to save the Content Services Manage Type Defaults configuration.

Using the PLM interface in pre-4.7 SAP systems

If you want to use Manage with the PLM interface in pre-SAP 4.7 systems, the following steps must be completed on the users workstation after Manage has been installed.

To configure Manage for use with the PLM interface in pre-SAP 4.7 systems:

1. Select **Start > Run > regedit**
2. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\Documentum\DocLink Server\Install\UseNewInterface**.
3. Change the **UseNewInterface** registry key value to **TRUE**
4. If the View component has been launched on the workstation, open the Task Manager and end the **dmapi.exe** process.
5. Launch the View component again. The PLM interface will now be used for all document releases to SAP. Only the SAP Query Types labeled PLM will function now.

Configuring the View component

To configure the View component:

1. Connect to WebAdmin.
2. Click to expand the **Clients** subnode and select the **Content Services View** subnode.
The **Content Services View** screen appears.
3. Select **File > New > Content Services View** from the menu at the top of the **Content Services View** screen.
The **Content Services View Properties** window appears.
The field names are described in the following table.

Table 68. Parameters

Field name	Description
Available Formats\Best Formats	<p>Defines a list of Documentum content types to be used when the Manage component has defined Best Format. The first value defined is the most preferred format, and the last value defined the least preferred format. If this attribute is empty or if the object is not configured, then the View component uses the default content type or the content type defined by the Manage component.</p> <p>For example, if Best Formats is defined as PDF, HTML, the View component first checks for PDF content. If PDF content is not available, View then checks for HTML. If neither content type is available, View uses the default format (e.g. WinWord). If this attribute is not configured, then View displays the main document content.</p>
Filter Formats	<p>Defines the formats to generated with a Documentum Content Server filter. The formats defined here must be a sub-set of the formats defined in Best Formats. Any format configured here forces the filter mechanism to executed to generate the required rendition. Has no effect if not configured. You must have the corresponding filter installed on the server in order to use this feature.</p> <p>For example, you may have a Word-to-HTML filter installed on the Documentum Content Server. The preferred format configured in Best Formats is HTML. When viewing a WinWord document linked with the Best Format, the View component does not find a HTML rendition, and displays the Word document. Because HTML is configured as a filter format, View now launches the filter on the Documentum Content Server and displays the document in HTML.</p>

Field name	Description
Standard Attributes\Attributes to Display	The attributes defined here will be used as column header in View's outline view or will be displayed upon request in WebView.
Force Login	If this attribute is selected, the user must enter a password each time a document is launched. This is useful in an environment where several people share the same workstation. This attribute is turned off by default.

4. For each of the formats and attributes that you want to define:
 - a. Choose the item from the list box.
 - b. Click the right arrow to add the rule to the relevant list.

Note: You can rearrange the order of these items with the up/down arrow or delete them with the delete button.
5. Click **OK** to save the Content Services View configuration.

Chapter 22

API and DQL

Run DQL queries and server APIs from Documentum Administrator pages that contain a Tools menu.

- Use the Dql Enter Query page to test whether DQL SELECT statements return the expected values
- Use the Api Tester page to send method calls directly to the server

Running DQL queries

The Dql Enter Query page enables you to test whether a DQL SELECT statement returns the expected values. Use this page as a tool for testing DQL.

The number of rows returned by a DQL statement is limited based on the width of the rows requested. The query results may be truncated. When this happens, a warning message appears.

1. Select **Tools > Dql Editor**.
 2. Type the query in the text box.
 3. To display the SQL statement produced by the query, select **Show the SQL**.
 4. Click **Execute**.
- The query results are returned.

Running server APIs

The API Tester page enables you to enter methods directly in the API text field by typing the method name and its arguments as a continuous string, with commas separating the parts.

For example, the following command creates a folder:

```
API> create,s0,dm_folder
```

Note: Methods entered in the API text field bypass the Documentum Foundation Classes (DFC) and directly access the Documentum Client Libraries (DMCL). Therefore, the DFC cannot perform its usual validation of the methods.

To run server APIs:

1. Select **Tools > Api Tester**.
The API Tester page is displayed.
2. Select **Single-Line Command Entry** or **Script (multi-line) Entry**.
3. Enter the API.
 - If you are in Single-Line mode, enter the command and any necessary data in the **Command** and **Data** text boxes.
 - If you are in Script Entry mode, type the method and its arguments in the **Commands** text box.
4. To display the SQL statement produced by the query, select **Show the SQL**.
5. Click **Execute**.
The results are returned.

Search

This chapter includes:

- Run a simple search, page 613
- Run an advanced search, page 616
- View search results, page 620
- View your most recent results but do not relaunch the search, page 623
- Improve your search experience, page 623
- Saved searches, page 626
- Search templates, page 628
- Set search preferences, page 631

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, page 631](#), 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.

When displaying search results, Documentum Administrator displays files with the most matching words first. If your repository has been indexed for parts of speech, Documentum Administrator also displays files that include variations of the words you typed. For example, if you type *scanning* then Documentum Administrator also looks for files that contain the words *scan*, *scanned*, and *scanner*.

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, page 614](#).
 2. Click .
- If your search includes several terms, the results displayed first will contain all search terms, then Documentum Administrator will display the results that contain only some of the search terms.
- Tip:** To stop the search, click **Stop** .
3. See [View search results, page 620](#).

Further define search terms

You can use the syntax in [Table 69, page 614](#) to further define search terms within a simple search or within the **Contains** field in an advanced search.

Table 69. Further define search terms

Syntax	Description
Quotation marks around a word or phrase: " "	To search for an exact word or phrase, type quotation marks around the word or phrase. For a simple search (including the Contains field in an advanced search), if you do not use quotation marks, Documentum Administrator 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> . This option is disabled when searching for more than one word or if your repository has not been indexed for variations. Quotation marks cannot be used to match the exact case of a word.
The AND and OR operators	To get results that contain two search terms, type AND between the terms. A term can be a word or quoted phrase. To get results that contain at least one term, type OR between the words or the quoted phrases. 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: <code>knowledge or management and discovery</code> then your results must contain either knowledge or they must contain management, and discovery.

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. <u>Use this syntax cautiously</u>. 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. <u>Use this syntax cautiously</u>. 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> <p>To specify that certain terms must be processed together, use parentheses. When using parenthesis, you <u>must</u> 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 <u>either</u> management <u>or</u> discovery.</p>
Parentheses around terms: <i>()</i>	

Syntax	Description
The multiple-character wildcard: *	<p>If the repository is indexed, you can use the multiple-character wildcard to indicate additional characters anywhere in a word. It matches zero or more characters. The multiple-character wildcard is only available or 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 of external sources. For those, you should use truncation operators, such as the Begin with operator.</p> <p>Note: If you use wildcards, then Documentum Administrator will not display results that include variations of the words you typed. For example, if you type</p> <pre>d*ment</pre> <p>then your results must contain: document, development, deployment, department, etc. but not documented or documentation.</p>
The single-character wildcard: ?	<p>If the repository is indexed, 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 or 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.</p>

Note:

- 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", Documentum Administrator returns documents with that string of three words. If you type hardware, and software without quotation marks, Documentum Administrator 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.

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 Documentum Administrator 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, page 617](#).
3. Click **Search**.
Tip: To stop the search, in the result page, click **Stop** .
4. See [View search results, page 620](#).

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, page 616](#).

Tip: 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, page 614](#).
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 Documentum Administrator 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 **Step b** and **Step c** 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. [Table 70, page 618](#) 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 70. 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 Table 71, page 619. In the remaining fields, select or type values. If you type multiple words, they are searched for as a phrase. For example, if you type "knowledge management" then Documentum Administrator 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. 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>." 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>. 4. To remove a property from the search criteria, click Remove for that property.

Field	Description	
Date	<p>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.</p> <p>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.</p>	
Size	Select a size range.	
<i>Properties when searching for email messages</i>	Subject	Type the words for which to search. To further define your search, see Further define search terms, page 614 .
	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. [Table 71, page 619](#) describes the operators available in the Advanced Search page.

Table 71. Select a property-to-value relationship

Operator	Description
Relational operators:	
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.
Truncation operators:	
Begins with	The truncation operators can be used in place of the multiple-character wildcard.
	Returns results in which the property value begins with the value you typed. Same as using an ending wildcard.

Operator	Description
Ends with	Returns results in which the property value ends with the value you typed. Same as using an ending 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.
Other operators:	
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.

View search results

In search results, you can do these:

- To turn highlighting on or off, click or .
- If your organization includes the smart navigation feature, your 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, page 621](#).

- 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, page 621](#).
- To revise the search, and run it again, click **Edit** , and set values as described in [Enter values for an advanced search, page 617](#), 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, page 626](#).
- If your organization includes the templates feature, you can save the search as a search template so that it can be run again with different parameters, as described in [Create a search template, page 629](#).
- To save results from an external source into a repository, see [Save search results from external sources, page 623](#).

Smart navigation

If smart navigation is available, then 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. Smart navigation is available only if Documentum Administrator includes the Extended Search option, and is configured for smart navigation.

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.

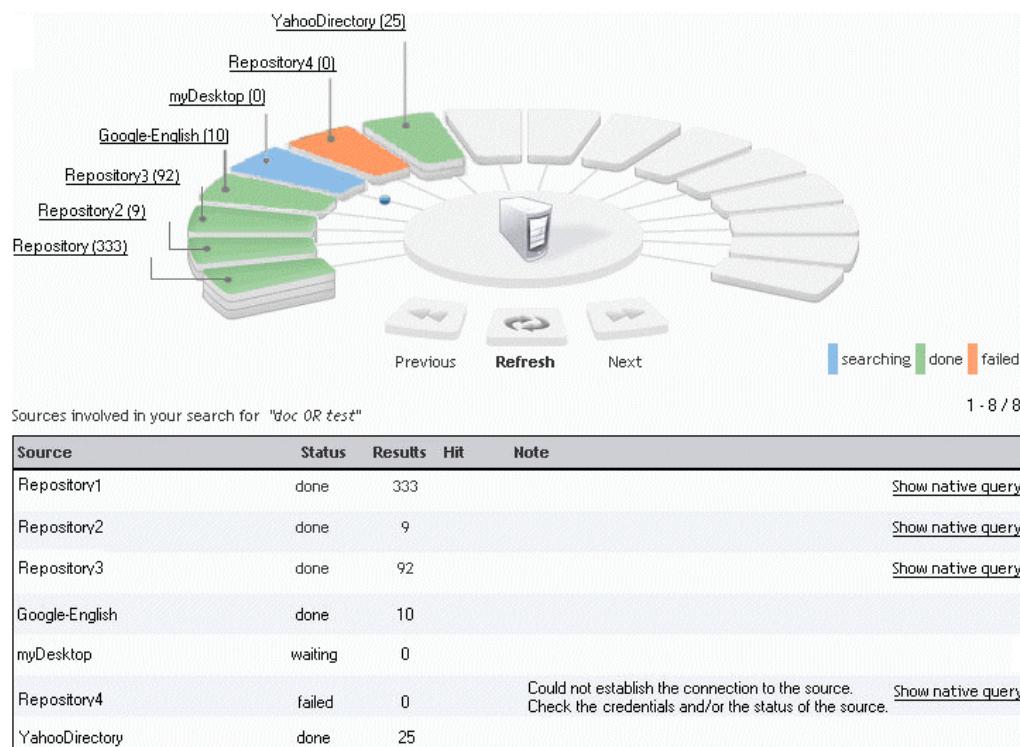
Documentum Administrator computes sub clusters using the strategy defined in your user preferences. To set your preferences, click , and then follow the appropriate steps in [Set search preferences, page 631](#).

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 30, page 622](#). Search monitoring allows you to see which search sources return results the fastest. Search monitoring is available if the search monitoring Extended Search option is installed.

To display search monitoring, click **Status**  as soon as the search has started.

To replay 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 30. 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.

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**.

View your most recent results but do not relaunch the search

This procedure applies only to your current Documentum Administrator session.

To view your most recent search results:

1. At the top of the Documentum Administrator page, click the arrow next to the magnifying glass icon.
2. Click **Last Results**.

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, page 613](#), and [Run an advanced search, page 616](#). 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.

This section describes these aspects that influence your search experience:

- [How configuration can impact your search experience, page 624](#)
- [Index a repository, page 625](#)
- [Searchable items, page 625](#)

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. 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, page 625](#), 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 through Webtop 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, Documentum Administrator 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.

- **External sources**

When querying an external source, the results displayed in Documentum Administrator 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.

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.

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.

Note:

- 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.

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: .

This section includes these:

- [Save a search to run again later, page 626](#)
- [Run a saved search, page 627](#)
- [View the results of a saved search but do not relaunch the search, page 627](#)
- [Edit a saved search, page 627](#)
- [Copy a saved search, page 628](#)

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.

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**.
Documentum Administrator runs the search.
Tip: To stop the search, in the result page, click **Stop** .
4. See [View search results, page 620](#).

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.

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, page 617](#), 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**.

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, page 617](#), 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**.

Search templates

Search templates are available only if your organization uses the Extended Search option, and has set up 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: .

This section includes these:

- [Run a search from a search template, page 628](#)
- [Create a search template, page 629](#)
- [Edit a search template, page 629](#)
- [Modify a search template definition, page 630](#)
- [Copy a search template, page 631](#)

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**.
- Tip:** To stop the search, in the result page, click **Stop** .
6. See [View search results, page 620](#).

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, page 616](#)), 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**.

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**.

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, page 617](#).
5. Click **Search**.
Tip: 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.

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**.

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 Documentum Administrator is configured to search external sources.
4. In the **Smart Navigation** area (if available), 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.
Smart navigation is available only if Documentum Administrator includes the Extended Search option, and is configured for smart navigation.
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, page 43](#).

To retrieve the default configuration of the search locations, and of smart navigation, click **Restore defaults**.

Email Messages

This chapter includes:

- Email message archive import support, page 633
- Storing email attachments, page 634
- Import email messages and attachments to the repository, page 634
- Open an email message for viewing, page 637
- Transform an email message to HTML or PDF, page 638
- Export an email message from the repository, page 638
- Locate and open an email attachment, page 638
- Create and edit a copy of an email attachment, page 639
- Export an email attachment from the repository, page 639
- Locate the email to which an attachment belongs, page 640

Email message archive import support

Webtop imports email messages with or without attachments dm_email_message type, and in Outlook Message Format to the repository, and exports email messages to your local file system. With Webtop 6.5, you can import email messages dm_message_archive type, and in Email Message Format (EMCMF). This format stores content, metadata, and attachment information all together as a single unit of information. By default, email message archive import in Webtop 6.5 is disabled.

To enable the message archive import support, perform the following configuration changes during the installation of WDK based application.

Enabling the message archive import support

1. Enable the <messageArchive-support> in <WebApp Root>/wdk/app.xml
With this change, for import of Outlook Message Format (.msg), the object type is set to dm_message_archive type, and in Email Message Format (EMCMF).
2. Uncomment the executables section for ExMRE.exe in <WebApp Root>/wdk/contentXfer/ucf.installer.config.xml under Windows platform setting.
With this change, the ExMRE.exe gets downloaded, and installed to your client machine.

Webtop supports the following two modes to import for dm_message_archive type:

- **Collaboration mode**

If you have enabled the message archive import support, Webtop imports email messages dm_message_archive type, and in Email Message Format in the Collaboration mode. By default, Webtop uses the Collaboration mode during import.

- **Archive Mode**

To change the Collaboration mode to Archive mode, perform the following configuration changes during the installation of WDK based application:

Set the <store-emf-object-as-archive> to true in <WebApp Root>/wdk/app.xml.

Storing email attachments

This section describes how Webtop stores email attachments in Collaboration, and Archive modes.

In Collaboration mode

When you import an email message in Webtop, and the email message has an attachment, the attachments get stored in a hidden folder (the attachment folder) by default in the Collaboration mode. The attachment folder is located in the same location where you import the email message, and does not appear to you while listing messages. You must use the Find hidden objects option through the Advanced Search page to locate this attachment folder.

In Archive mode

When you import an email message in Webtop, and the email message has an attachment, then smaller attachments remain embedded in the email message content in Archive mode, and the larger attachments are stored as renditions of the dm_message_archive object. If the email message has an embedded message, then the embedded message is stored as a VDM child object in the same location as the parent message.

Import email messages and attachments to the repository

When you import an email message to the repository, the message is saved to the repository for viewing but not for editing. If the message has attachments, those also are saved for viewing, and but not editing.

The message can be exported from the repository with its attachments, and saved locally as a single file, with the attachments embedded within. Note that the message cannot be exported if the

Documentum Administrator installation uses HTTP Content Transfer, though the attachments still can be individually exported.

To import email messages and attachments to the repository:

1. In Microsoft Outlook, do one of these:
 - Drag-and-drop one or more email messages to a location in Documentum Administrator.
Skip to [Step 4](#)
 - Save one or more email messages to a location on your computer.
2. In Documentum Administrator, navigate to the repository location to which to import the email messages.
3. Select **File > Import**. Then click **Add Files**. Then select an email message, and click **OK**. To add multiple email messages, repeat the sequence. When you have finished, click **Next**.
Tip: Instead of using the File menu, you can drag-and-drop the email message or messages from your computer to the location in Documentum Administrator.
4. Set properties as described in [Table 72, page 635](#). If importing more than one email message, set properties for each message individually by clicking **Next**.

Table 72. Properties for imported email messages

Field	Description
File	<i>You cannot change this property.</i>
Name	Enter a name for the email message in the repository.
Type	<i>Do not change this property. This assigns the default type for email messages, which is either dm_message_archive or a subtype of dm_message_archive.</i>
Format	<i>Do not change this property.</i>
Lifecycle ID	To assign a lifecycle to the email message, click Select , and assign the lifecycle.

5. After setting properties, click **Finish**.

Email conversion to EMC MF format

Email message (.msg) files are imported as a type or subtype of the dm_message_archive type and are converted to the EMC MF format. The conversion of native email messages to EMC MF format is handled by UCF.

The following functions have been enhanced in Webtop 6.5x to support this:

- Import. When a user imports an email message (.msg), the email message converts to EMC MF format and gets stored as a dm_message_archive type. All attachments in the email are imported and related to the email.
- Export. When a user exports an EMC MF object, the object converts to native email format (.msg) for viewing by Outlook.

- View Properties and Listing pages. The Properties and Listing pages have been enhanced to show email centric attributes such as To, From, Date Sent and Subject.
- Transform. EMC MF messages can be transformed to HTML, XML, or PDF.

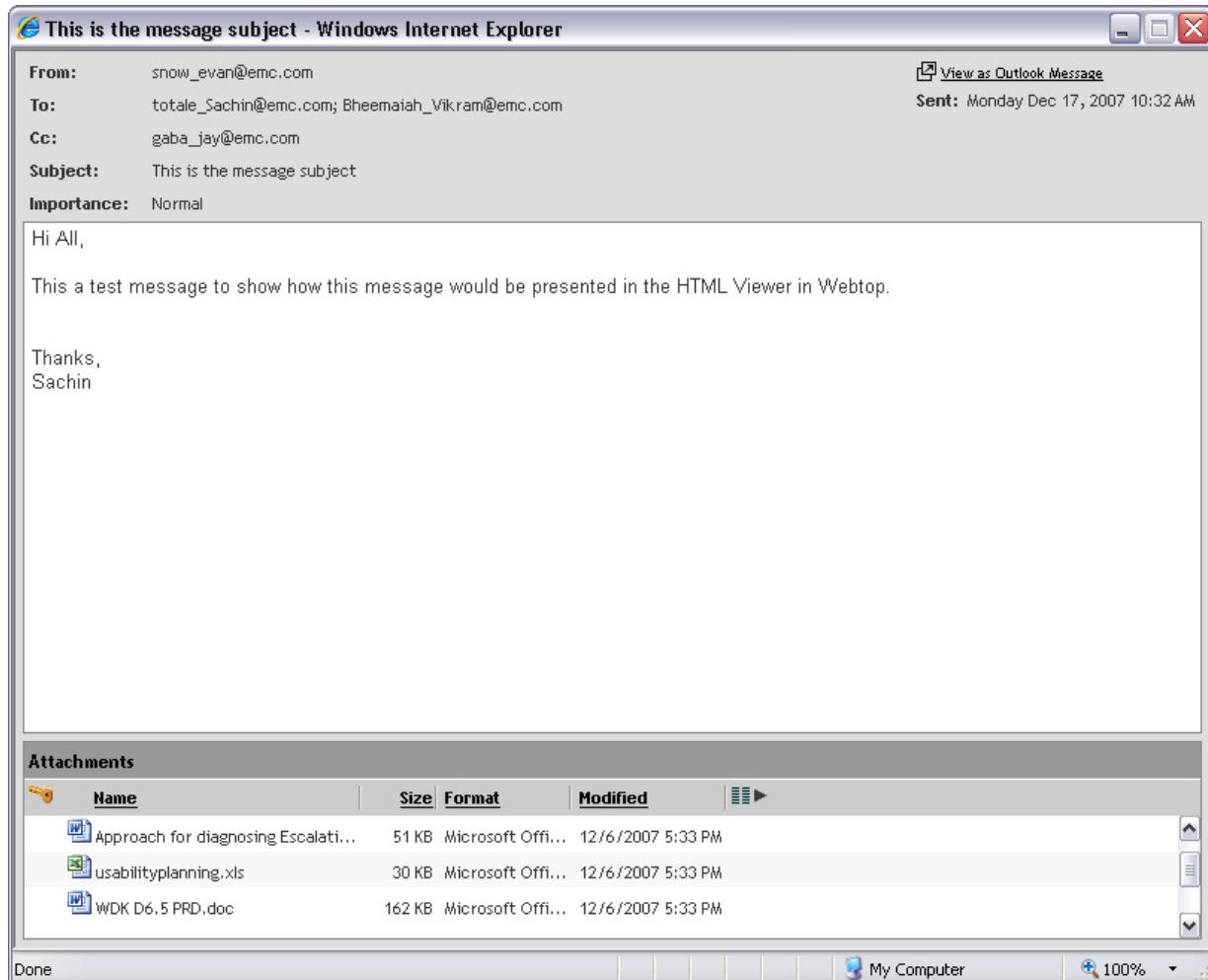
Note: By default, the Email conversion to EMC MF format feature is disabled. If you enable this feature, there is a delay when you first import or export an email message, and the delay occurs due to downloading a large executable file that initializes this feature.

Enabling email message archive import support in Webtop save the Outlook messages (.msg) in email message format (EMCMF) with type as dm_message_archive on import. To convert existing dm_email_message objects to dm_message_archive, refer the *Webtop Email Migration Guide*.

Disabling email message archive import support in WDK based applications, on import of Outlook messages (.msg) files get imported as dm_email_message object, and the import of .msg files fail in case you set the type to dm_message_archive manually.

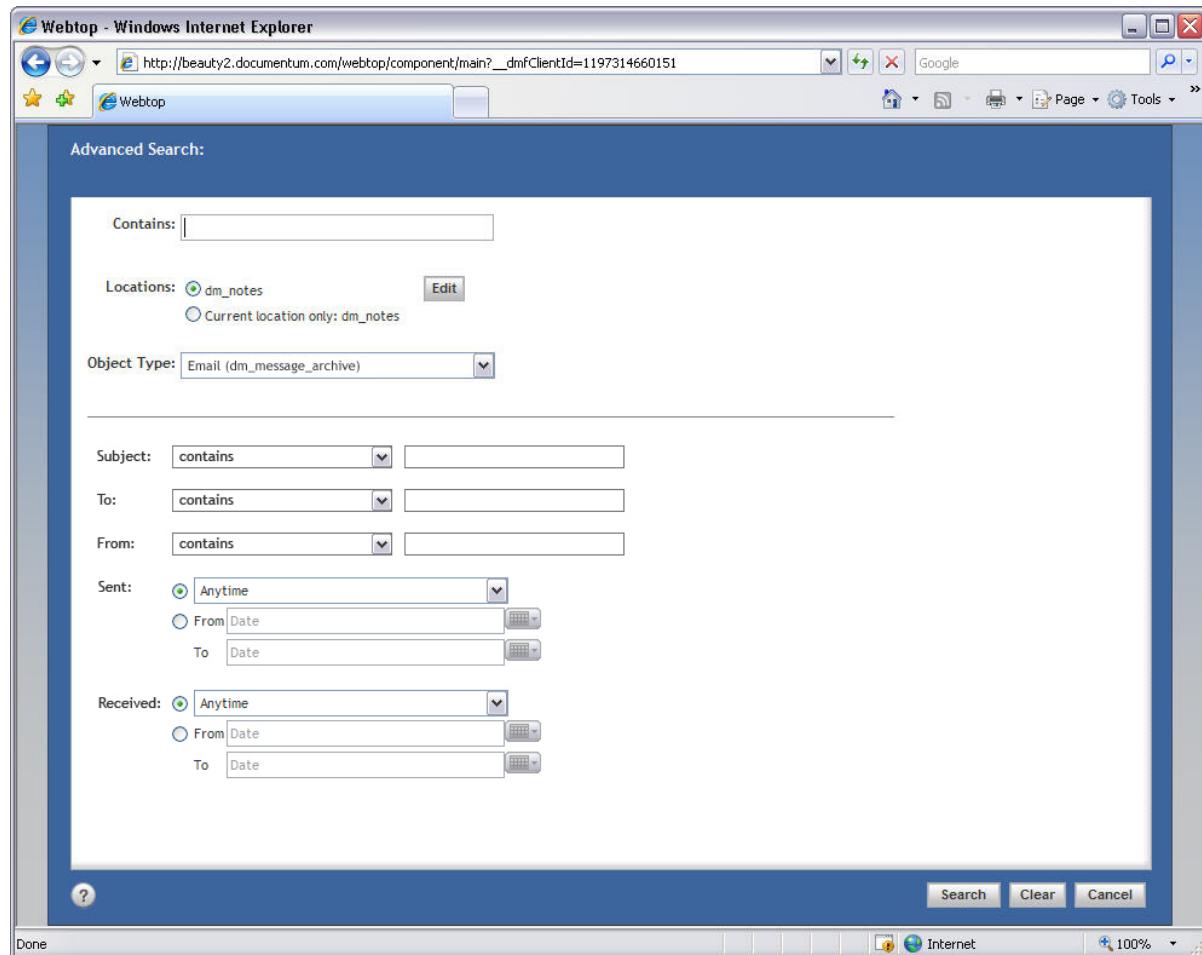
Webtop allows viewing of emails through a special HTML viewer. The HTML viewer provides user access to related email attachments. Attachments can only be viewed but they can also be found through a search results screen. To version an attachment, the user may copy and paste the attachment to a location within the repository and make that attachment a new, independent object.

Figure 31. HTML viewer for email



Users also see an enhanced search screen in Webtop, to search on email specific attribute values (Figure 32, page 637).

Figure 32. Enhanced search



Also available is a conversion utility for emails already in a repository. This utility is run as a separate application to convert existing emails to the EMCMF format.

Open an email message for viewing

Once an email message is imported into the repository, you can view it in read-only mode. You cannot edit it.

To open an email message for viewing:

1. Navigate to the email message, and select it.

Note: When displaying a list that includes email messages, you can choose to add additional column information pertinent to the email messages, such as the sender, and recipients. To add columns to a list, see [Select the columns that appear in lists, page 43](#).

2. Select **File > View**.

Transform an email message to HTML or PDF

To transform an email message to HTML or PDF:

1. Navigate to the email message, and select it.
2. Select one of these:
 - Tools > Transformation > HTML Rendition
 - Tools > Transformation > PDF Rendition

Export an email message from the repository

When you export an email message, Documentum Administrator creates a copy of the email as a .msg file in the location you choose. Any attachments to the message are embedded in the exported .msg file.

You cannot export email messages if your installation uses HTTP Content Transfer.

To export an email message 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:
 - If exporting one message, set options, and click **OK**.
 - If exporting 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 to export, select the location, and click **OK**.

Locate and open an email attachment

This section describes how to locate, and open an email attachment in Collaboration mode.

You can open an email attachment, and view it in read-only mode. You cannot edit the attachment, but you can create a copy of the attachment, and edit the copy, as explained in [Create and edit a copy of an email attachment, page 639](#).

To locate and open an email attachment:

1. Open the email message that contains the attachment, as described in [Open an email message for viewing, page 637](#).

Tip: You can also locate an attachment by searching. To do so, type all or part of the attachment's name into the search box above the tree navigation pane. For more information on searching, see [Chapter 23, Search](#).

2. Click the **View Properties** link.

Create and edit a copy of an email attachment

This section describes how to copy, and edit an email attachment in Collaboration mode.

To create and edit a copy of an email attachment:

1. Open the email message that contains the attachment, as described in [Open an email message for viewing, page 637](#).
- Tip:** You can also locate an attachment by searching. To do so, type all or part of the attachment's name into the search box above the tree navigation pane. For more information on searching, see [Chapter 23, Search](#).
2. Right-click the attachment, and select **Add To Clipboard**.
 3. Navigate to the location to which to copy the attachment, and open the location so that the location's files, and folders are displayed in the content pane. Select **Edit > Copy Here**.
 4. If the clipboard appears, select the email message attachment, and click **Copy**.
 5. To edit the copy, select the copy, and select **File > Edit**.
 6. To perform any other standard Documentum Administrator operation on the copy, use the procedure for performing that operation.

Export an email attachment from the repository

This section describes how to export an email attachment in Collaboration mode.

To export an email attachment:

1. Open the email message that contains the attachment, as described in [Open an email message for viewing, page 637](#).
2. Right-click the attachment, and select **Export**.
3. If prompted to set export options, do so, and click **OK**.
4. If prompted for the location to which to export, select the location, and click **OK**.

Note: In Archive mode, navigate to the email message, and select it. Go to **View > Renditions**, and then perform export.

Locate the email to which an attachment belongs

This section describes how to locate an email to which an attachment belongs in Collaboration mode. For Archive mode, refer to the [In Archive mode, page 634](#) section for details on how email attachments are stored in Archive mode.

To locate the email to which an attachment belongs:

1. Search for the email attachment by typing all or part of the attachment's name into the search box above the tree navigation pane. For more information on searching, see [Chapter 23, Search](#).
2. Right-click the attachment, and select **View > Location**

Chapter 25

Inbox

This chapter includes:

- [Inbox overview, page 641](#)
- [Open a task or notification, page 642](#)
- [Perform a task, page 642](#)
- [Complete a task, page 643](#)
- [Accept a task that has been assigned to multiple users, page 643](#)
- [Reject a task, page 644](#)
- [Delegate a task, page 644](#)
- [Repeat a task, page 645](#)
- [Change your availability for tasks, page 645](#)
- [Work queue tasks, page 646](#)

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, page 646](#).

A task can include attached files that you are asked to edit or review. Attached files continue to the next user in the workflow.

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**.
 - To perform an action, see the appropriate procedure:
 - Perform a task, page 642
 - Complete a task, page 643
 - Accept a task that has been assigned to multiple users, page 643
 - Reject a task, page 644
 - Delegate a task, page 644
 - Repeat a task, page 645
 - Select a task from the queue, page 647

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, page 44](#).
 - 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, page 643](#).
 - 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, page 643](#).

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**.
3. If prompted for a password, type your password.
4. Click **OK**.
5. 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, page 44](#).
 - c. Click **OK**.
6. If prompted, select the next task to forward from the **Select Next Forward Tasks** list.
7. Click **OK**.

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, page 642](#)
 - [Complete a task, page 643](#)
 - [Reject a task, page 644](#)
 - [Delegate a task, page 644](#)
 - [Repeat a task, page 645](#)

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**.

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, page 44](#).
4. Click **OK**.

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, page 44](#).
5. Click **OK**.

Change your availability for tasks

The top of your Inbox displays your availability to receive tasks.

To change your availability to receive tasks:

1. Click **Inbox**.
2. At the top of your Inbox, click one of these:
 - **I am available**
 - **I am currently set to unavailable**
3. Do one of these:
 - To make yourself available, deselect the checkbox that changes your status to unavailable.
 - To make yourself unavailable, select the checkbox that changes your status to unavailable, then click **edit**, then select another user to receive your tasks, and then click **OK**. For detailed steps see [Locate an item in a selection dialog box, page 44](#).

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.

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.

This section includes these:

- Manage tasks in your queue Inbox, page 646
- Get the next available task in a work queue , page 647
- Select a task from the queue, page 647

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**.

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** .

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.

Tip: 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.

Chapter 26

Workflows and Quickflows

This chapter includes:

- Start a workflow, page 649
- Send a quickflow, page 651
- View workflows, page 651
- Pause a workflow, page 652
- Resume a paused workflow, page 652
- Stop a workflow, page 652
- Email the workflow supervisor or a workflow performer, page 653
- Process a failed task in a workflow, page 653
- Change the workflow supervisor, page 654
- Save workflow information as a Microsoft Excel spreadsheet, page 654
- View aggregated report for workflow performance, page 654
- Create a workflow template, page 655

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**.
 - To start a workflow by first selecting one or more files, navigate to the files, and select them, then select **Tools > Workflow > Start Attachments**.
2. Select the workflow template, and click **OK**. For detailed steps see [Locate an item in a selection dialog box, page 44](#).
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, page 44](#).
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**.

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.
Tip: 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, page 44](#).
4. In the **Priority** drop-down list, select the priority.
5. In the **Instructions** field, type any messages for the users.
6. To receive a notification when a user completes the review, select the **Return to Me** checkbox.
7. To require each user to enter an electronic signoff when completing the review, select the **Require signoff** checkbox.
8. Click **OK**.

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, page 651](#).

2. To view a specific workflow, select the workflow, then select File > View.

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

Tip: 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.

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

Tip: 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.

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**
Tip: 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**.

Email the workflow supervisor or a workflow performer

To email the workflow supervisor or a workflow performer:

1. Select **Tools > Workflow > Workflow Reporting**
Tip: 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.

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**.

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**.

Save workflow information as a Microsoft Excel spreadsheet

The availability of this procedure depends on your organization's configuration of Documentum Administrator.

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**.

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**.

Create a workflow template

To create a new workflow template, select **File > New > Workflow Template** to open Workflow Manager. Use that application's Help for instructions on creating the new workflow template.

Work Queues

This chapter includes:

- [Work queue roles, page 657](#)
- [Set up a new work queue, page 658](#)
- [Set up work assignment matching, page 659](#)
- [Work queue policies, page 661](#)
- [Define a queue category, page 664](#)
- [Define a work queue, page 665](#)
- [Define work queue override policies, page 666](#)
- [Manage work queue users, page 667](#)
- [Monitor work queues, page 671](#)
- [Create business calendars, page 674](#)

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 [Table 73, page 658](#).

Table 73. 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.
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.
Queue_manager	Monitors work queues, assigns roles to queues, and assigns users to work on queue items. Queue managers can reassign, and suspend tasks.
	Queue managers who have CREATE_GROUP privileges can create work queues.
Queue_admin	Creates work queues, and queue policies. Members of the queue_admin role <i>do not</i> by default have the administrator role.
	Queue administrators who have CREATE_GROUP privileges can create work queues.
Process_report_admin	Runs historical workflow reports from the Workflow menu.

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, page 659](#) provides detailed information on work assignment matching.
- Create the queue policies you will need for the queue.
[Work queue policies, page 661](#) provides more specifics on queue policies.

- Create the queue categories.

[Define a queue category, page 664](#) explains how to create queue categories.

- Create the work queue.

[Define a work queue, page 665](#) provides more specifics on defining work queues.

- Create override policies.

[Define work queue override policies, page 666](#) explains the optional step of defining override policies for work queue policies.

- Create the process templates used for the work queue in Process Builder.

When a work queue is the performer for a task, the check box to delegate the activity's work to someone else must be selected in the activity definition.

Procedures to define process templates are found in the *Documentum Process Builder User Guide*.

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.

When a workflow process runs, and the system creates a new item for a work queue, it checks the work queue skills that are defined in the task based on the activity mapping rules set up in the activity template in Process Builder. (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.

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.

See *Documentum Process Builder User Guide: Working with Activities*.

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.

The process template in Process Builder must have these skills defined for the task, as well.

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**.

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.

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.

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 Documentum 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 or a Process Builder activity template.

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. The *Documentum Process Builder User Guide* provides information on creating a priority module.

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.

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**.
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, page 662](#) 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. The Queue Task Rework Decision in Process Builder uses the percent quality check setting to determine if the work item is routed for quality 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**.

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**.

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, page 664](#), and [Work queue policies, page 661](#) 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.

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**.

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.

This section includes these:

- [Add a user or group to a work queue, page 667](#)
- [Remove a user or group from a work queue, page 668](#)
- [Add skills to work assignment processor profiles , page 668](#)
- [Update the processor profile in a work queue, page 670](#)

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**.

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 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 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.

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 username, 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.
Documentum Administrator 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.

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 username, 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**.

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 dashboard 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, page 672](#)
 - [Unassign a work queue task from a user, page 673](#)
 - [Move a work queue task to another work queue, page 673](#)
 - [Suspend a work queue task, page 673](#)
 - [Unsuspend a work queue task, page 674](#)
 - [Add a user or group to a work queue, page 667](#)
 - [Remove a user or group from a work queue, page 668](#)
 - [Add skills to work assignment processor profiles , page 668](#)
 - [Update the processor profile in a work queue, page 670](#)

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**

Tip: This action is also available through the **Task Manager**.

5. Select the user to whom to assign the tasks.
6. Click **OK**.

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**.

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, page 673](#).

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**.

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**.
Tip: 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.

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**.
Tip: This action is also available through the **Task Manager**.

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.

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. A process designer can then use the Process Builder application to select a specific calendar for an entire process or for a specific activity. In this way, timers for a process are calculated based on actual work hours.

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.

Lifecycles

This chapter includes:

- [View Lifecycles, page 677](#)
- [Assign a lifecycle to a file, page 678](#)
- [Remove a lifecycle from a file, page 678](#)
- [Promote a file to the next lifecycle state, page 678](#)
- [Demote a file to its previous lifecycle state, page 679](#)
- [Suspend a file from its current lifecycle state, page 679](#)
- [Resume a suspended file, page 679](#)

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 (RM) 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 [Table 74, page 678](#) for descriptions of common lifecycle states.

Table 74. 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.

Assign a lifecycle to a file

To assign a lifecycle to a file:

1. Navigate to the file, and select it.
Tip: 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, page 44](#).
 - 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.

Remove a lifecycle from a file

To remove a lifecycle from a file:

1. Navigate to the file, and select it.
Tip: You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Remove**.

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.
Tip: 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.

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.
Tip: You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Demote**.
3. Click **Demote**.

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.
Tip: You can perform this procedure on multiple files by selecting multiple files.
2. Select **Tools > Lifecycle > Suspend**.
3. Click **Suspend**.

Resume a suspended file

To resume a suspended file:

1. Navigate to the file, and select it.
Tip: 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**.

Chapter 29

Collaborate with Other Users

This chapter includes the following topics:

- [Create and edit formatted text, page 681](#)
- [Discussions, page 682](#)
- [Notes, page 685](#)
- [Contextual folders and cabinets, page 686](#)
- [Calendars, page 687](#)
- [Data tables, page 692](#)
- [Rooms, page 697](#)
- [Manage room membership, page 704](#)
- [Manage users as a non-administrator, page 707](#)

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 75. 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.
	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.

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.

The following topics describe how to use discussions:

- [View discussions, page 683](#)
- [Add and edit comments, page 683](#)
- [Delete comments, page 684](#)
- [Discussions in search results, page 684](#)

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.

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 discussion icon ( 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.

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.

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.

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 Documentum Administrator 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).

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.

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.

The following topics describe how to use calendars:

- [Create calendars and events, page 687](#)
- [Specify recurring event properties, page 689](#)
- [View calendars and events, page 690](#)
- [Edit calendars and events, page 690](#)
- [Delete calendars and events, page 691](#)
- [Calendars in search results, page 691](#)
- [Export and import with calendars, page 691](#)

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 [Table 76, page 688](#).

Table 76. 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.
Notes	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:
	<i>You are invited to the following meeting: Topic: meeting name Date: recurrence pattern or start date, time, duration Location: location To view the event, point your browser to: event.drl Or open this event in your desktop calendar: ICS inline attachment</i>
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.

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

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.

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**.

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.

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.

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.

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. Another usability enhancement allows for in-place editing of notes.

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.

The following topics describe how to use data tables:

- [Create data tables and entries, page 692](#)
- [View data tables, page 695](#)
- [View data table entries, page 695](#)
- [Edit data tables, page 696](#)
- [Edit data table entries, page 696](#)
- [Delete data tables, page 697](#)
- [Import and export with data tables, page 697](#)

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 [Table 77, page 693](#). 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 77. 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.

Field type	Description
Traffic light	For fields displaying blank, red, yellow, or green values, indicating the overall status of entries.
Choice list	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). 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. To allow users to choose more than one value for this field, select the checkbox labeled Allow multiple choices .
Member list	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.
Discussion	For including a discussion field in the entry. A data table can have only one discussion field.
Attachments	For including an attachments field in the entry. A data table can have only one attachments field.

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 78. 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.
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.

Field type	Description
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.

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.

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 Documentum Administrator 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.

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.

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

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.

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.

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 Documentum Administrator, 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 Documentum Administrator.

The following topics describe how to use rooms:

- [Visit a room, page 698](#)
- [Link to a room, page 698](#)
- [Objects governed by rooms, page 699](#)
- [Create a room, page 700](#)
- [Edit the properties of a room, page 701](#)
- [About room membership, page 702](#)
- [Copy a room, page 703](#)
- [Move or link to a room, page 703](#)
- [Delete a room, page 703](#)

Visit a room

Rooms are like folders in the Documentum Administrator 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.

Link to a room

You can add a link to a room's home page anywhere in the repository that permits links.

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.

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 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.

Create a room

You can create a room anywhere in a repository that allows folders.

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 Documentum Administrator 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.

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).

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.

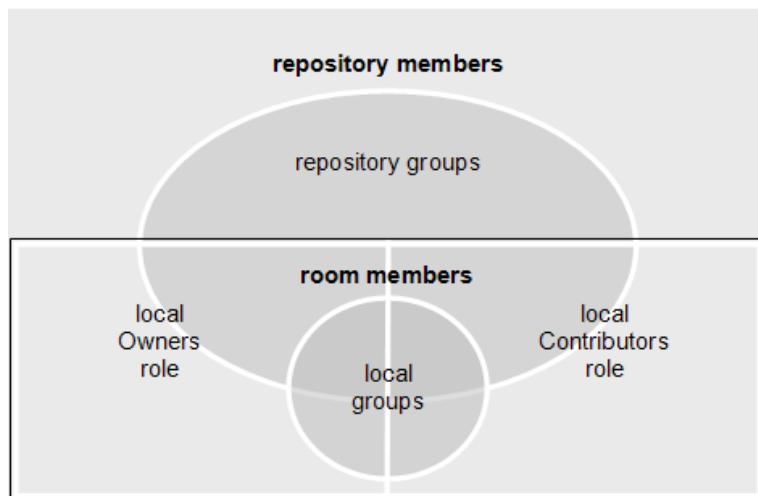
- **Contributor** role usually grants RELATE permission over room objects. Most room members are contributors.
- **Owner** role permits member list management, and usually grants DELETE permission over room objects. Room creators are room owners by default.

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 33. Repository members in relation to room members, groups, and roles



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:

1. 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.

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).

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.

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)
 - **Delete all versions of linked objects**

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.

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.

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, like LDAP users do, for instance. Such mixed groups might perform confidential or proprietary work, and can benefit from membership in the same room.

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, page 707](#)
- [Modify users, page 708](#)
- [Unlist users \(conceal members\), page 709](#)
- [Restricted folders , page 709](#)

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 username.
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.

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.

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.
- Applications outside of WDK, such as the Workflow Manager.

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.

Note: 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.

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*

Chapter 30

My Documentum for Microsoft Outlook Administration

My Documentum for Microsoft Outlook (MyD Outlook) is an add-in to Microsoft Outlook that enables end users to work with email messages, their associated attachments and other files from Microsoft Outlook (or from their local file system) in a Documentum repository, thereby providing interaction between these emails and files with standard Documentum functionality. Along with the message or file, MyD Outlook automatically saves the object properties, such as sender's name, recipient's names, date, and subject.

In addition to this introductory section, you can find information on the following topics relating to the administration of My Documentum for Microsoft Outlook version 6 in this chapter:

- [Profiles, page 713](#)
- [Overview page, page 720](#)
- [Column Setup \(Views\), page 720](#)
- [Client Setup, page 724](#)

Note: Administration tasks for My Documentum for Microsoft Outlook version 6.5 SP1 and later are performed via Documentum Administrator (DA). However, many of the settings that are configured through the DA browser interface are written to a configuration file called **DCO_System_Settings.xml**. This file is located in the global repository and not on each individual repository in use by MyD Outlook, and consists of sections affecting both server and client environments. Server settings that are listed in this XML file include, among others, the list of available repositories, object types, and access rights. The following sections describe MyD Outlook configuration using the DA browser interface

While the **DCO_System_Settings.xml** file does reflect settings for your MyD Outlook environment and allow for other customizations, for most day-to-day administration of MyD Outlook, you use Documentum Administrator.

Management and administration of your MyD Outlook environment, including profiles, repositories, user configurations and other options are all performed in DA.

Repositories must be specifically enabled for use with My Documentum for Microsoft Outlook. They are enabled when one of three scenarios has occurred:

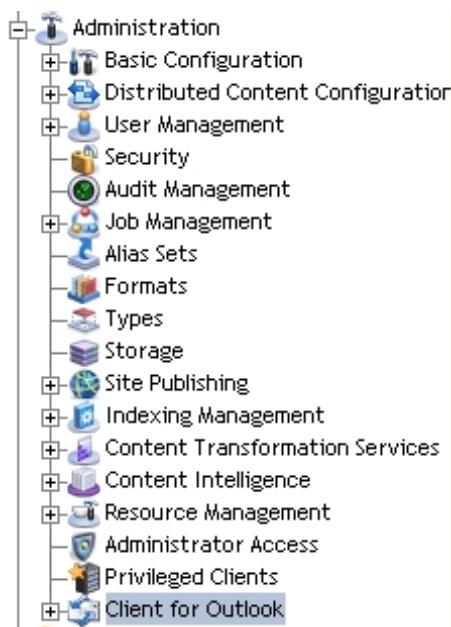
- If the repository was never enabled, and an administrator navigates to the Profiles folder on the repository
- If the repository was never enabled and no profiles were created, it is enabled upon the creation of the first profile
- If the repository is enabled through a change to the **dco_system_settings.xml** file by adding the repository name to the following section in the global repository's XML file:

```
<Repositories>
<Repository name="name of repository" />
</Repositories>
```

where **name of repository** is replaced by the name of your repository.

Once the MyD Outlook DocApps have been installed on the repository, you will see a node called **Client for Outlook** under the repository's Administration node. The node appears in the following location in the Administration tree:

Figure 34. Location of Client for Outlook node in Documentum Administrator



The sub-nodes under Client for Outlook are:

- **Profiles**, to create, and modify MyD Outlook profiles
- **Overview**. The Overview page shows repositories enabled for use with MyD Outlook, and their current status, as well as other information related to your server environment.
- **Column Setup**. This page is the interface for an administrator to define and manage MyD Outlook view in Microsoft Outlook for end users.
- **Client Setup**. The Client Setup dialog box manages settings for client synchronization intervals, history sessions, maximum disk space allowances, the email address required for an end user to contact a MyD Outlook administrator for support, and the URL for the Documentum Foundation Services (DFS) server.

Profiles

A profile in MyD Outlook is a Documentum object type that defines a user's access to folder locations in a repository, default import settings (including permissions), and other options. An end-user requires a minimum **Browse** permission setting in order to use a particular profile, therefore any user with less than that permission level will not be able to see that profile in his or her Outlook client. For more information on security and permissions in Documentum, see [Permissions Overview](#) earlier in this document.

Topics related to profiles and covered in the Profiles section include:

- [Creating new profiles](#)
- [Modifying and deleting profiles](#)

Creating new profiles

To create new profiles on a MyD Outlook-enabled repository, you use Documentum Administrator.

To create a new profile:

1. Log in to Documentum Administrator (DA) with administrator privileges.
2. Click on **Client for Outlook** in the Administration tree and verify that the node is expanded.
3. Highlight (single left-click) **Profiles** in the left pane. This opens the Profiles folder on the right pane.

Note: Credentials must be provided for administrator login access to the global repository. If as an administrator you attempt to open the Profiles folder in DA under the **Client for Outlook** node and you have not previously specified these login credentials, you will be prompted to do so before proceeding with profile creation.

4. On the right pane, click **File>New>DCO Profile**. Clicking on **DCO Profile** brings you to the [Create](#) tab.

Figure 35. Create new DCO profile



The Create tab

After you have selected **File>New>DCO Profile**, the **Create** page appears with the **Create** tab..

Note: Note that the path to the profile objects is indicated at the top of each tab in the profile creation wizard.

Figure 36. Create tab

1. Create | 2. Info | 3. Target | 4. Import

wei_d6_test/System/Applications/DCO/Profiles

Name: *

To name the new profile:

1. On the **Create** tab, enter the name for your new profile in the **Name** field. This is a required field (as indicated by the * next to the field box).
2. Click **Next** to move to the **Info** tab.

The Info tab

The second tab, **Info** is displayed as shown in [Figure 37, page 714](#).

Figure 37. Info tab

1. Create | 2. Info | 3. Target | 4. Import | 5. Permissions

dco_CS65SP1_Glob/System/Applications/DCO/Profiles

Name *

Description
This is a new profile.

Available for use

Offline

Archive

Messages

Default View :

Completing the Info tab fields:

1. The name is pre-filled with the name you entered on the first tab, and is a required field. You may then enter a description for this profile for future reference in the **Description** field.
2. The **Availability** drop-down menu allows you to choose how the profile will be available, in both online and offline modes, online only or disabled.

Table 79. Descriptions of the Availability options for MyD Outlook profiles

Profile availability	Description
Online and offline	An Outlook user can mark folders and/or their contents as offline-enabled.
Online only	An Outlook user can only use folders and/or their contents in online mode.
Disabled	Profile is not available for use and will not be displayed on an end-user's Outlook client.

Note: To learn what effect changing the availability status of a profile once it has been accessed by end-users, see [Modifying a MyD Outlook profile](#).

3. The **Store as Archive** field (unchecked by default) determines whether attachments to email messages will be imported as immutable ("archive") objects in the repository and cannot be changed, or, if the checkbox is checked, message attachments will be imported as mutable ("collaborative"), in which case certain properties can be changed.
4. The **Default View** drop-down sets which view an end-user will be presented with when logging into MyD Outlook as shown in [Figure 37, page 714](#). These views are defined by an administrator in DA using the **Column View** node under **Client for Outlook**. See [Column View setup](#) for instructions on how to configure column views. Users can customize their default view to something other than what an administrator has chosen. Unless changed, the default is **Email Only** (only messages), however the configurable options include **EmailDocument** (messages and documents), **Documents Only** or a custom view that you have pre-defined in DA.

Note: The three default views above cannot be deleted.

Click **Next** to move to the [Target tab](#).

The Target tab

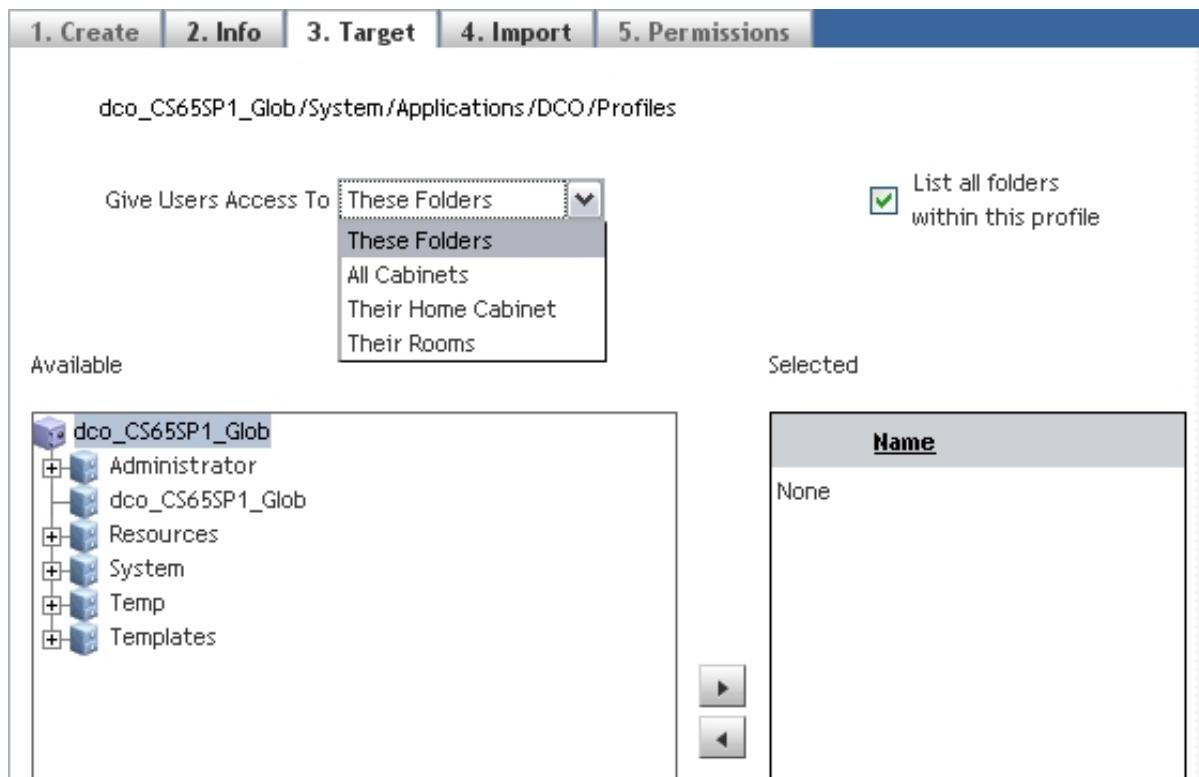
On the **Target** tab, you define to which repository folder(s) users will have access. Users can only see folder locations that have been enabled in that profile for MyD Outlook, and can only create objects within that folder, including creating new subfolders.

To enable a folder as a MyD Outlook profile target, simply select the folder from the list on the left side and click the

Figure 38. Right arrow button

button to move it to the right side. You can do this for as few or as many folders as required, as shown in [Figure 39, page 716](#). By **Ctrl-** or **Shift-** selecting the folders you wish to add as valid targets for this profile, you can move more than one folder at a time.

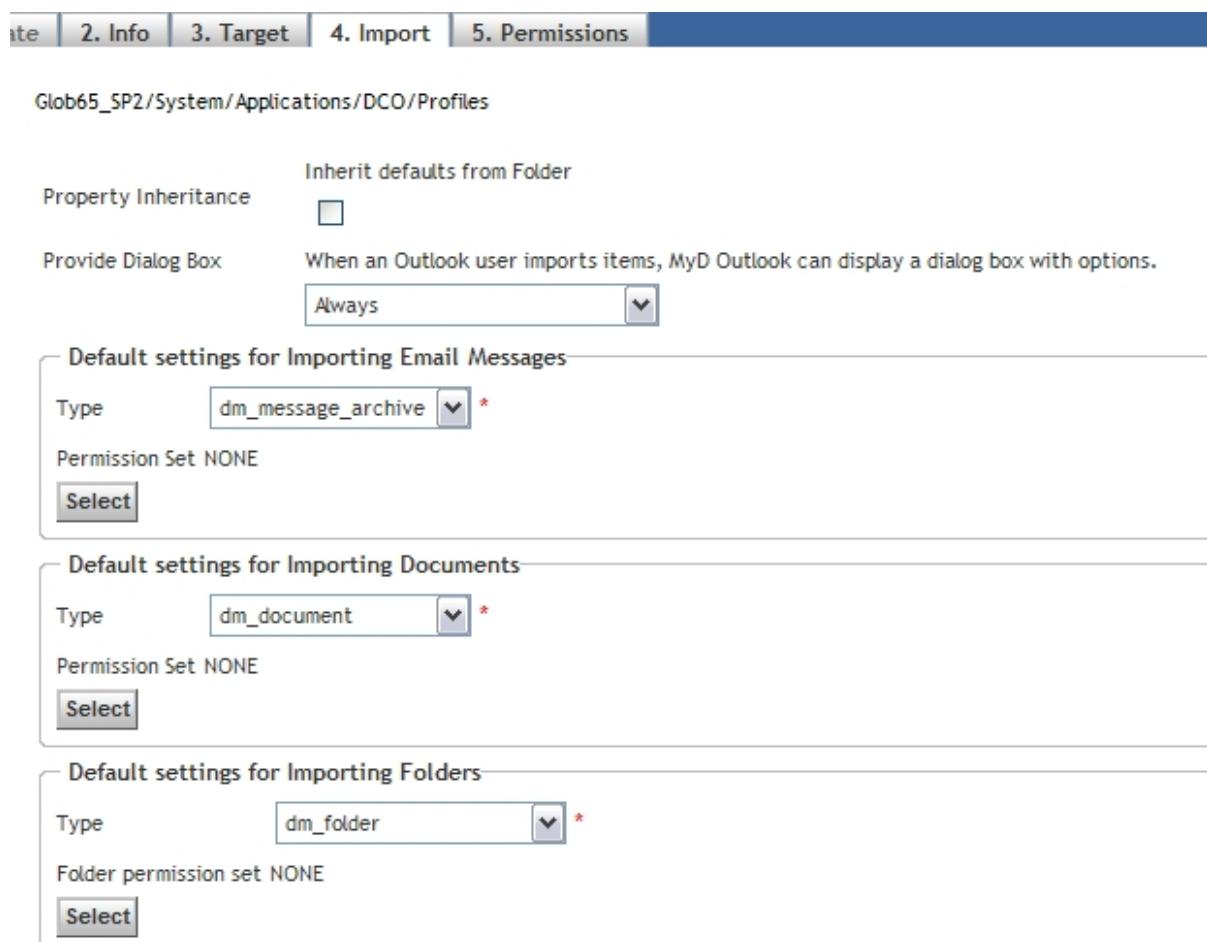
Alternatively, you can give access to all cabinets in the repository, the user's home cabinet only, or their rooms. If you enable the **Users see subfolders** checkbox, subfolders of those folders you have enabled as targets will be visible to end users in Outlook. In addition, if the box is checked, a user can create a subfolder under that target parent folder.

Figure 39. Selecting target destinations for MyD Outlook profiles

Once you have enabled target folders, or chosen any of the options in the access drop-down, click **Next** to proceed to the [Import](#) page.

The Import tab

The **Import** tab presents configuration options for importing objects into MyD Outlook as shown in [Figure 40, page 717](#).

Figure 40. Profile creation Import tab

This dialog box addresses default settings for importing email messages, documents, and folders, as well as objects' property inheritance and whether a user will be prompted to enter values in a properties dialog box when importing an object into the repository. [Figure 40, page 717](#) above displays the default import settings.

If the **Property Inheritance** checkbox is checked (it is unchecked by default), any items created in a particular folder in that profile will inherit keywords and any custom properties that are attached to the folder itself. For example, if one custom property of the folder is the name of a customer such as *The XYZ Company*, any object created in that folder will automatically also have *The XYZ Company* as one of its properties.

The **Provide Dialog Box** setting has two options: **Always** and **Only if a required field is empty**. In the former, each time the user imports an item, a dialog box will be presented prompting the user to manually click **Save** to complete the import. Otherwise, the only time a user would be prompted to manually save the item being imported is when at least one of the required fields contains no value (is empty). The default setting is **Always**.

The object types listed for importing email messages, documents and folders are determined by the object types defined in your environment. Based on the object types you have defined on your repository, the choices for the default settings for importing email messages, documents and folders will show only those types. By default, the message type is **dm_message_archive**, documents use

dm_document and folders use dm_folder. If you have created subtypes of any of these object types, they will also be displayed as possible options in the drop-down menu.

The default permission set for importing email messages, documents and folders is set to **NONE**, meaning that the default permissions for that object type in the repository will be used. If you wish to change the default permissions for a specific object type, see the following steps.

To set default permissions for the importing of emails, documents or folders:

1. Click on the **Select** button next to the Permission Set label under the specific object type you wish to configure.
2. The **Choose a permission set** window opens, initially listing all permission sets available.
3. To reduce the number of items displayed in the list, you can filter the choices by selecting from one of the following in the drop-down menu at the top right corner: **Show All**, **Show System Owned**, or **Show User Owned**.

Click **Next** to proceed to the [Permissions](#) tab.

The Permissions tab

The Permissions tab allows you to configure permissions for the new profile. Permissions for a MyD Outlook profile work similarly to any Documentum object type. In order to be able to use this profile and see the available folder targets in his or her Outlook navigation (left) pane, the user account must have a minimum of **Browse** permissions for this profile. For more information on how to set permissions and what their values represent, see either the [Permissions Overview](#) section in this document or the *Documentum Content Server Administration Guide Version 6.5*.

After you have created a new profile, you can verify that it has been added to the list of available profiles by single (left) clicking on the Profiles folder under the main Client for Outlook node on the left pane of DA.

Modifying and deleting a MyD Outlook profile

To access a profile's properties once it has been created, from the **Profiles** node in DA, right-click on the name of the profile you wish to view/modify and select **Properties**. Once a profile has been successfully created, in addition to being able to see the previously-created properties, you will notice that a new tab is added called **History**. This tab will serve show actions performed on the profile, by whom, the date and time of the action, as well as the current version of the profile.

To modify a profile you have already created:

1. Log in to Documentum Administrator (DA) with Administrator privileges.
2. Navigate to the **Client for Outlook** node under **Administration**, and expand the node.
3. Right-click on the highlighted profile name you wish to modify, and select **Properties**.
4. Review your profile settings and make any necessary changes, then click **Finish** to save the changes.

Note: If you modify a profile that is already in use, end users will not notice the changes until the next time they log in to the repository using that profile.

You may at some point deem it necessary to disable the availability of a certain profile. Making this change can affect end-users' MyD Outlook client environment. The [Table 80, page 719](#) table illustrates the potential effects of such a change:

Table 80. Effect of changing availability of MyD Outlook profile to disabled

Current client status	Effect on end-user MyD Outlook client
Checked-Out folder contains items	No effect. The client keeps track of checked-out documents and their locations in the repository by unique IDs, so the profile is not needed for keeping them checked out or for checking them in.
Documents are in queue to be imported	During full synchronization, some new documents for which the synchronization jobs are not created yet will be moved to the Lost and Found folder and will not be imported. For all other synchronization types (current folder, current folder with subfolders, etc.) there will be no effect.
Items added to the collisions folder during next sync	No effect. The client keeps track of the colliding items and their target locations in the repository by unique IDs, so the profile is not needed for detecting collisions or for prompting the user to save or delete the colliding items.
Any other items	The client discards any other cached documents, even offline-enabled ones, unless they remain accessible through other profiles.

To delete a profile:

1. Log in to Documentum Administrator (DA) with Administrator privileges.
2. Navigate to the **Client for Outlook** node under **Administration**, and expand the node.
3. Single left-click **Profiles** on the left, then single left-click the name of the profile you wish to delete on the right side to highlight it.
4. Right-click on the highlighted profile name you selected in step 3 above, and select **Delete**. As MyD Outlook profiles are Documentum objects, they can have more than one version and therefore you may be prompted to delete only the current version or all versions.
5. Users who had previously logged in to MyD Outlook using the profile you have deleted will no longer be able to access items saved to that profile's location(s) through MyD Outlook. Deleting a profile does not delete the items in the repository folders.

Note: Deleting a profile has the same effect on client machines that have accessed this profile as described in the [Table 80, page 719](#) table above.

Overview page

The Overview link under Client for Outlook in Documentum Administrator (DA) displays repository information on the right-side of the browser window, as shown in [Figure 41, page 720](#).

Figure 41. The My Documentum for Microsoft Outlook Overview panel in Documentum Administrator

Overview				
Repository status				
▲ Repository	Repository Status	Profile	Profile Availability	Profile Targets
camb_docapps_d6	disabled	Login		
camb_docapps_sp3	disabled	Login		
DCOD6docapp_dev	disabled	Login		
dcodocapp_mig_wei	enabled	Login		
dev_dco_d6	disabled	Login		
dev_dco_sp2_2_sp5_2	disabled	Login		
dev_dco_sp3	disabled	Login		
wei_53_test	disabled	Login		
wei_d6_test	enabled	bee tesqqw test wei333	Offline Offline Online Offline	/DCO/Bee 2 /System None /Temp /Templates

Each repository that has been configured for MyD Outlook is listed in this section. Shown are the current status of the repository (enabled or disabled), the profiles configured for this repository, and their availability (set during the creation of the profile, see [Creating new profiles](#)), and their target folder(s). A **Login** button appears for repositories that are not configured for automatic login by the administrator. Clicking the **Login** button in the Profile column will display a browser window prompting your for the administrator account login credentials. Once successfully logged in to that repository, the repository status will change to the current status of the repository (enabled or disabled) and the profiles associated with that repository will be displayed, as well as the target folder(s).

Column Setup (Views)

The next option under the Client for Outlook node is the **Column Setup** page as shown in [Figure 42, page 721](#). Here you define how MyD Outlook will display columns to end users. Although you have defined views and will assign one of them to each profile, an end user has the option to modify the view according to his or her preference, and that will override the way Outlook works on that end user's PC only (other users will not be affected).

Figure 42. The Column Setup panel

Column Setup
The views below determine which columns appear in Documentum Folders in Outlook. Outlook users can customize and switch between them.

View	Summary of selected columns
Documents and Messages View	Icon,Attachment,From,Subject,DCO_PropName_ReceivedDate,r_content_size,Format,Flag Status,DCO_PropName_CheckedOut...
Documents View	Icon,Subject,r_content_size,Format,DCO_PropName_ModifiedDate,Owner Name,Flag Status,DCO_PropName_CheckedOut,
Messages View	Importance,Icon,Attachment,From,Subject,DCO_PropName_ReceivedDate,r_content_size,Format,Flag Status...

New View Properties Delete View Duplicate View

Creating new views

To verify or modify the columns available in a particular view, click on the link for the name of the view in [Figure 42, page 721](#), which will bring you to the page to begin the selection process. If you wish to create another view not currently defined in the Column Setup page, click the **New View** button, name the view, then select the columns you wish to make visible.

Figure 43. Creating a new view

View

*Name:

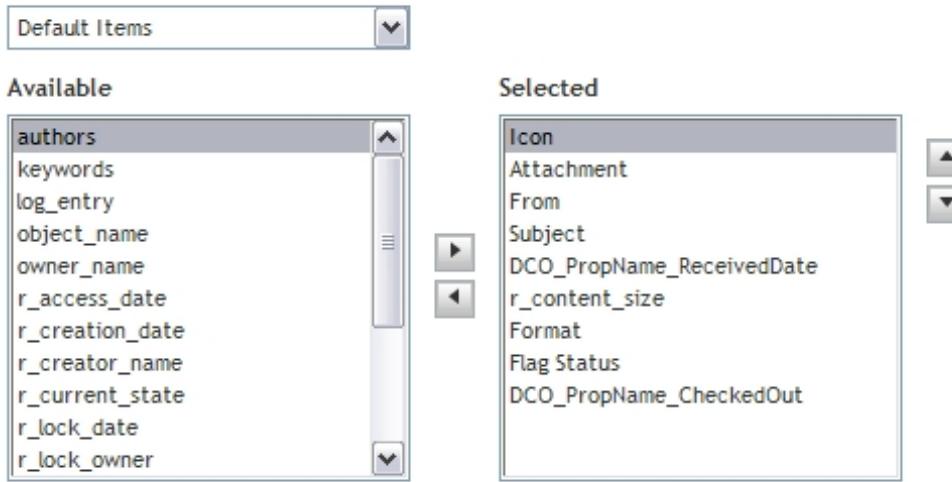
Columns: **Select** Icon,Attachment,From,Subject,DCO_PropName_ReceivedDate...

Sort By:

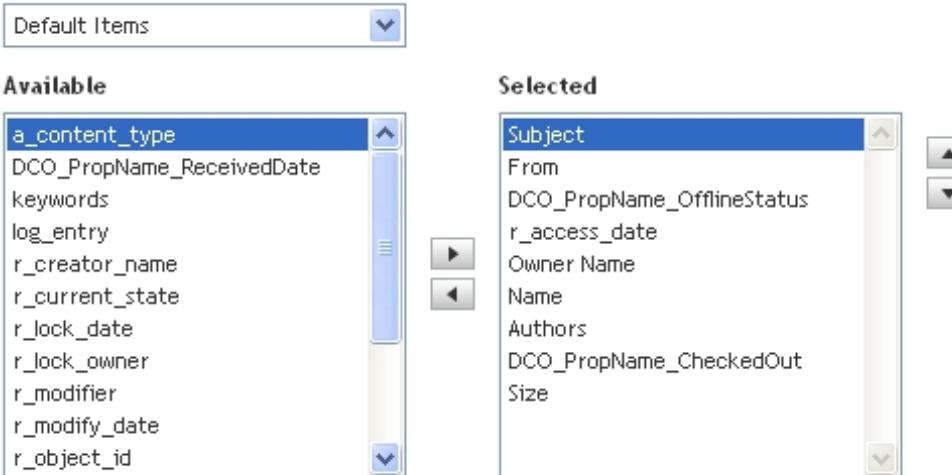
Sort Order:

Selecting columns

Click **Select** to choose columns you wish to be displayed on an end-user's machine, as shown in [Figure 44, page 722](#)

Figure 44. Selecting columns

In the drop-down box directly above the **Available** heading, you can select from which group you wish to add columns. The initial choice list is **Default Items**, however the drop-down menu includes, among others, fields from Outlook, document, and dco_profile. [Figure 45, page 722](#)

Figure 45. Column selector drop-down menu

The list of columns from which you can choose depends on which of the drop-down grouping you have selected.

To add a column to a view, click on the name of the attribute from the **Available** drop-down list, then click the

Figure 46. Right arrow

button to add the column to the view. Conversely, you can remove a column from the view by selecting it in the right (**Selected**) drop-down list and clicking the left-pointing arrow to move it back to the list of available columns.

Note: If you have defined a view that is currently in use by MyD Outlook end users, and you make a change to that view, you can select the checkbox next to **Replace this view currently used by the Outlook client**, and the next time an end user selects that view, the column selection on his or her machine will be updated to your new settings.

Note: To define the default column view, see [Creating new views](#).

Once you have defined the list of columns for this view, the **Sort by** drop-down menu is updated with your choices and only includes the columns that you have indicated.

Modifying, duplicating and deleting views

To modify an existing view:

1. Open the **Column Setup** node from Documentum Administrator.
2. In the right pane, single left-click on the description for that view in the **Summary of selected columns** column on the right. The **Properties** button comes into view. Select the **Properties** button to bring up the properties page.
3. Make the necessary changes and click **OK** to save your changes.

To duplicate (copy) an existing view:

1. Open the **Column Setup** node from Documentum Administrator.
2. Highlight the view you wish to copy from the **Column Setup** page. Highlight the entry you wish to duplicate by clicking in the right-hand column called **Summary of selected columns**. The **Duplicate View** button comes into focus.
3. Click **Duplicate View**. The View Setup page displays, and the name of the new view has been preceded with the words *Copy of* before the original name. You should rename the new view to something of your choosing. Note that all original settings have been copied.

To delete an existing view:

The default **Documents and Messages**, **Documents** and **Messages** views cannot be deleted.

1. Open the **Column Setup** node from Documentum Administrator.
2. Highlight the view you wish to delete from the **Column Setup** page by clicking in the right-hand column called **Summary of selected columns**. The **Delete View** button comes into focus.
A warning message appears, asking you if you are sure that you wish to delete this view.
3. Click **Delete View**.

Deleting views

To delete an existing view:

The default **DocumentOnly**, **EmailDocument** and **EmailOnly** views cannot be deleted.

1. Open the **Column Setup** node from Documentum Administrator.
2. Highlight the view you wish to delete from the **Column Setup** page by clicking in the right-hand column called **Summary of selected columns**. The **Delete View** button comes into focus.
A warning message appears, asking you if you are sure that you wish to delete this view.
3. Click **Delete View**.

Client Setup

An administrator can control the default options that end users can later modify for their client-side installations. [Figure 47, page 724](#) shows the configurable options. Note that the values for Sessions Kept in History and Maximum Disk Space Allowed are the initial values, and users are able to change either or both of them at any time. Any options marked with a red asterisk are required.

Figure 47. The Client Setup page

The screenshot shows the 'Client Setup' page with the following sections and settings:

- Automatic Synchronization:** Set to "Once a day at..." with a dropdown arrow. Next to it are fields for "Hour" (3) and "Minute" (00). A note states: "If Outlook is running, MyD Outlook can automatically sync content between Outlook and repositories."
- Sessions Kept in History, value between 1-10000:** Set to 20. A note says: "Outlook users can view a record of MyD Outlook synchronizations sessions."
- Maximum Disk Space Allowed, value between 10MB-500GB:** Set to 100 MB. A note says: "MyD Outlook uses disk space on a local drive to store temporary files and offline-enabled documents."
- Email Address for Support:** Set to tech_support@comp.com. A note says: "Outlook users can request support from the MyD Outlook Options dialog if you provide an email address."

- Automatic synchronization of content that a user is working with while connected to the repository can be configured using one of the following values: Once per hour, Once a day, or you may turn automatic synchronization off altogether, thereby forcing a user to perform the sync manually. The synchronization process does not synchronize settings, it only synchronizes content.

Note: If using either the once per hour or once per day option, the time that you select **must be indicated in military (24-hour) time format**, e.g., for 1:00 PM, enter 13 in the **Hour** field and 00 in the **Minute** field.

- End users can view the history of previous synchronization sessions. For more information on setting end-user preferences and viewing synchronization history on an end-user machine, refer to the *My Documentum for Microsoft Outlook version 6.5 SP2 User Guide*.

Note: The settings configured in the first three sections above (Automatic Synchronization, Sessions Kept in History and Maximum Disk Space Allowed) are only synchronized to the end-users' MyD Outlook clients the first time they synchronize with the server.

- In addition, an administrator can indicate the default value for the maximum storage space allowed on an end-user machine, but this value can also be configured on an end-user client machine using the **Options** dialog box in MyD Outlook. The same **Options** dialog box contains the email address to which MyD Outlook-related technical support requests from end users will be directed.

Taxonomies and Categories

This section includes the following:

- Taxonomies and categories overview, page 727
- Submitting an item for categorization, page 727

Taxonomies and categories overview

Taxonomies are hierarchies of categories into which you can organize content. A taxonomy provides an alternate way to organized content from the way it is organized in the repository's cabinet and folder structure.

Taxonomy functionality is available if Documentum Administrator is integrated with Documentum CIS server.

To navigate categories

1. Under the Cabinets node, click **Categories**.
2. Click a taxonomy.
3. Click a category. Continue clicking categories until you find the item you are looking for.

To move, copy, or perform other actions on categories, use the same procedures as you would for folders. To perform actions on content in categories, use the same procedures as you would for any file in the repository.

A template can specify that new content created from the template is linked to one or more categories. When a user creates new content from the template, the content is linked to categories for which the user has at least Browse permission.

Submitting an item for categorization

If CIS functionality is available, you can submit items for categorization. Submitting an item sends a request to a categorization queue. When CIS makes the assignment, the submitted item appears in the appropriate categories.

To submit a file for categorization

1. Navigate to and select the file to be submitted.

Tip: 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 the following:
 - If you are submitting one file, click **OK**.
 - If you are submitting multiple files, confirm submission for each file separately by clicking **Next**. After the last file, click **Finish**. To confirm submission for all remaining files at once, click **Finish** before you get to the last file.

Chapter 32

Forms

This chapter includes:

- Enter data in a form, page 729
- Format text in a form, page 729
- Create a new form, page 731
- Save As functionality, page 732

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, page 729](#).
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**.

Format text in a form

To format text in a form, use the buttons described in [Table 81, page 730](#). Some of the buttons may not appear.

Table 81. 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 Ctrl-X .
	Copies the selected text to your clipboard.
	In certain browsers, the browser security setting might disable this button. To copy text, press Ctrl-C .
	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 Ctrl-V .
B	Bolds the selected text.
I	Italicizes the selected text.
U	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.

Button	Description
	Changes the color of the selected text.
	Changes the background color of the selected text.
	Undoes the previous action.
	<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.
	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.

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 EMC Documentum Forms Builder. To use form functionality, you must be assigned the user role of `form_user`, which is defined by the Forms DocApp.

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, page 729](#).

Save As functionality

The **File > Save As** functionality in 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.

Chapter 33

Records

A record consists of recorded information that is evidence of your organization's operations.

A record is either formal or informal. Formal records are created explicitly by filling out form metadata, and assigning them to a formal file plan. Informal records are created when files are dragged-and-dropped into retention managed folders.

This chapter includes:

- [Declare an item as a formal record, page 733](#)
- [Link a record, page 738](#)
- [Create a record relationship, page 738](#)
- [View a record relationship, page 739](#)
- [Remove a record relationship, page 739](#)
- [Make library requests, page 739](#)

Declare an item as a formal record

The user must be part of the form_user group to create formal records, formal cabinets, and formal folders.

To declare an item as a formal record:

1. Navigate to, and select the document to be declared as a formal record.
2. Click **Records > Declare Formal Record**.
The screen displayed for multiple documents is slightly different from that displayed for one document. It includes an optional field to make one record or individual records of the documents selected.
3. Optionally, you can change the default setting for **Declare selected documents as from Individual records to One record** if you have multiple documents selected.
4. Click **Select** for the mandatory **File Plan**, and select a valid file plan, cabinet or folder. The icon for a valid plan, cabinet, or folder is highlighted. 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.
5. 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 properties. Additional properties include:

- **Type**, mandatory
 - **Form Template**, mandatory
 - **Unlink source documents**, optional
 - **Hide options**, optional
6. Select a value for the mandatory **Type**, and **Form Template** properties. The value selected for the **Type** indicates the type of formal record to create, DoD formal records according to Chapter 2 or Chapter 4 requirements or just regular formal records.
- The value for the **Form Template** is automatically populated according to the value selected for the **Type**.
7. Optionally, you can select the checkbox to **Unlink source documents** only if you want to allow anyone with **Unlink** privileges to remove the source document from its original location in a folder after it has been declared a formal record.
8. Click **Continue** to fill out the form displayed according to the **Form Template** selected. Tables are provided, for your reference if needed, to help you complete the applicable form, refer to [Enter values on the applicable form when declare formal record, page 734](#).
- The top of the form displayed indicates 1 of a number, depending on the number of documents selected, if you are declaring multiple documents as **Individual records**.
9. Click **Finish**.

Enter values on the applicable form when declare formal record

This section describes these:

- [Enter values for regular formal records, page 734](#)
- [Enter values for Chapter 2 formal records, page 735](#)
- [Enter values for Chapter 4 formal records, page 736](#)

Enter values for regular formal records

See [Table 82, page 734](#) for an explanation of common properties for regular formal records.

Table 82. Common properties for formal records

Property	Description
Name	The name of the document being declared.
Subject	The principal topic addressed in a document could be used.

Property	Description
Authors	The author of the document being declared a formal record.
Keywords	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.

Enter values for Chapter 2 formal records

There are two forms to choose from for declaring Chapter 2 records, one used to declare documents other than email as formal records, and another one used to declare email as formal records:

- Record DoD 5015 Ch2
- Email Record DoD 5015 Ch2

Do not use Email Record DoD 5015 Ch2 to declare email records from Documentum Administrator. This form is intended for use when declaring email records using RM Outlook Activator.

See [Table 83, page 735](#) for descriptions of properties that might need further explanation, beyond their property names.

Table 83. Common properties for Chapter 2 formal records

Property	Description
Subject	The principal topic addressed in a document could be used.
Media Type	The material or environment on which information is inscribed (microfiche, electronic, and paper for example).
Application Format	The format based on the application used to create the document being declared a record.
Originating Organization	The official name or code of the office responsible for the creation of the document being declared.
Received Date	The date you received the document.
Primary Addressees	The primary name of someone who authored the document.
Other Addressees	The name of anyone else responsible who can address any questions if necessary.
Locations	The location where the record is kept.

Property	Description
Project Name	The value 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 a value if you need additional security on top of the security provided by the value selected for the Project Name. This could be done to further restrict access to a subset of the members in the bigger group.

Enter values for Chapter 4 formal records

Chapter 4 formal records are created as classified or non-classified records differentiated only by their security level whereby any security level higher than zero makes it classified. A security level or ranking of zero is represented by a classification of *No Markings*. Though you can downgrade a classified record through a number of levels from Top Security for example, down to No Markings to make it non-classified (or declassified), you can only go one level up to make a non-classified record classified.

The form makes it possible for you to:

- Classify (file) classified or non-classified records manually or automatically based on the source it is derived from
- Change classification settings to upgrade or downgrade the record
- Schedule downgrade jobs
- Declassify classified records or turn non-classified records into classified records
- Identify reviewers if needed

See [Table 84, page 736](#) for descriptions of properties that might need further explanation, beyond their property names.

Table 84. Common properties for Chapter 4 formal records

Property	Description
Media Type	The material or environment on which information is inscribed (microfiche, electronic, and paper for example).
Format	The format based on the application used to create the document being declared a record.
Originating Organization	The official name or code of the office responsible for the creation of the document being declared.
Derived From	The source to use as the template for completing the form.

Property	Description
Classifying Agency	The name of the classifying agency when you are creating a classified record.
Classified By	The means by which to specify a valid user for this value.
Declassify On	The trigger needed to initiate declassification for classified records. Classified records at some point in time must be declassified. A blank is included among the triggers as the value to be selected for non-classified records when the Current Classification specifies <i>No Markings</i> .
Locations	The location where the record is kept.
Project Name	The value 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 a value if you need additional security on top of the security provided by the value selected for the Project Name. This could be done to further restrict access to a subset of the members in the bigger group.
Downgrade On	The trigger 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.
Downgrade On Date	The date of the downgrade, if the trigger includes a date.
Downgrade On Event	The event to be downgraded, if the trigger includes an event.
Target Downgrade Level	The security level to downgrade to. The formal record is declassified (becomes a non-classified record with no security) if you select <i>No Markings</i> which is equivalent to a ranking of "0" (zero). Any level higher than zero keeps the record classified.
Downgrade Instructions	Instructions for the downgrade.
Reviewed On	The date, and time the review was completed, if a review was involved.
Reasons for Classification	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.

Property	Description
Exemption Category	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. Declassification of a classified record is prevented (stopped) based on the value selected for this field.
Exemption Category (Extend)	The exemption category for the value when the value specified for Derived From is anything other than <i>Classification Guides</i> .

Link a record

Link a record stored in one policy managed folder to another policy managed folder if the record needs to be regulated by more than one policy managed folder. The record will now inherit policies from all locations.

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 open. Linking a record to a policy managed folder that has been closed is not permitted. Additionally, the containment policy must also allow it, and the link level of the containment policy must also be set to greater than "1".

You can perform this procedures on both formal, and informal records.

To link a record to an open folder or to a file plan:

1. Navigate to, and select the record.
2. Select **Edit > Add To Clipboard**.
3. Navigate to the policy managed folder (file plan) to which to link the record.
4. Select **Edit > Link here**.

Create a record relationship

Create a record relationship if a record needs to be related to another record or to another document. You might want to relate two or more records to ensure any further information that is not available in one record is accounted for in a related record.

Record relationships are uni-directional, meaning that the record selected first will be the parent to the second record selected, the child. The child can be reused in another relationship where it can be selected first to be the parent. You can create as many relationships as needed reusing the parent or child, and relating them to other records as needed.

You can perform this procedures on both formal, and informal records.

To create a record relationship:

1. Navigate to, and select a record.
2. Select **Records > Create Record Relationship**.
3. In the selection dialog box, select a second record or a document in a record, and click **OK**. For detailed steps see [Locate an item in a selection dialog box, page 44](#).
4. Select the relationship type.
5. Click **OK**.

View a record relationship

You can perform this procedures on both formal, and informal records.

To view a record relationship:

1. Navigate to, and select an item that is in a record relationship.
2. Click **View > Record Relationships**.

Remove a record relationship

You can perform this procedures on both formal, and informal records.

To remove a record relationship:

1. Navigate to, and select a record.
2. Click **View > Record Relationships**.
3. Select the appropriate item.
4. Click **Records > Remove Record Relationship**.
5. Click **OK**.

Make library requests

If your organization includes Physical Records Manager functionality, then you can make requests to reserve one or more physical objects to borrow. The library administrator decides who gets what, regardless of whose request came first.

For more information on library requests, and Physical Records Manager, see the documentation for EMC Documentum's Retention Policy Services Administrator, and EMC Documentum's Records Manager Administrator.

To make a library request:

1. Navigate to a physical object to reserve.

Contents in a container such as a box or 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, includes the folder, and the document on the manifest if those physical objects are in the selected box. The manifest identifies only the container if it has no contents.

2. Right-click the physical object, and select **Make Library Request**.

Tip: You can select, and right-click multiple physical objects at once.

3. Complete the fields as appropriate.

[Table 85, page 740](#) describes properties that might need further explanation, beyond their property names:

Table 85. Library requests

Property	Description
Date Requested	The 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. The Date Requested may or may not be honored by the Library Administrator. Even though you can make a library request, the Library Administrator will decide whether or not you can have one or more or any of the physical objects requested.
Notification Preference	Select the preferred means of communicating. The system does not use this though it is intended for direct communication from the Library Administrator.
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.

4. Click **Finish**.

To view your library requests, make sure no item is selected in the content pane, and click **View > My Requests**.

Note: Completed library requests are deleted from the system by a job. For more information on the state of a library request, see the *Records Manager Administrator User Guide* or *Retention Policy Services Administrator User Guide*.

Virtual Documents

This chapter includes:

- Virtual documents overview, page 743
- Create a virtual document, page 744
- View the structure of a virtual document, page 744
- View the content of a virtual document, page 745
- Add a descendant to a virtual document, page 745
- Rearrange descendants in a virtual document, page 747
- Remove a descendant from a virtual document, page 748
- Specify that a certain version of a descendant is always used, page 749
- Set a version label for a virtual document, page 749
- Create an archive of a virtual document, page 749
- Convert a virtual document to a simple document, page 750
- Set your virtual document preferences, page 751

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: 

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, page 745](#).

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**.

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)**.
Documentum Administrator 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, page 751](#).
3. Do one of these:
 - If Documentum Administrator displays the document's content, skip the rest of this procedure.
 - If Documentum Administrator prompts you to select between content, and structure, select **Open the content of the document**, and then click **OK**.
 - If Documentum Administrator 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)**.

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, page 744](#).

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, page 44](#).
- 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, Documentum Administrator 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 [Table 86, page 747](#).

A shortcut menu appears.

4. In the shortcut menu, select **Add here**.

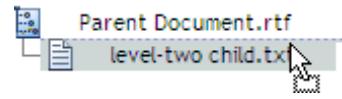
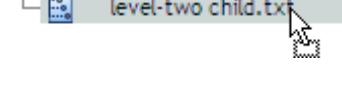
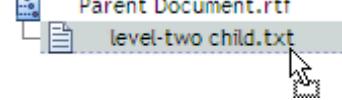
The file is added to the parent document. If you did not select a specific location within the descendants, the file is added as the last descendant in the document. If the intended parent is not a virtual document, the system automatically converts the document to a virtual document.

If the parent document is not already checked out to your computer, Documentum Administrator 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 86. 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, Documentum Administrator 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.
	

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, page 744](#).)
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, Documentum Administrator 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, page 744](#).
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 [Table 86, page 747](#).
A shortcut menu appears.
4. In the shortcut menu, click **Reposition**.
If the parent document is not already checked out to your computer, Documentum Administrator 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**.

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, page 744](#).
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, Documentum Administrator 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**.

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, page 751](#).

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, page 744](#).
2. Select **Tools > Virtual Document > Fix to Version**.
If the parent document is not already checked out to your computer, Documentum Administrator 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**.

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**.

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 [Table 3, page 53](#) in the topic [Set properties, page 53](#).
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.

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, page 748](#).
3. Select the virtual document.
4. Select **Tools > Virtual Document > Convert to Simple Document**.

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 [Table 87, page 751](#).

Table 87. 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.
Bindings	<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>

Property	Description
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.
	<ul style="list-style-type: none"> • Root and descendants: Copies the parent file, and all the descendants nested in the parent file, including descendants of descendants, and so on.
	<ul style="list-style-type: none"> • Root and link to existing descendants: Copies the parent file, and references the descendants.
	<ul style="list-style-type: none"> • 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.
	<ul style="list-style-type: none"> • Prompt me each time: Prompts you to select whether to download as read-only.

3. To save your changes, click **OK**.

PDF Annotations

This chapter includes these sections:

- PDF annotations overview, page 753
- Configure PDF Annotation Service to open when user views a PDF, page 753
- Add comments to a PDF document, page 754
- View comments in a PDF document, page 754

PDF annotations overview

If your organization has installed the EMC Documentum 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 Documentum Administrator.

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 Documentum Administrator to open PDF Annotation Service when you view a PDF.

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.

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.

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.

Chapter 36

Relationships

A relationship is a connection between two items in a repository. Relationships allow Documentum Administrator 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, page 44](#).
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**.

Chapter 37

Renditions and Transformations

This chapter describes the following:

- Renditions and transformations overview, page 757
- Viewing renditions, page 758
- Dragging and dropping renditions to the desktop, page 758
- Importing a rendition, page 759
- Setting a default rendition for an object, page 759
- Viewing the default rendition, page 760
- Overriding an object's default thumbnail, page 760
- Resetting renditions, page 761
- Transforming a document to PDF or HTML format, page 761
- Creating a rendition through transformation, page 762
- Creating a related object through transformation, page 763
- Replacing a file through transformation, page 764
- Creating a new version through transformation, page 765
- Creating a package through transformation, page 765
- Viewing saved transformation properties, page 766
- Enabling inbox notification, page 767

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 Documentum Administrator, 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 EMC Documentum 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, Documentum Administrator 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, page 762](#) for more information on automatically updating a rendition upon versioning.

Note: Some rendition, and transformation functionality is available only on repositories that are configured with EMC Documentum's Content Transformation Services products. Without the presence of these products, some rendition, and transformation functions described in this guide may not be available.

Note: Documentum Administrator does not allow multiple renditions of the same format. Therefore, for any new renditions created, Documentum Administrator replaces any existing renditions of the same format. For example, a Microsoft Word document can only have one Acrobat PDF rendition at any time.

Viewing renditions

All files in Documentum Administrator have a renditions page, whether or not they have more than a primary rendition.

To view renditions for a file:

1. Navigate to and select a file.
2. Do one of the following:
 - On the file's line item, click 
 - Select **View > Renditions**.

Dragging and dropping renditions to the desktop

You can select one ore more renditions from the Renditions page and drag and drop them to the desktop.

To use the drag-and-drop functionality, you must first enable the **drag-and-drop** option in your general preferences, as described in [Set your preferences, page 45](#).

To drag-and-drop a rendition to desktop:

1. Select a file, right-click the file, and choose **View > Renditions**.
The Renditions page lists all renditions of the selected file.
2. Drag a rendition and drop it on to your desktop.
The rendition object is copied to the desktop.

Importing a rendition

You may import a file from outside the repository to use as a new rendition for an existing repository object.

To import a file as a new rendition:

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, browse to locate the file you want to import.
4. In the **Format** field, select the rendition's file format if it is not automatically selected.
5. In the **Description** field, enter a description for the rendition. You can use this field to differentiate between multiple renditions of the same format.
6. Click **OK**.

The file is imported as a rendition of the selected primary rendition.

Setting a default rendition for an object

By default, the primary file of a repository object is used when you choose to view the object. However, you can select an alternate rendition of a file as the default rendition. This lets a rendition other than the primary rendition for previewing the file. For example, for a large, high resolution image file, you may set a smaller, low-resolution image as the default rendition. For video objects, a small section of the video (a sub-clip) may be taken and set as the default, allowing you to preview a brief section of the video rather than the entire primary file.

You can select any rendition of a file to be the default rendition.

A file can have only one default rendition. The icon  appears next to the default rendition. Video objects with a streamable default rendition are indicated with the icon .

Only users with at least Read permissions for the file can select a default rendition.

To set the default rendition:

1. Navigate to the file.
2. Do one of the following:
 - On the file's line item, click .
 - Select **View > Renditions**.
3. Select the rendition you want to set as the default rendition.
4. Right-click and select **Set as Preview** from the context menu.

Viewing the default rendition

The default rendition (if one has been set), is designated by the icon . If a video object has a streamable video as the default rendition, it is designated by the icon .

To view the default rendition, click the default rendition icon as indicated above. The appropriate application opens and displays or plays the default rendition.

If you experience any difficulty in playing an item's default rendition (audio or video), you can set your format preferences to use a specific application to open a file type. You may also have to configure your browser's settings for how to handle file types. See your browser's help for more instruction.

Overriding an object's default thumbnail

If configured to do so, Documentum Administrator creates thumbnails for new files when they are first created or imported into the repository. (New thumbnails may take some time to appear.) If a low-resolution thumbnail cannot be generated, the thumbnail appears as a representation of the file type, using the standard file format icon.

If no thumbnail can be delivered to or loaded in the browser, Documentum Administrator displays an icon to represent the broken thumbnail. The icon used to signal a broken thumbnail can be configured, but appears as a generic broken document icon () by default.

To override a default thumbnail:

1. Select a file and select **View > Properties > Info**.
2. Scroll down to the **Thumbnail** property.
3. Click **Replace**.
4. Select an alternate thumbnail rendition or import a new file to be used as the default rendition.
5. Click **OK** to save your changes.
The file's thumbnail refreshes.

Resetting renditions

Resetting renditions allows you to put an object through the import process again. This means that if expected renditions failed to generate during registration, or if an object has been versioned, you may choose to regenerate the current file's default renditions. This includes the thumbnail, low resolution rendition, and any storyboards, if applicable.

The original file and any renditions that have been generated manually during the file's lifetime, will be left untouched, unless the rendition has been set to be transformed every time the object is versioned. If this is the case, the transformation is performed again, and added as a rendition to the object, replacing the previous rendition.

Note: Content Transformation Services products must be installed and configured for your repository to generate renditions on import.

To reset renditions for an object:

1. Navigate to and select the file for which you want to reset renditions.
2. Select **Tools > Transform > Reset Renditions**.

Transforming a document to PDF or HTML format

Documentum Administrator uses EMC Documentum Content 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 Content 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 object's list of renditions.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

It may also be possible, depending on what other Documentum products are installed on your system, to transform a document to PDF or HTML formats with options. See [Creating a rendition through transformation, page 762](#) and [Creating a related object through transformation, page 763](#) for more information.

To transform a document to PDF or HTML:

1. Navigate to and select the document that you want to transform to PDF or HTML.
- Note:** You can transform a primary file or another rendition.
2. Select **Tools > Transform > PDF Rendition** or **Tools > Transform > HTML Rendition**.

The transformation request is immediately sent to the appropriate queue for processing.

Creating a rendition through transformation

Documentum Administrator uses EMC Documentum Content Transformation Services products to provide the functionality needed to transform a file and create a new rendition.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

Note: Not all features mentioned in the following procedure are available for all file formats and some file formats cannot be transformed. See [Renditions and transformations overview, page 757](#) for more information on renditions and transformations.

To create a new rendition through transformation:

1. Navigate to and select the file(s) that you want to transform to create a new rendition.

Note: You can transform a parent file or another rendition.

2. Select **Tools > Transform > More Formats**

3. The **Transform** wizard appears.

- a. In the **Select Transformation** tab, select a transformation profile and click **Next**.

- b. The **Transformation Details** tab may appear if there are any details that may be entered, or are required for the selected transformation.

Enter any information necessary for setting the parameters of the transformation and click **Next**.

- c. In the **Save As** tab, select **Create a New Rendition** and click **Next**.

The **Rendition Definition** screen appears.

- d. Enter a name for the rendition in the **Rendition Name** field.

If a rendition of this file in the same format already exists for any of the selected files, then you can differentiate the new rendition you are creating by giving the rendition a unique identifier in the **Rendition Description** field.

Note: If you are prompted that a file of the same format and description already exists, you can overwrite the existing file by clicking **Yes**. You can keep both the new file and the existing file by clicking **No**. Selecting **No**, requires that you go back and enter a unique description. This will depend on whether you already entered a **Rendition Description** in the previous step or if that description conflicts with an existing description for a rendition of the same name and format.

Select **Save Transformation** if you want this transformation to be performed automatically each time the primary file is versioned.

Select **Set as Default Preview** if you wish to set the new rendition as the default rendition for the object.

- e. Click **Finish**.

The transformation request is immediately sent to the appropriate queue for processing.

Creating a related object through transformation

Documentum Administrator uses EMC Documentum Content Transformation Services products to provide the functionality needed to transform a file and create a new related object.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

Note: Not all features mentioned in the following procedure are available for all file formats and some file formats cannot be transformed. See [Renditions and transformations overview, page 757](#) for more information on renditions and transformations.

To create a new related object through transformation:

1. Navigate to and select the file that you want to transform to create a new related object.
Note: You can transform a parent file or a rendition.
2. Select **Tools > Transform > More Formats**.
The **Transform** wizard appears.
3. In the **Select Transformation** tab, select a transformation profile and click **Next**.
4. The **Transformation Details** tab may appear if there are any details that may be entered, or are required for the selected transformation.
Enter any information necessary for setting the parameters of the transformation and click **Next**.
5. In the **Save As** tab, select **Create a New Object** and click **Next**.
6. The **New Object Definition** tab enables you to enter properties for the new object. The only required attribute is a name for the object. Do the following:
 - a. Enter a name for the new object. The parent file name is entered by default.
 - b. Enter a title for the object.
 - c. Select an object type.
 - d. Click **Edit** to enter an alternate permission set to the object. The permission set of the parent object is used by default.
 - e. Click **Edit** to apply a lifecycle to the object.

- f. Select the location for the new object. You have two options:
 - **Same as parent file**
This is selected by default. The new object is placed in the same cabinet or folder location as the original object.
 - **New location**
This requires you to select a new location.
 - g. Select **Save Transformation** if you want to perform this transformation each time the parent object is versioned.
7. Click **Finish**.
The transformation request is immediately sent to the appropriate queue for processing.

Replacing a file through transformation

Documentum Administrator uses EMC Documentum Content Transformation Services products to provide the functionality needed to transform a file and use the results to replace the original file.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

Note: Not all features mentioned in the following procedure are available for all file formats and some file formats cannot be transformed. See [Renditions and transformations overview, page 757](#) for more information on renditions and transformations.

To replace a file through transformation:

1. Navigate to and select the file that you want to transform and replace.
Note: You can transform a parent file or a rendition.
2. Select **Tools > Transform > More Formats**.
The **Transform** wizard appears.
3. In the **Select Transformation** tab, select a transformation profile and click **Next**.
4. The **Transformation Details** tab may appear if there are any details that may be entered, or are required for the selected transformation.
Enter any information necessary for setting the parameters of the transformation and click **Next**.
5. In the **Save As** tab, select **Overwrite Source**.
6. Click **Finish**.
The transformation request is immediately sent to the appropriate queue for processing.

Creating a new version through transformation

Documentum Administrator uses EMC Documentum Content Transformation Services products to provide the functionality needed to transform a file and use it as the new version of that file.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

Note: Not all features mentioned in the following procedure are available for all file formats and some file formats cannot be transformed. See [Renditions and transformations overview, page 757](#) for more information on renditions and transformations.

To create a new version of an object through transformation:

1. Navigate to and select the file that you want to transform to create a new version of the object.
Note: You can transform a parent file or a rendition.
2. Select **Tools > Transform > More Formats**.
The **Transform** wizard appears.
3. In the **Select Transformation** tab, select a transformation profile and click **Next**.
4. The **Transformation Details** tab may appear if there are any details that may be entered, or are required for the selected transformation.
Enter any information necessary for setting the parameters of the transformation and click **Next**.
5. In the **Save As** tab, select **Version Source**.
6. Click **Finish**.

The transformation request is immediately sent to the appropriate queue for processing.

Creating a package through transformation

Documentum Administrator uses EMC Documentum Content Transformation Services products to provide the functionality needed to transform a file and include it in a zip file. This feature is helpful for exceptionally large files. The file will be packaged into a zip file after the transformation is completed and will reside in the object's renditions list.

You can view the status of your transformation requests in the **Transformations** node of the navigation tree. An indicator also appears next to files that have transformation requests:

- A yellow indicator () indicates that the file has a pending transformation request.
- A green indicator () indicates that a transformation request is currently processing.
- A red indicator () indicates that a transformation request has failed.

Note: Not all features mentioned in the following procedure are available for all file formats and some file formats cannot be transformed. See [Renditions and transformations overview, page 757](#) for more information on renditions and transformations.

To create a package through transformation:

1. Navigate to and select the file that you want to transform to create a new package.
Note: You can transform a parent file or a rendition.
2. Select **Tools > Transform > More Formats**.
The **Transform** wizard appears.
3. In the **Select Transformation** tab, select a transformation profile and click **Next**.
4. The **Transformation Details** tab may appear if there are any details that may be entered, or are required for the selected transformation.
Enter any information necessary for setting the parameters of the transformation and click **Next**.
5. In the **Save As** tab, select **New Package**.
6. Click **Finish**.
The transformation request is immediately sent to the appropriate queue for processing.

Viewing saved transformation properties

Transformation properties appear for an object when that object has been set to perform a transformation each time it is versioned. This option can be set when creating a new rendition or a new object through transformation. The transformation request is stored and related to the source document. When the source document is versioned, the transformation is automatically applied to the new version using the same parameters as the original transformation and the transformation request is sent to the appropriate server for processing.

The Transformation Properties page lists all the saved transformations that will be applied to a document when it is versioned. You can also use the Transformation Properties page to remove a saved transformation from an object and to apply a saved transformation without waiting for a new version of the object.

To view transformation properties:

1. Navigate to an item with transformation properties.
2. Select **View > Properties > Transformation**.
The **Properties** page opens with the **Transformation Properties** tab selected. The saved transformations for the item are listed, detailing the name and description of the transformation profile used, the output format, and whether the output is a rendition or related object.
3. Click the transformation link in the **Name** column to display the parameters of the transformation. These parameters can be used to distinguish between different transformations saved for the object, that use the same transformation profile.

Enabling inbox notification

When performing a transformation, you can choose to receive notifications in your Inbox when the transformation is complete. In order to receive the notifications, you must enable this feature in your preferences . Otherwise, you may enable a notification on an individual transformation when entering and selecting the transformation details.

To enable inbox notification of transformations in your preferences:

1. Select **Tools > Preference**.
2. Navigate to the **General** tab.
3. Select the check box for **Turn Inbox Notification options on**.

Appendix A

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. [Table 88, page 769](#) describes the default keyboard shortcuts. Customized installations might vary.

Table 88. 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

Action	Microsoft Windows shortcut	Mac OS shortcut
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
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

Index

A

access control lists, 225 to 226
access levels, 226
accessibility mode
 selecting, 32, 40, 46
ACL replication job, 306
ACLS, 225 to 226
acs configuration mode, 156
acs configuration objects
 connection brokers, 156
 network locations, 157
 projection targets, 156 to 157
ACS read setting, 177
ACS Server Configuration Properties - Info page, 162
ACS Server Configuration Properties - Projections & Stores page, 156, 165
ACS servers
 properties defined, 162, 165
ACS servers, configuration, 145
ACS Write setting, 177
actions, 575
Actions page, 564
activation date, 603
active users, 669
Add Repository option
 log into new repositories, 41
adding
 group to permission set, 233, 237
 user to permission set, 233, 237
additional actions, 569
additional_media_properties key, 458
additional_metatag_file_exts key, 457
administration methods
 CAN_FETCH, 330
 CLEAN_LINKS, 331
 DB_STATS, 342
 DELETE_REPLICA, 331
 described, 328
 DESTROY_CONTENT, 332
DROP_INDEX, 344
ESTIMATE_SEARCH, 348
EXEC_SQL, 343
FINISH_INDEX_MOVES, 345
GET_LAST_SQL, 350
GET_PATH, 333
IMPORT_REPLICA, 334
LIST_RESOURCES, 350
LIST_TARGETS, 351
MAKE_INDEX, 343
MARK_FOR_RETRY, 348
MIGRATE_CONTENT, 334
MODIFY_TRACE, 349
MOVE_INDEX, 345
PURGE_CONTENT, 339
REPLICATE, 340
RESTORE_CONTENT, 340
results, 353
running, 329
SET_OPTIONS, 352
SET_STORAGE_STATE, 341
viewing, 328
advance queue processors, 647
Advanced Document Transformation Services, 489, 757
advanced searches
 run, 616
Agent component, 564
Agent services, 564
agent_connection_timeout key, 453
Agents, 575
alerts
 in Inbox, 642
alias sets, 666
 adding aliases, 358
 creating, 356
 default, 230
 deleting, 360
 described, 355
 example, 355
 in lifecycles, 678

locating, 356
modifying, 357
of a user, 203
using, 355
viewing, 357

aliases
 adding to alias set, 358
 described, 355
 using, 355
 where used, 355

API
 described, 611
 running, 611

application servers
 creating, 97
 deleting, 97
 modifying, 97
 server configuration objects, 87, 97

approving candidate documents, 532

Archive job, 307

Archive Link page, 564

archived and deleting documents,
 deleting, 568

archiving, content files, 307

\$ARG#s, 585

assemblies
 view, 749
 See also snapshots

Assign as Attributes option, 501

assignment policies
 rule execution, 420
 when triggered, 420

asynchronous
 transformations, 757

<at least one index entry>, 478

attached files
 in tasks, 641
 remove, 650
 view, 642

attachments
 copy, 639
 edit copy, 639
 locate, 640
 open, 638
 view, 637

attribute, 606

attribute map, 585, 588

attributes, 568, 582, 591
 common to all content delivery
 configurations, 439

local_diskfull_limit, 573
specific to a content delivery
 configuration, 439

attributes to display, 610

Audio/Video Transformation Services, 489

audit
 polices, 260

audit events
 in workflows, 651

Audit Management job, 307

audit trail entries, deleting, 307

audit trails
 deleting, 258, 260
 described, 249
 displaying, 260
 searching, 257
 verifying, 258, 260
 viewing, 257

auditing
 all objects, 254
 audit trails, 249
 choosing types, 259
 criteria, 260
 deleting audit trail entries, 307
 described, 249
 events, 249, 254, 260
 extended privileges, 249 to 250
 modifying, 254 to 256
 object instances, 252
 object type, 250
 removing audits, 254 to 256
 selection criteria, 259
 verifying audit trail entries, 250

authentication failure, resource agents, 542

Auto Generated, 232

Auto Manage, 585

Auto Manage page, 564

autocomplete
 accept a suggestion, 46
 clear cache, 46
 settings, 46

automatic tasks
 complete, 653
 failed, 653
 in workflows, 649

available
 for tasks, 645

B

background color, 731
 background operations
 view status, 48
 BAPI, 576
 best formats, 609
 binding password, changing, 141
 binding rules
 show broken bindings, 751
 specify, 749
 blob stores
 creating, 391
 described, 382
 distributed stores, and, 391
 linked stores, and, 391
 properties, 392
 BOCS
 pre-caching setting, 177
 BOCS config object Delete page, 174
 BOCS Message Routing, 179
 BOCS pre-caching, 177
 BOCS Server Configuration Properties -
 Info page, 173
 BOCS Server Connection page, 173
 BOCS servers
 about, 168
 communication protocols, 173
 creating, 169
 deleting, 174
 message routing, 179
 modifying, 173
 properties, 175
 BOCS Servers Configuration list page, 168
 BOCS servers, configuration, 145
 bookmarks
 add repository document or folder, 67
 subscriptions, 69
 Branch Office Caching Services
 (BOCS), 168
 breadcrumbs
 overview, 42
 Browse permissions, 226
 Business Process Manager, 101 to 102

C

C++ programs, 273
 cabinets
 create, 52
 histories, 53

properties, 53
 cached types
 creating, 97
 deleting, 97
 modifying, 97
 server configuration objects, 87, 97
 CAD Applications, 582
 CAD Interface, 582
 calendars
 create, 687
 create events, 688
 export and import, 691
 recurring events, 689
 Calendars, 675 to 676
 CAN_FETCH administration method, 330
 candidate documents
 approving, 532
 carrier types, 582
 categories
 adding evidence, 520
 clearing assignments, 533
 common tasks, 727
 copy, 64
 creating, 518
 delete, 64
 evidence for, 502
 link to multiple locations, 66
 navigate, 44
 navigating, 727
 overview, 727
 property rules, 521
 search, 616
 setting rules, 520
 submit items to, 44
 submitting items to, 727
 work queue categories, 664, 671
 categorization, submitting documents, 506
 category classes
 creating, 510
 setting properties, 510
 check_valid_filename key, 459
 checkin
 check in, 55
 Check in from file, 57
 common tasks, 54
 generate versions, 57
 generating renditions, 757
 overview, 54
 checking in, method content, 327
 checking integrity of linked objects, 576

checkout
cancel, 58
check out files, 55
directory, 54
location, 54
overview, 54
view checked out files, 59
view recently checked out, 59
child documents
in virtual documents, 743
Choose a file on the server filesystem page, 334, 336 to 338, 341, 354
Choose a folder page, 283
Choose a group page, 36
Choose a user/group page, 36, 239
Choose Network Location page
BOCS servers, 170
CIS, 499
CLEAN_LINKS administration
method, 331
clearing assignments, 533
Clients page, 564
clipboard
add to, 65
remove from, 65
view, 65
code pages, 87
collaborate
overview, 681
color
apply to background, 731
apply to text, 731
column header, 610
columns
display, 43
in lists, 43
comments
add in discussions, 683
delete in discussions, 684
edit in discussions, 684
reply to in discussions, 684
search for, 684
comparison operators, 660
compound terms, defined, 535
compression key, 455
condition composer, 577
confidence values, 502
configuration
ACS servers, 145
BOCS servers, 145
configuring process engine, 101 to 102
configuring queries, 576
configuring workflows, 576
confirming deletion, 35
connection broker
determining to which you are connected, 34
setting, 36
connection brokers
acs configuration objects, 156
LIST_TARGETS administration method, 351
select, 41
server configuration objects, 87, 94 to 96
Connection Brokers page, 37
Connection Info page, 298
connection_thread_timeout key, 453
connections
failures, 453
Consistency Checker job, 308
Consume URL, 179
content
common tasks, 51
in virtual document, 745
method, 327
Content Attribute page, 407
content delivery
logs, deleting, 474
logs, viewing, 474
publishing objects, 472
results page, 474
content delivery configuration, 439
Content Delivery Configuration - Extra
Arguments page, 452
content delivery configurations
Advanced page properties, 465
creating, 442
deactivating, 472
deleting, 470
duplicating configurations, 471
Info page properties, 464
locating, 441
modifying, 446
properties, 463
Replication page properties, 469
testing, 470
content delivery logs, 461
content file cleanup, 313
content files

archiving, 307
CAN_FETCH administration
 method, 330
copying, 340
determining directory locations, 333
distributed stores, 331
fetching, 330
migrating, 334
renditions, 318
restoring, 340
 without content objects, 313
content files, moving, 286
Content Intelligence Services
 changing passwords, 32
 configuration settings, 508
 introduction, 499
 setting up, 506
content migration job
 Rules tab, 434
 setting rules, 434
content migration jobs
 creating, 429
 described, 429
content objects, orphaned, 313
Content Replication job, 308
Content Server
 determining the version and
 platform, 33
 determining to which you are
 connected, 33
 LDAP directory servers, 143
 log files, 100
 multiple with LDAP, 143
 roles, 212
 startup, 87
Content Services for EMC Centera
 (CSEC), 402 to 403
Content Services for SAP Archive, 564
content storage management
 administration methods, 328
Content Storage Services
 described, 419
Content Transformation Services, 489
content types, 607
content warning job, 309
contextual folders
 create, 686
 overview, 686
Contributor role
 in collaborative services, 702
convert
 Desktop DRLs to Webtop URLs, 68
copying
 content files, 340
create_group privileges, 658
creating
 alias sets, 356
 application servers, 97
 blob stores, 391
 cached types, 97
 distributed stores, 394
 domain maps, 84
 domains, 84
 EMC Centera stores, 403
 external stores, 397
 far stores, 100
 federations, 103
 file stores, 383
 formats, 361
 global users, 190
 groups, 207
 indexes, 343
 indexing queue items, 486
 job sequences, 296
 jobs, 268
 linked stores, 389
 location objects, 416
 locations, 98
 methods, 321
 NetApp SnapLock stores, 411
 new objects through
 transformations, 763
 new version through
 transformations, 765
 object types, 366
 objects, 35
 permission sets, 233
 plug-ins, 418
 projection targets, 94, 96, 156 to 157
 renditions, 762
 replication jobs, 276
 roles, 213, 218
 server configuration objects, 85, 87 to
 88
 users, 186, 196, 198
 XML store, 397
creating a package
 through transformation, 765
 through transformations, 765
creating an Agent, 601

- creating an SAP User, 565
 - creating full-text events, 309
 - credentials
 - delete, 45
 - save, 40, 45
 - view, 45
 - criteria, auditing, 259
 - CSEC, 402
 - csv file
 - export to, 70
 - CTS
 - administration, 489
 - changing the logging interval, 491
 - changing the maximum number of queue items, 492
 - changing the notification setting, 492
 - changing the polling interval, 490
 - changing the queue item expiry, 493
 - changing the system operator, 491
 - changing user for an instance, 489
 - configuring an instance, 490
 - controlling instance, 494
 - log files, 491, 493
 - products, 489
 - refreshing a service, 495
 - starting a service, 495
 - stopping a service, 495
 - viewing a log file, 493
 - viewing instance details, 494
 - Current User's Permission Sets, 232
 - current version
 - create, 58
 - make, 57
 - overview, 58
 - custom attributes, 568
 - custom filter, 568, 570
- D**
- data dictionary publisher job, 312
 - data tables
 - create, 692
 - create entries, 694
 - edit, 696
 - import and export, 697
 - overview, 692
 - database space warning job, 312
 - databases, statistics, 319, 342
 - date format, 603
 - date, effective, 475
 - date, expiration, 475
 - DB_STATS administration method, 342
 - DB2, 312
 - DCS, 681
 - deactivating
 - jobs, 305
 - debugging, 456
 - default renditions
 - setting, 759
 - viewing, 760
 - Define Version page, 291
 - Delete permissions, 226
 - DELETE_REPLICA administration method, 331
 - deleting
 - alias sets, 360
 - application servers, 97
 - archived and linked documents, 568
 - audit trails, 258, 260
 - cached types, 97
 - content files, 339
 - content files from distributed stores, 331
 - content objects, 332
 - far stores, 100
 - formats, 362
 - groups, 209
 - inbox items, dequeued, 316
 - jobs, 304
 - linked store links, 331
 - locations, 98, 383
 - log files, 316
 - logs, Site Caching Services, 318
 - methods, 328
 - mount points, 383
 - network location projections, 160
 - objects, 35, 229
 - objects types, 375
 - permissions required, 229
 - plug-ins, 383
 - projection targets, 96
 - renditions, unwanted, 318
 - roles, 215, 219
 - sever configuration objects, 101
 - storage areas, 383
 - users, 201
 - users from group, 209
 - versions, unwanted, 320
 - descendants
 - add, 745 to 746

- in virtual documents, 743
- locate, 744
- remove, 748
- reorder, 747 to 748
 - view, 744
- description attribute, 606
- Desktop DRLs
 - convert to Webtop URLs, 68
- DESTROY_CONTENT administration method, 332
- destroying indexes, 344
- details
 - workflows, 651
- DIR, 582, 606
- DIR attributes, 585, 588
- directories
 - checkout, 54
- disable_dctm_tag key, 454
- discussions
 - add comments, 683
 - delete comments, 684
 - edit comments, 684
 - overview, 682
 - reply to comments, 684
 - search for comments, 684
- disk capacity, 309
- disk usage, 319
- displaying
 - audit trails, 260
- distributed configurations, 146
- distributed content
 - configuration, 145
 - configuring settings, 177
 - dm_dist_transfer_config, 177
 - System Information page, 34
- distributed operations job, 312
- distributed repositories
 - distributed operations job, 312
- distributed storage areas
 - copying content files, 340
 - importing files, 334
- distributed storage, content
 - replication, 308
- distributed stores
 - blob stores, and, 391
 - creating, 394
 - described, 382, 393
 - modifying, 394
 - properties, 395
 - removing content files, 331
- replicating objects within components, 276
- uses, 393
- distributed transfer
 - ACS read setting, 177
 - ACS write setting, 177
 - BOCS pre-caching setting, 177
- Distributed Transfer Settings Properties - Info page, 177
- distributed transfer settings, configuring, 177
- dm_ACLRepl_job, 306
- dm_ACLReplication job, 306
- dm_archive, 569
- dm_AuditMgt job, 307
- dm_check_password program, 83
- dm_ConsistencyChecker job, 308
- dm_ContentReplication job, 308
- dm_ContentWarning job, 309
- dm_DataDictionaryPublisher job, 312
- dm_DBWarning job, 312
- dm_dist_transfer_config, 177
- dm_DistOperations job, 312
- dm_DMArchive job, 307
- dm_Dmclean job, 313
- dm_DMfilescan job, 313
- dm_dms_config, 179
- dm_doc_type, 569
- dm_FederationCopy job, 313
- dm_FederationExport job, 313
- dm_FederationImport job, 314
- dm_FederationStatus job, 314
- dm_FederationUpdate job, 314
- dm_FileReport job, 314
- dm_FTCreateEvents job, 309
- dm_FTIndexAgentBoot job, 311
- dm_LDAPSynchronization job, 315
- dm_LogPurge job, 316
- dm_message_archive
 - assigned to email messages, 635
- dm_QmPriorityAging job, 664
- dm_QmThresholdNotification job, 663
- dm_QueueMgt job, 316
- dm_RemoveExpiredRetnObjects job, 317
- dm_RenditionMgt job, 318
- dm_SCSLogPurgeJob job, 318
- dm_StateOfDocbase job, 318
- dm_SwapInfo job, 319
- dm_UpdateStats job, 319
- dm_UserChgHomeDb job, 319

- dm_UserRename job, 320
- dm_VersionMgt job, 320
- dm_webc_config object, 440
- dm_webc_target object, 440
- dm_WfmsTimer job, 320
- DMCL, 573
- DMCL trace, 274
- dmcl.ini, 573
- dmclean job, 313
- dmfilescan job, 313
- DMS, 582
- doc profiles, 666
- docbase configuration object
 - described, 73
 - modifying, 74
 - synchronization page, 75
- docbase configuration objects
 - modifying, 74
- Docbasic, 273, 321
- document confidence scores, 502
- document format, 587
- document sets
 - creating, 529
 - property rules, 521
- Document Transformation Services, 489, 757
- document type, 568, 605
- DocumentDescription, 582
- DocumentNumber, 582
- documents
 - common tasks, 51
 - listing, 314
 - publishing, 472
 - removing unwanted versions, 320
 - transforming to HTML, 761
 - transforming to PDF, 761
- DocumentStatus, 583
- DocumentType, 583
- Documentum Administrator
 - about, 29
 - basic configuration, 73
 - connecting to, 31
 - connection brokers, 36
 - content delivery configurations, 439
 - distributed content configuration, 145
 - intended audience, 27
 - System Information page, 32
 - using, 34
 - version connected to, 34
- Documentum Client for Outlook
 - column setup, 720
 - Column view, 715
 - Permissions tab, 718
- Documentum Collaborative Services, 681
- Documentum content types, 609
- Documentum object type, 605
- Documentum Offline Client, 75
- Documentum page, 564
- Documentum query, 576, 578, 585, 590
- Documentum Site Caching Services, logs, 318
- domain authentication, 83
- domain controllers, 84
- domain maps, 83 to 84
- domains, 84
 - log into, 40
- DQL queries
 - described, 611
 - running, 611
- DQL query, 578
- DQL statement, 578
- DQL statements, 350
- Drag and drop
 - rendition, desktop, 758
- drag-and-drop
 - enable, 45
 - to add descendants, 746
 - to check in from file, 58
 - to create relationship, 755
 - to export, 63, 638
 - to import, 61, 635
 - to move descendants, 748
 - to perform actions, 47
 - to subscribe to items, 70
- DROP_INDEX administration method, 344
- dynamic priorities, 664

E

- editing an Agent, 601
- editing an SAP User, 565
- editing connections to an SAP server, 565
- effective label, 475
- email messages
 - attachments, 637 to 640
 - export, 638 to 639
 - import, 634
 - lifecycles, 635
 - overview, 633
 - send links, 68

- transform, 638
 - view, 637
 - EMC Centera Store Properties - Info page, 405
 - EMC Centera stores
 - creating, 403, 407
 - described, 402
 - modifying, 405
 - end-to-end tester, 453, 470
 - error_threshold key, 454
 - ESTIMATE_SEARCH administration method, 348
 - events
 - auditing, 254, 260
 - described, 249
 - removing audits, 256
 - evidence
 - defining for categories, 520
 - propagating, 505
 - understanding, 502
 - evidence terms, 535
 - Excel file
 - export to, 71
 - exclude_folders key, 458
 - exclude_formats key, 459
 - EXEC_SQL administration method, 343
 - executing
 - administration methods, 329
 - methods, 324
 - SQL statements, 343
 - expiration date, 603
 - export_media_properties key, 458
 - export_relations key, 458
 - export_threshold_count key, 456
 - exporting
 - method content, 326
 - express user
 - role, 41
 - extended privileges, 250
 - extensions_to_compress key, 455
 - external filters. See filter programs, 569
 - external free stores, 397
 - external stores
 - creating, 397
 - described, 382, 396
 - external file store, 396
 - external free store, 397
 - external URL store, 397
 - external XML store, 397
 - limitations, 396
 - plug-ins, 396
 - external URL stores, 397
 - external XML store, 397
 - Extra Arguments page, 452
- F**
- Failover page
 - LDAP server configurations, 135, 139
 - far stores
 - creating, 100
 - deleting, 100
 - modifying, 100
 - server configuration object, 87
 - server configuration objects, 100
 - favorites
 - add repository document or folder, 67
 - recently used files, 59
 - repositories, 41
 - subscriptions, 69
 - federation copy job, 313
 - federation export job, 313
 - federation import job, 314
 - federation status job, 314
 - federation update job, 314
 - federations
 - ACL replication, 306
 - adding members, 106
 - creating, 103
 - deleting, 107
 - described, 102
 - job status, 314
 - jobs, 313 to 314
 - modifying, 105
 - removing members, 107
 - users, 187, 190
 - users and groups, 313 to 314
 - file
 - save as, 732
 - file formats
 - associate with object types, 60
 - preferences, 60
 - restore default associations, 61
 - file report jobs, 314
 - file stores
 - creating, 383
 - described, 382
 - migrating content, 334
 - modifying, 386
 - properties, 387

File_ATTRIBUTES, FULL_CHECKSUM,
SPARSE_CHECKSUM, OFF, 462
filename_replace_char key, 459
files
 attach, 642, 650
 cancel checkout, 58
 check in, 55
 check out, 55
 common tasks, 51
 copy, 64
 copy locally, 62
 create, 51
 delete, 64
 demote, 679
 deselect, 42
 drag-and-drop, 47
 edit, 55
 export, 62
 histories, 53
 import, 61
 lifecycle states, 678, 682
 lifecycles, 52, 56, 61, 678
 link to multiple locations, 66
 link to other repositories, 66
 promote, 678
 properties, 53
 remove, 650
 remove lifecycles, 678
 renditions, 757 to 758
 replace, 58
 select, 42
 send to review, 649
 send to workflows, 649
 transforming, 757
 unlock, 58
 versions, 57
 view, 59
 view locations, 67
 virtual documents, 743
 virtual links, 60
filter formats, 609
filter programs, 569
filters, 569
 in lists, 42
 in selection dialog box, 44
 in work queues, 648, 659 to 661
filters, custom, 569
Find All Versions option
 in searches, 619
Find Hidden Objects option

 in searches, 619
FINISH_INDEX_MOVES administration
 method, 345
folder security
 permissions, 228
 WIP content, 228
folders
 contextual, 686
 copy, 64
 create, 52
 delete, 64
 deselect, 42
 display on startup, 45
 drag-and-drop, 47
 histories, 53
 link to multiple locations, 66
 properties, 53
 select, 42
 view locations, 67
force login, 610
force_serialized key, 457
format, 587
format key, 457
format properties, 362
format string, 588
formats
 creating, 361
 deleting, 362
 described, 361
 locating, 361
 modifying, 362
 preferences, 60 to 61
 properties, 362
 viewing, 362
forms
 common tasks, 729
 create, 731
 enter data in, 729
 format text, 729
From Source page, 277
full_refresh_backup key, 459
full-text indexes
 estimating results, 348
 marking content files, 348
 tracing, 349
full-text indexing
 administration methods, 328
 creating events, 309
 creating queue items, 486
 described, 477

-
- index agents, 477
 - index servers, 477
 - queue items, 483, 486
 - reindexing a repository, 309

 - G**
 - General tab
 - in preferences, 45
 - Get Next Task, 647
 - Get Next Task Automatically, 647
 - Get Task
 - enable, 674
 - select, 647
 - GET_LAST_SQL administration
 - method, 350
 - GET_PATH administration method, 333
 - global registries
 - described, 146
 - network locations, 146 to 147
 - global users, 102
 - creating, 190
 - governed objects
 - overview, 699
 - group rename job, 315
 - groups
 - add to a work queue, 667
 - adding users, 208
 - attributes of, 210
 - creating, 207
 - deleting, 209
 - described, 204
 - exporting in a federation, 313
 - federations, 313
 - importing in a federation, 314
 - in work queues, 667 to 668, 670
 - LDAP, 315
 - locating, 206
 - modifying, 208
 - of a user, 203
 - reassigning, 210
 - removing users, 209
 - renaming, 315
 - user management, 183
 - viewing where used, 206

 - H**
 - hidden objects
 - display, 46

 - in searches, 619
 - highlights
 - in search results, 620
 - historical reports
 - workflows, 654
 - histories
 - of repository items, 53
 - home repositories, 319
 - host name, 565
 - hot keys
 - overview, 769
 - HTML, 609
 - renditions, 757
 - transforming to, 761
 - view links, 60
 - HTML renditions, generating, 569
 - HTML source, 731
 - HTTP, 460

 - I**
 - I am available
 - select, 645
 - I am currently set to unavailable
 - select, 645
 - IMPORT_REPLICA administration
 - method, 334
 - importing
 - method content, 324
 - renditions, 759
 - users, 196, 198
 - Inbox
 - available for tasks, 645
 - columns displayed, 43
 - common tasks, 641
 - display on startup, 45
 - get next task, 647
 - manage tasks, 646
 - open items, 642
 - overview, 641
 - unavailable for tasks, 645
 - view, 642
 - work queues, 647
 - inboxes, 316
 - Increment Priority, 664
 - index agent startup job, 311
 - index agents, 477
 - described, 478
 - disabled, 481
 - enabling, 481

modifying properties, 482
properties, 482
starting, 479
stopping, 479
index servers, 477
described, 478
logs, 483
properties, 482
starting, 479
stopping, 479
indexes
creating, 343
destroying, 344
moving, 345
indexing
registering types, 369
Info page
ACS servers, 162
distributed transfer settings, 177
LDAP server configurations, 115, 119
network locations, 147
permission sets, 233, 237, 242
replication job, 276
repository configuration, 77
Info tab, 270
information availability, 575
information integrity, 575
Ingest, 450
ingest from a content delivery
configuration, 473
ingest_workflow key, 460
Ingestion, 439
Initial Priority, 663
Inspection Lots, 570
integrity checking, 600
integrity of documents, 590
Interactive Delivery Services, 439
effective labels, 475
Interactive Delivery Services Accelerated,
IDSx
publishing, replication, 439
internationalization
code pages, 87
locales, 87
introducing
WebAdmin, 563
IP address, 565

J

Java method execution
application servers, 87
Java methods, 273, 321
JMX Service URL, 541 to 542
Job Properties - Qualifier Rules page, 272
Job Properties - Rules page
records migration, 289
job reports
viewing, 303
job runs, 603
job sequences
choosing repositories, 300
creating, 296
repository version, 296
required privileges, 296
jobs, 575
arguments, 274
content migration jobs, 429
creating, 268
deactivating on failure, 305
default repository, 265
deleting, 304
described, 265, 305
dm_ACLRepl_, 306
dm_ACLReplication, 306
dm_AuditMgt, 307
dm_ConsistencyChecker, 308
dm_ContentReplication, 308
dm_ContentWarning, 309
dm_DataDictionaryPublisher, 312
dm_DBWarning, 312
dm_DistOperations, 312
dm_DMArchive, 307
dm_DMClean, 313
dm_DMfilescan, 313
dm_FederationCopy, 313
dm_FederationExport, 313
dm_FederationStatus, 314
dm_FederationUpdate, 314
dm_FileReport, 314
dm_FTCreateEvents, 309
dm_FTIndexAgentBoot, 311
dm_GroupRename, 315
dm_LDAPSynchronization, 315
dm_LogPurge, 316
dm_QmPriorityAging job, 664
dm_QueueMgt, 316
dm_RemoveExpiredRetnObjects, 317

- dm_RenditionMgt, 318
 - dm_StateOfDocbase, 318
 - dm_SwapInfo, 319
 - dm_UpdateStats, 319
 - dm_UserChgHomeDb, 319
 - dm_UserRename, 320
 - dm_VersionMgt, 320
 - dm_WfmsTimer, 320
 - dmFederationImport, 314
 - in shortcuts, 67
 - Info tab, 270
 - job sequences, 296, 300
 - locating, 266
 - locating a method, 275
 - method executed, 273
 - modifying, 304
 - qualifier rules, 272
 - queueperson argument, 274
 - records migration jobs, 286
 - replication, 276
 - required privileges, 265
 - running, 302
 - schedules, 271
 - SCSLogPurgeJob, 318
 - Sysobject Info tab, 275
 - trace levels, 303
 - trace logs, 304
 - viewing reports, 303
 - window_interval argument, 274
 - jobs running modes, 602
- K**
- keyboard
 - hot keys, 769
 - shortcuts, 769
- L**
- languages
 - choose, 40
 - filter for, 42
 - Last Results option
 - in searches, 623
 - LDAP
 - binding password, 141
 - changing passwords, 40
 - jobs, 315
 - mapping, 131
 - synchronization, 315
 - System Information page, 34
 - LDAP directory servers
 - about, 110
 - multiple Content Servers, 143
 - LDAP Server Configuration list page, 111
 - LDAP Server Configuration Properties - Failover page, 135, 139
 - LDAP Server Configuration Properties - Info, 115, 119
 - LDAP Server Configuration Properties - Mapping page, 126, 132
 - LDAP Server Configuration Properties - Sync & Authentication, 121, 124
 - LDAP server configurations
 - adding or modifying, 113
 - failover settings, 135, 139
 - LDAP directory, 115, 119
 - mapping, 126, 132
 - secure connection information, 115, 119
 - synchronization, 121, 124
 - understanding, 112
 - user authentication, 121, 124
 - LDAP synchronization job, 315
 - LDIF file formats, 196, 198
 - licenses
 - Content Services for EMC Centera (CSEC), 403
 - licenses, configuring, 37
 - lifecycles
 - apply, 52, 678
 - assign, 52, 56, 61, 635, 678
 - common tasks, 677
 - demote, 679
 - filter for, 42
 - overview, 677
 - promote, 678
 - remove, 678
 - resume, 679
 - states, 678, 682
 - suspend, 679
 - Lightweight Directory Access Protocol
 - changing passwords, 40
 - Link to Folders option, 501
 - linked stores
 - blob stores, and, 391
 - creating, 389
 - deleting links, 331
 - described, 382
 - modifying, 390

properties, 390
linking, 600
linking Documentum to SAP, 576
linking objects, 575, 582
linking processes, 575
linking SAP to Documentum, 576
links
 common tasks, 65
 create, 67, 731
 delete, 64
 in email messages, 68 to 69
 subscriptions, 69
 to multiple locations, 66
 to other repositories, 66
 view locations of, 67
LIST_RESOURCES administration
 method, 350
LIST_TARGETS administration
 method, 351
lists
 click filenames, 59
 columns, 43
 filenames, 59
 filter, 42, 44
 navigate, 42, 44
 sort, 42
 Starts With field, 42
 view, 42
load operations, 319
local_diskfull_limit, 573
locating
 alias sets, 356
 groups, 206
 jobs, 266
 method for a job, 275
 permission sets, 231
 storage areas, 380
 users, 185
location objects
 creating, 416
 described, 379
 file stores, 384
 modifying, 416
locations
 creating, 98
 deleting, 98, 383
 described, 416
 log in, 40
 logging into, 31
 modifying, 98
server configuration object, 87
server configuration objects, 98
view, 67
lock_exitifbusy_flag key, 454
lock_retry_count key, 454
lock_sleep_interval key, 453
locked files
 overview, 54
 retain lock on checkin, 57
 set preferences for, 752
 sort by, 42, 59
 view, 59
 when check out virtual document, 752
locked ports, 454
locked users, 187, 191
locking ports, 453
log files
 Content Server, 100
 storing, 456
log purge job, 316
logfile, 602
logging, 456
login parameters, 564
logon details, 564
logs
 content delivery, 474
 deleted by dm_LogPurge, 316
 index server, 483
 job trace, 304
 purging, 316
 Site Caching Services, 318
 user reassign, 204
lookup key values, 588

M

make_html (filter option), 569
MAKE_INDEX administration
 method, 343
make_pdf (filter option), 569
make_text (filter option), 569
Manage, 605
Managing
 temporary disk space, 573
Manually Created, 232
Map Property page, 131
map rule, 593
Mapping page
 LDAP server configurations, 126, 132
mapping, LDAP, 131

MARK_FOR_RETRY administration
 method, 348

match filters
 assign to a queue, 661

matching filters
 enable multiple skills, 660

Max Priority, 663

max_cached_ssl_sockets key, 454

max_entries_per_zipfile key, 455

maximum file transfer, 461

MBean resources, 543

Media Transformation Services, 489

Medical ImagingTransformation Services, 489

member list for a room
 open, 702

menus
 open with right-click, 47

messages
 view, 48

messaging server
 configuration, 179
 dm_dms_config, 179

metadata
 export, 70

method_trace_level key, 456

methods, 326
 checking in content, 327
 creating, 321
 deleting, 328
 described, 321
 DMCL trace, 274
 executed by a job, 273
 exporting content, 326
 importing content, 324
 jobs, 268
 locating for a job, 275
 modifying, 321
 running, 324
 storing executable program, 321
 tracing, 274
 viewing results, 326

Microsoft Active Directory, 315

MIGRATE_CONTENT administration
 method, 334

migration policies
 described, 419

min_size_worth_compressing key, 455

minimum file transfer, 461

MODIFY_TRACE administration
 method, 349

modifying
 alias sets, 357
 application servers, 97
 cached types, 97
 distributed stores, 394
 docbase configuration objects, 74
 far stores, 100
 file stores, 386
 formats, 362
 groups, 208
 index agent properties, 482
 jobs, 304
 linked stores, 390
 location objects, 416
 locations, 98
 method content, 326
 methods, 321
 object types, 368
 objects, 35
 plug-ins, 418
 projection targets, 94 to 96, 156 to 157
 roles, 214, 219
 server configuration objects, 87
 server root locations, 400
 storage area state, 341
 users, 203

modifying content, 326

modifying replication settings
 content delivery configuration, 450

mount point objects
 described, 379

mount points
 aliases, 414
 deleting, 383
 described, 414
 file system path, 414

MOVE_INDEX administration
 method, 345

moving
 indexes, 345

mssql_store_varchar key, 456

multiple replication targets, 439

My Documentum
 access, 49
 folder, 49

My Documentum for Microsoft Outlook, 711

 Client Setup, 724

- client synchronization settings, 724
- column selection for views, 721
- column selector drop-down menu, 722
- column view setup, 715
- configuration file, 711
- Create tab for new profile, 713
- creating new profiles, 713
- creating new views, 721
- DCO_System_Settings.xml file, 711
- default view, 715
- deleting a profile, 719
- deleting an existing view, 723 to 724
- duplicating (copying) an existing view, 723
- Info tab, 714
- maximum storage space for client machines, 725
- modifying an existing view, 723
- modifying, duplicating and deleting views, 723
- overview page, 720
- Permissions tab, 718
- profile import preferences, 716
- profile import settings, 717
- profile modify, 718
- profile target settings, 715
- profiles, 713
- tree location in Documentum Administrator, 712
- My Files
 - columns, 43
 - display on startup, 45
 - view, 59
- My Home Cabinet, 42
- My Work Queues, 671
- My Workflows
 - view, 652
- MyD Outlook. *See* My Documentum for Microsoft Outlook
- N**
 - navigation path
 - overview, 42, 44
- NetApp SnapLock Store Properties - Info page, 412
- NetApp SnapLock stores
 - creating, 411
 - described, 410
 - modifying, 412
- Netscape iPlanet, 315
- Network Location object Delete page, 151
- network location projects, 160
- Network Location Properties - Info page, 151
- network locations, 146
 - about, 146
 - acs configuration objects, 157
 - copying, 149
 - creating, 147
 - delete warning, 151
 - deleting, 150 to 151
 - described, 146
 - global registries, 146 to 147
 - modifying, 149
 - properties, 151
 - restrictions on creating, 146
 - server configuration objects, 87, 96
 - viewing, 149
- Network Locations list page, 146
- New ACS Server Configuration - Info page, 162
- New ACS Server Configuration - Projections & Stores page, 162
- New BOCS Caching Job - SysObject Info page, 294
- New BOCS Server Configuration - Info page, 169
- New Content Delivery - Extra Arguments page, 452
- New EMC Centera Store - Info page, 403
- New Job - From Source page, 277
- New Job - Info page, 268, 297
- New Job - Method page, 269
- New Job - Qualifier Rules page, 272
- New Job - Schedule page, 269, 287, 297
- New Job - SysObject Info page, 269, 288
- New Job Sequence - Connection Info page, 298
- New Job Sequence - SysObject Info page, 299
- New LDAP Server Configuration - Failover page, 135, 139
- New LDAP Server Configuration - Info page, 115, 119
- New LDAP Server Configuration - Mapping page, 126, 132
- New LDAP Server Configuration - Sync & Authentication page, 121, 124
- New Network Location - Info page, 147

-
- New Permission Set - Info page, 233, 242
 New Permission Set - Permissions page, 233, 242
 New Record Migration Job - Rules page, 287
 New Records Migration Job - Info page, 287
 New Records Migration Job - Rules page, 289
 New Replication Job - Info page replication job, 276
 New Replication Job - Replication Options page, 278
 New Replication Job - Schedule page replication job, 277
 New Replication Job - SysObject Info page replication job, 279
 New Replication Job - To Target page, 277
 New SnapLock Store - Info page, 411
 new window open, 47
 None permissions, 226
 notes
 create, 685
 delete, 685
 editing, 685
 searching for, 685
 Notification page, 547
 notifications
 in work queues, 663
 overview, 641
 set, 70
 numbered lists, 730
- O**
- object instances
 auditing, 252
 removing audits, 255
 unregistering audits, 255
 object key, 593
 object types
 associate with file formats, 60 to 61
 auditing, 250
 creating, 366
 creating indexes, 343
 defined, 60
 deleting, 375
 described, 365
 modifying, 368
- privileges, 375
 removing audits, 254
 Superusers, 368
 object_id, 569
 objects
 auditing, 254
 creating, 35
 deleting, 35
 modifying, 35
 permissions, 226
 Superuser access to, 231
 viewing, 35
 Offline Client, 75
 offline mode
 access, 49
 operating system information, 350
 Oracle, 312
 ordered lists, 730
 orphaned content objects, 313
 override policies, 666
 Owner role
 in collaborative services, 702
- P**
- parent documents
 of virtual documents, 743
 passwords
 binding, changing, 141
 changing, 32, 40
 in debug tracing output, 454
 path, 569
 PDF, 609
 PDF documents
 add comments, 754
 annotate, 753
 configure annotation services, 753
 view comments, 754
 Percent Quality Check, 664
 Permission Set Properties - Info page, 237, 242
 Permission Set Properties - Permissions page, 237, 242
 permission sets
 adding users, 239
 creating, 225 to 226, 233
 deleting, 225 to 226
 deleting users, 241
 described, 225 to 226
 locating, 231 to 232

managing, 225 to 226
replica objects, 284
replication, 306
Superusers, 227
sysadmin, 227
system, 228
topics, 225
user privileges, 226
validations, 233
viewing where used, 232

permissions, 226
access levels, 226
creating permission sets, 233
deleting objects, 229
folder security, 228
locating, 231
modifying, 237
object, 226
object level, 225 to 226
object owner, 226
of a user, 203
overview, 226
viewing where used, 232

Permissions page
permission sets, 233, 237, 242

phrase order, 505

PLM Interface, 582

plug-ins
Content Services for EMC Centera (CSEC), 403
creating, 418
deleting, 383
described, 417
EMC Centera stores, 402
external stores, 396
modifying, 418
NetApp SnapLock stores, 410

policies, 661, 666
audit, 260
work queue override policies, 666

Policy
Adaptive, Fixed, Trickle, 461

policy inheritance
viewing, 376

ports
locking, 453

possible format, 607

possible version, 607

Post URL, 179

post_webroot_switch_script key, 459

pre_webroot_switch_script key, 458

preferences
columns displayed, 43
general, 45
searches, 631
set, 45
virtual documents, 751

preferred format, 609

primary renditions, 757

priority levels, 663 to 664

privileges, 226
jobs, 265

process template, 659

Process_report_admin, 658

processor profile, 659, 669

processor profiles, 668

productivity, 575

profile object, 572

Profiles
Create tab, 713
creating new in My Documentum for Microsoft Outlook, 713

My Documentum for Microsoft Outlook, 713

My Documentum for Microsoft Outlook import, 716

projection targets, 87
creating, 94, 96, 156 to 157
deleting, 94, 96, 156 to 157
modifying, 94 to 96, 156 to 157

Projections & Stores page, 156
ACS servers, 165

properties
blob store, 392
defined, 365
distributed store, 395
file stores, 387
index servers, 482
linked store, 390
set, 53
view, 53
viewing for saved transformations, 766

properties, repeating, 475

Property rules, 521

publish_contentless_documents key, 455

publish_folder_properties key, 455

publish_source_version_labels key, 455

publishing documents
by date, 475
connection failures, 453

- effective label, 475
 - parallel publishes, 457
 - serial publishes, 457
 - timeout interval, 453
 - publishing objects, 472
 - PURGE_CONTENT administration method, 339
- Q**
- Qualifier Rules page, 272
 - quality check, 664
 - queries, 576
 - search queries, 621
 - queue categories. *See* work queue categories
 - queue items, indexing
 - creating, 486
 - described, 483
 - removing by status, 485
 - removing individual, 485
 - resubmitting failed, 485
 - resubmitting individual objects, 484
 - status, 484
 - viewing, 486
 - queue management job, 316
 - queue policies, 660, 663, 667
 - queue processors
 - enable selective pull, 674
 - manage, 667
 - Queue_admin, 658
 - Queue_advance_processor, 658
 - Queue_manager, 658
 - Queue_processor, 658
 - queueperson argument, 274
 - queues
 - work queues, 657
 - quickflows
 - send, 651
- R**
- Read permissions, 226
 - read-only view
 - of email messages, 637
 - of files, 59
 - reassigning
 - groups, 210
 - roles, 215, 219
 - records
 - common tasks, 733
 - declare formal records, 733
 - link, 738
 - record relationships, 738 to 739
 - remove relationship, 739
 - records migration job
 - required privileges, 286
 - Rules page, 289
 - records migration jobs, 270
 - creating, 286
 - described, 286
 - selection criteria, 290
 - version criteria, 291
 - refreshing
 - a CTS service, 495
 - register an HVP worker, 602
 - register for indexing, types, 369
 - Regulatory Publishing Transformation Services, 757
 - reindexing a repository, 309
 - Relate permissions, 226
 - related items
 - creating through transformations, 763
 - delete, 64
 - transformations, 757
 - relations
 - common tasks, 755
 - relationships
 - common tasks, 755
 - create, 755
 - delete, 756
 - remove, 756
 - view, 755
 - removing
 - audits, 254 to 256
 - renaming, 315
 - rendition, 587
 - rendition manager job, 318
 - renditions, 318, 607, 757
 - associated with one version, 757
 - creating, 762
 - deleting, 318
 - importing, 759
 - overview, 757
 - primary, 757
 - resetting, 761
 - setting a default, 759
 - viewing, 758
 - viewing the default, 760
 - repeating properties, 475

replacing a file
 through transformation, 764
 through transformations, 764

replica objects
 permission set, 284

replicas
 importing, 334

REPLICATE administration method, 340

Replicating Documentum in SAP, 576

replicating Documentum objects
 example, 593

replicating objects, 575

replicating SAP in Documentum, 576

replicating SAP objects, 592

replicating SAP objects example, 591

replicating systems, 590

replication, 600

replication from SAP to Documentum, 575

replication jobs
 creating, 276
 described, 276
 Info tab, 270
 options, 282
 replication folder, choosing, 283
 source repository, selecting, 280
 storage areas, 284
 target repository, selecting, 281
 user, 284

replication operation
 rollback, File system and RDBMS, 463

Replication Options page, 278

report template, 601

reports
 job, 303
 workflows, 654

repositories
 accessibility mode, 32, 40, 46
 add, 41
 adding to a federation, 106
 browse, 44
 change, 41
 changing home, 319
 changing passwords, 32
 connection information for job
 sequences, 300
 deleting log files, 316
 described, 73
 determining to which you are
 connected, 33
 enabling for CIS, 507

favorites, 41

federations, 102 to 103, 105

groups, 204

job sequences, 300

jobs, 265

log files, 456

log in, 39, 41

log into accessibility mode, 40

log out, 41

multiple, 40 to 41, 59

names, 41

navigate, 42

overview, 39

reindexing, 309

remove, 41

removing a federation, 107

removing a federation member, 107

saved credentials, 40, 45

state of, 318

troubleshooting, 318

users, 184

Repository Configuration Properties - Info page, 77

Repository Configuration Properties - Synchronization page, 82

repository host, 34

repository information
 export, 70

repository owner, 228

repository_name, 569

repository_password, 569

repository_user, 569

required folder, 607

required status, 607

required version, 606

Reset, 46, 729

Resource Agent Authentication page, 542

Resource Agent Properties - Info page, 541

resource agent resources
 attributes, 545
 general information, 544
 log file, 548
 managing, 543
 notifications, 547
 operations, 546
 starting operations, 546

resource agents
 adding, 541
 authentication failure, 542
 deleting, 543

- managing, 540
 - properties, 542
 - resources, 543
 - Resource Agents list page, 540
 - resource logs
 - resource agent resources, 548
 - Resource Management
 - resource agents, managing, 540
 - understanding, 540
 - Resource Properties - Attributes page, 545
 - Resource Properties - Info page, 544
 - Resource Properties - Log page, 548
 - Resource Properties - Notifications page, 547
 - Resource Properties - Operations page, 546
 - Resources on Agent list page, 543
 - Restore Default
 - in Formats tab, 61
 - RESTORE_CONTENT administration
 - method, 340
 - results
 - external sources, 623
 - searches, 620 to 621, 623, 627
 - retention store
 - EMC Centera, 402
 - retention stores
 - described, 383
 - reviews
 - common tasks, 641
 - quickflows, 651
 - workflows, 649
 - Rich Text Editor
 - in collaborative services, 681
 - right-click
 - to perform actions, 47
 - role
 - express user, 41
 - roles
 - attributes of, 214 to 215, 219 to 220
 - creating, 213, 218
 - deleting, 215, 219
 - described, 212
 - in work queues, 657
 - modifying, 214, 219
 - Process_report_admin, 658
 - Queue_admin, 658
 - Queue_advance_processor, 658
 - Queue_manager, 658
 - Queue_processor, 658
 - reassigning, 215, 219
 - user management, 183
 - room membership
 - about, 702
 - add members, 704
 - add members to a local group, 706
 - change local roles, 705
 - create local group, 705
 - edit local group properties, 705
 - invite members, 704
 - manage, 704
 - remove local groups from a room, 706
 - remove members, 705
 - rooms
 - copy, 703
 - create, 700
 - delete, 703
 - edit properties of, 701
 - governed objects, 699
 - local groups, 702
 - local roles, 702
 - membership, 702
 - move, 703
 - overview, 697
 - visit, 698
 - RTE
 - in collaborative services, 681
 - rule composer, 582
 - rules
 - setting for categories, 520
 - Rules page
 - record migration job, 289
 - Rules tab, 434
 - running
 - administration methods, 329
 - jobs, 302
- ## S
- Sample PI Sheet, 570
 - SAP CAD interface, 576
 - SAP connection parameters, 585
 - SAP document type, 606
 - SAP object, 585
 - SAP page, 564
 - SAP queries, 576
 - SAP query, 590
 - SAP router, 565
 - SAP server, 564, 576
 - SAP table query, 576
 - SAP user, 564, 576, 601

save as
 file, 732

saved credentials
 delete, 45
 set, 40, 45
 view, 45

saved transformations
 removing, 766

Schedule page
 replication job, 277

scheduled events, 576

schedules for a job, 271

SCS Log Purge job, 318

scs_admin_config object, 439

Search Builder page, 131

search templates
 copy, 631
 create, 629
 edit, 629
 modify, 630
 run, 628

searches
 advanced searches, 616
 configuration, 624
 copy, 628
 edit, 616, 627
 experience, 623
 export results, 70
 external results, 623
 highlight results, 620
 indexed repository, 625
 last results, 623, 627
 monitor, 620 to 621
 operators, 614, 619
 overview, 613
 preferences, 631
 results, 620 to 621, 623, 627, 631
 saved searches, 626 to 627
 search templates, 628 to 631
 searchable items, 625
 simple searches, 613 to 614
 status, 620 to 621

searching
 audit trails, 257

Secondary LDAP Server page, 138

securities, 226

selection criteria
 records migration jobs, 290

Selection Criteria page, 290

selection dialog boxes

locate an item, 44

server configuration mode, 156

server configuration object
 duplicating, 86
 far stores, 87
 locations, 87

server configuration objects
 application servers, 87, 97
 Business Process Manager, 101 to 102
 cached types, 87
 connection brokers, 87, 94 to 96
 creating, 87 to 88
 deleting, 101
 described, 85
 far stores, 100
 general properties, 88
 info page, 88
 locations, 98
 modifying, 87
 network locations, 87, 96
 process engine, 101 to 102
 projection targets, 87, 94 to 96

server details, 564

server name, 565

server root location
 modifying, 400

servers
 creating, 85
 server configuration objects, 85

sessions
 accessibility mode, 40, 46
 log in, 39, 41
 log out, 41
 user, 183

Set Access Permissions page, 236

Set as Preview option, 759

SET_OPTIONS administration
 method, 352

SET_STORAGE_STATE administration
 method, 341

setting
 trace levels, 303

settings
 preferences, 45

shortcuts
 keyboard hot keys, 769
 links, 65
 recently used files, 59
 subscriptions, 69
 to items in other repositories, 66

Show More, 53
 showing all, 184 to 185
 simple documents
 convert to, 750
 simple search
 run, 613
 simple searches
 run, 614
 sites
 histories, 53
 properties, 53
 skill attributes, 660
 skill profile, 659
 Skills for Work Assignment Match, 670
 smart navigation
 search results, 621, 631
 snapshots
 create, 750
 freeze, 750
 unfreeze, 750
 version labels, 749
 view, 749 to 750
 software version
 view, 50
 source_attrs_only key, 457
 specific method, 568
 spell check, 731
 SQL Server, 312
 SQL statements, 343, 350
 Staging, 678
 Start Operation page, 546
 starting
 a CTS service, 495
 Starts With field
 in lists, 42
 State of Repository job, 318
 status
 background operations, 48
 status bar
 messages in, 48
 status flags, 607
 status of a federation, 314
 stemming, 504
 stopping
 a CTS service, 495
 storage
 blob stores, 382, 391 to 392
 deleting, 383
 described, 379, 382
 distributed stores, 382, 393 to 395
 EMC Centera stores, 402 to 403, 405, 407
 external stores, 382, 396 to 397, 400
 far stores, 87
 file stores, 382 to 383, 386 to 387
 linked stores, 382, 389 to 390
 locating, 380
 NetApp SnapLock stores, 410 to 412
 retention stores, 383
 streaming stores, 382
 thumbnail stores, 382
 turbo stores, 382
 viewing properties, 383
 storage areas
 changing state, 341
 migrating records, 286
 moving content between storage areas, 429
 restoring content files, 340
 Storage Parameters page, 405
 storage policies
 described, 419
 store_log key, 456
 streaming stores
 described, 382
 structure
 of virtual document, 744 to 748
 virtual documents, 747 to 748
 submitting documents, 531
 Submitting documents, 506
 subscript, 730
 subscriptions
 cancel, 70
 columns displayed, 43
 create, 69
 display on startup, 45
 subscribe, 69
 subscribe other users, 70
 unsubscribe, 70
 view, 69
 superscript, 730
 Superusers, 365
 ACL entry evaluation and, 231
 modifying object type definitions, 368
 permission sets, 227
 supervisors
 change, 654
 swap info job, 319
 swap space, 319
 Sybase, 312

Sync & Authentication page
 LDAP server configurations, 121, 124
sync_on_zero_updates key, 460
Synchronization page
 repository configuration, 82
synchronizing
 taxonomies, 527
 users and groups, 315
sysadmin
 permission sets, 227
SysObject Info page
 replication job, 279
Sysobject Info tab, 275
SysObjects
 Superuser access to, 231
System Information page, 32
system name, 565
system number, 565
system permission sets, 228
System Permission Sets, 232

T

tables, 731
tasks
 accept, 643
 attach files, 642
 automatic, 653
 complete, 643
 delegate, 644
 failed, 653
 open, 642
 overview, 641, 649
 perform, 642
 reassign, 644
 reject, 644
 repeat, 645
 select, 647
 suspend, 646
 unsuspend, 646
 work queues, 646, 671
taxonomies
 bringing online, 526
 common tasks, 727
 creating, 509, 512
 defined, 501
 navigate, 44
 overview, 727
 setting properties, 512
 submitting items to, 727

synchronizing, 527
taking offline, 526
TCP port
 file transfer authentication, SSH
 service, 460
templates
 lifecycles, 52, 56, 61, 635, 678
 remove lifecycles, 678
 search templates, 628 to 631
temporary disk space
 local_diskfull_limit, 573
 managing, 573
terms
 common words, 536
test processing, 528
test results, 578
text
 create links from, 731
 format, 729
text renditions, generating, 569
thresholds, 663
thumbnail stores
 described, 382
thumbnails
 overriding default, 760
 view, 42
time format, 603
timeouts
 connection thread, 453
 publishing method, 453
To Target page, 277
trace level, 602
trace levels
 setting, 303
trace logs
 jobs, 304
trace output, 456
trace_passwords key, 454
tracing, 352, 454
 full-text indexing operations, 349
 user-defined methods, 274
transaction capability
 number of files, 463
 size of files, 463
transform_type key, 460
transformations, 757
 creating a package, 765
 creating new objects, 763
 creating new renditions, 762
 creating new version, 765

- enabling Inbox notification, 767
 - overview, 757
 - profiles, 757
 - properties, 766
 - replacing a file, 764
 - results, 757, 763 to 765
 - viewing saved, 766
 - transforming
 - document to HTML, 761
 - document to PDF, 761
 - translations
 - filter for, 42
 - troubleshooting, 318
 - turbo stores
 - described, 382
 - types
 - choosing, 259
 - navigating, 365
 - register for indexing, 369
- U**
- unavailable
 - for tasks, 645
 - UNIX
 - Windows domain authentication, 83 to 85
 - update condition, 593
 - Update Statistics job, 319
 - updating federations, 314
 - URLs
 - create links, 731
 - use_docbase_formats key, 452
 - use_format_extensions key, 457
 - use_text_file_extensions key, 453
 - user authentication, 110
 - user change home repository job, 319
 - user management, 183
 - User managers
 - create new user, 707
 - in collaborative services, 707
 - modify users, 708
 - restricted folders, 709
 - unlink users, 709
 - user privileges, 35, 226
 - user rename job, 320
 - user sessions, 183
 - users
 - add to a work queue, 667
 - adding to a group, 208
 - adding to permission sets, 233, 237, 239
 - assign tasks, 672
 - attributes, 198
 - changing for a CTS instance, 489
 - changing state, 202
 - creating, 186, 196, 198
 - deleting, 201
 - deleting from permission sets, 241
 - described, 184
 - exporting in a federation, 313
 - federations, 102, 313
 - global, 102, 187, 190
 - home repository, 319
 - importing, 196
 - importing in a federation, 314
 - in work queues, 667 to 668, 670
 - LDAP, 315
 - LDFI file formats, 196, 198
 - locating, 184 to 185
 - modifying, 203
 - monitor queue users, 671
 - reassign logs, 204
 - reassign tasks, 672
 - reassigning, 202
 - renaming, 315, 320
 - replication job, 284
 - sessions, 183
 - user management, 183
 - viewing alias sets, 203
 - viewing documents, 203
 - viewing groups, 203
 - viewing permission sets, 203
 - viewing workflows, 203
- V**
- value to be used in the comparison, 660
 - VDM
 - overview, 743
 - verifying
 - audit trails, 258
 - verifying audit trail entries, 250
 - verifying audit trails, 260
 - version, 587
 - version criteria
 - records migration jobs, 291
 - version labels, 606
 - add, 749
 - version management job, 320

- version of software
 - view, 50
- Version permissions, 226
- versioning a file
 - through transformation, 765
- versions
 - current version, 57 to 58
 - delete, 64
 - deleting, 229
 - removing a saved transformation, 766
 - renditioning, 757
 - save new, 55
 - saved transformations, 766
 - view, 57
- view
 - index server logs, 483
- view directory
 - default location, 59
- viewing
 - administration methods, 328
 - alias sets, 357
 - audit trails, 257, 260
 - formats, 362
 - index server properties, 482
 - job reports, 303
 - job trace logs, 304
 - method results, 326
 - objects, 35
 - permission sets, where used, 232
 - storage area properties, 383
- viewing an Agent, 601
- viewing an SAP User, 565
- viewing connections to an SAP Server, 565
- Virtual Document Manager
 - overview, 743
- virtual documents
 - add descendants, 745 to 746
 - common tasks, 743
 - content, 745
 - convert to simple documents, 750
 - create, 744
 - fix to a version, 749
 - move descendants, 747 to 748
 - overview, 743
 - preferences, 751
 - remove descendants, 748
 - reorder descendants, 747 to 748
 - show broken bindings, 751
 - snapshots, 749 to 750
 - structure, 744
- version labels, 749
- view content, 745
- view structure, 744
- virtual links
 - view, 60

W

- WDK
 - view version, 50
- Web Development Kit
 - view version, 50
- WebAdmin
 - introducing, 563
- WfmsTimer job, 320
- window_interval argument, 274
- windows
 - open new, 47
- Windows
 - domain authentication for UNIX repositories, 83
- WIP, 678
 - folder security, 228
- work assignment match
 - add filters to a queue, 661
 - processor profiles, 670
- work assignment match filters
 - add to a queue, 661
 - remove from a queue, 661
- work assignment matching
 - configure, 659
 - define filters, 660
 - set skills in process template, 659
- work assignment processor profiles
 - add skills, 668 to 669
 - change skills, 669
 - delete skills, 670
- Work Queue Assignment page, 667
- work queue categories
 - create, 664
 - define, 664
 - delete, 665
- Work Queue Management, 660, 665 to 666, 671 to 674
- Work Queue Monitor, 667 to 671
 - select views, 671
- work queue override policies, 667
- work queue policies
 - configure quality checks, 664
 - create, 663

- delete, 664
 - modify, 663
 - override, 666
 - overview, 661
 - set priorities, 664
 - set priorities dynamically, 664
 - set thresholds, 663
 - Work Queue Properties page, 661, 665, 668
 - work queue skill info, 660
 - work queue tasks
 - assign, 672
 - move, 673
 - reassign, 672
 - resume, 674
 - suspend, 673
 - unassign, 673
 - unsuspend, 674
 - work queue users
 - manage work queue users, 667
 - work queues
 - add groups, 667
 - add users, 667
 - assign tasks, 672
 - categories, 664
 - configure notifications, 663
 - create, 658, 661, 665
 - define, 665
 - delete, 666
 - get next task, 647
 - groups, 667 to 668, 670
 - manage your Inbox, 646
 - modify, 672
 - monitor, 671
 - move categories, 666
 - move tasks to new queues, 673
 - overview, 657
 - perform tasks, 646
 - policies, 661
 - queue policies, 661
 - reassign tasks, 672 to 673
 - remove a group, 668
 - remove a user, 668
 - resume suspended tasks, 674
 - roles, 657
 - select tasks, 647
 - set priorities, 663
 - suspend tasks, 673
 - unassign tasks, 673
 - unsuspend tasks, 674
 - update, 671
 - users, 667 to 668, 670
 - view, 671
 - Workflow Manager
 - open, 655
 - Workflow Reporting
 - change supervisor, 654
 - workflow reports, 658
 - workflows, 320, 576
 - attach files, 650
 - audit events, 651
 - complete failed tasks, 653
 - complete tasks, 643
 - create workflow templates, 655
 - details, 651
 - email participants, 653
 - failed tasks, 653
 - finish tasks, 643
 - My Workflows, 652
 - of a user, 203
 - overview, 649
 - pause, 652
 - reject tasks, 644
 - reports, 654
 - resume, 652
 - retry failed tasks, 653
 - start, 649
 - stop, 652
 - supervisor, 654
 - view, 651
 - Workflow Reporting, 651
 - Write permissions, 226
- X**
- XML, 601
 - XML store, creating, 397